Completeness Theorems with Constructive Proofs for Finite Deterministic 2-Party Functions (full version)

Daniel Kraschewski Jörn Müller-Quade

Institute of Cryptography and Security, Faculty of Informatics,
Karlsruhe Institute of Technology, Germany

{kraschewski,mueller-quade}@kit.edu

Abstract

In this paper we present simple but comprehensive combinatorial criteria for completeness of finite deterministic 2-party functions with respect to information-theoretic security. We give a general protocol construction for efficient and statistically secure reduction of oblivious transfer to any finite deterministic 2-party function that fulfills our criteria. For the resulting protocols we prove universal composability. Our results are tight in the sense that our criteria still are necessary for any finite deterministic 2-party function to allow for implementation of oblivious transfer with statistical privacy and correctness.

We unify and generalize results of Joe Kilian (1991, 2000) in two ways. Firstly, we show that his completeness criteria also hold in the UC framework. Secondly, what is our main contribution, our criteria also cover a wide class of primitives that are not subject of previous criteria. We show that there are non-trivial examples of finite deterministic 2-party functions that are neither symmetric nor asymmetric and therefore have not been covered by existing completeness criteria so far.

As a corollary of our work, every finite deterministic 2-party function is either complete or can be considered equivalent to a non-complete symmetric 2-party function—this assertion holds true with respect to active adversaries as well as passive adversaries. Thereby known results on non-complete symmetric 2-party functions are strengthened.

Keywords: oblivious transfer, complete primitives, information-theoretic security, universal composability, secure function evaluation.

Contents

1 Introduction

Oblivious transfer in the sense of a trusted erasure channel (Rabin-OT) was introduced in [Rab81] and later in [Cré88] proven to be equivalent to $\binom{2}{1}$-OT, where a receiver Bob may learn only one of two bits sent by Alice. Oblivious transfer turned out to be complete in the sense that every secure multiparty computation can be implemented using OT [Kil88, GL91, CvdGT95, IPS08]. Thereby, enduring interest in OT arised in cryptography and for numerous primitives it has been investigated, whether they allow for implementation of OT. In our work we exhaustively treat this question for the class of "finite deterministic 2-party functions", sometimes also referred to as "crypto gates". Such primitives are characterized by some finite alphabetes $\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}$ and some mappings $f_{\mathrm{A}} \in \Omega_{\mathrm{A}}^{\Upsilon_{\mathrm{A}} \times \Upsilon_{\mathrm{B}}}$, $f_{\mathrm{B}} \in \Omega_{\mathrm{B}}^{\Upsilon_{\mathrm{A}} \times \Upsilon_{\mathrm{B}}}$, such that on input $x \in \Upsilon_{\mathrm{A}}$ from Alice and $y \in \Upsilon_{\mathrm{B}}$ from Bob the primitive outputs $f_{\mathrm{A}}(x, y)$ to Alice and $f_{\mathrm{B}}(x, y)$ to Bob.

1.1 Related work

In the literature one finds OT protocols for the bounded-classical-storage model [CCM98] and the bounded-quantum-storage model [DFR$^+$07] as well as noisy classical [CMW05, Wul09] and quantum channels [May95, May96], the latter taking commitments for granted. Further, there are reductions of $\binom{2}{1}$-OT to weaker OT versions that leak additional information [CK90, DKS99, Wul07] and to Rabin-OT [Cré88]. OT-combiners implement OT from granted sets of OTs with faulty members [MPW07, HIKN08]. For reversing the direction of $\binom{2}{1}$-OT a protocol is known with optimal number of OT calls [WW06]. Relative to complexity assumptions all-or-nothing laws have been shown [BMM99, HNRR06, MPR10], i.e. all non-trivial primitives are complete. Our work has several, nowadays folklore reduction techniques in common with all the aforementioned literature.

We unify and generalize the results of [Kil91, Kil00], where completeness criteria for symmetric (i.e. both parties receive the same output) and asymmetric (i.e. only one party learns the function output) 2-party functions were provided with respect to information-theoretic security. We import a main argument for the necessity of our criteria from [Kil91]. Our sufficiency proof is independent from [Kil91, Kil00], since our results are more general and we use a very strict notion of security.

There are also results regarding whether various symmetric 2-party functions can be reduced to each other [MPR09] and what can be implemented from scratch when there is only a passive adversary [Kus92, KMQR09]. A corollary of our work extends all these results to non-symmetric primitives; some results of [KMQR09] already build on an early manuscript of our work [KMQ08].

1.2 Our contribution

We expose a wide class of complete finite deterministic 2-party functions that are essentially neither symmetric nor asymmetric and hence are not subject of statistical completeness criteria in the literature so far. Further, by surprisingly simple combinatorial criteria to the respective function tables we give a precise characterization of *all* finite deterministic 2-party functions that allow for statistically secure implementation of OT. We provide an efficient and universally composable protocol scheme for OT from any finite deterministic 2-party function fulfilling our criteria. Our results are tight, as the necessity of our criteria still holds when only correctness and privacy of the implemented OT are required.

As a remarkable corollary of our work all non-complete finite deterministic 2-party functions turn out symmetric. This strengthens several known results for non-complete symmetric 2-party functions [Kus92, MPR09, KMQR09].

Functionality: $\mathcal{F}_{\mathrm{SFE}}^{(F)}$

Let F be characterized by the output functions $f_{\mathrm{A}} : \Upsilon_{\mathrm{A}} \times \Upsilon_{\mathrm{B}} \to \Omega_{\mathrm{A}}$ and $f_{\mathrm{B}} : \Upsilon_{\mathrm{A}} \times \Upsilon_{\mathrm{B}} \to \Omega_{\mathrm{B}}$, where $\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}$ are Alice's input and output alphabet and $\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}$ are Bob's input and output alphabet.

- Upon receiving input (x, i) from Alice, verify that $(x, i) \in \Upsilon_{\mathrm{A}} \times \mathbb{N}$ and that there is no recorded tuple $(\tilde{x}, i, \texttt{Alice})$; else ignore that input. Next, record $(x, i, \texttt{Alice})$ and send $(\texttt{processing}, \texttt{Alice}, i)$ to the adversary.
- Upon receiving input (y, i) from Bob, verify that $(y, i) \in \Upsilon_{\mathrm{B}} \times \mathbb{N}$ and that there is no recorded tuple $(\tilde{y}, i, \texttt{Bob})$; else ignore that input. Next, record $(y, i, \texttt{Bob})$ and send $(\texttt{processing}, \texttt{Bob}, i)$ to the adversary.
- Upon receiving a message $(\texttt{Delivery}, \texttt{Alice}, i)$ from the adversary, verify that there are recorded tuples $(x, i, \texttt{Alice})$ and $(y, i, \texttt{Bob})$ and the former is not marked; else ignore that input. Next, mark the recorded tuple $(x, i, \texttt{Alice})$, compute $a \leftarrow f_{\mathrm{A}}(x, y)$ and output (a, i) to Alice.
- Upon receiving a message $(\texttt{Delivery}, \texttt{Bob}, i)$ from the adversary, verify that there are recorded tuples $(x, i, \texttt{Alice})$ and $(y, i, \texttt{Bob})$ and the latter is not marked; else ignore that input. Next, mark the recorded tuple $(y, i, \texttt{Bob})$, compute $b \leftarrow f_{\mathrm{B}}(x, y)$ and output (b, i) to Bob.

When a party is corrupted, the adversary is granted unrestricted access to the channel between $\mathcal{F}_{\mathrm{SFE}}^{(F)}$ and the corrupted party, including the ability of deleting and/or forging arbitrary messages.

Figure 1: The ideal functionality for secure evaluation of a 2-party function F. Adapted and simplified version of the Secure Function Evaluation functionality in [Can01]. Note that via the parameter i only the same multi-session ability is achieved as in [Can01] by multiple session IDs.

1.3 Organization of this paper

The rest of this paper is organized as follows. In Section 2 we briefly present our results. Thereto, we first refer to the security notion that we use (Section 2.1), then introduce the notations needed for formulation of our results (Section 2.2) and, last but not least, state our completeness criteria in form of a Classification Theorem (Section 2.3). In Section 3 we give an intuitive exposition of how one can prove this theorem; a formal proof is located in Section 4. To make it self-contained, all definitions, lemmata, etc. from the rest of the paper are also restated in Section 4. In Section 5 we give a conclusion of our work and post some open questions that we find interesting to investigate.

2 Presentation of our results

2.1 Notion of security

We prove our classification results in the UC framework [Can01] with static corruption and statistical security, i.e. the adversarial entities $\mathcal{A}, \mathcal{S}$ and the environment $\mathcal{Z}$ are computationally unbounded. Nonetheless, in our case the running time of a simulator $\mathcal{S}$ will always be polynomial in the running time of the according adversary $\mathcal{A}$. Since we implement $\binom{2}{1}$-OT from given 2-party functions, in the real model there always is a hybrid functionality that provides access to the latter (see Figure 1). Since $\binom{2}{1}$-OT can be considered a special 2-party function that on input $(b_0, b_1) \in \{0,1\}^2$ from Alice and $c \in \{0,1\}$ from Bob outputs b_c to Bob and a special "nothing" symbol $\perp$ to Alice, we omit an explicit definition of the ideal functionality $\mathcal{F}_{\mathrm{OT}}$.

2.2 Basic concepts

A finite deterministic 2-party function can be characterized by its input and output alphabets and output functions (q.v. Figure 1). By $\mathfrak{F}_{\mathsf{fin,det}}$ we denote the set of all tuples $(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B})$, where $\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}$ are non-empty finite alphabets and $f_\mathrm{A}, f_\mathrm{B}$ are mappings from $\Upsilon_\mathrm{A} \times \Upsilon_\mathrm{B}$ to Ω_A and from $\Upsilon_\mathrm{A} \times \Upsilon_\mathrm{B}$ to Ω_B respectively (cf. Notation 2 in Section 4.1.1). For convenience we will not always differentiate pedantically between the mathematical object $F \in \mathfrak{F}_{\mathsf{fin,det}}$ and the corresponding primitive $\mathcal{F}_{\mathrm{SFE}}^{(F)}$, but from the context should be always clear what is meant.

Our notion of $\mathfrak{F}_{\mathsf{fin,det}}$ turns out a bit too detailed, since Alice and Bob can always relabel their input-output tuples of a given 2-party function without any side effects. There is no need for distinguishing between some $F \in \mathfrak{F}_{\mathsf{fin,det}}$ and any relabelled version of F. By the following definition we can abstract from those irrelevant details (cf. Definition 33 in Section 4.5):

Definition (Consistent renamings)**.** Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and let $F' := (\Upsilon'_\mathrm{A}, \Upsilon'_\mathrm{B}, \Omega'_\mathrm{A}, \Omega'_\mathrm{B}, f'_\mathrm{A}, f'_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$. Then F and F' are *consistent renamings* of each other, if there exist some injective mappings $\rho_\mathrm{A} : \Upsilon_\mathrm{A} \times \Omega_\mathrm{A} \to \Upsilon'_\mathrm{A} \times \Omega'_\mathrm{A}$ and $\rho_\mathrm{B} : \Upsilon_\mathrm{B} \times \Omega_\mathrm{B} \to \Upsilon'_\mathrm{B} \times \Omega'_\mathrm{B}$ and some bijective mappings $\sigma_\mathrm{A} : \Upsilon_\mathrm{A} \to \Upsilon'_\mathrm{A}$ and $\sigma_\mathrm{B} : \Upsilon_\mathrm{B} \to \Upsilon'_\mathrm{B}$, such that for all $x \in \Upsilon_\mathrm{A}$, $y \in \Upsilon_\mathrm{B}$ it holds:

$$\begin{aligned} \rho_\mathrm{A}\big(x, f_\mathrm{A}(x,y)\big) &= \big(\sigma_\mathrm{A}(x), f'_\mathrm{A}(\sigma_\mathrm{A}(x), \sigma_\mathrm{B}(y))\big) \\ \rho_\mathrm{B}\big(y, f_\mathrm{B}(x,y)\big) &= \big(\sigma_\mathrm{B}(y), f'_\mathrm{B}(\sigma_\mathrm{A}(x), \sigma_\mathrm{B}(y))\big) \end{aligned}$$

Moreover, there may exist input symbols that are kind of "redundant" in the sense that an actively corrupted party can always input some corresponding "dominating" input symbols and at the same time perfectly simulate honest behaviour. This concept plays an important role in our proofs and results. We formally grasp it by the following definition (cf. Definition 3 in Section 4.1.1):

Definition (Redundancy)**.** Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$. Then an input symbol $y' \in \Upsilon_\mathrm{B}$ is *redundant*, if there exists some corresponding *dominating* input symbol $y \in \Upsilon_\mathrm{B} \setminus \{y'\}$, such that the following two conditions hold:

1. For all $x \in \Upsilon_\mathrm{A}$ we have that $f_\mathrm{A}(x,y) = f_\mathrm{A}(x,y')$, i.e. from her own output Alice does never learn whether Bob did input y or y'.

2. For all $x, x' \in \Upsilon_\mathrm{A}$ with $f_\mathrm{B}(x,y') \neq f_\mathrm{B}(x',y')$ we have that $f_\mathrm{B}(x,y) \neq f_\mathrm{B}(x',y)$, i.e. by inputting y instead of y' Bob gets exactly the same or strictly more information.

For input symbols $x \in \Upsilon_\mathrm{A}$ redundancy is defined analogously. If neither Υ_A nor Υ_B contains any redundant input symbols, F is called *redundancy-free*.

W.l.o.g. actively corrupted parties always use dominating input symbols instead of the corresponding redundant ones. Also, there is no need to constrain what honest parties may learn. Therefore, in presence of an active adversary we can consider any 2-party functions equivalent when they only differ in some redundant input symbols (cf. Definition 36 in Section 4.5):

Definition (Equivalent 2-party functions)**.** Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and $F' := (\Upsilon'_\mathrm{A}, \Upsilon'_\mathrm{B}, \Omega'_\mathrm{A}, \Omega'_\mathrm{B}, f'_\mathrm{A}, f'_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$. Then F and F' are *equivalent*, if they can be transformed into consistent renamings of each other by successive[1] removal of redundant input symbols from $\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}$, $\Upsilon'_\mathrm{A}, \Upsilon'_\mathrm{B}$ and according adjustment of $f_\mathrm{A}, f_\mathrm{B}, f'_\mathrm{A}, f'_\mathrm{B}$. Let $[F]$ denote the resulting equivalence class.

[1] Note that a step-by-step removal of one symbol at a time is crucial here. There may exist distinct input symbols that dominate each other but must not be removed both.

	0	1
0	0/0	0/0
1	0/0	0/1

	0	1
0	0/0	0/0
1	0/0	1/0

	0	1
0	0/0	0/0
1	0/0	1/1

Figure 2: Function tables of the three types of OT-cores (Alice's inputs label the rows, Bob's inputs label the columns; outputs are denoted a/b, meaning that Alice learns a and Bob learns b).

Given any $F \in \mathfrak{F}_{\mathsf{fin,det}}$, one can show quite easily that all redundancy-free $\bar{F}, \bar{F}' \in [F]$ are consistent renamings of each other, i.e. the redundancy-free version of F is unique up to consistent renaming.

2.3 Completeness criteria for *all* finite deterministic 2-party functions

With the definitions and notations from Section 2.2 we can now formulate our completeness criteria. (The respective restatements in Section 4 are Definition 35, Definition 25 and Theorem 39.)

Definition (Symmetric 2-party functions)**.** Let $F' \in \mathfrak{F}_{\mathsf{fin,det}}$. If F' is a consistent renaming of some $F = (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$ with $\Omega_\mathrm{A} = \Omega_\mathrm{B}$ and $f_\mathrm{A} = f_\mathrm{B}$, then F' is called *symmetric.*

Definition (OT-cores)**.** Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$. A quadruple $(x, x', y, y') \in \Upsilon_\mathrm{A}^2 \times \Upsilon_\mathrm{B}^2$ is an *OT-core* of F, if the following three conditions are met (q.v. Figure 2):

1. We have that $f_\mathrm{A}(x, y) = f_\mathrm{A}(x, y')$.
2. We have that $f_\mathrm{B}(x, y) = f_\mathrm{B}(x', y)$.
3. We have that $f_\mathrm{A}(x', y) \neq f_\mathrm{A}(x', y')$ or $f_\mathrm{B}(x, y') \neq f_\mathrm{B}(x', y')$ (or both).

Theorem (Classification theorem)**.** *For each $F \in \mathfrak{F}_{\mathsf{fin,det}}$ it holds:*

1. *For the $\mathcal{F}_\mathrm{SFE}^{(F)}$-hybrid model there exists an OT protocol that is statistically secure against passive adversaries, iff F has an OT-core.*
2. *If for the $\mathcal{F}_\mathrm{SFE}^{(F)}$-hybrid model there does not exist any OT protocol that is statistically secure against passive adversaries, then F is symmetric.*
3. *For the $\mathcal{F}_\mathrm{SFE}^{(F)}$-hybrid model there exists an OT protocol that is statistically secure against active adversaries, iff the redundancy-free version of F has an OT-core.*
4. *If for the $\mathcal{F}_\mathrm{SFE}^{(F)}$-hybrid model there does not exist any OT protocol that is statistically secure against active adversaries, then the redundancy-free version of F is symmetric.*

Note that, when there is an active adversary, only the third function in Figure 2 is complete on its own. The redundancy free versions of the other two functions just collapse to simple binary channels. This collapsing can be prevented, when there are additional input symbols. In Figure 3 one can see, how OT-cores can be complemented to redundancy-free 2-party functions of minimum size.

For symmetric and asymmetric 2-party functions our completeness criteria coincide with the criteria from [Kil91, Kil00]. More concretely, we can directly translate the completeness criteria of [Kil91, Kil00] to our notations as follows.

	0	1
0	0/0	0/0
1	0/0	0/1
2	0/1	0/0

	0	1
0	0/0	0/0
1	0/0	0/1
2	0/1	0/2
3	0/2	0/2

	0	1
0	0/0	0/0
1	0/0	0/1
2	0/1	1/2

	0	1
0	0/0	0/0
1	0/0	1/1

Figure 3: Function tables of the four minimal complete 2-party functions. Up to consistent renaming and interchanging the roles of Alice and Bob every function table of a complete 2-party function $F \in \mathfrak{F}_{\mathsf{fin,det}}$ contains at least one of these examples as a submatrix.

[Kil91]: A symmetric 2-party function F is complete, iff it contains an OT-core. This holds true, regardless whether the adversary is active or passive.

[Kil00]: Given an active adversary, an asymmetric 2-party function F' (with Bob being the receiver) is complete, iff for every input symbol $y \in \Upsilon_{\mathrm{B}}$ there exists some other input symbol $y' \in \Upsilon_{\mathrm{B}}$ that is not dominated by y; in other words, F' is complete, iff its redundancy-free version is non-trivial in the sense that both input alphabets have cardinality 2 or more. Given only a passive adversary, an asymmetric 2-party function F' is complete, iff it has an OT-core.

However, our criteria are much more comprehensive than that of [Kil91, Kil00], since ours also cover 2-party functions that are neither symmetric nor asymmetric. An illustrating example is the third function in Figure 3, which is complete but not subject of the criteria in [Kil91, Kil00].

3 How to prove the Classification Theorem

A fundamental tool in our proof strategy is the connection between presence of OT-cores and the question whether a 2-party function is symmetric (cf. Lemma 38 in Section 4.5):

Lemma (Symmetrization lemma)**.** *Each $F \in \mathfrak{F}_{\mathsf{fin,det}}$ that does not have any OT-core is symmetric.*

One way to proof this lemma can be sketched as follows. For $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, f_{\mathrm{A}}, f_{\mathrm{B}}) \in \mathfrak{F}_{\mathsf{fin,det}}$ we can define an equivalence relation on $(\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}}) \cup (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})$ induced as follows:

$$(x,a) \sim (y,b) \quad :\Leftarrow \quad f_{\mathrm{A}}(x,y) = a \ \wedge \ f_{\mathrm{B}}(x,y) = b$$

Let the according equivalence classes be denoted by $[x,a]$ or $[y,b]$. For all $x, x' \in \Upsilon_{\mathrm{A}}$, $a, a' \in \Omega_{\mathrm{A}}$ some simple induction yields the following implication (else F would have an OT-core):

$$(x,a) \sim (x',a') \quad \Rightarrow \quad \big\{ y \in \Upsilon_{\mathrm{B}} \,\big|\, f_{\mathrm{A}}(x,y) = a \big\} = \big\{ y \in \Upsilon_{\mathrm{B}} \,\big|\, f_{\mathrm{A}}(x',y) = a' \big\}$$

Thereby, we cannot find any $x \in \Upsilon_{\mathrm{A}}$, $a, a' \in \Omega_{\mathrm{A}}$ with $a \neq a'$ and $(x,a) \sim (x,a')$; the analog holds for $y \in \Upsilon_{\mathrm{A}}$, $b, b' \in \Omega_{\mathrm{A}}$. Hence, via the mappings $\rho_{\mathrm{A}} : (x,a) \mapsto \big(x, [x,a]\big)$ and $\rho_{\mathrm{B}} : (y,b) \mapsto \big(y, [y,b]\big)$ we get a consistent renaming of F and this consistent renaming is obviously symmetric.

By the Symmetrization Lemma and some results in the literature we can already argue for the assertions 1 and 2 of our Classification Theorem. On the one hand, when F has no OT-core, F can be considered symmetric by our Symmetrization Lemma. However, in [Kil91] it has been shown that no reduction of OT to a symmetric 2-party function without OT-core can yield correctness

	0	1	2	3
0	0/0	0/0	0/0	0/0
1	0/0	1/0	0/1	1/1
2	0/1	1/1	1/2	0/2

Figure 4: A complete 2-party function needing a carefully chosen, non-symmetric input distribution.

and privacy at the same time, even if there is only a passive adversary—Alice can always exactly determine Bob's information about her inputs to the underlying 2-party function and vice versa.

On the other hand, when F has an OT-core and there is only a passive adversary, we can trivially implement one of the 2-party functions in Figure 2. However, each of them can be transformed into a non-trivial noisy channel (shown to be complete in [CMW05]) by the following protocol with expected 4 function calls. Alice first inputs a random bit b and then the inverse $\neg b$; Bob inputs independent random bits in both steps. The protocol is restarted until nowhere output "1" occurs. Afterwards Alice uses the last value of b as a one-time pad, which Bob knows with probability $\frac{2}{3}$.

Once assertion 1 of the Classification Theorem is shown, assertion 2 follows by the Symmetrization Lemma. Analogously assertion 4 follows from assertion 3, so all we have to do is proving assertion 3. One direction, the necessity of OT-cores, already follows from the passive case. Proving sufficiency for the active case is much more challenging and can be seen as our main contribution.

Our overall strategy for reducing OT in presence of an active adversary to a finite deterministic 2-party function having an OT-core proceeds in two steps. First, Alice and Bob generate some amount of correlated data by repeated invocation of the 2-party function with randomized input. Within a subsequent test step each party has to partially unveil its data, so that significant cheating can be detected. Then, on top of the remaining data an invocation of OT is built. In Section 3.1 we examine what input distributions are adequate and how the test step has to be performed. In Section 3.2 we construct a protocol for OT from such correlated data and we examine its security.

3.1 Secure generation of correlated data

We start our examination with some negative example (see Figure 4), which shows that choosing an adequate input distribution is not trivial. In the first place, the example in Figure 4 shows that letting Alice and Bob use uniformly random input is not necessarily secure. In our example there would be an undetectable cheating strategy[2] for a corrupted Bob: He picks a uniformly random input symbol from $\{2,3\}$ instead of $\{0,1,2,3\}$ and after each invocation of the 2-party function with probability $\frac{1}{2}$ locally relabels his input-output tuple by $(2,0)\mapsto(0,0)$, $(2,1)\mapsto(0,0)$, $(2,2)\mapsto(1,1)$, $(3,0)\mapsto(1,0)$, $(3,1)\mapsto(1,0)$, $(3,2)\mapsto(0,1)$. Thereby he can perfectly simulate honest behaviour, but at the same time does learn all of Alice's inputs to the 2-party function.

We circumvent this problem by more asymmetric input distributions: We pick an OT-core and let the corresponding input symbols be input with relatively high probability, while all other input symbols have a relatively low probability and are only needed for the test step. However, the example in Figure 4 also shows that we must choose the OT-core carefully. E.g. the OT-core in the upper left corner would be a bad choice, since the abovementioned cheating strategy can be adjusted to every protocol that assigns equal probability to Bob's input symbols "0" and "1". Still, significant cheating is possible for any input distribution with high probability for "0" and "1", as inputting "0" and "1" each once can be perfectly simulated by inputting "2" and "3" each once.

[2]Note that such an undetectable cheating strategy cannot exist for symmetric 2-party functions, as there Alice will notice any change in Bob's output distribution.

Actually, a main part of our work consists in proving that there always exists a "good" OT-core, if only the redundancy-free version of the considered 2-party function has any OT-core at all. In the following we first state our protocol for generation of correlated data (Section 3.1.1), then we introduce some algebraic structure that abstractly represents how a corrupted party can deviate from the protocol (Section 3.1.2) and finally we argue that there always is an OT-core that is "robust" against all such cheating strategies (Section 3.1.3).

3.1.1 The protocol for generating correlated data

A detailed description of the protocol with more concrete parameters can be found in Section 4.1.2 (Definition 12), it basically proceeds as follows.

1. **Invocation of F:** Alice and Bob call the underlying 2-party function F with randomized input for k times (k being the security parameter) and record their respective input-output tuples. A protocol parameter assigns what probability mass functions are to be used.

2. **Control A:** Alice challenges Bob on some polynomial subset of the recorded data, where he has to reveal his input-output tuples. Alice aborts the protocol if Bob obviously lies (i.e. his announcement is inconsistent with Alice's recorded input-output tuples) or his input distribution appears faulty. The test set is then removed from the recorded data.

3. **Control B:** This step equals the previous one with interchanged roles of Alice and Bob.

4. **Output:** Both parties announce where they have used input symbols that were only for test purposes. All corresponding elements are removed from the recorded input-output tuples by both parties. When too much of the recorded data has been deleted, the protocol is aborted; else each party outputs its remaining string of recorded input-output tuples.

We call this scheme *offline protocol*, since after the protocol step **Invocation of** F never again acces to F is needed.

At this point we want to emphasize that although offline protocols are not completely symmetric in Alice and Bob, most of our arguments are—in fact solely in the proof of Lemma 17 in Section 4.2 we have to explicitely take care of this asymmetry. This convenient circumstance is predicated on the fact that a corrupted party only can get some polynomially small advantage by adversarial choice of the test set in protocol step **Control A** or **Control B** respectively. Our protocol for reduction of OT to correlated data is robust against such polynomially small advantages.

3.1.2 Algebraic idealization of cheating strategies

In this section we define and investigate a class of functions $\eta : \Upsilon_{\mathrm{A}} \times \Upsilon_{\mathrm{B}}^2 \to \mathbb{R}_{\geq 0}$ that characterize how a corrupted Bob may cheat in an offline protocol. For symmetry reasons our results will directly carry over to the case that Alice is corrupted. Our intuition is that $\eta(x, y, y')$ quantifies the relative frequency of events in protocol step **Control A**, where F was invoked with input (x, y), but Bob successfully claims that he did input y'. We call such functions *cheating situations*. For convenience we use the notation $\eta(X, Y, Y') := \sum_{x \in X, y \in Y, y' \in Y'} \eta(x, y, y')$ for any $X \subseteq \Upsilon_{\mathrm{A}}$, $Y, Y' \subseteq \Upsilon_{\mathrm{B}}$ (cf. Notation 1 in Section 4.1.1). Also for convenience, we speak of a situation $(x, y)_F$ when we mean that F was called with input x from Alice and input y from Bob. We have the following six conditions to cheating situations (cf. Definition 7 in Section 4.1.1):

1. It holds that $\eta(\Upsilon_A, \Upsilon_B, \Upsilon_B) = 1$.
2. For all $x \in \Upsilon_A$ it holds that $\eta(x, \Upsilon_B, \Upsilon_B) > 0$, i.e. Alice did use her complete input alphabet.
3. For all $x \in \Upsilon_A$, $y \in \Upsilon_B$ it holds that $\eta(x, y, \Upsilon_B) = \eta(x, \Upsilon_B, \Upsilon_B) \cdot \eta(\Upsilon_A, y, \Upsilon_B)$, i.e. Bob's actual input distribution is independent of Alice's input distribution.
4. For all $x \in \Upsilon_A$, $y' \in \Upsilon_B$ it holds that $\eta(x, \Upsilon_B, y') = \eta(x, \Upsilon_B, \Upsilon_B) \cdot \eta(\Upsilon_A, \Upsilon_B, y')$, i.e. Bob's claimed input distribution appears independent of Alice's input distribution.
5. (a) For all $x \in \Upsilon_A$, $y, y' \in \Upsilon_B$ with $f_A(x, y) \neq f_A(x, y')$ it holds that $\eta(x, y, y') = 0$; else in the test step **Control A** Bob would be caught cheating immediately.
   (b) For all $x, x' \in \Upsilon_A$, $y, y' \in \Upsilon_B$ with $f_B(x, y) = f_B(x', y)$ and $f_B(x, y') \neq f_B(x', y')$ it holds that $\eta(x, y, y') = \eta(x', y, y') = 0$; else Bob would run an overwhelming risk of being caught cheating, since he cannot distinguish between situations $(x, y)_F$ and $(x', y)_F$ but must perfectly distinguish between these situations in the test step **Control A**.

Given some 2-party function $F \in \mathfrak{F}_{\mathsf{fin,det}}$, the set $\mathfrak{N}_F$ of all according cheating sitations has a very handy algebraic structure. On the one hand, cheating situations can be considered independent of (honest) Alice's input distribution, since they can be rescaled canonically to every input distribution that has non-zero probability for all $x \in \Upsilon_A$ (cf. Lemma 19 and Corollary 20 in Section 4.2.2). On the other hand, when we fix Alice's input distribution, i.e. for all $x \in \Upsilon_A$ the $\eta(x, \Upsilon_B, \Upsilon_B)$ are fixed, then our six conditions can be subsumed by a linear equation system, i.e. the set of all remaining cheating situations is a convex and bounded polytope in the linear space $\mathbb{R}^{\Upsilon_A \times \Upsilon_B^2}$ (q.v. Remark 8 and Remark 9 in Section 4.1.1).

Also the abovementioned conditions 5a and 5b play a fundamental role in our proofs. Therefore we sum them up by an extra notation (cf. Notation 4 in Section 4.1.1):

Notation (Risk-free lies). For $F = (\Upsilon_A, \Upsilon_B, \Omega_A, \Omega_B, f_A, f_B) \in \mathfrak{F}_{\mathsf{fin,det}}$ and $x \in \Upsilon_A$, $y, y' \in \Upsilon_B$ let $(x, y) \overset{F}{\rightsquigarrow} (x, y')$ denote that the following two conditions are fulfilled:

- It holds that $f_A(x, y) = f_A(x, y')$.
- For all $\tilde{x} \in \Upsilon_A$ with $f_B(x, y) = f_B(\tilde{x}, y)$ it holds that $f_B(x, y') = f_B(\tilde{x}, y')$.

The intuition behind that notation is that Bob can claim a situation $(x, y)_F$ to be a situation $(x, y')_F$, iff $(x, y) \overset{F}{\rightsquigarrow} (x, y')$. At least he cannot do so too often, if $(x, y) \overset{F}{\not\rightsquigarrow} (x, y')$. For all cheating situations η and all $x \in \Upsilon_A$, $y, y' \in \Upsilon_B$ with $(x, y) \overset{F}{\not\rightsquigarrow} (x, y')$ it holds that $\eta(x, y, y') = 0$.

Note that the "$\overset{F}{\rightsquigarrow}$"-relation links cheating situations to redundancy matters, since an input symbol $y' \in \Upsilon_B$ is redundant, iff there exists some $y \in \Upsilon_B \backslash \{y'\}$, such that $(x, y) \overset{F}{\rightsquigarrow} (x, y')$ for all $x \in \Upsilon_A$. In other words, the "$\overset{F}{\rightsquigarrow}$"-relation describes some kind of "local redundancy".

Given that Alice is uncorrupted, for every non-aborted run of an offline protocol with overwhelming probability there exists some cheating situation η, such that up to some polynomially small error the mappings $(x, y) \mapsto \eta(x, \Upsilon_B, y)$ and $(x, y) \mapsto \eta(x, y, \Upsilon_B)$ describe the prescribed and the actual joint input distribution to the underlying 2-party function respectively (cf. Corollary 24 in Section 4.2.2). Thus we have to look for some kind of "robust" OT-cores $(\tilde{x}, \tilde{x}', \tilde{y}, \tilde{y}')$, so that there does not exist any essentially non-trivial cheating situation η with $\eta(\Upsilon_A, \Upsilon_B, \{\tilde{y}, \tilde{y}'\}) = 1$. Then in the protocol step **Invocation of** F even a corrupted Bob's input distribution has to be polynomially close to honest behaviour.

3.1.3 Existence of robust OT-cores

In this section we argue that whenever a redundancy-free 2-party function $F \in \mathfrak{F}_{\mathsf{fin,det}}$ has any OT-core $(\tilde{x}, \tilde{x}', \tilde{y}, \tilde{y}')$, then F also has an OT-core $(\tilde{x}, \tilde{x}', \bar{y}, \bar{y}')$, such that for every cheating situation η with $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \{\bar{y}, \bar{y}'\}) = 1$ it holds that $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, y) = \eta(\Upsilon_\mathrm{A}, y, \Upsilon_\mathrm{B})$ for all $y \in \Upsilon_\mathrm{B}$. Intuitively, $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, y)$ and $\eta(\Upsilon_\mathrm{A}, y, \Upsilon_\mathrm{B})$ stand for Bob's claimed and actual input frequency of y respectively, i.e. we show that Bob practically cannot lie about his actual input distribution when he is demanded to use no other input symbols than $\bar{y}, \bar{y}'$. Note that Alice's input symbols $\tilde{x}, \tilde{x}'$ have stayed the same; hence in a second step we can analogously find an OT-core $(\bar{x}, \bar{x}', \bar{y}, \bar{y}')$ that is also "robust" against all relevant cheating attempts of Alice and stays "robust" against a possibly malicious Bob.

Given an OT-core $(\tilde{x}, \tilde{x}', \tilde{y}, \tilde{y}')$ of a redundancy-free 2-party function $F \in \mathfrak{F}_{\mathsf{fin,det}}$, we can find an OT-core with the desired "robustness" by just picking some $\bar{y}, \bar{y}' \in \Upsilon_\mathrm{B}$, such that $(\tilde{x}, \tilde{x}', \bar{y}, \bar{y}')$ is an OT-core and the following set has minimum size:

$$\Phi(\bar{y}, \bar{y}') \;:=\; \big\{ y \in \Upsilon_\mathrm{B} \;\big|\; \forall\, x \in \Upsilon_\mathrm{A} : (x, y) \overset{F}{\rightsquigarrow} (x, \bar{y}) \;\vee\; (x, y) \overset{F}{\rightsquigarrow} (x, \bar{y}') \big\}$$

Intuitively spoken, within an offline protocol that assigns high input probability only to $\bar{y}, \bar{y}'$ Bob cannot use any input symbol $y \in \Upsilon_\mathrm{B} \setminus \Phi(\bar{y}, \bar{y}')$ too often; at least for some specific $x \in \Upsilon_\mathrm{A}$ he practically cannot claim a situation $(x, y)_F$ to be $(x, \bar{y})_F$ or $(x, \bar{y}')_F$ without being caught cheating. In general it will not necessarily hold that $\Phi(\bar{y}, \bar{y}') = \{\bar{y}, \bar{y}'\}$, nontheless we can show now that the chosen OT-core $(\tilde{x}, \tilde{x}', \bar{y}, \bar{y}')$ is "robust" in the abovementioned sense. So, let some arbitrary cheating situation η with $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \{\bar{y}, \bar{y}'\}) = 1$ be given. By the following eight steps we show that $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, y) = \eta(\Upsilon_\mathrm{A}, y, \Upsilon_\mathrm{B})$ for all $y \in \Upsilon_\mathrm{B}$ (q.v. the proof of Lemma 29 in Section 4.3).

1. Since the "$\overset{F}{\rightsquigarrow}$"-relation is transitive, we observe that $\Phi(y, y') \subseteq \Phi(\bar{y}, \bar{y}')$ for all $y, y' \in \Phi(\bar{y}, \bar{y}')$.

2. We want to exploit the minimality of $\Phi(\bar{y}, \bar{y}')$, but it yields that $\big|\Phi(\bar{y}, \bar{y}')\big| \leq \big|\Phi(y, y')\big|$ only in case that $(\tilde{x}, \tilde{x}', y, y')$ is an OT-core. However, note that $f_\mathrm{A}(\tilde{x}, \bar{y}) = f_\mathrm{A}(\tilde{x}, \bar{y}')$, since $(\tilde{x}, \tilde{x}', \bar{y}, \bar{y}')$ is an OT-core. Further, for all $y \in \Phi(\bar{y}, \bar{y}')$ by definition of Φ we have that $(\tilde{x}, y) \overset{F}{\rightsquigarrow} (\tilde{x}, \bar{y})$ or $(\tilde{x}, y) \overset{F}{\rightsquigarrow} (\tilde{x}, \bar{y}')$, what in turn implies that $f_\mathrm{A}(\tilde{x}, y) = f_\mathrm{A}(\tilde{x}, \bar{y})$ or $f_\mathrm{A}(\tilde{x}, y) = f_\mathrm{A}(\tilde{x}, \bar{y}')$. Putting things together, we can conclude that $f_\mathrm{A}(\tilde{x}, y) = f_\mathrm{A}(\tilde{x}, y')$ for all $y, y' \in \Phi(\bar{y}, \bar{y}')$. Therefore, by the following construction we can split $\Phi(\bar{y}, \bar{y}')$ into disjoint subsets Y, Y', such that $(\tilde{x}, \tilde{x}', y, y')$ actually is an OT-core for all $y \in Y$, $y' \in Y'$. We define:

$$\begin{aligned} Y \;&:=\; \big\{ y \in \Phi(\bar{y}, \bar{y}') \;\big|\; f_\mathrm{A}(\tilde{x}', \bar{y}) = f_\mathrm{A}(\tilde{x}', y) \;\wedge\; f_\mathrm{B}(\tilde{x}, y) = f_\mathrm{B}(\tilde{x}', y) \big\} \\ Y' \;&:=\; \big\{ y' \in \Phi(\bar{y}, \bar{y}') \;\big|\; f_\mathrm{A}(\tilde{x}', \bar{y}) \neq f_\mathrm{A}(\tilde{x}', y') \;\vee\; f_\mathrm{B}(\tilde{x}, y') \neq f_\mathrm{B}(\tilde{x}', y') \big\} \end{aligned}$$

   Now, by the minimality of $\Phi(\bar{y}, \bar{y}')$ and our observation in step 1 it follows that $\Phi(\bar{y}, \bar{y}') = \Phi(y, y')$ for all $y \in Y$, $y' \in Y'$.

3. Now, for each $(x, \hat{y}) \in \Upsilon_\mathrm{A} \times \Phi(\bar{y}, \bar{y}')$ at least one of the following assertions must hold true:

$$\forall y \in Y : (x, \hat{y}) \overset{F}{\rightsquigarrow} (x, y) \qquad\qquad \forall y' \in Y' : (x, \hat{y}) \overset{F}{\rightsquigarrow} (x, y')$$

   Otherwise we had some $x \in \Upsilon_\mathrm{A}$, $\hat{y} \in \Phi(\bar{y}, \bar{y}')$, $y \in Y$, $y' \in Y'$, such that $(x, \hat{y}) \overset{F}{\not\rightsquigarrow} (x, y)$ and $(x, \hat{y}) \overset{F}{\not\rightsquigarrow} (x, y')$ and thereby $\hat{y} \notin \Phi(y, y')$, what is a contradiction to $\hat{y} \in \Phi(\bar{y}, \bar{y}') = \Phi(y, y')$ (cf. the final sentence of step 2).

4. For every $\hat{y} \in \Phi(\bar{y}, \bar{y}') \setminus \{\bar{y}\}$ we find some $x \in \Upsilon_A$, such that $\forall y' \in Y' \cup \{\hat{y}\} : (x, y') \overset{F}{\not\rightsquigarrow} (x, \bar{y})$.

   This follows from step 3, F being redundancy-free and the transitivity of the "$\overset{F}{\rightsquigarrow}$"-relation. Since F is redundancy-free, we find some $x \in \Upsilon_A$, such that $(x, \hat{y}) \overset{F}{\not\rightsquigarrow} (x, \bar{y})$. This not only is one part of the assertion above, but it also yields by step 3 that $(x, \hat{y}) \overset{F}{\rightsquigarrow} (x, y')$ for all $y' \in Y'$, since $\bar{y} \in Y$ by construction of Y. Now, if we could find any $y' \in Y'$ with $(x, y') \overset{F}{\rightsquigarrow} (x, \bar{y})$, in contradiction to our choice of x this would imply that $(x, \hat{y}) \overset{F}{\rightsquigarrow} (x, \bar{y})$, due to the transitivity of the "$\overset{F}{\rightsquigarrow}$"-relation.

5. For all $\hat{y} \in \Phi(\bar{y}, \bar{y}') \setminus \{\bar{y}\}$ we have that $\eta(\Upsilon_A, \Upsilon_B, \bar{y}) \leq \eta(\Upsilon_A, Y \setminus \{\hat{y}\}, \Upsilon_B)$, i.e. Bob's claimed input frequency of $\bar{y}$ cannot be greater than his actual overall input frequency of symbols in $Y \setminus \{\hat{y}\}$.

   Otherwise we could find some $\hat{y} \in \Phi(\bar{y}, \bar{y}') \setminus \{\bar{y}\}$, such that $\eta(x, \Upsilon_B, \bar{y}) > \eta(x, Y \setminus \{\hat{y}\}, \Upsilon_B)$ for all $x \in \Upsilon_A$ (cf. the conditions 3 and 4 to cheating situations). However, by step 4 we can choose x such that Bob cannot claim any situation $(x, y')_F$ with $y' \in Y' \cup \{\hat{y}\}$ to be a situation $(x, \bar{y})_F$; the same holds for $y' \in \Upsilon_B \setminus \Phi(\bar{y}, \bar{y}')$ by definition. He may do so only for situations $(x, y')_F$ with $y' \in Y \setminus \{\hat{y}\}$, but these are to few, as $\eta(x, \Upsilon_B, \bar{y}) > \eta(x, Y \setminus \{\hat{y}\}, \Upsilon_B)$.

6. We observe that $\eta(\Upsilon_A, \Upsilon_B \setminus \Phi(\bar{y}, \bar{y}'), \Upsilon_B) = 0$, since $\eta(\Upsilon_A, \Upsilon_B \setminus \Phi(\bar{y}, \bar{y}'), \{\bar{y}, \bar{y}'\}) = 0$ by construction of Φ and $\eta(\Upsilon_A, \Upsilon_B, \{\bar{y}, \bar{y}'\}) = 1$, i.e. $\eta\big(\Upsilon_A, \Upsilon_B, \Upsilon_B \setminus \{\bar{y}, \bar{y}'\}\big) = 0$, by assumption.

7. For all $\hat{y}' \in \Phi(\bar{y}, \bar{y}') \setminus \{\bar{y}'\}$ we have that $\eta(\Upsilon_A, \Upsilon_B, \bar{y}) \geq \eta(\Upsilon_A, Y \cup \{\hat{y}'\}, \Upsilon_B)$, i.e. Bob's claimed input frequency of $\bar{y}$ cannot be less than his actual overall input frequency of symbols in $Y \cup \{\hat{y}'\}$.

   Since the assertion of step 3 is symmetric in Y and Y', analogously to step 4 for every $\hat{y}' \in \Phi(\bar{y}, \bar{y}') \setminus \{\bar{y}'\}$ we find some $x \in \Upsilon_A$, such that $\forall y \in Y \cup \{\hat{y}'\} : (x, y) \overset{F}{\not\rightsquigarrow} (x, \bar{y}')$. We can use that to prove the analog of step 5: For all $\hat{y}' \in \Phi(\bar{y}, \bar{y}') \setminus \{\bar{y}'\}$ we have that $\eta(\Upsilon_A, \Upsilon_B, \bar{y}') \leq \eta(\Upsilon_A, Y' \setminus \{\hat{y}'\}, \Upsilon_B)$. Moreover, we have that $\eta(\Upsilon_A, \Upsilon_B, \{\bar{y}, \bar{y}'\}) = 1$ by assumption and that $\eta(\Upsilon_A, \Phi(\bar{y}, \bar{y}'), \Upsilon_B) = 1$ by step 6. Conclusively, for every $\hat{y}' \in \Phi(\bar{y}, \bar{y}') \setminus \{\bar{y}'\}$ we get that $\eta(\Upsilon_A, \Upsilon_B, \bar{y}) = 1 - \eta(\Upsilon_A, \Upsilon_B, \bar{y}') \geq 1 - \eta(\Upsilon_A, Y' \setminus \{\hat{y}'\}, \Upsilon_B) = \eta(\Upsilon_A, Y \cup \{\hat{y}'\}, \Upsilon_B)$.

8. By combination of step 5 and step 7, for all $\hat{y}, \hat{y}' \in \Phi(\bar{y}, \bar{y}')$ with $\hat{y}' \neq \bar{y}'$ and $\hat{y} \neq \bar{y}$ we can conclude that $\eta(\Upsilon_A, Y \cup \{\hat{y}'\}, \Upsilon_B) \leq \eta(\Upsilon_A, Y \setminus \{\hat{y}\}, \Upsilon_B)$. This can be exploited as follows. On the one hand, we can choose $\hat{y} = \bar{y}'$, i.e. $Y \setminus \{\hat{y}\} = Y$, whereby for all $\hat{y}' \in Y' \setminus \{\bar{y}'\}$ it follows that $\eta\big(\Upsilon_A, \hat{y}', \Upsilon_B\big) \leq 0$, i.e. $\eta\big(\Upsilon_A, Y' \setminus \{\bar{y}'\}, \Upsilon_B\big) = 0$. On the other hand, we can choose $\hat{y}' = \bar{y}$, i.e. $Y \cup \{\hat{y}'\} = Y$, whereby for all $\hat{y} \in Y \setminus \{\bar{y}\}$ it follows that $\eta\big(\Upsilon_A, \hat{y}, \Upsilon_B\big) \leq 0$, i.e. $\eta\big(\Upsilon_A, Y \setminus \{\bar{y}\}, \Upsilon_B\big) = 0$. Conclusively, using that $\eta(\Upsilon_A, \Upsilon_B \setminus \Phi(\bar{y}, \bar{y}'), \Upsilon_B) = 0$ by step 6, we get that $\eta\big(\Upsilon_A, \Upsilon_B \setminus \{\bar{y}, \bar{y}'\}, \Upsilon_B\big) = 0$, i.e. $\eta\big(\Upsilon_A, \{\bar{y}, \bar{y}'\}, \Upsilon_B\big) = 1$. Now, since $\eta\big(\Upsilon_A, \Upsilon_B, \{\bar{y}, \bar{y}'\}\big) = 1$ by assumption and neither $\bar{y}$ nor $\bar{y}'$ is redundant, one can infer rather straightforwardly that $\eta(\Upsilon_A, \Upsilon_B, y) = \eta(\Upsilon_A, y, \Upsilon_B)$ for all $y \in \Upsilon_B$, as claimed.

3.2 Reduction of OT to correlated data

We now sketch a protocol that implements OT from the correlated data produced by an appropriate offline protocol. Within this sketch we also informally argue for the protocol's security. We refer to Section 4.4 for a detailed protocol description and formal security proofs. Given a redundancy-free 2-party function F that has some OT-core $(\tilde{x}, \tilde{x}', \tilde{y}, \tilde{y}')$, the protocol proceeds as follows.

0. W.l.o.g. we may assume that the OT-core $(\tilde{x}, \tilde{x}', \tilde{y}, \tilde{y}')$ is of the first or last type in Figure 2; else we interchange the roles of Alice and Bob. W.l.o.g. we also assume that Alice's and Bob's actual input and output symbols coincide with that of Figure 2, i.e. $\tilde{x} = \tilde{y} = 0$ and so on. Furthermore, w.l.o.g. we assume that $(\tilde{x}, \tilde{x}', \tilde{y}, \tilde{y}')$ is a "robust" OT-core, for whose existence we have argued in Section 3.1.3.

1. Alice and Bob execute an offline protocol (as sketched in Section 3.1.1), where the probability mass functions n_{A} and n_{B} that stand for Alice's and Bob's prescribed input distribution respectively, are such that $n_{\mathrm{A}}(0) \approx \frac{1}{3}$ and $n_{\mathrm{A}}(1) \approx \frac{2}{3}$ and $n_{\mathrm{B}}(0) \approx n_{\mathrm{B}}(1) \approx \frac{1}{2}$. Note that in general these will not be the exact input probabilities, as for meaningful tests in the protocol steps **Control A** and **Control B** we still need all other inputs to be used with some polynomial frequency. However, for growing security parameter the relative frequency of the other inputs may polynomially converge to zero. Further note that even if a party is corrupted, its actual input distribution in non-aborted protocol runs must be polynomially close to honest behaviour, since $(\tilde{x}, \tilde{x}', \tilde{y}, \tilde{y}')$ was chosen to be a "robust" OT-core.

2. We want to handle all possible types of OT-cores analogously, therefore we let Alice announce where she got output "1". All corresponding input-output tuples are deleted from the recorded data by both parties. When Alice tries to delete too little, Bob aborts the protocol. He also aborts the protocol when he has to delete some input output-tuple other than $\big(1, f_{\mathrm{B}}(1,1)\big)$. Since Alice cannot distinguish between situations $(0,0)_F$ and $(0,1)_F$, this forces her to play honestly up to some polynomially small fraction of the recorded data.

3. Now most of the remaining input-output tuples belong to situations $(0,0)_F$, $(0,1)_F$, $(1,0)_F$. Since all according outputs are "0", it suffices that Alice and Bob henceforth only keep track of their recorded input strings. Note that at this stage about one quarter of the remaining recorded data belongs to situations $(0,0)_F$, one quarter to $(0,1)_F$ and one half to $(1,0)_F$.

4. Alice deletes some elements from her recorded input string, such that afterwards the string is balanced (i.e. it contains the same number of "0"s and "1"s). She annonces the corresponding indices to Bob, who deletes the according elements from his recorded data. If Alice tries to delete too much, Bob aborts the protocol.

5. Alice randomly permutes her recorded input string, such that afterwards each element at an odd possition is different from its subsequent element. She announces the permutation to Bob, who permutes his input string accordingly. Thereby their input strings become strings of pairs (each starting at an odd position), such that a pair "01" or "10" on Bob's side indicates the respective inverted pair "10" or "01" on Alice's side and a pair "00" on Bob's side gives him no information about the pair on Alice's side. If Bob finds a pair "11" (starting at an odd position), he aborts the protocol. Note that about half of Bob's pairs are "00", one quarter is "01" and one quarter is "10".

   Further note that primarily there is only one way Alice may get some additional information about where Bob has "00"-pairs: She chooses the permutation adversarially, so that some "11"-pairs are produced on her side. However, since her input string is roughly balanced since the beginning of step 3, she must produce roughly as much "00"-pairs as "11"-pairs on her side and for each "00"-pair she is caught cheating by Bob with probability $\frac{1}{2}$. So even a corrupted Alice may know at most polynomially few positions where Bob has "00"-pairs.

6. Since Bob now can reconstruct about half of Alice's input string and Alice has only few information about where exactly Bob can do that, we can treat the recorded data like the result of Rabin-OT calls and adapt standard reduction techniques[3]. To that effect we rename Alices input string into a string of half length over the alphabet $\{0,1\}$ and accordingly for Bob over the alphabet $\{0,1,\perp\}$; in particular the renaming is "01"$\mapsto$"0", "10"$\mapsto$"1" on Alice's side and "10"$\mapsto$"0", "01"$\mapsto$"1", "00"$\mapsto$"$\perp$" on Bob's side. When a party cheated, we can represent that by a special symbol "$\top$" in that party's string. However, the symbol "$\top$" may occur only with some polynomial relative frequency, say less than $k^{-\gamma}$. Let $\kappa := \lceil k^{1-\gamma} \rceil$.

7. Now, let $b_0, b_1 \in \{0,1\}$ be Alice's $\binom{2}{1}$-OT input and let $c \in \{0,1\}$ be Bob's choice bit. Alice chooses two random bit strings $\tilde{b}_0, \tilde{b}_1 \in \{0,1\}^\kappa$ with $\bigoplus_{j=1}^{\kappa} \tilde{b}_0[j] = b_0$ and $\tilde{b}_0[j] \oplus \tilde{b}_1[j] = b_0 \oplus b_1$ for $j = 1, \ldots, \kappa$. Bob chooses a random bit string $\tilde{c} \in \{0,1\}^\kappa$ with $\bigoplus_{j=1}^{\kappa} \tilde{c}[j] = c$.

8. Alice and Bob respectively partition their recorded input strings into κ consecutive substrings of equal length l with l as large as possible; remaining elements are discarded. Let $\tilde{s}_{\mathrm{A}}^{(j)}$ denote Alices j-th substring and $\tilde{s}_{\mathrm{B}}^{(j)}$ Bob's j-th substring. Note that by our choice of κ at least one of the $\tilde{s}_{\mathrm{A}}^{(j)}$ does not contain the symbol "$\top$". Further note that for each $\tilde{s}_{\mathrm{B}}^{(j)}$ about half of the contained elements equal "$\perp$", because of the permutation at the beginning of step 3.

   For $j = 1, \ldots, \kappa$ now the following subprotocol is executed:

   (a) Bob chooses some disjoint random sets $K_0^{(j)}, K_1^{(j)} \subseteq \{1, \ldots, l\}$ of equal cardinality $\lceil \frac{l}{3} \rceil$, such that no element of $\tilde{s}_{\mathrm{B}}^{(j)}$ indexed by $K_{\tilde{c}[j]}^{(j)}$ is "$\perp$". He announces $\left(K_0^{(j)}, K_1^{(j)}\right)$ to Alice. Note that Alice does not get any information about at least one of the $\tilde{c}[j]$, since the corresponding $\tilde{s}_{\mathrm{A}}^{(j)}$ does not contain the symbol "$\top$". Hence she stays ignorant of Bob's choice bit c.

   (b) For $i = 0, 1$ Alice uses the XOR of the elements in $\tilde{s}_{\mathrm{A}}^{(j)}$ indexed by $K_i^{(j)}$ as a one-time pad for $\tilde{b}_i[j]$. She sends the according cyphertexts to Bob, who learns $\tilde{b}_{\tilde{c}[j]}[j]$ by reconstructing the needed one-time pad from $\tilde{s}_{\mathrm{B}}^{(j)}$. Note that for each j Bob cannot get some information about both bits $\tilde{b}_0[j], \tilde{b}_1[j]$ at the same time, since more than one third of the elements in $\tilde{s}_{\mathrm{B}}^{(j)}$ equals "$\perp$". Hence he may learn at most one of Alice's $\binom{2}{1}$-OT inputs b_0, b_1.

9. Alice outputs the nothing symbol "$\perp$" and Bob computes and outputs $b_c = \bigoplus_{j=1}^{\kappa} \tilde{b}_{\tilde{c}[j]}[j]$. Correctness of Bob's output can be shown by induction on the Hamming weight of $\tilde{c}$.

We conclude this section with some remarks about how one can prove universal composability of this protocol, i.e. that it is simulatable (q.v. Section 4.4.3 and Section 4.4.4). Access to the underlying 2-party function F is in the ideal model only simulated, so the simulator can compute all the $\tilde{s}_{\mathrm{A}}^{(j)}$ or $\tilde{s}_{\mathrm{B}}^{(j)}$ respectively and hence extract the OT input of a corrupted Alice or Bob. Moreover, when Bob is corrupted, the simulator can fake a real protocol run that matches the ideal Alice's inputs b_0, b_1 as follows: Just before step 8b is entered the κ-th time, the simulator inputs the extracted choice bit c into the ideal functionality $\mathcal{F}_{\mathrm{OT}}$, thus learning b_c, and then revises $\tilde{b}_0[\kappa]$ and $\tilde{b}_1[\kappa]$ accordingly.

[3]Note that due to a subtle issue we cannot directly apply the results of [CK90, DKS99, Wul07] for reduction of OT to weak OT; e.g. in our case a corrupted Alice can choose to learn some prefix of Bob's string. In contrast, weak OT does not allow the adversary to influence when exactly additional information is leaked.

4 Formal proof of the Classification Theorem

In this section we formally proof our Classification Theorem. We start with the basic definitions and notations needed for our proof (Section 4.1). Then (in Section 4.2) we show that cheating situations are a sufficiently accurate description of how a malicious party may influence the actual joint input distributions in an offline protocol. We exploit this (in Section 4.3) to show that any redundancy-free 2-party function F always has a "robust" OT-core, if only F has any OT-core at all. Then (in Section 4.4) we give a protocol for reduction of OT to 2-party functions that have such a "robust" OT-core and formally prove its security in the UC framework. Finally, we put things together, thus obtaining a formal proof for our Classification Theorem (Section 4.5).

4.1 Basic definitions & notations

In this section we just state the definitions and notations our formal proofs are based upon (Section 4.1.1); throughout the rest of the paper we will extensively use these concepts without explicitely referring to here each single time. We also give a detailed description of our protocol for generating correlated data from a given 2-party function (Section 4.1.2).

4.1.1 Algebraic & combinatorial notations

Notation 1 (Finite sums of function values). For any arbitrary set T with some finite subset $S \subseteq T$ and any mapping $g : T \to \mathbb{R}$ we set $g(S) := \sum_{\omega \in S} g(\omega)$ for convenience. For functions with more arguments we use the canonical extension of this notation.

Notation 2 (Finite deterministic 2-party functions). Let $\mathfrak{F}_{\mathsf{fin,det}}$ denote the set of all 6-tuples $(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B})$, where $\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}$ are non-empty finite alphabets and $f_\mathrm{A}, f_\mathrm{B}$ are mappings from $\Upsilon_\mathrm{A} \times \Upsilon_\mathrm{B}$ to Ω_A and from $\Upsilon_\mathrm{A} \times \Upsilon_\mathrm{B}$ to Ω_B respectively, i.e. $f_\mathrm{A} : \Upsilon_\mathrm{A} \times \Upsilon_\mathrm{B} \to \Omega_\mathrm{A}$ and $f_\mathrm{B} : \Upsilon_\mathrm{A} \times \Upsilon_\mathrm{B} \to \Omega_\mathrm{B}$.

Definition 3 (Redundancy)**.** Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$. Then an input symbol $y' \in \Upsilon_\mathrm{B}$ is *redundant*, if there exists some corresponding *dominating* input symbol $y \in \Upsilon_\mathrm{B} \setminus \{y'\}$, such that the following two conditions hold:

1. For all $x \in \Upsilon_\mathrm{A}$ we have that $f_\mathrm{A}(x, y) = f_\mathrm{A}(x, y')$.
2. For all $x, x' \in \Upsilon_\mathrm{A}$ with $f_\mathrm{B}(x, y') \neq f_\mathrm{B}(x', y')$ we have that $f_\mathrm{B}(x, y) \neq f_\mathrm{B}(x', y)$.

For input symbols $x \in \Upsilon_\mathrm{A}$ redundancy is defined analogously. If neither Υ_A nor Υ_B contains any redundant input symbols, F is called *redundancy-free*.

Notation 4 (Risk-free lies). For $F = (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and $x, x' \in \Upsilon_\mathrm{A}$, $y, y' \in \Upsilon_\mathrm{B}$ let $(x, y) \overset{F}{\rightsquigarrow} (x', y')$ denote that the following three conditions are fulfilled:

1. It holds that $x = x'$.
2. It holds that $f_\mathrm{A}(x, y) = f_\mathrm{A}(x, y')$.
3. For all $\tilde{x} \in \Upsilon_\mathrm{A}$ with $f_\mathrm{B}(x, y) = f_\mathrm{B}(\tilde{x}, y)$ it holds that $f_\mathrm{B}(x, y') = f_\mathrm{B}(\tilde{x}, y')$.

Remark 5. For every $F = (\Upsilon_A, \Upsilon_B, \Omega_A, \Omega_B, f_A, f_B) \in \mathfrak{F}_{\mathsf{fin,det}}$ the relation given by Notation 4 is a quasi-order over $(\Upsilon_A \times \Upsilon_B)$, i.e. it is transitive and reflexive.

Remark 6. For $F = (\Upsilon_A, \Upsilon_B, \Omega_A, \Omega_B, f_A, f_B) \in \mathfrak{F}_{\mathsf{fin,det}}$ an input symbol $y' \in \Upsilon_B$ is redundant, iff there exists some $y \in \Upsilon_B \backslash \{y'\}$, such that $(x, y) \overset{F}{\rightsquigarrow} (x, y')$ for all $x \in \Upsilon_A$.

Definition 7 (Cheating situations)**.** For $F = (\Upsilon_A, \Upsilon_B, \Omega_A, \Omega_B, f_A, f_B) \in \mathfrak{F}_{\mathsf{fin,det}}$ let $\mathfrak{N}_F$ denote the set of all mappings $\eta : \Upsilon_A \times \Upsilon_B^2 \to \mathbb{R}_{\geq 0}$ for that hold the following five conditions:

1. We have that $\eta(\Upsilon_A, \Upsilon_B, \Upsilon_B) = 1$.
2. For all $x \in \Upsilon_A$ we have that $\eta(x, \Upsilon_B, \Upsilon_B) > 0$.
3. For all $x \in \Upsilon_A$, $y \in \Upsilon_B$ we have that $\eta(x, y, \Upsilon_B) = \eta(x, \Upsilon_B, \Upsilon_B) \cdot \eta(\Upsilon_A, y, \Upsilon_B)$.
4. For all $x \in \Upsilon_A$, $y' \in \Upsilon_B$ we have that $\eta(x, \Upsilon_B, y') = \eta(x, \Upsilon_B, \Upsilon_B) \cdot \eta(\Upsilon_A, \Upsilon_B, y')$.
5. For all $x \in \Upsilon_A$, $y, y' \in \Upsilon_B$ with $(x, y) \overset{F}{\not\rightsquigarrow} (x, y')$ we have that $\eta(x, y, y') = 0$.

The mappings $\eta \in \mathfrak{N}_F$ are called *cheating situations* for F. A cheating strategy $\eta \in \mathfrak{N}_F$ is called *normalized*, if for all $x \in \Upsilon_A$ it holds that $\eta(x, \Upsilon_B, \Upsilon_B) = \frac{1}{|\Upsilon_A|}$. It is called *harmless*, if for all $y \in \Upsilon_B$ it holds that $\eta(\Upsilon_A, \Upsilon_B, y) = \eta(\Upsilon_A, y, \Upsilon_B)$.

Remark 8. Let $F := (\Upsilon_A, \Upsilon_B, \Omega_A, \Omega_B, f_A, f_B) \in \mathfrak{F}_{\mathsf{fin,det}}$. Then the set of all normalized cheating situations for F is a convex and bounded polytope in the linear space $\mathbb{R}^{\Upsilon_A \times \Upsilon_B^2}$. Since this polytope can be described by *finitely* many linear inequations, it is the convex hull of a *finite* set of vertices.

Remark 9. Let $F \in \mathfrak{F}_{\mathsf{fin,det}}$ and let $\eta, \eta' \in \mathfrak{N}_F$ be normalized. Then for every $s \in \mathbb{R}$ the mapping $\tilde{\eta} := s \cdot \eta + (1 - s) \cdot \eta'$ is a normalized cheating situation for F, if only $\mathrm{Image}(\tilde{\eta}) \subseteq \mathbb{R}_{\geq 0}$.

4.1.2 Offline protocols

In this section we formally state the protocol scheme by which we produce correlated data from some given 2-party function. However, before we do that, we formally introduce how we handle strings over finite alphabets.

Notation 10. Let s be a finite string over some alphabet Ω. By $|s|$ we denote the length of s. By $|s|_\alpha$ with $\alpha \in \Omega$ we denote the number of appereances of α in s. We canonically extend this notation to subalphabets $T \subseteq \Omega$ by $|s|_T := \sum_{\alpha \in T} |s|_\alpha$. By $s[i]$ with $i \in \{1, \ldots, |s|\}$ we denote the i-th element of s. For $n \in \mathbb{N}$ and a given index set $K = \{k_1, \ldots, k_n\} \subset \mathbb{N}$ with $0 < k_1 < \ldots < k_n \leq |s|$, we denote the string $s[k_1]\, s[k_2] \ldots s[k_n]$ by $s[k_1, \ldots, k_n]$ or simply by $s[K]$. Further, for some given strings s_A and s_B of the same length $|s_A| = |s_B|$, we define the *compound string* $s_A \times s_B$, whose i-th element just is the tuple $\big(s_A[i], s_B[i]\big)$.

Notation 11. For $F = (\Upsilon_A, \Upsilon_B, \Omega_A, \Omega_B, f_A, f_B) \in \mathfrak{F}_{\mathsf{fin,det}}$ let Π_F denote the set of all tuples $(n_A, n_B, \alpha, \beta, \gamma)$, where $n_A : \Upsilon_A \to \mathbb{R}_{\geq 0}$ and $n_B : \Upsilon_B \to \mathbb{R}_{\geq 0}$ are some probability mass functions and $\alpha, \beta, \gamma \in \mathbb{R}_{>0}$, such that $\beta < \frac{1}{2}$.

Definition 12 (Offline protocols)**.** Let $F := (\Upsilon_A, \Upsilon_B, \Omega_A, \Omega_B, f_A, f_B) \in \mathfrak{F}_{\mathsf{fin,det}}$. Further let $(n_A, n_B, \alpha, \beta, \gamma) \in \Pi_F$ and let $\tilde{X} := \{x \in \Upsilon_A \mid n_A(x) > 0\}$ and $\tilde{Y} := \{y \in \Upsilon_B \mid n_B(y) > 0\}$. Let k denote the security parameter and let $K := \{1, \ldots, k\}$. Then the offline protocol $\pi_F(n_A, n_B, \alpha, \beta, \gamma)$ proceeds as follows:

0. **Initialization:** Alice initializes two empty strings $s_{\mathrm{A}}^{\mathsf{in}}, s_{\mathrm{A}}^{\mathsf{out}}$ and an index set $K_{\mathrm{A}} \leftarrow K$. Bob analogously initializes $s_{\mathrm{B}}^{\mathsf{in}}, s_{\mathrm{B}}^{\mathsf{out}}, K_{\mathrm{B}}$. Let the probability mass functions $\tilde{n}_{\mathrm{A}}, \tilde{n}_{\mathrm{B}}$ be defined by:

$$\tilde{n}_{\mathrm{A}}: \quad \Upsilon_{\mathrm{A}} \to \mathbb{R}_{>0}, \quad x \mapsto \begin{cases} n_{\mathrm{A}}(x) & \text{if } \tilde{X} = \Upsilon_{\mathrm{A}} \\ (1-k^{-\alpha}) \cdot n_{\mathrm{A}}(x) & \text{if } x \in \tilde{X} \text{ and } \tilde{X} \neq \Upsilon_{\mathrm{A}} \\ k^{-\alpha} \cdot |\Upsilon_{\mathrm{A}} \backslash \tilde{X}|^{-1} & \text{if } x \in \Upsilon_{\mathrm{A}} \backslash \tilde{X} \end{cases}$$

$$\tilde{n}_{\mathrm{B}}: \quad \Upsilon_{\mathrm{B}} \to \mathbb{R}_{>0}, \quad y \mapsto \begin{cases} n_{\mathrm{B}}(y) & \text{if } \tilde{Y} = \Upsilon_{\mathrm{B}} \\ (1-k^{-\alpha}) \cdot n_{\mathrm{B}}(y) & \text{if } y \in \tilde{Y} \text{ and } \tilde{Y} \neq \Upsilon_{\mathrm{B}} \\ k^{-\alpha} \cdot |\Upsilon_{\mathrm{B}} \backslash \tilde{Y}|^{-1} & \text{if } y \in \Upsilon_{\mathrm{B}} \backslash \tilde{Y} \end{cases}$$

1. **Invocation of F:** According to $\tilde{n}_{\mathrm{A}}$ Alice randomly chooses some input symbol $x \in \Upsilon_{\mathrm{A}}$; Bob randomly chooses some $y \in \Upsilon_{\mathrm{B}}$ according to $\tilde{n}_{\mathrm{B}}$. Then F is invoked with the input tuple (x, y), i.e. Alice learns $a := f_{\mathrm{A}}(x, y)$ and Bob learns $b := f_{\mathrm{B}}(x, y)$. Alice concatenates x to $s_{\mathrm{A}}^{\mathsf{in}}$ and a to $s_{\mathrm{A}}^{\mathsf{out}}$ respectively; Bob concatenates y to $s_{\mathrm{B}}^{\mathsf{in}}$ and b to $s_{\mathrm{B}}^{\mathsf{out}}$ respectively.

   This protocol step is executed for k times.

2. **Control A:** Alice picks some uniformly random index set $\bar{K}_{\mathrm{A}} \subseteq K_{\mathrm{A}}$ with[4] $|\bar{K}_{\mathrm{A}}| = k^{\frac{1}{2}+\beta}$ and sends $\bar{K}_{\mathrm{A}}$ to Bob, who announces $\big(\hat{s}_{\mathrm{B}}^{\mathsf{in}}[\bar{K}_{\mathrm{A}}], \hat{s}_{\mathrm{B}}^{\mathsf{out}}[\bar{K}_{\mathrm{A}}]\big) := \big(s_{\mathrm{B}}^{\mathsf{in}}[\bar{K}_{\mathrm{A}}], s_{\mathrm{B}}^{\mathsf{out}}[\bar{K}_{\mathrm{A}}]\big)$. Alice aborts the protocol in the following two cases:

   - Bob obviously lies, i.e. there exists some index $i \in \bar{K}_{\mathrm{A}}$ with $s_{\mathrm{A}}^{\mathsf{out}}[i] \neq f_{\mathrm{A}}\big(s_{\mathrm{A}}^{\mathsf{in}}[i], \hat{s}_{\mathrm{B}}^{\mathsf{in}}[i]\big)$ or $\hat{s}_{\mathrm{B}}^{\mathsf{out}}[i] \neq f_{\mathrm{B}}\big(s_{\mathrm{A}}^{\mathsf{in}}[i], \hat{s}_{\mathrm{B}}^{\mathsf{in}}[i]\big)$.
   - Bob's input distribution significantly differs from its expected value, i.e. there exist some $X \subseteq \Upsilon_{\mathrm{A}}$, $Y \subseteq \Upsilon_{\mathrm{B}}$ with:

$$\Big| \big| s_{\mathrm{A}}^{\mathsf{in}}[\bar{K}_{\mathrm{A}}] \times \hat{s}_{\mathrm{B}}^{\mathsf{in}}[\bar{K}_{\mathrm{A}}] \big|_{X \times Y} - \tilde{n}_{\mathrm{A}}(X) \cdot \tilde{n}_{\mathrm{B}}(Y) \cdot k^{\frac{1}{2}+\beta} \Big| \quad > \quad k^{\frac{1}{4}+\beta}$$

   At the end of this protocol step Alice sets $K_{\mathrm{A}} \leftarrow K_{\mathrm{A}} \backslash \bar{K}_{\mathrm{A}}$ and Bob sets $K_{\mathrm{B}} \leftarrow K_{\mathrm{B}} \backslash \bar{K}_{\mathrm{A}}$.

3. **Control B:** This protocol step proceeds analogously to **Control A** with interchanged roles of Alice and Bob.

4. **Output:** Alice announces the set $K'_{\mathrm{A}} := \big\{ i \in K_{\mathrm{A}} \;\big|\; s_{\mathrm{A}}^{\mathsf{in}}[i] \in \tilde{X} \big\}$, then Bob announces $K'_{\mathrm{B}} := \big\{ i \in K_{\mathrm{B}} \;\big|\; s_{\mathrm{B}}^{\mathsf{in}}[i] \in \tilde{Y} \big\}$; let $K' := K'_{\mathrm{A}} \cap K'_{\mathrm{B}}$. When $|K'| < k - k^{1-\gamma}$, the protocol is aborted; else Alice outputs $s_{\mathrm{A}}^{\mathsf{in}}[K'] \times s_{\mathrm{A}}^{\mathsf{out}}[K']$ and Bob outputs $s_{\mathrm{B}}^{\mathsf{in}}[K'] \times s_{\mathrm{B}}^{\mathsf{out}}[K']$.

4.2 Linking offline protocols to cheating situations

In this section we show that, given any 2-party function $F = (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, f_{\mathrm{A}}, f_{\mathrm{B}}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and given that Alice is honest, there always exists some cheating strategy $\eta \in \mathfrak{N}_F$, such that the actual and the prescribed input distributions in the step **Invocation of** F of a corresponding offline protocol are polynomially close to the mappings $(x, y) \mapsto \eta(x, y, \Upsilon_{\mathrm{B}})$ and $(x, y') \mapsto \eta(x, \Upsilon_{\mathrm{B}}, y')$ respectively.

[4] W.l.o.g. it holds that $k^{\frac{1}{2}+\beta} \in \mathbb{N}$, since w.l.o.g. we have that $\beta \in \mathbb{Q}$ and $k \in \{l^{\zeta} \,|\, l \in \mathbb{N}\}$ with ζ being some constant integer, such that $\zeta \cdot (\frac{1}{2} + \beta) \in \mathbb{N}$.

4.2.1 Blurred cheating situations

As mentioned above, cheating situations will characterize the actual and claimed input distributions in an offline protocol only up to some polynomial error. Therefore, in this section we define a class of functions that fulfill the conditions to cheating situations only up to some error parameter. Then we show that by these *blurred cheating situations* we can strictly bound a corrupted Bob's deviation from honest behaviour.

Definition 13 (Blurred cheating situations)**.** For $F = (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and $\varepsilon, \delta \in \mathbb{R}_{>0}$ let $\tilde{\mathfrak{N}}_F(\varepsilon, \delta)$ denote the set of all mappings $\nu : \Upsilon_\mathrm{A} \times \Upsilon_\mathrm{B}^2 \to \mathbb{R}_{\geq 0}$ that meet the following five conditions:

1. It holds that $\nu(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Upsilon_\mathrm{B}) = 1$.
2. For all $x \in \Upsilon_\mathrm{A}$ it holds that $\nu(x, \Upsilon_\mathrm{B}, \Upsilon_\mathrm{B}) \geq \delta$.
3. For all $x \in \Upsilon_\mathrm{A}$, $y \in \Upsilon_\mathrm{B}$ it holds that $\left|\nu(x, y, \Upsilon_\mathrm{B}) - \nu(x, \Upsilon_\mathrm{B}, \Upsilon_\mathrm{B}) \cdot \nu(\Upsilon_\mathrm{A}, y, \Upsilon_\mathrm{B})\right| < \varepsilon$.
4. For all $x \in \Upsilon_\mathrm{A}$, $y' \in \Upsilon_\mathrm{B}$ it holds that $\left|\nu(x, \Upsilon_\mathrm{B}, y') - \nu(x, \Upsilon_\mathrm{B}, \Upsilon_\mathrm{B}) \cdot \nu(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, y')\right| < \varepsilon$.
5. For all $x \in \Upsilon_\mathrm{A}$, $y, y' \in \Upsilon_\mathrm{B}$ with $(x, y) \overset{F}{\not\to} (x, y')$ it holds that $\nu(x, y, y') < \varepsilon$.

Notation 14. Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and let $\pi := \pi_F(n_\mathrm{A}, n_\mathrm{B}, \alpha, \beta, \gamma)$, such that $(n_\mathrm{A}, n_\mathrm{B}, \alpha, \beta, \gamma) \in \Pi_F$. Further let $\varepsilon, \Delta \in \mathbb{R}_{>0}$. Let k denote the security parameter. Then by $\Lambda_\mathrm{A}(\pi, \varepsilon, \Delta)$ we denote the set[5] of all protocol runs of π that are aborted or for that it holds:

- For $K := \{1, \ldots, k\}$ and every $X \subseteq \Upsilon_\mathrm{A}, Y \subseteq \Upsilon_\mathrm{B}$ we have:

$$
\begin{aligned}
k^{\Delta} &> \left||s_\mathrm{A}^{\mathsf{in}}[K]|_X - k \cdot \tilde{n}_\mathrm{A}(X)\right| && (1)\\
k^{(\frac{1}{2}+\beta)\Delta} &> \left||s_\mathrm{A}^{\mathsf{in}}[\bar{K}_\mathrm{A}] \times s_\mathrm{B}^{\mathsf{in}}[\bar{K}_\mathrm{A}]|_{X\times Y} - k^{-\frac{1}{2}+\beta} \cdot |s_\mathrm{A}^{\mathsf{in}}[K] \times s_\mathrm{B}^{\mathsf{in}}[K]|_{X\times Y}\right| && (2)\\
k^{\Delta} &> \left||s_\mathrm{A}^{\mathsf{in}}[K] \times s_\mathrm{B}^{\mathsf{in}}[K]|_{X\times Y} - |s_\mathrm{B}^{\mathsf{in}}[K]|_Y \cdot \tilde{n}_\mathrm{A}(X)\right| && (3)\\
k^{\frac{1}{4}+\beta} &\geq \left|\left|s_\mathrm{A}^{\mathsf{in}}[\bar{K}_\mathrm{A}] \times \hat{s}_\mathrm{B}^{\mathsf{in}}[\bar{K}_\mathrm{A}]\right|_{X\times Y} - \tilde{n}_\mathrm{A}(X) \cdot \tilde{n}_\mathrm{B}(Y) \cdot k^{\frac{1}{2}+\beta}\right| && (4)\\
|K'| &\geq k - k^{1-\gamma} && (5)
\end{aligned}
$$

- For all $x \in \Upsilon_\mathrm{A}$, $y, y' \in \Upsilon_\mathrm{B}$ with $(x, y) \overset{F}{\not\to} (x, y')$ we have:

$$
\left|s_\mathrm{A}^{\mathsf{in}}[\bar{K}_\mathrm{A}] \times s_\mathrm{B}^{\mathsf{in}}[\bar{K}_\mathrm{A}] \times \hat{s}_\mathrm{B}^{\mathsf{in}}[\bar{K}_\mathrm{A}]\right|_{(x,y,y')} < k^{\varepsilon} \qquad (6)
$$

By $\Lambda_\mathrm{B}(\pi, \varepsilon, \Delta)$ we denote the set of all protocol runs that are aborted or for that it holds:

- For $K := \{1, \ldots, k\}$ and every $X \subseteq \Upsilon_\mathrm{A}, Y \subseteq \Upsilon_\mathrm{B}$ we have:

$$
\begin{aligned}
k^{\Delta} &> \left||s_\mathrm{B}^{\mathsf{in}}[K]|_Y - k \cdot \tilde{n}_\mathrm{B}(Y)\right| && (7)\\
k^{(\frac{1}{2}+\beta)\Delta} &> \left||s_\mathrm{A}^{\mathsf{in}}[\bar{K}_\mathrm{B}] \times s_\mathrm{B}^{\mathsf{in}}[\bar{K}_\mathrm{B}]|_{X\times Y} - k^{-\frac{1}{2}+\beta}|s_\mathrm{A}^{\mathsf{in}}[K] \times s_\mathrm{B}^{\mathsf{in}}[K]|_{X\times Y}\right| && (8)\\
k^{\Delta} &> \left||s_\mathrm{A}^{\mathsf{in}}[K] \times s_\mathrm{B}^{\mathsf{in}}[K]|_{X\times Y} - |s_\mathrm{A}^{\mathsf{in}}[K]|_X \cdot \tilde{n}_\mathrm{B}(Y)\right| && (9)\\
k^{\frac{1}{4}+\beta} &\geq \left|\left|\hat{s}_\mathrm{A}^{\mathsf{in}}[\bar{K}_\mathrm{B}] \times s_\mathrm{B}^{\mathsf{in}}[\bar{K}_\mathrm{B}]\right|_{X\times Y} - \tilde{n}_\mathrm{A}(X) \cdot \tilde{n}_\mathrm{B}(Y) \cdot k^{\frac{1}{2}+\beta}\right| && (10)\\
|K'| &\geq k - k^{1-\gamma} && (11)
\end{aligned}
$$

[5]Equivalently, one can consider $\Lambda_\mathrm{A}(\pi, \varepsilon, \Delta)$ a predicate on protocol runs. Note that $\Lambda_\mathrm{A}(\pi, \varepsilon, \Delta)$ is well-defined as long as at least one party is honest. W.l.o.g. we assume that this is always the case.

- For all $x, x' \in \Upsilon_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$ for that exists some $y' \in \Upsilon_{\mathrm{A}}$ with $f_{\mathrm{A}}(x,y) = f_{\mathrm{A}}(x,y')$ and $\big(f_{\mathrm{A}}(x',y), f_{\mathrm{B}}(x',y)\big) \neq \big(f_{\mathrm{A}}(x',y'), f_{\mathrm{B}}(x',y')\big)$ we have:

$$\big|s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{B}}] \times \hat{s}^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{B}}] \times s^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{B}}]\big|_{(x,x',y)} \quad < \quad k^{\varepsilon} \tag{12}$$

We say that some predicate P holds for *almost all* (non-aborted) protocol runs in $\Lambda_{\mathrm{A}}(\pi,\varepsilon,\Delta)$, when there exists some constant $k_0 \in \mathbb{N}$, such that P holds for all (non-aborted) protocol runs in $\Lambda_{\mathrm{A}}(\pi,\varepsilon,\Delta)$ with security parameter greater than k_0; analogously for $\Lambda_{\mathrm{B}}(\pi,\varepsilon,\Delta)$

Lemma 15 (Stability of random distributions)**.** *Let $(X_k)_{k\in\mathbb{N}}$ be some sequence of binomially and/or hypergeometrically distributed random variables X_k, such that $\mathbf{P}[0 \leq X_k \leq k] = 1$ for all $k \in \mathbb{N}$. Further let $\Delta \in \mathbb{R}$, such that $\Delta > \frac{1}{2}$. Then the probability $\mathbf{P}\big[|X_k - \mathbf{E}(X_k)| \geq k^{\Delta}\big]$ is negligible in k.*

Proof. Hoeffding's inequality (Theorem 2 in [Hoe63]) implies that for all $n \in \mathbb{N}, c \in \mathbb{R}_{>0}$ and every binomially distributed random variable X with $\mathbf{P}[0 \leq X \leq n] = 1$ it holds:

$$\mathbf{P}\big[|X - \mathbf{E}(X)| \geq c\big] \quad \leq \quad 2 \cdot \exp\big(-2c^2 \cdot n^{-1}\big)$$

In chapter 6 of [Hoe63] it was shown that this estimation also holds when X is distributed hypergeometrically. Thereby for all $k \in \mathbb{N}$ follows:

$$\mathbf{P}\big[|X_k - \mathbf{E}(X_k)| \geq k^{\Delta}\big] \;\leq\; 2 \cdot \exp\big(-2k^{2\Delta-1}\big) \qquad \square$$

Corollary 16. *Let $\mathcal{H}$ be some memoryless random source that samples from some finite alphabet Ω. Let $p : \Omega \to \mathbb{R}$, $x \mapsto \mathbf{P}[\mathcal{H} \text{ outputs } x]$. Further let $\mathcal{A}$ be some arbitrary algorithm that on input $k \in \mathbb{N}$ sequentially samples up to k random symbols $X_1, \ldots, X_N \xleftarrow{\mathrm{r}} \mathcal{H}$, i.e. N is a random variable with $\mathbf{P}[1 \leq N \leq k] = 1$ and N may be correlated with $(X_1, \ldots, X_N)$. Then for all $\Delta \in \mathbb{R}$ with $\Delta > \frac{1}{2}$ and all $S \subseteq \Omega$ the probability $\mathbf{P}\left[\big||X_1 \ldots X_N|_S - N \cdot p(S)\big| \geq k^{\Delta}\right]$ is negligible in k.*

Proof. For our proof we make $\mathcal{A}$ a bit more powerful: $\mathcal{A}$ always samples exactly k random symbols $X_1, \ldots, X_k \xleftarrow{\mathrm{r}} \mathcal{H}$ and then computes and outputs N.

Now, for $n \in \{1, \ldots, k\}$, $S \subseteq \Omega$ let $\mathcal{X}_n(S) := |X_1 \ldots X_n|_S$. Analogously to the proof of Lemma 15 for all $n \in \{0, \ldots, k\}$, $S \subseteq \Omega$ it always holds:

$$\mathbf{P}\big[|\mathcal{X}_n(S) - n \cdot p(S)| \geq k^{\Delta}\big] \;\leq\; \mathbf{P}\big[|\mathcal{X}_n(S) - n \cdot p(S)| \geq n^{\Delta}\big] \;\leq\; 2 \cdot \exp\big(-2n^{2\Delta-1}\big)$$

Further, for $n < k^{\Delta}$ it trivially holds that $\mathbf{P}\big[|\mathcal{X}_n(S) - n \cdot p(S)| \geq k^{\Delta}\big] = 0$. Hence follows:

$$\mathbf{P}\big[|\mathcal{X}_N(S) - N \cdot p(S)| \geq k^{\Delta}\big] \;\leq\; \sum_{n=\lceil k^{\Delta} \rceil}^{k} \mathbf{P}\big[|\mathcal{X}_n(S) - n \cdot p(S)| \geq k^{\Delta}\big] \;\leq\; \frac{2(k - k^{\Delta})}{\exp\big(2k^{\Delta(2\Delta-1)}\big)} \qquad \square$$

Lemma 17. *Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, f_{\mathrm{A}}, f_{\mathrm{B}}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and $\pi := \pi_F(n_{\mathrm{A}}, n_{\mathrm{B}}, \alpha, \beta, \gamma)$, such that $(n_{\mathrm{A}}, n_{\mathrm{B}}, \alpha, \beta, \gamma) \in \Pi_F$. Let $\varepsilon, \Delta \in \mathbb{R}_{>0}$, such that $\alpha < \varepsilon$ and $(2 - \Delta)\beta < \frac{\Delta}{2}$ and $\frac{1}{2} < \Delta$. Then, when Alice is honest, a protocol run with fresh randomness for all parties lies in $\Lambda_{\mathrm{A}}(\pi,\varepsilon,\Delta)$ with overwhelming probability. Analogously, when Bob is honest, a protocol run with fresh randomness for all parties lies in $\Lambda^{\pi}_{\mathrm{B}}(\pi,\varepsilon,\Delta)$ with overwhelming probability.*

Proof. When Alice is honest, then $|s^{\mathsf{in}}_{\mathrm{A}}[K]|_X$ with $X \subseteq \Upsilon_{\mathrm{A}}$ is a binomially distributed random variable with expected value $k \cdot \tilde{n}_{\mathrm{A}}(X)$. Hence, by Lemma 15 only with negligible probability it may happen that $\big||s^{\mathsf{in}}_{\mathrm{A}}[K]|_X - k \cdot \tilde{n}_{\mathrm{A}}(X)\big| \geq k^{\Delta}$. Analogously, for each $X \subseteq \Upsilon_{\mathrm{A}}$, $Y \subseteq \Upsilon_{\mathrm{B}}$ only with negligible probability it may happen that $\big||s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{A}}] \times s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{B}}]|_{X\times Y} - k^{-\frac{1}{2}+\beta}|s^{\mathsf{in}}_{\mathrm{A}}[K] \times s^{\mathsf{in}}_{\mathrm{B}}[K]|_{X\times Y}\big| \geq k^{(\frac{1}{2}+\beta)\Delta}$, since $|s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{A}}] \times s^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}]|_{X\times Y}$ is hypergeometrically distributed and its expected value is $k^{-\frac{1}{2}+\beta}|s^{\mathsf{in}}_{\mathrm{A}}[K] \times s^{\mathsf{in}}_{\mathrm{B}}[K]|_{X\times Y}\big|$. Thereby, inequation (1) and inequation (2) of Notation 14 are shown. Inequation (3) follows by Corollary 16, since in the protocol step **Invocation of** F an honest Alice can be seen as a memoryless random source with output distribution according to $\tilde{n}_{\mathrm{A}}$, while the behaviour of a possibly corrupted Bob can be depicted by an algorithm $\mathcal{A}$ that depending on the result of previous invocations of F decides what to input into F in the current turn. Further, when Alice is honest, by definition of π (Definition 12) the following two inequalities hold in every non-aborted protocol run:

$$\begin{aligned} k^{\frac{1}{4}+\beta} &\geq \Big|\big|s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{A}}] \times \hat{s}^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}]\big|_{X'\times Y'} - \tilde{n}_{\mathrm{A}}(X') \cdot \tilde{n}_{\mathrm{B}}(Y') \cdot k^{\frac{1}{2}+\beta}\Big| \\ |K'| &\geq k - k^{1-\gamma} \end{aligned}$$

Now, for the case that Alice is honest only inequation (6) is left, which is a bit harder to prove. Let $\tilde{x} \in \Upsilon_{\mathrm{A}}$, $\tilde{y}, \tilde{y}' \in \Upsilon_{\mathrm{B}}$, such that $(\tilde{x}, \tilde{y}) \overset{F}{\nrightarrow} (\tilde{x}, \tilde{y}')$. In case of $f_{\mathrm{A}}(\tilde{x}, \tilde{y}) \neq f_{\mathrm{A}}(\tilde{x}, \tilde{y}')$ we clearly have that $\big|s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{A}}] \times s^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}] \times \hat{s}^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}]\big|_{(\tilde{x},\tilde{y},\tilde{y}')} = 0$ for every non-aborted run with honest Alice, since else Alice would have ignored an obvious lie of Bob in protocol step **Control A**. In case of $f_{\mathrm{A}}(\tilde{x}, \tilde{y}) = f_{\mathrm{A}}(\tilde{x}, \tilde{y}')$ we find some $\tilde{x}' \in \Upsilon_{\mathrm{A}}$ with $f_{\mathrm{B}}(\tilde{x}, \tilde{y}) = f_{\mathrm{B}}(\tilde{x}', \tilde{y})$ and $f_{\mathrm{B}}(\tilde{x}, \tilde{y}') \neq f_{\mathrm{B}}(\tilde{x}', \tilde{y}')$. On the one hand, Bob cannot distinguish situations where F was invoked with input $(\tilde{x}, \tilde{y})$ from situations with input $(\tilde{x}', \tilde{y})$ better than by guessing. On the other hand, he has to answer according challenges in protocol step **Control A** differently, when he wants to simulate successfully that he did input $\tilde{y}'$ instead of $\tilde{y}$. Now we can adduce a simple hybrid argument. We could change the model as follows: Whenever Bob tries to simulate that he did input $\tilde{y}'$ instead of $\tilde{y}$ and Alice's input to F was $\tilde{x}$ or $\tilde{x}'$, we replace Alice's input by some fresh random symbol $\mathbf{x} \in \{\tilde{x}, \tilde{x}'\}$ with $\mathbf{P}[\mathbf{x}{=}\tilde{x}] = \frac{\tilde{n}_{\mathrm{A}}(\tilde{x})}{\tilde{n}_{\mathrm{A}}(\tilde{x})+\tilde{n}_{\mathrm{A}}(\tilde{x}')}$ and $\mathbf{P}[\mathbf{x}{=}\tilde{x}'] = \frac{\tilde{n}_{\mathrm{A}}(\tilde{x}')}{\tilde{n}_{\mathrm{A}}(\tilde{x})+\tilde{n}_{\mathrm{A}}(\tilde{x}')}$ and update Alice's memory consistently. This does not change the distribution of protocol runs in any way. So, in case of $\big|s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{A}}] \times s^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}] \times \hat{s}^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}]\big|_{(\tilde{x},\tilde{y},\tilde{y}')} \geq k^{\varepsilon}$ we can bound the probability p that Bob is not caught cheating as follows:

$$p \quad \leq \quad \left(\frac{\max\big(\tilde{n}_{\mathrm{A}}(\tilde{x}), \tilde{n}_{\mathrm{A}}(\tilde{x}')\big)}{\tilde{n}_{\mathrm{A}}(\tilde{x}) + \tilde{n}_{\mathrm{A}}(\tilde{x}')}\right)^{k^{\varepsilon}} \quad = \quad \left(1 - \frac{\min\big(\tilde{n}_{\mathrm{A}}(\tilde{x}), \tilde{n}_{\mathrm{A}}(\tilde{x}')\big)}{\tilde{n}_{\mathrm{A}}(\tilde{x}) + \tilde{n}_{\mathrm{A}}(\tilde{x}')}\right)^{k^{\varepsilon}}$$

Moreover, by definition of π (Definition 12) we can estimate $\min_{x\in\Upsilon_{\mathrm{A}}}\big(\tilde{n}_{\mathrm{A}}(x)\big) > \frac{k^{-\alpha}}{|\Upsilon_{\mathrm{A}}|}$, if only the security parameter k is great enough. Hence, for almost all security parameters k follows:

$$p \quad \leq \quad \left(1 - \frac{\min_{x\in\Upsilon_{\mathrm{A}}}\big(\tilde{n}_{\mathrm{A}}(x)\big)}{\tilde{n}_{\mathrm{A}}(\tilde{x}) + \tilde{n}_{\mathrm{A}}(\tilde{x}')}\right)^{k^{\varepsilon}} \quad < \quad \left(1 - \tfrac{k^{-\alpha}}{|\Upsilon_{\mathrm{A}}|}\right)^{k^{\varepsilon}} \quad \leq \quad \exp\left(-\tfrac{k^{\varepsilon-\alpha}}{|\Upsilon_{\mathrm{A}}|}\right)$$

This is negligible, since $\alpha < \varepsilon$ by assumption.

When Bob is honest, we can almost analogously prove that a protocol run with fresh randomness for all parties lies in $\Lambda^{\pi}_{\mathrm{B}}(\pi, \varepsilon, \Delta)$ with overwhelming probability. Only inequation (8) is a bit more

intricate to prove. Here, the random variable $|s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{B}}] \times s^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{B}}]|_{X\times Y}$ with $X \subseteq \Upsilon_{\mathrm{A}}$, $Y \subseteq \Upsilon_{\mathrm{B}}$ has expectation $k^{\frac{1}{2}+\beta} \cdot |K \backslash \bar{K}_{\mathrm{A}}|^{-1} \cdot |s^{\mathsf{in}}_{\mathrm{A}}[K \backslash \bar{K}_{\mathrm{A}}] \times s^{\mathsf{in}}_{\mathrm{B}}[K \backslash \bar{K}_{\mathrm{A}}]|_{X\times Y}$. Nonetheless, by Lemma 15 for arbitrary but constant $\Delta' \in \mathbb{R}$ with $\frac{1}{2} < \Delta'$ follows that only with negligible probability may happen:

$$\left| |s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{B}}] \times s^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{B}}]|_{X\times Y} - \frac{k^{\frac{1}{2}+\beta} \cdot |s^{\mathsf{in}}_{\mathrm{A}}[K \backslash \bar{K}_{\mathrm{A}}] \times s^{\mathsf{in}}_{\mathrm{B}}[K \backslash \bar{K}_{\mathrm{A}}]|_{X\times Y}}{k - k^{\frac{1}{2}+\beta}} \right| \quad \geq \quad k^{(\frac{1}{2}+\beta)\Delta'}$$

Furthermore, when at least one party is honest, by definition of π (Definition 12) for every non-aborted protocol run it holds:

$$\left| |s^{\mathsf{in}}_{\mathrm{A}}[K \backslash \bar{K}_{\mathrm{A}}] \times s^{\mathsf{in}}_{\mathrm{B}}[K \backslash \bar{K}_{\mathrm{A}}]|_{X\times Y} - |s^{\mathsf{in}}_{\mathrm{A}}[K] \times s^{\mathsf{in}}_{\mathrm{B}}[K]|_{X\times Y} \right| \quad \leq \quad |\bar{K}_{\mathrm{A}}| \quad = \quad k^{\frac{1}{2}+\beta}$$

Thereby, that $\left| |s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{B}}] \times s^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{B}}]|_{X\times Y} - k^{-\frac{1}{2}+\beta} |s^{\mathsf{in}}_{\mathrm{A}}[K] \times s^{\mathsf{in}}_{\mathrm{B}}[K]|_{X\times Y} \right| \geq k^{(\frac{1}{2}+\beta)\Delta'} + 2k^{2\beta}$ may happen only with negligible probability. Finally, for almost all security parameters k we can estimate $k^{(\frac{1}{2}+\beta)\Delta'} + 2k^{2\beta} \leq k^{(\frac{1}{2}+\beta)\Delta}$, since $2\beta < (\frac{1}{2}+\beta)\Delta$ by assumption and we can choose $\Delta' < \Delta$. □

Lemma 18. *Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, f_{\mathrm{A}}, f_{\mathrm{B}}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and $\pi := \pi_F(n_{\mathrm{A}}, n_{\mathrm{B}}, \alpha, \beta, \gamma)$, such that $(n_{\mathrm{A}}, n_{\mathrm{B}}, \alpha, \beta, \gamma) \in \Pi_F$. Further let $\varepsilon, \Delta, \omega, \omega' \in \mathbb{R}_{>0}$ and let $\alpha < \omega' < (\frac{1}{2}+\beta)(1-\Delta)$ and $\omega < \min(\frac{1}{4}, 1-\Delta)$ and $\varepsilon \leq \frac{1}{2} + \beta - \omega$. Then for almost all non-aborted runs in $\Lambda_{\mathrm{A}}(\pi, \varepsilon, \Delta)$ there exists some $\nu \in \tilde{\mathfrak{N}}_F(k^{-\omega}, k^{-\omega'})$, such that for all $x \in \Upsilon_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$ it holds:*

$$\begin{aligned} k^{-\omega} &> \left| \nu(x, \Upsilon_{\mathrm{B}}, y') - \tilde{n}_{\mathrm{A}}(x) \cdot \tilde{n}_{\mathrm{B}}(y') \right| \\ k^{-\omega} &> \left| \nu(x, y, \Upsilon_{\mathrm{B}}) - k^{-1} \cdot \left| s^{\mathsf{in}}_{\mathrm{A}}[K] \times s^{\mathsf{in}}_{\mathrm{B}}[K] \right|_{(x,y)} \right| \end{aligned}$$

Proof. Let $\nu : \Upsilon_{\mathrm{A}} \times \Upsilon_{\mathrm{B}}^2 \to \mathbb{R}_{\geq 0}$, $(x, y, y') \mapsto k^{-\frac{1}{2}-\beta} \left| s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{A}}] \times s^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}] \times \hat{s}^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}] \right|_{(x,y,y')}$. First, let us check that $\nu \in \tilde{\mathfrak{N}}_F(k^{-\omega}, k^{-\omega'})$, i.e. ν fulfills the five conditions of Definition 13:

1. For all non-aborted runs in $\Lambda_{\mathrm{A}}(\pi, \varepsilon, \Delta)$ we have that $\nu(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}}) = 1$ by construction.

2. By definition (Notation 14) for all non-aborted runs in $\Lambda_{\mathrm{A}}(\pi, \varepsilon, \Delta)$ and all $x \in \Upsilon_{\mathrm{A}}$ it holds:

$$\begin{aligned} \nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}}) &= k^{-\frac{1}{2}-\beta} |s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{A}}] \times s^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}]|_{\{x\}\times\Upsilon_{\mathrm{B}}} \\ &\overset{(2)}{>} k^{-\frac{1}{2}-\beta} \left(k^{-\frac{1}{2}+\beta} |s^{\mathsf{in}}_{\mathrm{A}}[K] \times s^{\mathsf{in}}_{\mathrm{B}}[K]|_{\{x\}\times\Upsilon_{\mathrm{B}}} - k^{(\frac{1}{2}+\beta)\Delta} \right) \\ &= k^{-1} |s^{\mathsf{in}}_{\mathrm{A}}[K]|_x - k^{(\frac{1}{2}+\beta)(\Delta-1)} \\ &\overset{(1)}{>} k^{-1} \left(k \cdot \tilde{n}_{\mathrm{A}}(x) - k^{\Delta} \right) - k^{(\frac{1}{2}+\beta)(\Delta-1)} \\ &= \tilde{n}_{\mathrm{A}}(x) - k^{\Delta-1} - k^{(\frac{1}{2}+\beta)(\Delta-1)} \end{aligned}$$

   For almost all security parameters k we can estimate that from below by $k^{-\omega'}$, since we have that $\alpha < \omega' < (\frac{1}{2}+\beta)(1-\Delta) < 1-\Delta$ by assumption and $\tilde{n}_{\mathrm{A}}(x) > k^{-\alpha} |\Upsilon_{\mathrm{A}}|^{-1}$ for all $x \in \Upsilon_{\mathrm{A}}$ if only k is great enough.

3. By definition (Notation 14) for all non-aborted runs in $\Lambda_{\mathrm{A}}(\pi,\varepsilon,\Delta)$ and all $x \in \Upsilon_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$ it holds:

$$\begin{aligned}
& \big|\nu(x,y,\Upsilon_{\mathrm{B}}) - \nu(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}})\cdot\nu(\Upsilon_{\mathrm{A}},y,\Upsilon_{\mathrm{B}})\big| \\
= \;& \big|k^{-\frac{1}{2}-\beta}|s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{A}}] \times s^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}]|_{(x,y)} - k^{-1-2\beta}|s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{A}}]|_x \cdot \big|s^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}]\big|_y\big| \\
\overset{(2)}{<} \;& \big|k^{-1}|s^{\mathsf{in}}_{\mathrm{A}}[K] \times s^{\mathsf{in}}_{\mathrm{B}}[K]|_{(x,y)} - k^{-1-2\beta}|s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{A}}]|_x \cdot |s^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}]|_y\big| + k^{(\frac{1}{2}+\beta)(\Delta-1)} \\
\overset{(2)}{<} \;& \big|k^{-1}|s^{\mathsf{in}}_{\mathrm{A}}[K] \times s^{\mathsf{in}}_{\mathrm{B}}[K]|_{(x,y)} - k^{-\frac{3}{2}-\beta}|s^{\mathsf{in}}_{\mathrm{A}}[K]|_x \cdot |s^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}]|_y\big| + 2k^{(\frac{1}{2}+\beta)(\Delta-1)} \\
\overset{(2)}{<} \;& \big|k^{-1}|s^{\mathsf{in}}_{\mathrm{A}}[K] \times s^{\mathsf{in}}_{\mathrm{B}}[K]|_{(x,y)} - k^{-2}|s^{\mathsf{in}}_{\mathrm{A}}[K]|_x \cdot |s^{\mathsf{in}}_{\mathrm{B}}[K]|_y\big| + 3k^{(\frac{1}{2}+\beta)(\Delta-1)} \\
\overset{(1)}{<} \;& \big|k^{-1}|s^{\mathsf{in}}_{\mathrm{A}}[K] \times s^{\mathsf{in}}_{\mathrm{B}}[K]|_{(x,y)} - k^{-1}\cdot\tilde{n}(x)\cdot|s^{\mathsf{in}}_{\mathrm{B}}[K]|_y\big| + 3k^{(\frac{1}{2}+\beta)(\Delta-1)} + k^{\Delta-1} \\
\overset{(3)}{<} \;& 3k^{(\frac{1}{2}+\beta)(\Delta-1)} + 2k^{\Delta-1}
\end{aligned}$$

   For almost all security parameters k we can estimate that from above by $k^{-\omega}$, since $\beta < \frac{1}{2}$ by definition (Notation 11) and $\Delta < 1-\omega$ by assumption.

4. By definition (Notation 14) for all non-aborted runs in $\Lambda_{\mathrm{A}}(\pi,\varepsilon,\Delta)$ and all $x \in \Upsilon_{\mathrm{A}}$, $y' \in \Upsilon_{\mathrm{B}}$ it holds:

$$\begin{aligned}
& \big|\nu(x,\Upsilon_{\mathrm{B}},y') - \nu(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}})\cdot\nu(\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},y')\big| \\
= \;& \big|k^{-\frac{1}{2}-\beta}|s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{A}}] \times \hat{s}^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}]|_{(x,y')} - k^{-1-2\beta}|s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{A}}]|_x \cdot \big|\hat{s}^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}]\big|_{y'}\big| \\
\overset{(4)}{\leq} \;& \big|\tilde{n}_{\mathrm{A}}(x)\cdot\tilde{n}_{\mathrm{B}}(y') - k^{-1-2\beta}|s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{A}}]|_x \cdot |\hat{s}^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}]|_{y'}\big| + k^{-\frac{1}{4}} \\
\overset{(4)}{\leq} \;& \big|\tilde{n}_{\mathrm{A}}(x)\cdot\tilde{n}_{\mathrm{B}}(y') - k^{-\frac{1}{2}-\beta}\cdot\tilde{n}_{\mathrm{A}}(x)\cdot|\hat{s}^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}]|_{y'}\big| + 2k^{-\frac{1}{4}} \\
\overset{(4)}{\leq} \;& \big|\tilde{n}_{\mathrm{A}}(x)\cdot\tilde{n}_{\mathrm{B}}(y') - \tilde{n}_{\mathrm{A}}(x)\cdot\tilde{n}_{\mathrm{B}}(y')\big| + 3k^{-\frac{1}{4}}
\end{aligned}$$

   For almost all security parameters k we can estimate that from above by $k^{-\omega}$, since $\omega < \frac{1}{4}$ by assumption.

5. By definition (Notation 14) for all non-aborted runs in $\Lambda_{\mathrm{A}}(\pi,\varepsilon,\Delta)$ and all $x \in \Upsilon_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$ with $(x,y) \overset{F}{\rightsquigarrow} (x,y')$ it holds:

$$\nu(x,y,y') \quad = \quad k^{-\frac{1}{2}-\beta}\big|s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{A}}] \times s^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}] \times \hat{s}^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}]\big|_{(x,y,y')} \quad \overset{(6)}{<} \quad k^{\varepsilon-\frac{1}{2}-\beta} \quad \leq \quad k^{-\omega}$$

So for all non-aborted protocol runs in $\Lambda_{\mathrm{A}}(\pi,\varepsilon,\Delta)$ it holds that $\nu \in \tilde{\mathfrak{N}}_F(k^{-\omega}, k^{-\omega'})$. Still there are two properties of ν left to be shown:

- By definition (Notation 14) for all non-aborted runs in $\Lambda_{\mathrm{A}}(\pi,\varepsilon,\Delta)$ and all $x \in \Upsilon_{\mathrm{A}}$, $y' \in \Upsilon_{\mathrm{B}}$ it holds:

$$\begin{aligned}
\big|\nu(x,\Upsilon_{\mathrm{B}},y') - \tilde{n}_{\mathrm{A}}(x)\cdot\tilde{n}_{\mathrm{B}}(y')\big| &= \big|k^{-\frac{1}{2}-\beta}|s^{\mathsf{in}}_{\mathrm{A}}[\bar{K}_{\mathrm{A}}] \times \hat{s}^{\mathsf{in}}_{\mathrm{B}}[\bar{K}_{\mathrm{A}}]|_{(x,y')} - \tilde{n}_{\mathrm{A}}(x)\cdot\tilde{n}_{\mathrm{B}}(y')\big| \\
&\overset{(4)}{\leq} \big|\tilde{n}_{\mathrm{A}}(x)\cdot\tilde{n}_{\mathrm{B}}(y') - \tilde{n}_{\mathrm{A}}(x)\cdot\tilde{n}_{\mathrm{B}}(y')\big| + k^{-\frac{1}{4}} \\
&\leq k^{-\omega}
\end{aligned}$$

- By definition (Notation 14) for all non-aborted runs in $\Lambda_{\mathrm{A}}(\pi,\varepsilon,\Delta)$ and all $x \in \Upsilon_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$ it holds:

$$\begin{aligned} & \left|\nu(x,y,\Upsilon_{\mathrm{B}}) - k^{-1}\cdot|s_{\mathrm{A}}^{\mathsf{in}}[K]\times s_{\mathrm{B}}^{\mathsf{in}}[K]|_{(x,y)}\right| \\ = \; & \left|k^{-\frac{1}{2}-\beta}|s_{\mathrm{A}}^{\mathsf{in}}[\bar{K}_{\mathrm{A}}]\times s_{\mathrm{B}}^{\mathsf{in}}[\bar{K}_{\mathrm{A}}]|_{(x,y)} - k^{-1}\cdot|s_{\mathrm{A}}^{\mathsf{in}}[K]\times s_{\mathrm{B}}^{\mathsf{in}}[K]|_{(x,y)}\right| \\ \overset{(2)}{<} \; & \left|k^{-1}|s_{\mathrm{A}}^{\mathsf{in}}[K]\times s_{\mathrm{B}}^{\mathsf{in}}[K]|_{(x,y)} - k^{-1}\cdot|s_{\mathrm{A}}^{\mathsf{in}}[K]\times s_{\mathrm{B}}^{\mathsf{in}}[K]|_{(x,y)}\right| + k^{(\frac{1}{2}+\beta)(\Delta-1)} \end{aligned}$$

  For almost all security parameters k we can estimate that from above by $k^{-\omega}$, since $\beta < \frac{1}{2}$ by definition (Notation 11) and $\Delta < 1-\omega$ by assumption. □

4.2.2 From blurred cheating situations to non-blurred cheating situations

Now we show that every blurred cheating situation is sufficiently close to a non-blurred cheating situation, so that even a corrupted Bob's actual and prescribed input distributions in a non-aborted offline protocol will be polynomially close to the mappings $(x,y) \mapsto \eta(x,y,\Upsilon_{\mathrm{B}})$ and $(x,y') \mapsto \eta(x,\Upsilon_{\mathrm{B}},y')$ respectively with overwhelming probability, where η is a (non-blurred) cheating situation for the underlying 2-party function.

Lemma 19 (Rescalability of cheating situations)**.** *Let $F := (\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},\Omega_{\mathrm{A}},\Omega_{\mathrm{B}},f_{\mathrm{A}},f_{\mathrm{B}}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and let $\eta \in \mathfrak{N}_F$. Further let $\tau : \Upsilon_{\mathrm{A}} \to \mathbb{R}_{>0}$, such that $\sum_{x\in\Upsilon_{\mathrm{A}}}\tau(x)\cdot\eta(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}}) = 1$. Then the mapping $\tilde{\eta} : \Upsilon_{\mathrm{A}}\times\Upsilon_{\mathrm{B}}^2 \to \mathbb{R}_{\geq 0}$, $(x,y,y') \mapsto \tau(x)\cdot\eta(x,y,y')$ is a cheating situation for F.*

Proof. We just have to check the five conditions of Definition 7:

1. We have that $\tilde{\eta}(\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}}) = \sum_{x\in\Upsilon_{\mathrm{A}}}\tau(x)\cdot\eta(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}}) = 1$.
2. For all $x \in \Upsilon_{\mathrm{A}}$ we have that $\tilde{\eta}(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}}) > 0$, since $\tau(x) > 0$ and $\eta(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}}) > 0$.
3. For all $x \in \Upsilon_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$ we have that $\tilde{\eta}(x,y,\Upsilon_{\mathrm{B}}) = \tau(x)\cdot\eta(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}})\cdot\eta(\Upsilon_{\mathrm{A}},y,\Upsilon_{\mathrm{B}})$, whereby especially follows $\tilde{\eta}(\Upsilon_{\mathrm{A}},y,\Upsilon_{\mathrm{B}}) = \eta(\Upsilon_{\mathrm{A}},y,\Upsilon_{\mathrm{B}})$. Hence we can conclude:

$$\tilde{\eta}(x,y,\Upsilon_{\mathrm{B}}) \;=\; \underbrace{\tau(x)\cdot\eta(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}})}_{\tilde{\eta}(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}})}\cdot\underbrace{\eta(\Upsilon_{\mathrm{A}},y,\Upsilon_{\mathrm{B}})}_{\tilde{\eta}(\Upsilon_{\mathrm{A}},y,\Upsilon_{\mathrm{B}})} \;=\; \tilde{\eta}(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}})\cdot\tilde{\eta}(\Upsilon_{\mathrm{A}},y,\Upsilon_{\mathrm{B}})$$

4. For all $x \in \Upsilon_{\mathrm{A}}$, $y' \in \Upsilon_{\mathrm{B}}$ we have that $\tilde{\eta}(x,\Upsilon_{\mathrm{B}},y') = \tau(x)\cdot\eta(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}})\cdot\eta(\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},y')$, whereby especially follows $\tilde{\eta}(\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},y') = \eta(\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},y')$. Hence we can conclude:

$$\tilde{\eta}(x,\Upsilon_{\mathrm{B}},y') \;=\; \underbrace{\tau(x)\cdot\eta(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}})}_{\tilde{\eta}(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}})}\cdot\underbrace{\eta(\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},y')}_{\tilde{\eta}(\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},y')} \;=\; \tilde{\eta}(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}})\cdot\tilde{\eta}(\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},y')$$

5. For all $x \in \Upsilon_{\mathrm{A}}$, $y,y' \in \Upsilon_{\mathrm{B}}$ with $(x,y)_F \not\rightsquigarrow (x,y')_F$ we have that $\tilde{\eta}(x,y,y') = 0$, since $\eta(x,y,y') = 0$. □

Corollary 20 (Normalizability of cheating situations)**.** *Let $F := (\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},\Omega_{\mathrm{A}},\Omega_{\mathrm{B}},f_{\mathrm{A}},f_{\mathrm{B}}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and let $\eta \in \mathfrak{N}_F$. Then there exists a unique normalized cheating situation $\tilde{\eta} \in \mathfrak{N}_F$, such that $\eta(\Upsilon_{\mathrm{A}},y,\Upsilon_{\mathrm{B}}) = \tilde{\eta}(\Upsilon_{\mathrm{A}},y,\Upsilon_{\mathrm{B}})$ and $\eta(\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},y') = \tilde{\eta}(\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},y')$ for all $x \in \Upsilon_{\mathrm{A}}$, $y,y' \in \Upsilon_{\mathrm{B}}$.*

Proof. Let $\tilde{\eta} : \Upsilon_{\mathrm{A}} \times \Upsilon_{\mathrm{B}}^2 \to \mathbb{R}_{\geq 0}$, $(x, y, y') \mapsto \frac{\eta(x,y,y')}{|\Upsilon_{\mathrm{A}}| \cdot \eta(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}})}$. Note that $\tilde{\eta} \in \mathfrak{N}_F$ by Lemma 19 and that $\tilde{\eta}$ is normalized by construction. Moreover, by construction for all $x \in \Upsilon_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$ it holds that $\frac{\eta(x,y,y')}{\eta(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}})} = \frac{\tilde{\eta}(x,y,y')}{\tilde{\eta}(x,\Upsilon_{\mathrm{B}},\Upsilon_{\mathrm{B}})}$. Now, using the conditions 3 and 4 of Definition 7 respectively, we can conclude that $\eta(\Upsilon_{\mathrm{A}}, y, \Upsilon_{\mathrm{B}}) = \tilde{\eta}(\Upsilon_{\mathrm{A}}, y, \Upsilon_{\mathrm{B}})$ and $\eta(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, y') = \tilde{\eta}(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, y')$ for all $x \in \Upsilon_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$. □

Lemma 21. *Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, f_{\mathrm{A}}, f_{\mathrm{B}}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and let $\varepsilon, \delta \in \mathbb{R}_{>0}$, $\nu \in \tilde{\mathfrak{N}}_F(\varepsilon, \delta)$. Further let $\bar{\nu} : \Upsilon_{\mathrm{A}} \times \Upsilon_{\mathrm{B}}^2 \to \mathbb{R}_{\geq 0}$, $(x, y, y') \mapsto \frac{\nu(x,y,y')}{|\Upsilon_{\mathrm{A}}| \cdot \nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}})}$. Then it holds that $\bar{\nu} \in \tilde{\mathfrak{N}}_F(\frac{2\varepsilon}{\delta|\Upsilon_{\mathrm{A}}|}, \frac{1}{|\Upsilon_{\mathrm{A}}|})$.*

Proof. We just have to check the five conditions of Definition 13:

1. By construction it holds that $\bar{\nu}(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}}) = \sum_{x \in \Upsilon_{\mathrm{A}}} \frac{\nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}})}{|\Upsilon_{\mathrm{A}}| \cdot \nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}})} = 1$.

2. For all $x \in \Upsilon_{\mathrm{A}}$ it holds that $\bar{\nu}(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}}) = \frac{\nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}})}{|\Upsilon_{\mathrm{A}}| \cdot \nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}})} = |\Upsilon_{\mathrm{A}}|^{-1}$.

3. For all $x \in \Upsilon_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$ we have:

$$\begin{aligned} \left|\bar{\nu}(x, y, \Upsilon_{\mathrm{B}}) - \tfrac{\nu(\Upsilon_{\mathrm{A}}, y, \Upsilon_{\mathrm{B}})}{|\Upsilon_{\mathrm{A}}|}\right| &= \left|\bar{\nu}(x, y, \Upsilon_{\mathrm{B}}) - \tfrac{\nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}}) \cdot \nu(\Upsilon_{\mathrm{A}}, y, \Upsilon_{\mathrm{B}})}{|\Upsilon_{\mathrm{A}}| \cdot \nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}})}\right| \\ &< \left|\bar{\nu}(x, y, \Upsilon_{\mathrm{B}}) - \tfrac{\nu(x, y, \Upsilon_{\mathrm{B}})}{|\Upsilon_{\mathrm{A}}| \cdot \nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}})}\right| + \tfrac{\varepsilon}{|\Upsilon_{\mathrm{A}}| \cdot \nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}})} \\ &\leq \tfrac{\varepsilon}{\delta|\Upsilon_{\mathrm{A}}|} \end{aligned}$$

   Thereby especially follows $\left|\bar{\nu}(\Upsilon_{\mathrm{A}}, y, \Upsilon_{\mathrm{B}}) - \nu(\Upsilon_{\mathrm{A}}, y, \Upsilon_{\mathrm{B}})\right| < \frac{\varepsilon}{\delta}$. Hence we can conclude:

$$\begin{aligned} \left|\bar{\nu}(x, y, \Upsilon_{\mathrm{B}}) - \bar{\nu}(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}}) \cdot \bar{\nu}(\Upsilon_{\mathrm{A}}, y, \Upsilon_{\mathrm{B}})\right| &= \left|\bar{\nu}(x, y, \Upsilon_{\mathrm{B}}) - \tfrac{\bar{\nu}(\Upsilon_{\mathrm{A}}, y, \Upsilon_{\mathrm{B}})}{|\Upsilon_{\mathrm{A}}|}\right| \\ &< \left|\tfrac{\nu(\Upsilon_{\mathrm{A}}, y, \Upsilon_{\mathrm{B}})}{|\Upsilon_{\mathrm{A}}|} - \tfrac{\bar{\nu}(\Upsilon_{\mathrm{A}}, y, \Upsilon_{\mathrm{B}})}{|\Upsilon_{\mathrm{A}}|}\right| + \tfrac{\varepsilon}{\delta|\Upsilon_{\mathrm{A}}|} \\ &< \left|\tfrac{\nu(\Upsilon_{\mathrm{A}}, y, \Upsilon_{\mathrm{B}})}{|\Upsilon_{\mathrm{A}}|} - \tfrac{\nu(\Upsilon_{\mathrm{A}}, y, \Upsilon_{\mathrm{B}})}{|\Upsilon_{\mathrm{A}}|}\right| + \tfrac{2\varepsilon}{\delta|\Upsilon_{\mathrm{A}}|} \end{aligned}$$

4. For all $x \in \Upsilon_{\mathrm{A}}$, $y' \in \Upsilon_{\mathrm{B}}$ we have:

$$\begin{aligned} \left|\bar{\nu}(x, \Upsilon_{\mathrm{B}}, y') - \tfrac{\nu(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, y')}{|\Upsilon_{\mathrm{A}}|}\right| &= \left|\bar{\nu}(x, \Upsilon_{\mathrm{B}}, y') - \tfrac{\nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}}) \cdot \nu(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, y')}{|\Upsilon_{\mathrm{A}}| \cdot \nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}})}\right| \\ &< \left|\bar{\nu}(x, \Upsilon_{\mathrm{B}}, y') - \tfrac{\nu(x, \Upsilon_{\mathrm{B}}, y')}{|\Upsilon_{\mathrm{A}}| \cdot \nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}})}\right| + \tfrac{\varepsilon}{|\Upsilon_{\mathrm{A}}| \cdot \nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}})} \\ &\leq \tfrac{\varepsilon}{\delta|\Upsilon_{\mathrm{A}}|} \end{aligned}$$

   Thereby especially follows $\left|\bar{\nu}(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, y') - \nu(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, y')\right| < \frac{\varepsilon}{\delta}$. Hence we can conclude:

$$\begin{aligned} \left|\bar{\nu}(x, \Upsilon_{\mathrm{B}}, y') - \bar{\nu}(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}}) \cdot \bar{\nu}(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, y')\right| &= \left|\bar{\nu}(x, \Upsilon_{\mathrm{B}}, y') - \tfrac{\bar{\nu}(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, y')}{|\Upsilon_{\mathrm{A}}|}\right| \\ &< \left|\tfrac{\nu(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, y')}{|\Upsilon_{\mathrm{A}}|} - \tfrac{\bar{\nu}(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, y')}{|\Upsilon_{\mathrm{A}}|}\right| + \tfrac{\varepsilon}{\delta|\Upsilon_{\mathrm{A}}|} \\ &< \left|\tfrac{\nu(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, y')}{|\Upsilon_{\mathrm{A}}|} - \tfrac{\nu(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, y')}{|\Upsilon_{\mathrm{A}}|}\right| + \tfrac{2\varepsilon}{\delta|\Upsilon_{\mathrm{A}}|} \end{aligned}$$

5. For all $x \in \Upsilon_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$ with $(x, y) \overset{F}{\nrightarrow} (x, y')$ it holds that $\bar{\nu}(x, y, y') = \frac{\nu(x,y,y')}{|\Upsilon_{\mathrm{A}}| \cdot \nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}})} < \frac{\varepsilon}{\delta|\Upsilon_{\mathrm{A}}|}$, since $\nu(x, y, y') < \varepsilon$ and $\nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}}) \geq \delta$. □

Lemma 22. *Let $m, n \in \mathbb{N}$, $A \in \mathbb{R}^{m\times n}$, $u \in \mathbb{R}^m$, such that $K := \{x \in \mathbb{R}^n \mid Ax \leq u\} \neq \emptyset$ (the less-or-equal relation is componentwise). Then for every norm on $\mathbb{R}^n$ there exists some constant $C \in \mathbb{R}_{\geq 0}$, such that for all $x \in \mathbb{R}^n$ it holds that $\min_{\gamma\in K} \|x-\gamma\| \leq C \cdot \min_{\varepsilon\in\mathbb{R}^m, Ax\leq u+\varepsilon} \|\varepsilon\|$.*

Proof. Since all norms on $\mathbb{R}^n$ are equivalent, it suffices to give a proof for the L^∞-norm. However, all our arguments and estimations in this proof hold for every L^p-norm. For technical reasons we reformulate our Lemma, such that the original assertion is a direct corollary of the reformulation. Let $l, m, n \in \mathbb{N}$, $A \in \mathbb{R}^{m\times n}$, $u \in \mathbb{R}^m$, $B \in \mathbb{R}^{l\times n}$, $v \in \mathbb{R}^m$, such that for $K := \{x \in \mathbb{R}^n \mid Ax \leq u\}$ and $V := \{x \in \mathbb{R}^n \mid Bx = v\}$ it holds that $K \cap V \neq \emptyset$. We will show that there exists some $C \in \mathbb{R}_{\geq 0}$, such that for all $x \in V$ it holds that $\min_{\gamma\in K\cap V} \|x-\gamma\| \leq C \cdot \min_{\varepsilon\in\mathbb{R}^m, Ax\leq u+\varepsilon} \|\varepsilon\|$.

Our proof is by induction on $n - \mathrm{Rank}(B)$. In case of $\mathrm{Rank}(B) = n$ our assertion is trivially true. So let us consider the case $\mathrm{Rank}(B) < n$. Let $a_1^{\mathrm{T}}, \ldots, a_m^{\mathrm{T}}, b_1^{\mathrm{T}}, \ldots, b_l^{\mathrm{T}}$ denote the rows of A and B respectively. W.l.o.g. we assume that $a_1^{\mathrm{T}}, \ldots, a_m^{\mathrm{T}} \notin \mathrm{Span}(b_1^{\mathrm{T}}, \ldots, b_l^{\mathrm{T}})$; else we could delete the according rows from A (and the according coefficients from u) without changing $K \cap V$. For the same reason we may assume that for each $i \in \{1, \ldots, m\}$ there exists some $x \in K \cap V$ with $a_i^{\mathrm{T}} x = u_i$. When these assumptions yield an empty matrix A, again our assertion is trivially true.

Now, for each $i \in \{1, \ldots, m\}$ we set $\tilde{V}_i := \{x \in V \mid a_i^{\mathrm{T}} x = u_i\}$. For each $i \in \{1, \ldots, m\}$ we assumed that $a_i^{\mathrm{T}} \notin \mathrm{Span}(b_1^{\mathrm{T}}, \ldots, b_l^{\mathrm{T}})$ and $K \cap \tilde{V}_i \neq \emptyset$. So by induction hypothesis for each $i \in \{1, \ldots, m\}$ we find some $\tilde{C}_i \in \mathbb{R}_{\geq 0}$, such that for all $x \in \tilde{V}_i$ it holds:

$$\min_{\gamma\in K\cap\tilde{V}_i} \|x-\gamma\| \;\leq\; \tilde{C}_i \cdot \min_{\varepsilon\in\mathbb{R}^m, Ax\leq u+\varepsilon} \|\varepsilon\|$$

Further, for each $i \in \{1, \ldots, m\}$ we find some $\tilde{e}_i \in \mathrm{Kernel}(B)$ with $a_i^{\mathrm{T}} \tilde{e}_i = 1$, since by assumption we have that $a_i^{\mathrm{T}} \notin \mathrm{Span}(b_1^{\mathrm{T}}, \ldots, b_l^{\mathrm{T}})$. Let $C := \max_{i=1}^m \big(\|\tilde{e}_i\| + \tilde{C}_i \|A\tilde{e}_i\| + \tilde{C}_i\big)$.

Thereby, on the one hand for each $x \in V \setminus K$ we find some $j \in \{1, \ldots, m\}$ with $a_j^{\mathrm{T}} x > u_j$ and we can set $\tilde{x} := x - (a_j^{\mathrm{T}} x - u_j)\tilde{e}_j$. This yields that $\tilde{x} \in \tilde{V}_j$ and hence we get:

$$\begin{aligned}
\min_{\gamma\in K\cap V} \|x-\gamma\| &\leq \|x-\tilde{x}\| + \min_{\gamma\in K\cap V} \|\tilde{x}-\gamma\| \\
&\leq \|x-\tilde{x}\| + \min_{\gamma\in K\cap\tilde{V}_j} \|\tilde{x}-\gamma\| \\
&\leq \|x-\tilde{x}\| + \tilde{C}_j \cdot \min_{\varepsilon\in\mathbb{R}^m, A\tilde{x}\leq u+\varepsilon} \|\varepsilon\| \\
&\leq \|x-\tilde{x}\| + \tilde{C}_j \left(\|A(x-\tilde{x})\| + \min_{\varepsilon\in\mathbb{R}^m, Ax\leq u+\varepsilon} \|\varepsilon\|\right) \\
&= (a_j^{\mathrm{T}} x - u_j)\|\tilde{e}_j\| + \tilde{C}_j \left((a_j^{\mathrm{T}} x - u_j)\|A\tilde{e}_j\| + \min_{\varepsilon\in\mathbb{R}^m, Ax\leq u+\varepsilon} \|\varepsilon\|\right) \\
&\leq \left(\|\tilde{e}_j\| + \tilde{C}_j\|A\tilde{e}_j\| + \tilde{C}_j\right) \cdot \min_{\varepsilon\in\mathbb{R}^m, Ax\leq u+\varepsilon} \|\varepsilon\| \\
&\leq C \cdot \min_{\varepsilon\in\mathbb{R}^m, Ax\leq u+\varepsilon} \|\varepsilon\|
\end{aligned}$$

On the other hand, for all $x \in V \cap K$ it holds that $\min_{\gamma\in K\cap V} \|x-\gamma\| \leq C \cdot \min_{\varepsilon\in\mathbb{R}^m, Ax\leq u+\varepsilon} \|\varepsilon\|$, since $\min_{\gamma\in K\cap V} \|x-\gamma\| = 0$. □

Lemma 23 (Linear smoothness)**.** *Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, f_{\mathrm{A}}, f_{\mathrm{B}}) \in \mathfrak{F}_{\mathsf{fin},\mathsf{det}}$. Then there exists some constant $C \in \mathbb{R}_{\geq 0}$, such that for all $\varepsilon, \delta \in \mathbb{R}_{>0}$, $\nu \in \tilde{\mathfrak{N}}_F(\varepsilon, \delta)$ there exists a cheating situation $\eta \in \mathfrak{N}_F$ with $\max_{x\in\Upsilon_{\mathrm{A}}, y,y'\in\Upsilon_{\mathrm{B}}} \big|\nu(x,y,y') - \eta(x,y,y')\big| < \frac{C\varepsilon}{\delta}$.*

Proof. As stated in Remark 8, the set of all normalized cheating situations for F is a convex polytope in the linear space $\mathbb{R}^{\Upsilon_{\mathrm{A}}\times\Upsilon_{\mathrm{B}}^2}$. So by Lemma 22 (instantiated with the L^∞-norm) we find some constant $\bar{C} \in \mathbb{R}_{\geq 0}$, such that for all $\gamma \in \mathbb{R}_{>0}$, $\bar{\nu} \in \tilde{\mathfrak{N}}(\gamma, |\Upsilon_{\mathrm{A}}|^{-1})$ there exists a normalized cheating situation $\bar{\eta} \in \mathfrak{N}_F$ with $\big|\bar{\nu}(x,y,y') - \bar{\eta}(x,y,y')\big| < \bar{C}\gamma$ for all $x \in \Upsilon_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$.

Now let $\varepsilon, \delta \in \mathbb{R}_{>0}$, $\nu \in \tilde{\mathfrak{N}}_F(\varepsilon, \delta)$ and $\bar{\nu} : \Upsilon_{\mathrm{A}} \times \Upsilon_{\mathrm{B}}^2 \to \mathbb{R}_{\geq 0}$, $(x, y, y') \mapsto \frac{\nu(x,y,y')}{|\Upsilon_{\mathrm{A}}| \cdot \nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}})}$. By Lemma 21 it holds that $\bar{\nu} \in \tilde{\mathfrak{N}}(\frac{2\varepsilon}{\delta|\Upsilon_{\mathrm{A}}|}, \frac{1}{|\Upsilon_{\mathrm{A}}|})$. So, by our choice of $\bar{C}$ we find some normalized cheating situation $\bar{\eta} \in \mathfrak{N}_F$ with $\big|\bar{\nu}(x, y, y') - \bar{\eta}(x, y, y')\big| < \frac{2\bar{C}\varepsilon}{\delta|\Upsilon_{\mathrm{A}}|}$ for all $x \in \Upsilon_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$. Now, we define the mapping $\eta : \Upsilon_{\mathrm{A}} \times \Upsilon_{\mathrm{B}}^2 \to \mathbb{R}_{\geq 0}$, $(x, y, y') \mapsto |\Upsilon_{\mathrm{A}}| \cdot \nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}}) \cdot \bar{\eta}(x, y, y')$. Note that $\eta \in \mathfrak{N}_F$ by Lemma 19, since $\bar{\eta}$ is normalized. Furthermore, for all $x \in \Upsilon_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$ it follows:

$$\big|\nu(x, y, y') - \eta(x, y, y')\big| \;=\; |\Upsilon_{\mathrm{A}}| \cdot \nu(x, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}}) \cdot \big|\bar{\nu}(x, y, y') - \bar{\eta}(x, y, y')\big| \;<\; \tfrac{2\bar{C}\varepsilon}{\delta} \qquad \square$$

Corollary 24. *Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, f_{\mathrm{A}}, f_{\mathrm{B}}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and $\pi := \pi_F(n_{\mathrm{A}}, n_{\mathrm{B}}, \alpha, \beta, \gamma)$, such that $(n_{\mathrm{A}}, n_{\mathrm{B}}, \alpha, \beta, \gamma) \in \Pi_F$. Further let $\varepsilon, \Delta \in \mathbb{R}_{>0}$ and let $\alpha < \min\big(\frac{1}{4}, (\frac{1}{2}+\beta)(1-\Delta)\big)$ and $\varepsilon < \frac{1}{2}+\beta-\alpha$. Then there exists some constant $\gamma' \in \mathbb{R}_{>0}$, such that for almost all non-aborted runs in $\Lambda_{\mathrm{A}}(\pi, \varepsilon, \Delta)$ there exists some cheating situation $\eta \in \mathfrak{N}_F$ that for all $x \in \Upsilon_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$ fulfills the following two conditions:*

$$\begin{aligned} k^{-\gamma'} &> \Big|\eta(x, y, \Upsilon_{\mathrm{B}}) - k^{-1} \cdot \big|s_{\mathrm{A}}^{\mathsf{in}}[K] \times s_{\mathrm{B}}^{\mathsf{in}}[K]\big|_{(x,y)}\Big| \\ k^{-\gamma'} &> \big|\eta(x, \Upsilon_{\mathrm{B}}, y') - n_{\mathrm{A}}(x) \cdot n_{\mathrm{B}}(y')\big| \end{aligned}$$

Proof. We find some constants $\omega, \omega', \gamma' \in \mathbb{R}_{>0}$, such that it holds:

$$\alpha \;<\; \omega' \;<\; \omega \;<\; \min\big(\tfrac{1}{4}, (\tfrac{1}{2}+\beta)(1-\Delta), \tfrac{1}{2}+\beta-\varepsilon\big) \qquad \text{and} \qquad \gamma' \;<\; \min(\alpha, \omega-\omega')$$

Note that thereby $\omega < 1 - \Delta$, since $\beta < \frac{1}{2}$ by definition (Notation 11). Hence, by Lemma 18 for almost all non-aborted runs in $\Lambda_{\mathrm{A}}(\pi, \varepsilon, \Delta)$ there exists some $\nu \in \tilde{\mathfrak{N}}_F(k^{-\omega}, k^{-\omega'})$, such that for all $x \in \Upsilon_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$ it holds:

$$\begin{aligned} k^{-\omega} &> \Big|\nu(x, y, \Upsilon_{\mathrm{B}}) - k^{-1} \cdot \big|s_{\mathrm{A}}^{\mathsf{in}}[K] \times s_{\mathrm{B}}^{\mathsf{in}}[K]\big|_{(x,y)}\Big| \\ k^{-\omega} &> \big|\nu(x, \Upsilon_{\mathrm{B}}, y') - \tilde{n}_{\mathrm{A}}(x) \cdot \tilde{n}_{\mathrm{B}}(y')\big| \end{aligned}$$

Note that by construction (Definition 12) we can estimate $\big|n_{\mathrm{A}}(x) \cdot n_{\mathrm{B}}(y) - \tilde{n}_{\mathrm{A}}(x) \cdot \tilde{n}_{\mathrm{B}}(y)\big| \leq 2k^{-\alpha}$ for all $x \in \Upsilon_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$. Furthermore, by Lemma 23 we find some constant $C \in \mathbb{R}_{\geq 0}$, such that for all security parameters k and all blurred cheating situations $\nu \in \tilde{\mathfrak{N}}_F(k^{-\omega}, k^{-\omega'})$ there exists a cheating situation $\eta \in \mathfrak{N}_F$ with $\max_{x \in \Upsilon_{\mathrm{A}}, y, y' \in \Upsilon_{\mathrm{B}}} \big|\nu(x, y, y') - \eta(x, y, y')\big| < Ck^{\omega'-\omega}$. Hence, for almost all non-aborted runs in $\Lambda_{\mathrm{A}}(\pi, \varepsilon, \Delta)$ there exists some $\eta \in \mathfrak{N}_F$, such that for all $x \in \tilde{X}$, $y, y' \in \tilde{Y}$ it holds:

$$\begin{aligned} k^{-\omega} + Ck^{\omega'-\omega}|\Upsilon_{\mathrm{B}}| &> \Big|\eta(x, y, \Upsilon_{\mathrm{B}}) - k^{-1} \cdot \big|s_{\mathrm{A}}^{\mathsf{in}}[K] \times s_{\mathrm{B}}^{\mathsf{in}}[K]\big|_{(x,y)}\Big| \\ 2k^{-\alpha} + k^{-\omega} + Ck^{\omega'-\omega}|\Upsilon_{\mathrm{B}}| &> \big|\eta(x, \Upsilon_{\mathrm{B}}, y') - n_{\mathrm{A}}(x) \cdot n_{\mathrm{B}}(y')\big| \end{aligned}$$

For great enough security parameter k we may estimate both left sides from above by $k^{-\gamma'}$, since we did choose $\gamma' < \min(\alpha, \omega - \omega')$ right at the start of this proof. $\square$

4.3 OT-cores & robustness

In this section we restate the definition of OT-cores. Furthermore, we formally define what is meant by a *robust* OT-core and we show that every redundancy-free 2-party function actually has a robust OT-core, if only it has any OT-core at all.

Definition 25 (OT-cores)**.** Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$. A quadruple $(x, x', y, y') \in \Upsilon_\mathrm{A}^2 \times \Upsilon_\mathrm{B}^2$ is an *OT-core* of F, if the following three conditions are met:

1. We have that $f_\mathrm{A}(x, y) = f_\mathrm{A}(x, y')$.
2. We have that $f_\mathrm{B}(x, y) = f_\mathrm{B}(x', y)$.
3. We have that $f_\mathrm{A}(x', y) \neq f_\mathrm{A}(x', y')$ or $f_\mathrm{B}(x, y') \neq f_\mathrm{B}(x', y')$ (or both).

Definition 26 (Robustness)**.** Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and let $\gamma' \in \mathbb{R}$. Further let $\pi := \pi_F(n_\mathrm{A}, n_\mathrm{B}, \alpha, \beta, \gamma)$ with $(n_\mathrm{A}, n_\mathrm{B}, \alpha, \beta, \gamma) \in \Pi_F$. Then π is called γ'-*robust*, if there exist some sets Γ_A, Γ_B of protocol runs of π with:

- If Alice is honest, then a protocol run with fresh randomness for all parties lies in Γ_A with overwhelming probability and in all non-aborted runs in Γ_A for all $x \in \Upsilon_\mathrm{A}$, $y \in \Upsilon_\mathrm{B}$ it holds:
$$\left| n_\mathrm{A}(x) \cdot n_\mathrm{B}(y) - |K'|^{-1} \cdot \left| s_\mathrm{A}^{\mathsf{in}}[K'] \times s_\mathrm{B}^{\mathsf{in}}[K'] \right|_{(x,y)} \right| \quad < \quad k^{-\gamma'}$$
- If Bob is honest, then a protocol run with fresh randomness for all parties lies in Γ_B with overwhelming probability and in all non-aborted runs in Γ_B for all $x \in \Upsilon_\mathrm{A}$, $y \in \Upsilon_\mathrm{B}$ it holds:
$$\left| n_\mathrm{A}(x) \cdot n_\mathrm{B}(y) - |K'|^{-1} \cdot \left| s_\mathrm{A}^{\mathsf{in}}[K'] \times s_\mathrm{B}^{\mathsf{in}}[K'] \right|_{(x,y)} \right| \quad < \quad k^{-\gamma'}$$

For convenience we just call a protocol *robust*, if it is γ'-robust for any $\gamma' \in \mathbb{R}_{>0}$. An OT-core $(x, x', y, y') \in \Upsilon_\mathrm{A}^2 \times \Upsilon_\mathrm{B}^2$ is called *robust*, if for all probability mass functions $n_\mathrm{A} : \Upsilon_\mathrm{A} \to \mathbb{R}$ and $n_\mathrm{B} : \Upsilon_\mathrm{B} \to \mathbb{R}$ with $n_\mathrm{A}(x, x') = n_\mathrm{B}(y, y') = 1$ there exist $\alpha, \beta, \gamma \in \mathbb{R}_{>0}$, such that $\beta > \frac{1}{2}$ and the protocol $\pi_F(n_\mathrm{A}, n_\mathrm{B}, \alpha, \beta, \gamma)$ is robust.

Notation 27 (Maskable inputs). Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$. For $Y \subseteq \Upsilon_\mathrm{B}$ we set:

$$\Phi_F(Y) \quad := \quad \left\{ \hat{y} \in \Upsilon_\mathrm{B} \;\middle|\; \forall x \in \Upsilon_\mathrm{A}\, \exists y \in Y :\, (x, \hat{y}) \overset{F}{\rightsquigarrow} (x, y) \right\}$$

Given $y_1, \ldots, y_n \in \Upsilon_\mathrm{B}$, we write $\Phi_F(y_1, \ldots, y_n)$ instead of $\Phi_F(\{y_1, \ldots, y_n\})$ for convenience.

Remark 28. Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and let $Y' \subseteq \Upsilon_\mathrm{B}$. Then by the transitivity of the "$\overset{F}{\rightsquigarrow}$"-relation (q.v. Remark 5) for all $Y \subseteq \Phi_F(Y')$ it follows that $\Phi_F(Y) \subseteq \Phi_F(Y')$.

Lemma 29. *Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$, such that F is redundancy-free. Further let $(\tilde{x}, \tilde{x}', \tilde{y}, \tilde{y}') \in \Upsilon_\mathrm{A}^2 \times \Upsilon_\mathrm{B}^2$ be an OT-core of F. Then there exist some $\bar{y}, \bar{y}' \in \Upsilon_\mathrm{B}$, such that $(\tilde{x}, \tilde{x}', \bar{y}, \bar{y}')$ also is an OT-core and every cheating situation $\eta \in \mathfrak{N}_F$ with $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \{\bar{y}, \bar{y}'\}) = 1$ is harmless (q.v. Definition 7).*

Proof. We pick $\bar{y}, \bar{y}' \in \Upsilon_\mathrm{B}$, such that $(\tilde{x}, \tilde{x}', \bar{y}, \bar{y}')$ is an OT-core and the set $\Phi_F(\bar{y}, \bar{y}')$ is of minimal cardinality. Let $\eta \in \mathfrak{N}_F$ be some arbitrary cheating situation for F with $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \{\bar{y}, \bar{y}'\}) = 1$. We have to show that η is a harmless cheating situation, i.e. $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, y) = \eta(\Upsilon_\mathrm{A}, y, \Upsilon_\mathrm{B})$ for all $y \in \Upsilon_\mathrm{B}$ (cf. Definition 7).

First we define some input sets $Y, Y' \subseteq \Upsilon_\mathrm{B}$ that form a disjoint decomposition of $\Phi_F(\bar{y}, \bar{y}')$:

$$\begin{aligned} Y \;&:=\; \left\{ y \in \Phi_F(\bar{y}, \bar{y}') \;\middle|\; f_\mathrm{A}(\tilde{x}', \bar{y}) = f_\mathrm{A}(\tilde{x}', y) \;\wedge\; f_\mathrm{B}(\tilde{x}, y) = f_\mathrm{B}(\tilde{x}', y) \right\} \\ Y' \;&:=\; \left\{ y' \in \Phi_F(\bar{y}, \bar{y}') \;\middle|\; f_\mathrm{A}(\tilde{x}', \bar{y}) \neq f_\mathrm{A}(\tilde{x}', y') \;\vee\; f_\mathrm{B}(\tilde{x}, y') \neq f_\mathrm{B}(\tilde{x}', y') \right\} \end{aligned}$$

By the following eight observations we show now that η is a harmless cheating situation.

Observation 1: For all $y \in Y$, $y' \in Y'$ we have that $(\tilde{x}, \tilde{x}', y, y')$ is an OT-core.

This can be shown as follows. Firstly, we have that $f_{\mathrm{A}}(\tilde{x}, \bar{y}) = f_{\mathrm{A}}(\tilde{x}, \bar{y}')$, since $(\tilde{x}, \tilde{x}', \bar{y}, \bar{y}')$ is an OT-core (cf. condition 1 of Definition 25). Secondly, by definition (Notation 27) we have for each $y \in \Phi(\bar{y}, \bar{y}')$ that $(\tilde{x}, y) \overset{F}{\rightsquigarrow} (\tilde{x}, \bar{y})$ or $(\tilde{x}, y) \overset{F}{\rightsquigarrow} (\tilde{x}, \bar{y}')$, what in turn implies that $f_{\mathrm{A}}(\tilde{x}, y) = f_{\mathrm{A}}(\tilde{x}, \bar{y})$ or $f_{\mathrm{A}}(\tilde{x}, y) = f_{\mathrm{A}}(\tilde{x}, \bar{y}')$ (cf. condition 2 of Notation 4). Putting things together, we can conclude that $f_{\mathrm{A}}(\tilde{x}, y) = f_{\mathrm{A}}(\tilde{x}, y')$ for all $y, y' \in \Phi_F(\bar{y}, \bar{y}')$. Now, by construction of Y and Y' directly follows that $(\tilde{x}, \tilde{x}', y, y')$ is an OT-core for all $y \in Y$, $y' \in Y'$.

Observation 2: For each $(x, \hat{y}) \in \Upsilon_{\mathrm{A}} \times \Phi_F(\bar{y}, \bar{y}')$ at least one of the following assertions holds true:

$$\forall y \in Y : (x, \hat{y}) \overset{F}{\rightsquigarrow} (x, y) \qquad\qquad \forall y' \in Y' : (x, \hat{y}) \overset{F}{\rightsquigarrow} (x, y')$$

Otherwise we had some $x \in \Upsilon_{\mathrm{A}}$, $\hat{y} \in \Phi_F(\bar{y}, \bar{y}')$, $y \in Y$, $y' \in Y'$, such that $(x, \hat{y}) \overset{F}{\not\rightsquigarrow} (x, y)$ and $(x, \hat{y}) \overset{F}{\not\rightsquigarrow} (x, y')$ and thereby $\hat{y} \notin \Phi_F(y, y')$. However, by observation 1 we had that $(\tilde{x}, \tilde{x}', y, y')$ would be an OT-core and by Remark 28 and the minimality of $\Phi_F(\bar{y}, \bar{y}')$ would follow that $\Phi_F(y, y') = \Phi_F(\bar{y}, \bar{y}')$. Now, we have a contradiction, as $\hat{y} \in \Phi_F(\bar{y}, \bar{y}') \setminus \Phi_F(y, y')$.

Observation 3: For all $\hat{y} \in \Phi_F(\bar{y}, \bar{y}')$ with $\hat{y} \neq \bar{y}$ there exists some $x \in \Upsilon_{\mathrm{A}}$, such that $\eta(x, \hat{y}, \bar{y}) = \eta(x, Y', \bar{y}) = 0$.

This follows by observation 2 and F being redundancy-free. Let $\hat{y} \in \Phi_F(\bar{y}, \bar{y}')$, such that $\hat{y} \neq \bar{y}$. Since F is redundancy-free, by Remark 6 we find some $x \in \Upsilon_{\mathrm{A}}$ with $(x, \hat{y}) \overset{F}{\not\rightsquigarrow} (x, \bar{y})$, what implies two things. Firstly, by condition 5 of Definition 7 we have that $\eta(x, \hat{y}, \bar{y}) = 0$, what is one part of what we have to show. Secondly, by observation 2 it follows that $(x, \hat{y}) \overset{F}{\rightsquigarrow} (x, y')$ for all $y' \in Y'$. Now, if we could find some $y' \in Y'$ with $(x, y') \overset{F}{\rightsquigarrow} (x, \bar{y})$, by Remark 5 this would imply that $(x, \hat{y}) \overset{F}{\rightsquigarrow} (x, \bar{y})$ in direct contradiction to our choice of x. So, for all $y' \in Y'$ it must hold that $(x, y') \overset{F}{\not\rightsquigarrow} (x, \bar{y})$ and thus $\eta(x, Y', \bar{y}) = 0$.

Observation 4: It holds that $\eta(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}} \setminus \Phi_F(\bar{y}, \bar{y}'), \Upsilon_{\mathrm{B}}) = 0$.

To prove this, we just have to combine that $\eta(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \{\bar{y}, \bar{y}'\}) = 1$ by assumption, i.e. $\eta(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Upsilon_{\mathrm{B}} \setminus \{\bar{y}, \bar{y}'\}) = 0$, and that $\eta(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}} \setminus \Phi_F(\bar{y}, \bar{y}'), \{\bar{y}, \bar{y}'\}) = 0$ by construction of Φ_F (cf. Notation 27 and condition 5 of Definition 7).

Observation 5: For all $\hat{y} \in \Phi_F(\bar{y}, \bar{y}')$ with $\hat{y} \neq \bar{y}$ it holds that $\eta(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \bar{y}) \leq \eta(\Upsilon_{\mathrm{A}}, Y \setminus \{\hat{y}\}, \Upsilon_{\mathrm{B}})$.

This can be shown as follows. Let $\hat{y} \in \Phi_F(\bar{y}, \bar{y}')$, such that $\hat{y} \neq \bar{y}$. By observation 3 we find some $x \in \Upsilon_{\mathrm{A}}$, such that $\eta(x, Y' \cup \{\hat{y}\}, \bar{y}) = 0$. Further, note that $\eta(x, \Upsilon_{\mathrm{B}} \setminus \Phi_F(\bar{y}, \bar{y}'), \bar{y}) = 0$ by observation 4. Hence it holds:

$$\eta(x, \Upsilon_{\mathrm{B}}, \bar{y}) \;=\; \eta(x, \Phi_F(\bar{y}, \bar{y}'), \bar{y}) \;=\; \eta(x, Y \setminus \{\hat{y}\}, \bar{y}) \;\leq\; \eta(x, Y \setminus \{\hat{y}\}, \Upsilon_{\mathrm{B}})$$

By condition 3 and condition 4 of Definition 7 now follows the claimed inequality.

Observation 6: For all $\hat{y}' \in \Phi_F(\bar{y}, \bar{y}')$ with $\hat{y}' \neq \bar{y}'$ it holds that $\eta(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \bar{y}) \geq \eta(\Upsilon_{\mathrm{A}}, Y \cup \{\hat{y}'\}, \Upsilon_{\mathrm{B}})$.

The proof is mainly analogous to that of observation 5. Analogously to observation 3, for all $\hat{y}' \in \Phi_F(\bar{y}, \bar{y}')$ with $\hat{y}' \neq \bar{y}'$ there exists some $x \in \Upsilon_{\mathrm{A}}$, such that $\eta(x, \hat{y}', \bar{y}) = \eta(x, Y, \bar{y}) = 0$. Hence analogously to observation 5, for every $\hat{y}' \in \Phi_F(\bar{y}, \bar{y}')$ with $\hat{y}' \neq \bar{y}'$ it holds that

$\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \bar{y}') \leq \eta(\Upsilon_\mathrm{A}, Y'\backslash\{\hat{y}'\}, \Upsilon_\mathrm{B})$. Now, since $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \{\bar{y}, \bar{y}'\}) = 1$ by assumption and $\eta(\Upsilon_\mathrm{A}, \Phi_F(\bar{y}, \bar{y}'), \Upsilon_\mathrm{B}) = 1$ by observation 4, we can conclude:

$$\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \bar{y}) \;=\; 1 - \eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \bar{y}') \;\geq\; 1 - \eta(\Upsilon_\mathrm{A}, Y'\backslash\{\hat{y}'\}, \Upsilon_\mathrm{B}) \;=\; \eta(\Upsilon_\mathrm{A}, Y \cup \{\hat{y}'\}, \Upsilon_\mathrm{B})$$

Observation 7: We have that $\eta(\Upsilon_\mathrm{A}, \{\bar{y}, \bar{y}'\}, \{\bar{y}, \bar{y}'\}) = 1$.

By observation 5 and observation 6 for all $\hat{y}, \hat{y}' \in \Phi_F(\bar{y}, \bar{y}')$ with $\hat{y} \neq \bar{y}$ and $\hat{y}' \neq \bar{y}'$ it holds:

$$\eta(\Upsilon_\mathrm{A}, Y\backslash\{\hat{y}\}, \Upsilon_\mathrm{B}) \;\;\geq\;\; \eta(\Upsilon_\mathrm{A}, Y \cup \{\hat{y}'\}, \Upsilon_\mathrm{B})$$

On the one hand, we can choose $\hat{y} = \bar{y}'$, i.e. $Y\backslash\{\hat{y}\} = Y$, whereby for all $\hat{y}' \in Y'\backslash\{\bar{y}'\}$ it follows that $\eta\big(\Upsilon_\mathrm{A}, \hat{y}', \Upsilon_\mathrm{B}\big) \leq 0$. On the other hand, we can choose $\hat{y}' = \bar{y}$, i.e. $Y \cup \{\hat{y}'\} = Y$, whereby for all $\hat{y} \in Y\backslash\{\bar{y}\}$ it follows that $\eta\big(\Upsilon_\mathrm{A}, \hat{y}, \Upsilon_\mathrm{B}\big) \leq 0$. Conclusively, we have that $\eta\big(\Upsilon_\mathrm{A}, \Phi_F(\bar{y}, \bar{y}')\backslash\{\bar{y}, \bar{y}'\}, \Upsilon_\mathrm{B}\big) = 0$. Note that $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Upsilon_\mathrm{B}\backslash\{\bar{y}, \bar{y}'\}) = 0$ by assumption and that $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}\backslash\Phi_F(\bar{y}, \bar{y}'), \{\bar{y}, \bar{y}'\}) = 0$ by observation 4. Finally, we get the claimed equality, as $\eta(\Upsilon_\mathrm{A}, \{\bar{y}, \bar{y}'\}, \{\bar{y}, \bar{y}'\})$ can be written as follows:

$$1 - \eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Upsilon_\mathrm{B}\backslash\{\bar{y}, \bar{y}'\}) - \eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}\backslash\Phi_F(\bar{y}, \bar{y}'), \{\bar{y}, \bar{y}'\}) - \eta\big(\Upsilon_\mathrm{A}, \Phi_F(\bar{y}, \bar{y}')\backslash\{\bar{y}, \bar{y}'\}, \{\bar{y}, \bar{y}'\}\big)$$

Observation 8: The cheating situation η is harmless, i.e. $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, y) = \eta(\Upsilon_\mathrm{A}, y, \Upsilon_\mathrm{B})$ for all $y \in \Upsilon_\mathrm{B}$.

Otherwise, since $\eta(\Upsilon_\mathrm{A}, y, \Upsilon_\mathrm{B}) = \eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, y) = 0$ for all $y \in \Upsilon_\mathrm{B}\backslash\{\bar{y}, \bar{y}'\}$ by observation 7, it must hold that either $\eta(\Upsilon_\mathrm{A}, \bar{y}, \Upsilon_\mathrm{B}) > \eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \bar{y})$ or $\eta(\Upsilon_\mathrm{A}, \bar{y}', \Upsilon_\mathrm{B}) > \eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \bar{y}')$. We have to show that neither can be true. For symmetry reasons it suffices to show impossibility of the latter; so let us assume that $\eta(\Upsilon_\mathrm{A}, \bar{y}', \Upsilon_\mathrm{B}) > \eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \bar{y}')$. By the conditions 3 and 4 of Definition 7 we can infer that $\eta(x, \bar{y}', \Upsilon_\mathrm{B}) > \eta(x, \Upsilon_\mathrm{B}, \bar{y}')$ for all $x \in \Upsilon_\mathrm{A}$. Thereby, since $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Upsilon_\mathrm{B}\backslash\{\bar{y}, \bar{y}'\}) = \eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}\backslash\{\bar{y}, \bar{y}'\}, \Upsilon_\mathrm{B}) = 0$ by observation 7, we can conclude that $\eta(x, \bar{y}', \{\bar{y}, \bar{y}'\}) > \eta(x, \{\bar{y}, \bar{y}'\}, \bar{y}')$ for all $x \in \Upsilon_\mathrm{A}$, or equivalently that $\eta(x, \bar{y}', \bar{y}) > \eta(x, \bar{y}, \bar{y}')$. By condition 5 of Definition 7, this especially implies that $(x, \bar{y}') \overset{F}{\rightsquigarrow} (x, \bar{y})$ for all $x \in \Upsilon_\mathrm{A}$, what is a contradiction to F being redundancy-free (q.v. Remark 6).

As our only assumption to η was that $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \{\bar{y}, \bar{y}'\}) = 1$, observation 8 concludes the proof. □

Lemma 30 (Quantizability of cheating situations)**.** *Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$. Then there exists some constant $\delta_F \in \mathbb{R}_{>0}$, such that for all $\eta \in \mathfrak{N}_F$, $\gamma \in \mathbb{R}_{\geq 0}$ with $\gamma < \frac{1}{|\Upsilon_\mathrm{B}|}$ there exists some $\eta' \in \mathfrak{N}_F$ that fulfills the following two conditions:*

1. *For all $y' \in \Upsilon_\mathrm{B}$ with $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, y') \leq \gamma \cdot \delta_F$ we have that $\eta'(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, y') = 0$.*
2. *For all $x \in \Upsilon_\mathrm{A}$, $y, y' \in \Upsilon_\mathrm{B}$ we have that $\big|\eta(x, y, y') - \eta'(x, y, y')\big| \leq 2\gamma \cdot |\Upsilon_\mathrm{A} \times \Upsilon_\mathrm{B}|$.*

Proof. As stated in Remark 8, the set of all normalized cheating situations for F is the convex hull of a finte set of vertices, say $\{\dot{\eta}_1, \ldots, \dot{\eta}_n\}$. We define:

$$\delta_F := \min\big\{\dot{\eta}_i(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, y') \;\big|\; y' \in \Upsilon_\mathrm{B},\, i \in \{1, \ldots, n\}, \text{ such that } \dot{\eta}_i(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, y') > 0\big\}$$

Now let some arbitrary $\eta \in \mathfrak{N}_F$, $\gamma \in \mathbb{R}_{\geq 0}$ with $\gamma < 1$ be given and let $\tilde{\eta}$ denote the normalized version of η (cf. Corollary 20). We have to find some $\eta' \in \mathfrak{N}_F$ that fulfills the conditions 1 and 2.

Let $Y' := \{y' \in \Upsilon_B \mid 0 < \tilde{\eta}(\Upsilon_A, \Upsilon_B, y') \leq \gamma \cdot \delta_F\}$. W.l.o.g. we assume that $Y' \neq \emptyset$, as else we could just set $\eta' := \eta$. Moreover, we find some $a_1, \ldots, a_n \in \mathbb{R}_{\geq 0}$, such that $\sum_{i=1}^n a_i \cdot \dot{\eta}_i = \tilde{\eta}$ and especially $\sum_{i=1}^n a_i = 1$. We set $I := \big\{i \in \{1, \ldots, n\} \;\big|\; \dot{\eta}_i(\Upsilon_A, \Upsilon_B, Y') > 0\big\}$, whereby we get:

$$\sum_{i \in I} a_i \cdot \delta_F \;\leq\; \sum_{i \in I} a_i \cdot \dot{\eta}_i(\Upsilon_A, \Upsilon_B, Y') \;\leq\; \sum_{i=1}^{n} a_i \cdot \dot{\eta}_i(\Upsilon_A, \Upsilon_B, Y') \;=\; \tilde{\eta}(\Upsilon_A, \Upsilon_B, Y') \;\leq\; \gamma \cdot \delta_F \cdot |Y'|$$

Since $\gamma < \frac{1}{|\Upsilon_B|}$ by assumption, this especially yields that $\sum_{i \in I} a_i \leq \gamma \cdot |Y'| < 1$. So, we can set $\bar{I} := \{1, \ldots, n\} \backslash I$ and $\tilde{\eta}' := (\sum_{i \in \bar{I}} a_i)^{-1} \cdot \sum_{i \in \bar{I}} a_i \cdot \dot{\eta}_i$, whereby for all $x \in \Upsilon_A$, $y, y' \in \Upsilon_B$ we get:

$$\begin{aligned}
\big|\tilde{\eta}(x,y,y') - \tilde{\eta}'(x,y,y')\big| \;&=\; \left|\sum_{i=1}^{n} a_i \cdot \dot{\eta}_i(x,y,y') - \frac{\sum_{i \in \bar{I}} a_i \cdot \dot{\eta}_i(x,y,y')}{\sum_{i \in \bar{I}} a_i}\right| \\
&\leq\; \left|\sum_{i \in I} a_i \cdot \dot{\eta}_i(x,y,y')\right| + \left|\left(1 - \frac{1}{\sum_{i \in \bar{I}} a_i}\right) \cdot \sum_{i \in \bar{I}} a_i \cdot \dot{\eta}_i(x,y,y')\right| \\
&\leq\; \left|\sum_{i \in I} a_i\right| + \left|\left(1 - \frac{1}{\sum_{i \in \bar{I}} a_i}\right) \cdot \sum_{i \in \bar{I}} a_i\right| \;=\; 2 \sum_{i \in I} a_i \;\leq\; 2\gamma \cdot |Y'|
\end{aligned}$$

Finally, let $\eta' : \Upsilon_A \times \Upsilon_B^2 \to \mathbb{R}_{\geq 0}$, $(x,y,y') \mapsto |\Upsilon_A| \cdot \eta(x, \Upsilon_B, \Upsilon_B) \cdot \tilde{\eta}'(x,y,y')$. Since $\tilde{\eta}'$ is normalized (cf. Remark 9), by Lemma 19 follows that $\eta' \in \mathfrak{N}_F$. Now we can put things together. On the one hand, by our choice of $\tilde{\eta}$ (q.v. Corollary 20) for every $y' \in \Upsilon_B$ with $\eta(\Upsilon_A, \Upsilon_B, y') \leq \gamma \cdot \delta_F$ it holds that $y' \in Y'$ and hence $\eta'(\Upsilon_A, \Upsilon_B, y') = \tilde{\eta}'(\Upsilon_A, \Upsilon_B, y') = 0$ by construction. On the other hand, for all $x \in \Upsilon_A$, $y, y' \in \Upsilon_B$ we have:

$$\big|\eta(x,y,y') - \eta'(x,y,y')\big| \;=\; |\Upsilon_A| \cdot \underbrace{\eta(x, \Upsilon_B, \Upsilon_B)}_{\leq 1} \cdot \underbrace{\big|\tilde{\eta}(x,y,y') - \tilde{\eta}'(x,y,y')\big|}_{\leq 2\gamma \cdot |Y'|} \;\leq\; 2\gamma \cdot |\Upsilon_A \times \Upsilon_B| \qquad \square$$

Corollary 31 (Existence of robust OT-cores)**.** *Let $F := (\Upsilon_A, \Upsilon_B, \Omega_A, \Omega_B, f_A, f_B) \in \mathfrak{F}_{\mathsf{fin},\mathsf{det}}$, such that F is redundancy-free and has an OT-core. Then F also has a robust OT-core.*

Proof. Let $F' := (\Upsilon_B, \Upsilon_A, \Omega_B, \Omega_A, f_B, f_A)$. Note that $F' \in \mathfrak{F}_{\mathsf{fin},\mathsf{det}}$. Further note that any quadruple $(x,x',y,y') \in \Upsilon_A^2 \times \Upsilon_B^2$ is an OT-core of F, iff (y,y',x,x') is an OT-core of F'. By assumption we find some $\tilde{x}, \tilde{x}' \in \Upsilon_A$, $\tilde{y}, \tilde{y}' \in \Upsilon_B$, such that $(\tilde{x}, \tilde{x}', \tilde{y}, \tilde{y}')$ is an OT-core of F. By Lemma 29 we find some $\bar{y}, \bar{y}' \in \Upsilon_B$, such that $(\tilde{x}, \tilde{x}', \bar{y}, \bar{y}')$ is an OT-core of F and every cheating situation $\eta \in \mathfrak{N}_F$ with $\eta(\Upsilon_A, \Upsilon_B, \{\bar{y}, \bar{y}'\}) = 1$ is harmless. Again by Lemma 29 we find some $\bar{x}, \bar{x}' \in \Upsilon_A$, such that $(\bar{y}, \bar{y}', \bar{x}, \bar{x}')$ is an OT-core of F' and every cheating situation $\eta \in \mathfrak{N}_{F'}$ with $\eta(\Upsilon_B, \Upsilon_A, \{\bar{x}, \bar{x}'\}) = 1$ is harmless.

Now, let $(n_A, n_B, \alpha, \beta, \gamma) \in \Pi_F$, such that $n_A(\Upsilon_A \backslash \{\bar{x}, \bar{x}'\}) = n_B(\Upsilon_B \backslash \{\bar{y}, \bar{y}'\}) = 0$ and $\alpha < \frac{1}{4}$. Further let $\varepsilon, \Delta \in \mathbb{R}_{>0}$, such that $\varepsilon < \frac{1}{2} + \beta - \alpha$ and $\frac{1}{2} < \Delta < 1 - \frac{2\alpha}{1+2\beta}$. Let $\pi := \pi_F(n_A, n_B, \alpha, \beta, \gamma)$ and $\Gamma_A := \Lambda_A(\pi, \varepsilon, \Delta)$ and $\Gamma_B := \Lambda_B(\pi, \varepsilon, \Delta)$. By Corollary 24 we find some constant $\gamma'_A \in \mathbb{R}_{>0}$, such that for almost all non-aborted runs in Γ_A there exists some cheating situation $\eta \in \mathfrak{N}_F$ that for all $x \in \Upsilon_A$, $y, y' \in \Upsilon_B$ fulfills the following two conditions:

$$\begin{aligned}
k^{-\gamma'_A} \;&>\; \Big|\eta(x,y,\Upsilon_B) - k^{-1} \cdot \big|s_A^{\mathsf{in}}[K] \times s_B^{\mathsf{in}}[K]\big|_{(x,y)}\Big| \\
k^{-\gamma'_A} \;&>\; \big|\eta(x,\Upsilon_B,y') - n_A(x) \cdot n_B(y')\big|
\end{aligned}$$

Moreover, by Lemma 30 we find some constant $\delta_F \in \mathbb{R}_{>0}$, such that for all $\eta \in \mathfrak{N}_F$ and almost all security parameters k there exist some $\eta' \in \mathfrak{N}_F$ that fulfills the following two conditions:

- For all $y' \in \Upsilon_\mathrm{B}$ with $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, y') \leq k^{-\gamma'_\mathrm{A}}$ we have that $\eta'(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, y') = 0$.
- For all $x \in \Upsilon_\mathrm{A}$, $y, y' \in \Upsilon_\mathrm{B}$ we have that $\left|\eta(x, y, y') - \eta'(x, y, y')\right| \leq 2k^{-\gamma'_\mathrm{A}} \cdot |\Upsilon_\mathrm{A} \times \Upsilon_\mathrm{B}| \cdot \delta_F^{-1}$.

Putting things together, for almost all non-aborted runs in Γ_A there exists some cheating strategy $\eta' \in \mathfrak{N}_F$ with $\eta'(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Upsilon_\mathrm{B} \setminus \{\bar{y}, \bar{y}'\}) = 0$, i.e. $\eta'(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \{\bar{y}, \bar{y}'\}) = 1$, and that for all $x \in \Upsilon_\mathrm{A}$, $y, y' \in \Upsilon_\mathrm{B}$ fulfills the following two conditions:

$$\begin{aligned}
\big(2 \cdot |\Upsilon_\mathrm{A} \times \Upsilon_\mathrm{B}^2| \cdot \delta_F^{-1} + 1\big) k^{-\gamma'_\mathrm{A}} &> \left|\eta'(x, y, \Upsilon_\mathrm{B}) - k^{-1} \cdot \left|s_\mathrm{A}^{\mathsf{in}}[K] \times s_\mathrm{B}^{\mathsf{in}}[K]\right|_{(x,y)}\right| \\
\big(2 \cdot |\Upsilon_\mathrm{A} \times \Upsilon_\mathrm{B}^2| \cdot \delta_F^{-1} + 1\big) k^{-\gamma'_\mathrm{A}} &> \left|\eta'(x, \Upsilon_\mathrm{B}, y') - n_\mathrm{A}(x) \cdot n_\mathrm{B}(y')\right|
\end{aligned}$$

Since by our choice of $\bar{y}, \bar{y}'$ every cheating situation $\eta \in \mathfrak{N}_F$ with $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \{\bar{y}, \bar{y}'\}) = 1$ is harmless, i.e. $\eta(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, y) = \eta(\Upsilon_\mathrm{A}, y, \Upsilon_\mathrm{B})$ for all $y \in \Upsilon_\mathrm{B}$, we can conclude that in almost all non-aborted runs in Γ_A for all $x \in \Upsilon_\mathrm{A}$, $y \in \Upsilon_\mathrm{B}$ it holds:

$$\left|n_\mathrm{A}(x) \cdot n_\mathrm{B}(y) - |K'|^{-1} \cdot \left|s_\mathrm{A}^{\mathsf{in}}[K'] \times s_\mathrm{B}^{\mathsf{in}}[K']\right|_{(x,y)}\right| < 2k^{-\gamma'_\mathrm{A}} \cdot \big(2 \cdot |\Upsilon_\mathrm{A} \times \Upsilon_\mathrm{B}^2| \cdot \delta_F^{-1} + 1\big)$$

For symmetry reasons[6] we anologously find some constant $\gamma'_\mathrm{B} \in \mathbb{R}_{>0}$, such that in almost all non-aborted runs in Γ_B for all $x \in \Upsilon_\mathrm{A}$, $y \in \Upsilon_\mathrm{B}$ it holds:

$$\left|n_\mathrm{A}(x) \cdot n_\mathrm{B}(y) - |K'|^{-1} \cdot \left|s_\mathrm{A}^{\mathsf{in}}[K'] \times s_\mathrm{B}^{\mathsf{in}}[K']\right|_{(x,y)}\right| < 2k^{-\gamma'_\mathrm{B}} \cdot \big(2 \cdot |\Upsilon_\mathrm{A} \times \Upsilon_\mathrm{B}^2| \cdot \delta_F^{-1} + 1\big)$$

So we just can pick $\gamma' \in \mathbb{R}_{>0}$, such that $\gamma' < \min(\gamma'_\mathrm{A}, \gamma'_\mathrm{B})$. Finally, by Lemma 17 we also have:

- If Alice is honest, then a protocol run of π with fresh randomness for all parties lies in Γ_A with overwhelming probability.
- If Bob is honest, then a protocol run of π with fresh randomness for all parties lies in Γ_B with overwhelming probability.

Conclusively, we just have to remove the protocol runs from Γ_A and Γ_B that have a too small security parameter; then Γ_A and Γ_B fulfill all requirements of Definition 26. □

4.4 Building OT from appropriate 2-party functions

In this section we show how one can reduce OT to any 2-party function $F \in \mathfrak{F}_{\mathsf{fin},\mathsf{det}}$ that has a robust OT-core (cf. Definition 26). We give a detailed protocol description in Section 4.4.1. Then we show that our protocol is a universally composable implementation of $\mathcal{F}_\mathrm{OT}$. Thereto we separately show simulatability when no party is corrupted (Section 4.4.2), when the receiver Bob is corrupted (Section 4.4.3) and when the sender Alice is corrupted (Section 4.4.4). We omit an explicit proof of simulatability when both parties are corrupted, because this is trivial.

[6] Although the protocol π is not symmetric in Alice and Bob, Notation 14 and all subsequent lemmata are.

4.4.1 The reduction protocol

Let $F := (\Upsilon_A, \Upsilon_B, \Omega_A, \Omega_B, f_A, f_B) \in \mathfrak{F}_{\mathsf{fin,det}}$ and let $(\bar{x}, \bar{x}', \bar{y}, \bar{y}') \in \Upsilon_A^2 \times \Upsilon_B^2$ be a robust OT-core of F. W.l.o.g. let $f_A(\bar{x}', \bar{y}) \neq f_A(\bar{x}', \bar{y}')$; else we interchange the roles of Alice and Bob. Let $\alpha, \beta, \gamma, \gamma', \gamma'', \Delta \in \mathbb{R}_{>0}$, such that $\beta > \frac{1}{2}$ and $\gamma' > \gamma''$ and $1 - \gamma'' > \Delta > \frac{1}{2}$ and we have that $\pi := \pi_F(n_A, n_B, \alpha, \beta, \gamma)$ is γ'-robust with the mappings $n_A : \Upsilon_A \to \mathbb{R}_{\geq 0}$ and $n_B : \Upsilon_B \to \mathbb{R}_{\geq 0}$ defined as follows:

$$n_A(x) = \begin{cases} \frac{1}{3} & \text{if } x = \bar{x} \\ \frac{2}{3} & \text{if } x = \bar{x}' \\ 0 & \text{else} \end{cases} \qquad n_B(y) = \begin{cases} \frac{1}{2} & \text{if } y \in \{\bar{y}, \bar{y}'\} \\ 0 & \text{else} \end{cases}$$

Let $(b_0, b_1) \in \{0,1\}^2$ denote Alice's OT-input and let $c \in \{0,1\}$ denote Bob's OT-input. Let k denote the security parameter. Our reduction protocol proceeds as follows:

1. Alice and Bob execute the offline-protocol π; let s_A and s_B denote their output strings.
2. Alice announces $\tilde{K} := \big\{ i \in \{1, \ldots, |s_A|\} \;\big|\; s_A[i] = \big(\bar{x}', f_A(\bar{x}', \bar{y}')\big) \big\}$. The protocol is aborted, if $|\tilde{K}| \leq \frac{1}{3}|s_A \times s_B| - k^{1-\gamma'}$ or Bob finds some index $i \in \tilde{K}$, such that $s_B[i] \neq \big(\bar{y}', f_B(\bar{x}', \bar{y}')\big)$; else all elements indexed by $\tilde{K}$ are deleted from s_A and s_B.
3. Alice and Bob locally rename the elements of s_A and s_B respectively by:

$$s_A[i] \;\leftarrow\; \begin{cases} 0 & \text{if } s_A[i] = \big(\bar{x}, f_A(\bar{x}, \bar{y})\big), \text{ what is equivalent to } s_A[i] = \big(\bar{x}, f_A(\bar{x}, \bar{y}')\big) \\ 1 & \text{if } s_A[i] = \big(\bar{x}', f_A(\bar{x}', \bar{y})\big) \\ \top & \text{else} \end{cases}$$

$$s_B[i] \;\leftarrow\; \begin{cases} 0 & \text{if } s_B[i] = \big(\bar{y}, f_B(\bar{x}, \bar{y})\big), \text{ what is equivalent to } s_B[i] = \big(\bar{y}, f_B(\bar{x}', \bar{y})\big) \\ 1 & \text{if } s_B[i] = \big(\bar{y}', f_A(\bar{x}, \bar{y}')\big) \\ \top & \text{else} \end{cases}$$

   If afterwards $|s_A|_\top \neq 0$ or $|s_B|_\top \neq 0$, the corresponding party aborts the protocol.
4. Alice deletes $\big||s_A|_0 - |s_A|_1\big|$ elements from s_A, such that afterwards $|s_A|_0 = |s_A|_1$. She announces the corresponding indices to Bob, who deletes the according elements from s_B, too. If afterwards the length of s_A and s_B is not an even number or Alice announced more than k^Δ indices, the protocol is aborted.
5. Alice randomly permutes the elements of s_A, such that afterwards for all $i \in \big\{1, \ldots, \frac{|s_A|}{2}\big\}$ it holds that $s_A[2i-1] \neq s_A[2i]$. She announces the permutation to Bob, who permutes s_B the same way. Bob aborts the protocol, if afterwards he finds some $i \in \big\{1, \ldots, \frac{|s_B|}{2}\big\}$ with $s_B[2i-1] = s_B[2i] = 1$.
6. From s_A and s_B Alice and Bob locally generate new strings $\tilde{s}_A \in \{0,1\}^{\frac{|s_A|}{2}}$ and $\tilde{s}_B \in \{0,1,\perp\}^{\frac{|s_B|}{2}}$ respectively, such that for all $i \in \{1, \ldots, |\tilde{s}_A|\}$ it holds:

$$\begin{aligned}
s_A[2i-1]{=}0 \;\wedge\; s_A[2i]{=}1 \;&\Rightarrow\; \tilde{s}_A[i]{=}0 \\
s_A[2i-1]{=}1 \;\wedge\; s_A[2i]{=}0 \;&\Rightarrow\; \tilde{s}_A[i]{=}1 \\
s_B[2i-1]{=}0 \;\wedge\; s_B[2i]{=}0 \;&\Rightarrow\; \tilde{s}_B[i]{=}\perp \\
s_B[2i-1]{=}1 \;\wedge\; s_B[2i]{=}0 \;&\Rightarrow\; \tilde{s}_B[i]{=}0 \\
s_B[2i-1]{=}0 \;\wedge\; s_B[2i]{=}1 \;&\Rightarrow\; \tilde{s}_B[i]{=}1
\end{aligned}$$

Furthermore, Alice partitions $\tilde{s}_\mathrm{A}$ into $\kappa := \lceil k^{1-\gamma''} \rceil$ consecutive substrings $\tilde{s}_\mathrm{A}^{(1)}, \ldots, \tilde{s}_\mathrm{A}^{(\kappa)}$ of equal length $l := \left\lfloor \frac{|\tilde{s}_\mathrm{A}|}{\kappa} \right\rfloor$. If $|\tilde{s}_\mathrm{A}| > \kappa \cdot l$, the remaining elements of $\tilde{s}_\mathrm{A}$ are just discarded. Bob partitions $\tilde{s}_\mathrm{B}$ analogously.

7. Alice chooses two random bit strings $\tilde{b}_0, \tilde{b}_1 \in \{0,1\}^\kappa$ with $\tilde{b}_0[j] \oplus \tilde{b}_1[j] = b_0 \oplus b_1$ for all $j \in \{1, \ldots, \kappa\}$ and $\bigoplus_{j=1}^{\kappa} \tilde{b}_0[j] = b_0$.
   Bob chooses a random bit string $\tilde{c} \in \{0,1\}^\kappa$ with $\bigoplus_{j=1}^{\kappa} \tilde{c}[j] = c$.

8. For all $j \in \{1, \ldots, \kappa\}$ the following subprotocol is executed:

   (a) Bob chooses some random sets $K_0^{(j)}, K_1^{(j)} \subseteq \{1, \ldots, l\}$ with:
   $$\begin{aligned} \left|K_0^{(j)}\right| \;=\; \left|K_1^{(j)}\right| &= \left\lceil \tfrac{l}{3} \right\rceil \\ K_0^{(j)} \cap K_1^{(j)} &= \emptyset \\ \forall\, i \in K_{\tilde{c}[j]}^{(j)}: \quad \tilde{s}_\mathrm{B}^{(j)}[i] &\neq \perp \end{aligned}$$
   He announces $\left(K_0^{(j)}, K_1^{(j)}\right)$ to Alice, who aborts the protocol, if one of the first two conditions is violated.

   (b) Alice computes $\hat{b}_0^{(j)} \leftarrow \tilde{b}_0[j] \oplus \bigoplus_{i \in K_0^{(j)}} \tilde{s}_\mathrm{A}^{(j)}[i]$ and $\hat{b}_1^{(j)} \leftarrow \tilde{b}_1[j] \oplus \bigoplus_{i \in K_1^{(j)}} \tilde{s}_\mathrm{A}^{(j)}[i]$ and sends $(\hat{b}_0^{(j)}, \hat{b}_1^{(j)})$ to Bob, who reconstructs $\tilde{b}_{\tilde{c}[j]}[j] = \hat{b}_{\tilde{c}[j]}^{(j)} \oplus \bigoplus_{i \in K_{\tilde{c}[j]}^{(j)}} \tilde{s}_\mathrm{B}^{(j)}[i]$.

9. Alice outputs $\perp$. Bob computes and outputs $b_c = \bigoplus_{j=1}^{\kappa} \tilde{b}_{\tilde{c}[j]}[j]$.

Notation 32. Whenever at least one party follows the reduction protocol honestly, we can keep track of the state of $s_\mathrm{A} \times s_\mathrm{B}$ during the protocol steps 1-5 as follows:

1. Let $r_1' \in \Upsilon_\mathrm{A}^*$ and $t_1' \in \Upsilon_\mathrm{B}^*$ denote the strings of input symbols that correspond to s_A and s_B respectively directly after step 1 of the reduction protocol. Although some party may be corrupted, $r_1' \in \Upsilon_\mathrm{A}^*$ and $t_1' \in \Upsilon_\mathrm{B}^*$ are well-defined by the invocations of F in the underlying offline protocol π.

2. Let r_2' and t_2' denote the strings that result from r_1' and t_1' respectively by applying the deletion announced by Alice in protocol step 2.

3. Given r_2', t_2' of equal length, we define $r_3', t_3' \in \{0, 1, \top\}^{|r_2' \times t_2'|}$ by:
   $$r_3'[i] \;:=\; \begin{cases} 0 & \text{if } r_2'[i] = \bar{x} \text{ and } f_\mathrm{A}\big(r_2'[i], t_2'[i]\big) = f_\mathrm{A}(\bar{x}, \bar{y}) = f_\mathrm{A}(\bar{x}, \bar{y}') \\ 1 & \text{if } r_2'[i] = \bar{x}' \text{ and } f_\mathrm{A}\big(r_2'[i], t_2'[i]\big) = f_\mathrm{A}(\bar{x}', \bar{y}) \\ \top & \text{else} \end{cases}$$
   $$t_3'[i] \;:=\; \begin{cases} 0 & \text{if } t_2'[i] = \bar{y} \text{ and } f_\mathrm{B}\big(r_2'[i], t_2'[i]\big) = f_\mathrm{B}(\bar{x}, \bar{y}) = f_\mathrm{B}(\bar{x}', \bar{y}) \\ 1 & \text{if } t_2'[i] = \bar{y}' \text{ and } f_\mathrm{B}\big(r_2'[i], t_2'[i]\big) = f_\mathrm{B}(\bar{x}, \bar{y}') \\ \top & \text{else} \end{cases}$$

4. Let r_4' and t_4' denote the strings that result from r_3' and t_3' respectively by applying the deletion announced by Alice in protocol step 4.

5. Let r_5' and t_5' denote the strings that result from r_4' and t_4' respectively by applying the permutation announced by Alice in protocol step 5.

4.4.2 Correctness of the protocol

It is not hard to verify, that the protocol from Section 4.4.1 does what it is supposed to do, as long as no party is corrupted. From Lemma 15 and our choice of the protocol parameters quite straightforwardly follows, that the protocol in a totally uncorrupted case is aborted only with negligible probability. It also is straightforward to see that an uncorrupted Bob does always output the correct value b_c at the end of each non-aborted protocol run with an uncorrupted Alice:

$$\bigoplus_{j=1}^{\kappa} \tilde{b}_{\tilde{c}[j]}[j] \;=\; \bigoplus_{j=1}^{\kappa} \big(\tilde{b}_0[j] \oplus (b_0 \oplus b_1)\tilde{c}[j]\big) \;=\; \bigoplus_{j=1}^{\kappa} \tilde{b}_0[j] \oplus (b_0 \oplus b_1) \bigoplus_{j=1}^{\kappa} \tilde{c}[j] \;=\; b_0 \oplus (b_0 \oplus b_1)c \;=\; b_c$$

4.4.3 Security against a corrupted receiver Bob

To prove security against a malicious Bob impersonated by some adversary $\mathcal{A}_{\mathrm{B}}$, we have to construct a simulator $\mathcal{S}$, such that the respective view of the environment $\mathcal{Z}$ in the ideal model is statistically indistinguishable from its view in the real model.

Given $\mathcal{A}_{\mathrm{B}}$, our simulator $\mathcal{S}$ works as follows. He internally simulates the real adversary $\mathcal{A}_{\mathrm{B}}$ and an honest Alice and provides them access to a simulated hybrid functionality $\mathcal{F}_{\mathrm{SFE}}^{(F)}$. The simulated Alice is given random input $(b_0, b_1) \in \{0,1\}^2$, as soon as the ideal functionality $\mathcal{F}_{\mathrm{OT}}$ sent a message $(\texttt{processing}, \texttt{Alice})$. All messages from $\mathcal{A}_{\mathrm{B}}$ to $\mathcal{Z}$ and vice versa are just forwarded by $\mathcal{S}$. When the simulated Alice enters step 8b of the simulated reduction protocol the κ-th time (i.e. $j = \kappa$), $\mathcal{S}$ revises $\tilde{b}_0[\kappa]$ and $\tilde{b}_1[\kappa]$ by the following procedure:

1. From the input and output of the simulated $\mathcal{F}_{\mathrm{SFE}}^{(F)}$ our simulator $\mathcal{S}$ for every $j \in \{1, \ldots, \kappa\}$ generates a string $\tilde{s}_{\mathrm{B}}^{(j)}$ like an honest Bob would have done. Wherever this is impossible due to dishonest behaviour of Bob/$\mathcal{A}_{\mathrm{B}}$, he uses a special symbol "$\top$".

2. The simulator choses a bit string $\tilde{c} \in \{0,1\}^\kappa$, such that $\big|\tilde{s}_{\mathrm{B}}^{(j)}[K_{\tilde{c}[j]}^{(j)}]\big|_\perp \leq \big|\tilde{s}_{\mathrm{B}}^{(j)}[K_{\neg\tilde{c}[j]}^{(j)}]\big|_\perp$ for all $j \in \{1, \ldots, \kappa\}$.

3. The simulator computes $c = \bigoplus_{j=1}^{\lceil k^\Delta \rceil} \tilde{c}[j]$. On behalf of the corrupted Bob $\mathcal{S}$ sends the bit c to the ideal functionality $\mathcal{F}_{\mathrm{OT}}$, receives $(\texttt{processing}, \texttt{Bob})$ from $\mathcal{F}_{\mathrm{OT}}$, sends $(\texttt{Delivery}, \texttt{Bob})$ to $\mathcal{F}_{\mathrm{OT}}$ and finally receives some bit b' from the ideal functionality $\mathcal{F}_{\mathrm{OT}}$.

4. Now $\mathcal{S}$ can revise $\tilde{b}_0[\kappa]$ and $\tilde{b}_1[\kappa]$ by:

$$\begin{aligned} \tilde{b}_{\tilde{c}[\kappa]}[\kappa] &\leftarrow b' \oplus \bigoplus_{j=1}^{\kappa-1} \tilde{b}_{\tilde{c}[j]}[j] \\ \tilde{b}_{\neg\tilde{c}[\kappa]}[\kappa] &\leftarrow \tilde{b}_{\tilde{c}[\kappa]}[\kappa] \oplus b_0 \oplus b_1 \end{aligned}$$

Except for this revision the simulation just follows the programs of an honest Alice and $\mathcal{A}_{\mathrm{B}}$. When the simulated Alice produces her regular output "$\perp$", the simulator sends $(\texttt{Delivery}, \texttt{Alice})$ to $\mathcal{F}_{\mathrm{OT}}$. Now, we have to see why our simulator makes the ideal model indistinguishable from the real model.

Proof. Let $(\bar{b}_0, \bar{b}_1)$ denote the ideal Alice's input from $\mathcal{Z}$ and let (b_0, b_1) be the simulated Alice's random input. By construction after the revision step of the simulation it always holds that

$\tilde{b}_1[j] \oplus \tilde{b}_0[j] = b_0 \oplus b_1$ for all $j \in \{1,\ldots,\kappa\}$ and $\bar{b}_c = \bigoplus_{j=1}^{\kappa} \tilde{b}_{\tilde{c}[j]}[j]$. Therefore, the simulation perfectly matches the ideal Alice's input, if only $b_0 \oplus b_1 = \bar{b}_0 \oplus \bar{b}_1$. Now, if for each $j \in \{1,\ldots,\kappa\}$ the environment $\mathcal{Z}$ is completely unaware about the bit value of $\tilde{b}_{\neg\tilde{c}[j]}[j]$, what is equivalent to $\left|\tilde{s}_{\mathrm{B}}^{(j)}[K^{(j)}_{\neg\tilde{c}[j]}]\right|_{\perp} > 0$, then $\mathcal{Z}$ also has no information about $b_0 \oplus b_1$. Hence, it suffices to prove that it may happen only with negligible probability that $\left|\tilde{s}_{\mathrm{B}}^{(j)}[K_0^{(j)}]\right|_{\perp} = \left|\tilde{s}_{\mathrm{B}}^{(j)}[K_1^{(j)}]\right|_{\perp} = 0$ for some $j \in \{1,\ldots,\kappa\}$. However, $\left|\tilde{s}_{\mathrm{B}}^{(j)}\right|_{\perp} \leq \frac{l}{3}$ is a necessary precondition for $\left|\tilde{s}_{\mathrm{B}}^{(j)}[K_0^{(j)}]\right|_{\perp} = \left|\tilde{s}_{\mathrm{B}}^{(j)}[K_1^{(j)}]\right|_{\perp} = 0$ by a simple counting argument.

Since the underlying offline protocol π is γ'-robust, by Definition 26 we find some set Γ_{A} of protocol runs of π, such that if Alice is honest, a protocol run of π with fresh randomness for all parties lies in Γ_{A} with overwhelming probability and in all non-aborted runs in Γ_{A} for all $x \in \{\bar{x}, \bar{x}'\}$, $y \in \{\bar{y}, \bar{y}'\}$ it holds:

$$\left| n_{\mathrm{A}}(x) \cdot n_{\mathrm{B}}(y) - |K'|^{-1} \cdot \left|s_{\mathrm{A}}^{\mathsf{in}}[K'] \times s_{\mathrm{B}}^{\mathsf{in}}[K']\right|_{(x,y)} \right| \;<\; k^{-\gamma'}$$

So, w.l.o.g. we may condition our considerations to the event that in step 1 of the simulated reduction protocol a run λ of π is produced with $\lambda \in \Gamma_{\mathrm{A}}$. Under this condition we will show now that $\min_{j\in\{1,\ldots,\kappa\}}\left|\tilde{s}_{\mathrm{B}}^{(j)}\right|_{\perp} \leq \frac{l}{3}$ may happen only with negligible probability. For symmetry reasons it suffices to consider $\tilde{s}_{\mathrm{B}}^{(1)}$, i.e. $j = 1$.

Using Notation 32, $\left|\tilde{s}_{\mathrm{B}}^{(1)}\right|_{\perp}$ can be interpreted as a hypergeometrically distributed random variable with expectation $l \cdot \left|r'_4 \times t'_4\right|_{(0,0)} \cdot \left|r'_4\right|_0^{-1}$. Hence, by Lemma 15 a non-aborted simulation with $\left|\tilde{s}_{\mathrm{B}}^{(1)}\right|_{\perp} \leq l \cdot \left|r'_4 \times t'_4\right|_{(0,0)} \cdot \left|r'_4\right|_0^{-1} - l^{\Delta}$ may happen only with negligible probability. By construction, in every non-aborted simulation it holds that $\left|r'_4 \times t'_4\right|_{(0,0)} \geq \left|r'_1 \times t'_1\right|_{(\bar{x},\bar{y})} - k^{\Delta}$ and $\left|r'_4\right|_0 \leq \left|r'_1\right|_{\bar{x}}$. Further, since we conditioned our considerations to the event that in step 1 of the simulated reduction protocol a run λ of π is produced with $\lambda \in \Gamma_{\mathrm{A}}$, for all non-aborted simulations follows:

$$\begin{aligned} \left| \tfrac{1}{6} \cdot \left|r'_1 \times t'_1\right| - \left|r'_1 \times t'_1\right|_{(\bar{x},\bar{y})} \right| &> k^{-\gamma'} \cdot \left|r'_1 \times t'_1\right| \\ \left| \tfrac{1}{3} \cdot \left|r'_1 \times t'_1\right| - \left|r'_1\right|_{\bar{x}} \right| &> 2k^{-\gamma'} \cdot \left|r'_1 \times t'_1\right| \end{aligned}$$

Hence, we can conclusively estimate:

$$\left|\tilde{s}_{\mathrm{B}}^{(1)}\right|_{\perp} \;>\; l \cdot \frac{\frac{1}{6} \cdot |r'_1 \times t'_1| - k^{-\gamma'} \cdot |r'_1 \times t'_1| - k^{\Delta}}{\frac{1}{3} \cdot |r'_1 \times t'_1| + 2k^{-\gamma'} \cdot |r'_1 \times t'_1|} - l^{\Delta} \;\geq\; l \cdot \left(\frac{\frac{1}{6} - k^{-\gamma'} - k^{\Delta} \cdot (k - k^{1-\gamma})^{-1}}{\frac{1}{3} + 2k^{-\gamma'}} - l^{\Delta-1} \right)$$

Now, we can choose some arbitrary constant $\varepsilon \in \mathbb{R}_{>0}$ and estimate the bracket term by $\frac{1/6-\varepsilon}{1/3+\varepsilon} - \varepsilon$ for alomst all security parameters k. For ε small enough, this especially yields $\left|\tilde{s}_{\mathrm{B}}^{(1)}\right|_{\perp} > \frac{l}{3}$. □

4.4.4 Security against a corrupted sender Alice

To prove security against a malicious Alice impersonated by some adversary $\mathcal{A}_{\mathrm{A}}$, we have to construct a simulator $\mathcal{S}$, such that the respective view of the environment $\mathcal{Z}$ in the ideal model is statistically indistinguishable from its view in the real model.

Given $\mathcal{A}_{\mathrm{A}}$, our simulator $\mathcal{S}$ works as follows. He internally simulates the real adversary $\mathcal{A}_{\mathrm{A}}$ and an honest Bob and provides them access to a simulated hybrid functionality $\mathcal{F}_{\mathrm{SFE}}^{(F)}$. The simulated

Bob is given random input $c \in \{0,1\}$, as soon as the ideal functionality $\mathcal{F}_{\mathrm{OT}}$ sent a message $(\texttt{processing}, \texttt{Bob})$. All messages from $\mathcal{A}_{\mathrm{A}}$ to $\mathcal{Z}$ and vice versa are just forwarded by $\mathcal{S}$. When the simulated Bob outputs some bit b_c, then by the following procedure $\mathcal{S}$ tries to compute $b_{\neg c}$:

1. From the input and output of the simulated $\mathcal{F}_{\mathrm{SFE}}^{(F)}$ our simulator $\mathcal{S}$ for every $j \in \{1,\ldots,\kappa\}$ generates a string $\tilde{s}_{\mathrm{A}}^{(j)}$ like an honest Alice would have done. Wherever this is impossible due to dishonest behaviour of Alice/$\mathcal{A}_{\mathrm{A}}$, he uses a special symbol "$\top$".

2. He chooses some $j' \in \{1,\ldots,\kappa\}$, such that $\tilde{s}_{\mathrm{A}}^{(j')}[i] \neq \top$ for all $i \in \{1,\ldots,l\}$. If this is impossible, $\mathcal{S}$ aborts the simulation and terminates.

3. He computes $b_{\neg c} = b_c \oplus \bigoplus_{i \in K_0^{(j')} \cup K_1^{(j')}} s_{\mathrm{A}}^{(j')}[i]$.

When $\mathcal{S}$ does not fail in his search for j', he finally sends (b_0, b_1) on behalf of the corrupted Alice to $\mathcal{F}_{\mathrm{OT}}$, receives $(\texttt{processing}, \texttt{Alice})$ from $\mathcal{F}_{\mathrm{OT}}$ and finally sends $(\texttt{Delivery}, \texttt{Bob})$ to $\mathcal{F}_{\mathrm{OT}}$. Again, we have to show that our simulator makes the ideal model indistinguishable from the real model.

Proof. When the simulated Bob's random input c equals the input the ideal Bob got from the environment $\mathcal{Z}$ and the simultor does not fail in his search for j', the simulation is clearly perfect. Hence, any environment $\mathcal{Z}$ might distinguish between real and ideal model better than with success rate $\frac{1}{2}$, only if it could gather some information about c. However, when $\mathcal{S}$ is successful in his search for j', then $\tilde{c}[j']$ and thereby also c are information-theoretically hidden from $\mathcal{A}_{\mathrm{A}}$ and $\mathcal{Z}$.

Since the underlying offline protocol π is γ'-robust, by Definition 26 we find some set Γ_{B} of protocol runs of π, such that if Bob is honest then a protocol run of π with fresh randomness for all parties lies in Γ_{B} with overwhelming probability and in all non-aborted runs in Γ_{B} for all $x \in \{\bar{x}, \bar{x}'\}$, $y \in \{\bar{y}, \bar{y}'\}$ it holds:

$$\left| n_{\mathrm{A}}(x) \cdot n_{\mathrm{B}}(y) - |K'|^{-1} \cdot \left| s_{\mathrm{A}}^{\mathsf{in}}[K'] \times s_{\mathrm{B}}^{\mathsf{in}}[K'] \right|_{(x,y)} \right| \quad < \quad k^{-\gamma'}$$

So, w.l.o.g. we may condition our considerations to the event that in step 1 of the simulated reduction protocol a run λ of π is produced with $\lambda \in \Gamma_{\mathrm{B}}$. Under this condition we will show now that the simulator $\mathcal{S}$ only with negligible probability fails in his search for j'.

Let $m_\top := \sum_{j=1}^{\kappa} |\tilde{s}_{\mathrm{A}}^{(j)}|_\top$. Note that our simulator $\mathcal{S}$ may fail in his search for j', only if $m_\top \geq \kappa$. Using Notation 32, let m denote the number of indices $i \in \{1,\ldots,\kappa \cdot l\}$ with $r_5'[2i-1] = r_5'[2i] = 0$. Further, let m' denote the number of indices $i \in \{1,\ldots,\kappa \cdot l\}$ with $r_5'[2i-1] = r_5'[2i] = 1$. Last but not least, let m_* denote the number of indices $i \in \{1,\ldots,\kappa \cdot l\}$ with $r_5'[2i-1] = \top$ or $r_5'[2i] = \top$. It obviously holds that $m_\top = m + m' + m_*$. So, it suffices to bound these three summands.

Estimation of m_*: By construction, for every non-aborted run of the simulated reduction protocol it holds:

$$\begin{aligned}
m_* &\leq \left|r_1'\right|_{\Upsilon_{\mathrm{A}} \setminus \{\bar{x},\bar{x}'\}} + \left|r_1' \times t_1'\right|_{(\bar{x}',\bar{y}')} - \left|r_1'[\tilde{K}] \times t_1'[\tilde{K}]\right|_{(\bar{x}',\bar{y}')} \\
&\leq \left|r_1'\right|_{\Upsilon_{\mathrm{A}} \setminus \{\bar{x},\bar{x}'\}} + \left|r_1' \times t_1'\right|_{(\bar{x}',\bar{y}')} - \left(|\tilde{K}| - \left|r_1'[\tilde{K}]\right|_{\bar{x}} - \left|r_1'\right|_{\Upsilon_{\mathrm{A}} \setminus \{\bar{x},\bar{x}'\}}\right) \\
&\leq 2\left|r_1'\right|_{\Upsilon_{\mathrm{A}} \setminus \{\bar{x},\bar{x}'\}} + \left|r_1' \times t_1'\right|_{(\bar{x}',\bar{y}')} - \left(\tfrac{1}{3}\left|r_1' \times t_1'\right| - k^{1-\gamma'} - \left|r_1'[\tilde{K}]\right|_{\bar{x}}\right)
\end{aligned}$$

Now, let $\tilde{m} := \left|r'_1[\tilde{K}]\right|_{\bar{x}}$. Since Alice/$\mathcal{A}_{\mathrm{A}}$ cannot distinguish situations where F was invoked with input $(\bar{x}, \bar{y})$ from situations with input $(\bar{x}, \bar{y}')$, we can estimate her overall probability of not being caught cheating in step 2 of the reduction protocol by $2^{-\tilde{m}}$. This holds due to the fact that for each $i \in \tilde{K}$ with $\big(r'_1[i], t'_1[i]\big) \in \big\{(\bar{x}, \bar{y}), (\bar{x}, \bar{y}')\big\}$ we could replace $s_{\mathrm{B}}[i]$ by a uniformly random symbol from $\{\bar{y}, \bar{y}'\}$ and update Bob's memory consistently without changing the distribution of protocol runs in any way. Hence, a non-aborted protocol run with $\tilde{m} \geq k^{1-\gamma'}$ may happen only with negligible probability. Thereby, we can further estimate:

$$m_* \;\leq\; 2\left|r'_1\right|_{\Upsilon_{\mathrm{A}}\setminus\{\bar{x},\bar{x}'\}} + \left|r'_1 \times t'_1\right|_{(\bar{x}',\bar{y}')} - \tfrac{1}{3}\left|r'_1 \times t'_1\right| + 2k^{1-\gamma'}$$

Furthermore, since we conditioned our considerations to the event that in step 1 of the simulated reduction protocol a run λ of π is produced with $\lambda \in \Gamma_{\mathrm{B}}$, we can conclude:

$$2\underbrace{\left|r'_1\right|_{\Upsilon_{\mathrm{A}}\setminus\{\bar{x},\bar{x}'\}}}_{<\,4k^{-\gamma'}\cdot|r'_1\times t'_1|} + \underbrace{\left|r'_1 \times t'_1\right|_{(\bar{x}',\bar{y}')} - \tfrac{1}{3}\left|r'_1 \times t'_1\right|}_{<\,k^{-\gamma'}\cdot|r'_1\times t'_1|} \;<\; 9k^{1-\gamma'}$$

Thereby we have that $m_* < 11k^{1-\gamma'}$.

Estimation of m: Since Alice/$\mathcal{A}_{\mathrm{A}}$ cannot distinguish situations where F was invoked with input $(\bar{x}, \bar{y})$ from situations with input $(\bar{x}, \bar{y}')$, we can estimate her overall probability of not being caught cheating in step 5 of the reduction protocol by $(3/4)^m$. Hence, a non-aborted protocol run with $m \geq k^{1-\gamma'}$ may happen only with negligible probability.

Estimation of m': The number of "1"-entries in $r'_5[1, \ldots, 2\kappa \cdot l]$ can be expressed as $2m'$ plus the number of "mixed pairs" $\big(r'_5[2i-1], r'_5[2i]\big) \in \big\{(0,1),(1,0)\big\}$ with $i \in \{1, \ldots, \kappa \cdot l\}$. This yields that $\left|r'_5[1, \ldots, \kappa \cdot l]\right|_1 \geq 2m' + \left|r'_5[1, \ldots, \kappa \cdot l]\right|_0 - 2m - m_*$ for every non-aborted protocol run. Hence, we can estimate:

$$\begin{aligned}
2m' \;&\leq\; \left|r'_5\right|_1 - \left|r'_5\right|_0 + \kappa - 1 + 2m + m_* \\
&=\; \left|r'_4\right|_1 - \left|r'_4\right|_0 + \kappa - 1 + 2m + m_* \\
&\leq\; \left|r'_3\right|_1 - \left|r'_3\right|_0 + k^{\Delta} + \kappa - 1 + 2m + m_* \\
&=\; \left|r'_2 \times t'_2\right|_{(\bar{x}',\bar{y})} - \left|r'_2\right|_{\bar{x}} + k^{\Delta} + \kappa - 1 + 2m + m_* \\
&=\; \left|r'_1 \times t'_1\right|_{(\bar{x}',\bar{y})} - \left|r'_1\right|_{\bar{x}} + \left|r'_1[\tilde{K}]\right|_{\bar{x}} + k^{\Delta} + \underbrace{\kappa - 1}_{<\,k^{1-\gamma''}} + \underbrace{2m + m_*}_{<\,13k^{1-\gamma'}}
\end{aligned}$$

The same way as in the estimation of m_*, we can conclude that a non-aborted protocol run with $\left|r'_1[\tilde{K}]\right|_{\bar{x}} = \tilde{m} \geq k^{1-\gamma'}$ may happen only with negligible probability. Thereby, we can further estimate:

$$2m' \;<\; \left|r'_1 \times t'_1\right|_{(\bar{x}',\bar{y})} - \left|r'_1\right|_{\bar{x}} + k^{\Delta} + 14k^{1-\gamma'} + k^{1-\gamma''}$$

Furthermore, since we conditioned our considerations to the event that in step 1 of the simulated reduction protocol a run λ of π is produced with $\lambda \in \Gamma_{\mathrm{B}}$, we can conclude:

$$\left|r'_1 \times t'_1\right|_{(\bar{x}',\bar{y})} - \left|r'_1\right|_{\bar{x}} \;<\; 3k^{-\gamma'} \cdot \left|r'_1 \times t'_1\right| \;<\; 3k^{1-\gamma'}$$

Thereby we have that $m' < (k^{\Delta} + 17k^{1-\gamma'} + k^{1-\gamma''})/2$.

Putting things together, we get that $m_\top < (k^\Delta + 41k^{1-\gamma'} + k^{1-\gamma''})/2$. Since $1-\gamma'' > \max(1-\gamma', \Delta)$ by construction of the reduction protocol, for almost all security parameters k we can estimate $m_\top < k^{1-\gamma''} \leq \kappa$. Thus, $\mathcal{S}$ fails in his search for j' only with negligible probability. □

4.5 The classification theorem

In this section we restate our Classification Theorem (and all concepts that are needed for its formulation) and prove it formally, using all the results we precedingly showed in Section 4.

Definition 33 (Consistent renamings)**.** Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and $F' := (\Upsilon'_\mathrm{A}, \Upsilon'_\mathrm{B}, \Omega'_\mathrm{A}, \Omega'_\mathrm{B}, f'_\mathrm{A}, f'_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$. Then F and F' are *consistent renamings* of each other, if there exist some injective mappings $\rho_\mathrm{A} : \Upsilon_\mathrm{A} \times \Omega_\mathrm{A} \to \Upsilon'_\mathrm{A} \times \Omega'_\mathrm{A}$ and $\rho_\mathrm{B} : \Upsilon_\mathrm{B} \times \Omega_\mathrm{B} \to \Upsilon'_\mathrm{B} \times \Omega'_\mathrm{B}$ and some bijective mappings $\sigma_\mathrm{A} : \Upsilon_\mathrm{A} \to \Upsilon'_\mathrm{A}$ and $\sigma_\mathrm{B} : \Upsilon_\mathrm{B} \to \Upsilon'_\mathrm{B}$, such that for all $x \in \Upsilon_\mathrm{A}$, $y \in \Upsilon_\mathrm{B}$ it holds:

$$\begin{aligned} \rho_\mathrm{A}\big(x, f_\mathrm{A}(x,y)\big) &= \big(\sigma_\mathrm{A}(x), f'_\mathrm{A}(\sigma_\mathrm{A}(x), \sigma_\mathrm{B}(y))\big) \\ \rho_\mathrm{B}\big(y, f_\mathrm{B}(x,y)\big) &= \big(\sigma_\mathrm{B}(y), f'_\mathrm{B}(\sigma_\mathrm{A}(x), \sigma_\mathrm{B}(y))\big) \end{aligned}$$

Remark 34. The relation given by Definition 33 is an equivalence relation.

Definition 35 (Symmetric 2-party functions)**.** Let $F' \in \mathfrak{F}_{\mathsf{fin,det}}$. If F' is a consistent renaming of some $F = (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$ with $\Omega_\mathrm{A} = \Omega_\mathrm{B}$ and $f_\mathrm{A} = f_\mathrm{B}$, then F' is called *symmetric*.

Definition 36 (Equivalent 2-party functions)**.** Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$ and $F' := (\Upsilon'_\mathrm{A}, \Upsilon'_\mathrm{B}, \Omega'_\mathrm{A}, \Omega'_\mathrm{B}, f'_\mathrm{A}, f'_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$. Then F and F' are *equivalent*, if they can be transformed into consistent renamings of each other by successive removal of redundant input symbols from Υ_A, Υ_B, Υ'_A, Υ'_B and according adjustment of $f_\mathrm{A}, f_\mathrm{B}, f'_\mathrm{A}, f'_\mathrm{B}$. Let $[F]$ denote the resulting equivalence class.

Remark 37. Let $F \in \mathfrak{F}_{\mathsf{fin,det}}$ and $\bar{F}, \bar{F}' \in [F]$, such that $\bar{F}$ and $\bar{F}'$ are redundancy-free. Then $\bar{F}$ and $\bar{F}'$ are consistent renamings of each other, i.e. the redundancy-free version of F is unique up to consistent renaming.

Lemma 38 (Symmetrization lemma)**.** *Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, f_\mathrm{A}, f_\mathrm{B}) \in \mathfrak{F}_{\mathsf{fin,det}}$, such that F does not have any OT-core. Then F is symmetric in the sense of Definition 35.*

Proof. Let $\mathcal{P}(\Upsilon_\mathrm{A})$ and $\mathcal{P}(\Upsilon_\mathrm{B})$ denote the power set of Υ_A and Υ_B respectively. Let $F' := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega', \Omega', f', f') \in \mathfrak{F}_{\mathsf{fin,det}}$, such that $\Omega' = \mathcal{P}(\Upsilon_\mathrm{B}) \times \mathcal{P}(\Upsilon_\mathrm{A})$ and for all $x \in \Upsilon_\mathrm{A}$, $y \in \Upsilon_\mathrm{B}$ it holds that $f'(x,y) = \big(f'_\mathrm{A}(x,y), f'_\mathrm{B}(x,y)\big)$ with:

$$\begin{aligned} f'_\mathrm{A}(x,y) &= \big\{y' \in \Upsilon_\mathrm{B} \,\big|\, f_\mathrm{A}(x,y') = f_\mathrm{A}(x,y)\big\} \\ f'_\mathrm{B}(x,y) &= \big\{x' \in \Upsilon_\mathrm{A} \,\big|\, f_\mathrm{B}(x',y) = f_\mathrm{B}(x,y)\big\} \end{aligned}$$

We will show now that F' is a consistent renaming of F. It suffices to prove that for all $x, x' \in \Upsilon_\mathrm{A}$, $y, y' \in \Upsilon_\mathrm{B}$ the following equivalences hold:

$$\begin{aligned} f_\mathrm{A}(x,y) = f_\mathrm{A}(x,y') &\;\Leftrightarrow\; f'(x,y) = f'(x,y') \\ f_\mathrm{B}(x,y) = f_\mathrm{B}(x',y) &\;\Leftrightarrow\; f'(x,y) = f'(x',y) \end{aligned}$$

Both equivalences can be shown analogously, so we just prove the first one. By construction it suffices to show the following implication for all $x \in \Upsilon_A$, $y, y' \in \Upsilon_B$:

$$f_A(x,y) = f_A(x,y') \quad \Rightarrow \quad f'_B(x,y) = f'_B(x,y')$$

We give a proof by contradiction, so let us assume that we find some $\tilde{x} \in \Upsilon_A$, $\tilde{y}, \tilde{y}' \in \Upsilon_B$ with $f_A(\tilde{x},\tilde{y}) = f_A(\tilde{x},\tilde{y}')$ and $f'_B(\tilde{x},\tilde{y}) \neq f'_B(\tilde{x},\tilde{y}')$, i.e. especially we find some $\tilde{x}' \in \Upsilon_A$ with:

$$\tilde{x}' \notin f'_B(\tilde{x},\tilde{y}) \quad \Leftrightarrow \quad \tilde{x}' \in f'_B(\tilde{x},\tilde{y}')$$

By construction of f'_B follows:

$$f_B(\tilde{x}',\tilde{y}) \neq f_B(\tilde{x},\tilde{y}) \quad \Leftrightarrow \quad f_B(\tilde{x}',\tilde{y}') = f_B(\tilde{x},\tilde{y}')$$

So, either $(\tilde{x},\tilde{x}',\tilde{y},\tilde{y}')$ or $(\tilde{x},\tilde{x}',\tilde{y}',\tilde{y})$ is an OT-core of F, what contradicts our choice of F. □

Theorem 39 (Classification theorem)**.** *For each $F \in \mathfrak{F}_{\mathsf{fin,det}}$ it holds:*

1. *For the $\mathcal{F}_{\mathrm{SFE}}^{(F)}$-hybrid model there exists an OT protocol that is statistically secure against passive adversaries, iff F has an OT-core.*
2. *If for the $\mathcal{F}_{\mathrm{SFE}}^{(F)}$-hybrid model there does not exist any OT protocol that is statistically secure against passive adversaries, then F is symmetric in the sense of Definition 35.*
3. *For the $\mathcal{F}_{\mathrm{SFE}}^{(F)}$-hybrid model there exists an OT protocol that is statistically secure against active adversaries, iff the redundancy-free version of F has an OT-core.*
4. *If for the $\mathcal{F}_{\mathrm{SFE}}^{(F)}$-hybrid model there does not exist any OT protocol that is statistically secure against active adversaries, then the redundancy-free version of F is symmetric in the sense of Definition 35.*

Proof. Instead of proving Theorem 39 directly, we prove the following five assertions, which as a whole imply Theorem 39. For all 2-party functions $F \in \mathfrak{F}_{\mathsf{fin,det}}$ we show:

1. When F does not have any OT-core, then F is symmetric.
2. When F is redundancy free and has an OT-core, then for the $\mathcal{F}_{\mathrm{SFE}}^{(F)}$-hybrid model there exists an OT protocol that is secure against active adversaries.
3. When F has an OT-core, then for the $\mathcal{F}_{\mathrm{SFE}}^{(F)}$-hybrid model there exists an OT protocol that is secure against passive adversaries.
4. When F does not have any OT-core, then for the $\mathcal{F}_{\mathrm{SFE}}^{(F)}$-hybrid model there does not exist any OT protocol that is secure against passive adversaries.
5. For the $\mathcal{F}_{\mathrm{SFE}}^{(F)}$-hybrid model there exists an OT protocol that is secure against active adversaries, iff the same holds for each $\mathcal{F}_{\mathrm{SFE}}^{(F')}$-hybrid model with $F' \in [F]$.

A	0	1	2	3	$\cdots$
0	0	0	0	0	$\cdots$
1	0	1	0	0	$\cdots$
2	0	0	1	0	$\cdots$
3	0	0	0	1	$\cdots$
$\vdots$	$\ddots$	$\ddots$	$\ddots$	$\ddots$	$\ddots$

B	0	1	2	3	$\cdots$
0	0	0	0	0	$\cdots$
1	0	1	1	1	$\cdots$
2	0	2	2	2	$\cdots$
3	0	3	3	3	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Figure 5: An *infinite* counterexample to our completeness criteria (Alice's inputs label the rows, Bob's inputs label the columns; Alice gets her output from the left table, Bob from the right one)

Assertion 1 just is Lemma 38. Assertion 2 follows by Corollary 31 and the protocol and security proofs in Section 4.4. Assertion 3 can be shown analogously to the second one, since with respect to passive adversaries any OT-core can be considered "robust"—in fact it suffices when in step 1 of the reduction protocol even corrupted parties follow the underlying offline protocol π honestly. Assertion 4 is proven in [Kil91], where only symmetric 2-party functions are considered and symmetric OT-cores are called "imbedded OR". Although another notion of security is used there, the arguments directly carry over. Finally, assertion 5 can be derived from the following easily verifyable facts:

- Instead of inputting a redundant input symbol into $\mathcal{F}_{\mathrm{SFE}}^{(F)}$ one can always use a corresponding dominating input symbol and will get exactly the same or strictly more information.
- Replacing F by some consistent renaming corresponds to locally relabeling the input-output tuples of $\mathcal{F}_{\mathrm{SFE}}^{(F)}$ by Alice and Bob. □

5 Conclusion & open questions

In this paper we showed that there is a wide class of primitives that have not been covered by existing completeness criteria, namely all 2-party functions that are essentially neither symmetric nor asymmetric. We solved this open problem by presenting simple but comprehensive criteria that combinatorially classify all complete deterministic 2-party functions with finite input and output alphabets. We proved constructively that our criteria are sufficient in the UC framework, which is the most restrictive common notion of security we know. Our criteria also turn out necessary even with respect to very weak notions of security. Therefore we consider them valid for virtually all reasonable security notions.

A remarkable corollary of our work is that every non-complete deterministic 2-party function with finite input and output alphabets is essentially symmetric. Thereby we extended the results of [Kus92, MPR09, KMQR09] to non-symmetric 2-party functions. The questions treated there become trivial for complete primitives and we have shown that every essentially non-symmetric 2-party function actually is complete.

However, our results are tightly bound to the case that the input alphabets are finte and of constant size. If the input alphabets are infinte or super-polynomially growing in the security parameter, there do exist counterexamples to our completeness criteria. E.g. in Figure 5 a 2-party function is depicted that has an OT-core (in the upper left corner) and is redundancy-free, but not complete. A corrupted Bob can completely go without ever inputting "0"; instead he can randomly

use any other input symbol, what may be recognized by Alice only with negligible probability. As Bob thereby always learns Alices input, there cannot be any polynomial-time reduction of OT to this primitive. We consider it an interesting open problem to find combinatorial completeness criteria for 2-party functions with (super-polynomially) growing input size.

Another interesting direction for future research would be expanding our results to 2-party functions that additionally use internal randomness. Some of our concepts, e.g. the notion of redundant input symbols and equivalent 2-party functions (cf. Section 2.2) or the concept of offline protocols and cheating situations (cf. Section 3.1.1 and Section 3.1.2), can be carried over to probabilistic 2-party functions rather straightforwardly. However, this does not hold for some crucial parts of our line of argument; e.g. apparently there is no way to generalize the "$\overset{F}{\rightsquigarrow}$"-relation (cf. Section 3.1.2) to the probabilistic case, as there inputting a redundant input symbol possibly can only be simulated by choosing randomly between *several* other input symbols. Therefore, also our method to find "robust" OT-cores (cf. Section 3.1.3) does not work for probabilistic 2-party functions in general.

References

[BMM99] Amos Beimel, Tal Malkin, and Silvio Micali. The all-or-nothing nature of two-party secure computation. In Michael J. Wiener, editor, *Advances in Cryptology, Proceedings of CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 80–97. Springer, 1999.

[Can01] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings of FOCS 2001*, pages 136–145, 2001. Revised version online available at `http://eprint.iacr.org/2000/067`.

[CCM98] Christian Cachin, Claude Crépeau, and Julien Marcil. Oblivious transfer with a memory-bounded receiver. In *Proceedings of FOCS 2001*, pages 493–502, 1998.

[CK90] Claude Crépeau and Joe Kilian. Weakening security assumptions and oblivious transfer (abstract). In Shafi Goldwasser, editor, *Advances in Cryptology, Proceedings of CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 2–7. Springer, 1990.

[CMW05] Claude Crépeau, Kirill Morozov, and Stefan Wolf. Efficient unconditional oblivious transfer from almost any noisy channel. In Carlo Blundo and Stelvio Cimato, editors, *SCN 2004*, volume 3352 of *Lecture Notes in Computer Science*, pages 47–59. Springer, 2005.

[Cré88] Claude Crépeau. Equivalence between two flavours of oblivious transfers. In Carl Pomerance, editor, *Advances in Cryptology, Proceedings of CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*, pages 350–354. Springer, 1988.

[CvdGT95] Claude Crépeau, Jeroen van de Graaf, and Alain Tapp. Committed oblivious transfer and private multi-party computation. In Don Coppersmith, editor, *Advances in Cryptology, Proceedings of CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 110–123. Springer, 1995.

[DFR+07] Ivan Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In Alfred Menezes, editor, *Advances in Cryptology, Proceedings of CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 360–378. Springer, 2007.

[DKS99] Ivan Damgård, Joe Kilian, and Louis Salvail. On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In *Advances in Cryptology, Proceedings of EUROCRYPT '99*, pages 56–73, 1999.

[GL91] Shafi Goldwasser and Leonid A. Levin. Fair computation of general functions in presence of immoral majority. In Alfred Menezes and Scott A. Vanstone, editors, *Advances in Cryptology, Proceedings of CRYPTO '90*, volume 537 of *Lecture Notes in Computer Science*, pages 77–93. Springer, 1991.

[HIKN08] Danny Harnik, Yuval Ishai, Eyal Kushilevitz, and Jesper Buus Nielsen. OT-combiners via secure computation. In Ran Canetti, editor, *Proceedings of TCC 2008*, volume 4948 of *Lecture Notes in Computer Science*, pages 393–411. Springer, 2008.

[HNRR06] Danny Harnik, Moni Naor, Omer Reingold, and Alon Rosen. Completeness in two-party secure computation: A computational view. *Journal of Cryptology*, 19(4):521–552, 2006.

[Hoe63] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, 1963.

[IPS08] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In David Wagner, editor, *Advances in Cryptology, Proceedings of CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 572–591. Springer, 2008.

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *Proceedings of STOC 1988*, pages 20–31. ACM, 1988.

[Kil91] Joe Kilian. A general completeness theorem for two-party games. In *Proceedings of STOC 1991*, pages 553–560. ACM, 1991.

[Kil00] Joe Kilian. More general completeness theorems for secure two-party computation. In *Proceedings of STOC 2000*, pages 316–324. ACM, 2000.

[KMQ08] Daniel Kraschewski and Jörn Müller-Quade. Completeness theorems with constructive proofs for symmetric, asymmetric and general 2-party-functions. Unpublished manuscript of the present work with different and more complicated proof techniques, based on the first author's diploma thesis [Kra06], 2008.

[KMQR09] Robin Künzler, Jörn Müller-Quade, and Dominik Raub. Secure computability of functions in the IT setting with dishonest majority and applications to long-term security. In Omer Reingold, editor, *Proceedings of TCC 2009*, volume 5444 of *Lecture Notes in Computer Science*, pages 238–255. Springer, 2009.

[Kra06] Daniel Kraschewski. Vollständigkeitskriterien von kryptographischen Primitiven. Diploma thesis, Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, 2006.

[Kus92] Eyal Kushilevitz. Privacy and communication complexity. *SIAM Journal on Discrete Mathematics*, 5(2):273–284, 1992.

[May95] Dominic Mayers. On the security of the quantum oblivious transfer and key distribution protocols. In Don Coppersmith, editor, *Advances in Cryptology, Proceedings of CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 124–135. Springer, 1995.

[May96] Dominic Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In Neal Koblitz, editor, *Advances in Cryptology, Proceedings of CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 343–357. Springer, 1996.

[MPR09] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. Complexity of multi-party computation problems: The case of 2-party symmetric secure function evaluation. In Omer Reingold, editor, *Proceedings of TCC 2009*, volume 5444 of *Lecture Notes in Computer Science*, pages 256–273. Springer, 2009.

[MPR10] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. A zero-one law for cryptographic complexity with respect to computational UC security. In Tal Rabin, editor, *Advances in Cryptology, Proceedings of CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 595–612. Springer, 2010.

[MPW07] Remo Meier, Bartosz Przydatek, and Jürg Wullschleger. Robuster combiners for oblivious transfer. In Salil P. Vadhan, editor, *Proceedings of TCC 2007*, volume 4392 of *Lecture Notes in Computer Science*, pages 404–418. Springer, 2007.

[Rab81] Michael O. Rabin. How to exchange secrets by oblivious transfer. Technical report, Aiken Computation Laboratory, Harvard University, 1981.

[Wul07] Jürg Wullschleger. Oblivious-transfer amplification. In Moni Naor, editor, *Advances in Cryptology, Proceedings of EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 555–572. Springer, 2007.

[Wul09] Jürg Wullschleger. Oblivious transfer from weak noisy channels. In Omer Reingold, editor, *Proceedings of TCC 2009*, volume 5444 of *Lecture Notes in Computer Science*, pages 332–349. Springer, 2009.

[WW06] Stefan Wolf and Jürg Wullschleger. Oblivious transfer is symmetric. In Serge Vaudenay, editor, *Advances in Cryptology, Proceedings of EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 222–232. Springer, 2006.