Anonymous Single-Round Server-Aided Verification

Elena Pagnin[1], Aikaterini Mitrokotsa[1], and Keisuke Tanaka[2]

[1] Chalmers University of Technology, Gothenburg, Sweden
{elenap, aikmitr}@chalmers.se
[2] Tokyo Intitute of Technology, Japan
keisuke@is.titech.ac.jp

Abstract. Server-Aided Verification (SAV) is a method that can be employed to speed up the process of verifying signatures by letting the verifier outsource part of its computation load to a third party. Achieving fast and reliable verification under the presence of an untrusted server is an attractive goal in cloud computing and internet of things scenarios.
In this paper, we describe a simple framework for SAV where the interaction between a verifier and an untrusted server happens via a single-round protocol. We propose a security model for SAV that refines existing ones and includes the new notions of SAV-*anonymity* and *extended unforgeability*. In addition, we apply our definitional framework to provide the first generic transformation from any signature scheme to a single-round SAV scheme that incorporates verifiable computation. Our compiler identifies two independent ways to achieve SAV-anonymity: *computationally*, through the privacy of the verifiable computation scheme, or *unconditionally*, through the adaptibility of the signature scheme.
Finally, we define three novel instantiations of SAV schemes obtained through our compiler. Compared to previous works, our proposals are the only ones which simultaneously achieve existential unforgeability and soundness against collusion.

Keywords. Server-Aided Verification, Digital Signatures, Anonymity, Verifiable Computation.

1 Introduction

The design of new efficient and secure signature schemes is often a challenging task, especially when the target devices on which the scheme should run have *limited resources*, as it happens in the Internet of Things (IoT). Nowadays many IoT devices can perform quite *expensive* computations. For instance, smartphones have gained significant computational power. Carrying out several expensive tasks, however, leads to undesirable consequences as, *e.g.*, draining the battery of the device [11]. We consider signed auctions as a motivating example in an IoT setting. In signed auctions, bidders sign their offers to guarantee that the amount is correct and that the offer belongs to them. The auctioneer considers a bid valid only if its signature is verified. Imagine that the auctioneer checks the validity of the bids using a resource-limited device. In this case, running the signature verification algorithm several times drastically affects the device's performance. In this setting one may wonder:

> Can an auctioneer *efficiently*, *securely* and *privately* check the authenticity of signed bids using a *resource-limited* device?

This paper addresses the above question in case the auctioneer has access to a computationally powerful, yet untrusted, server. This is indeed the setting of server-aided verification.

1.1 Previous Work

The concept of Server-Aided Verification (SAV) was introduced in the nineties in two independent works [1,18], and refined for the case of signature and authentication schemes by Girault and Lefranc [15]. The aim of SAV is to guarantee security and reliability of the outcome of a verification procedure when part of the computation is offloaded from a trusted device, called the verifier, to an untrusted one, the server. In particular, [18] allows multiple accesses to the server, while [1] enables a card or RFID tag to sign and verify an RSA signature by interacting with a server both in the signing and in the verification phase. A similar approach was used ten years later by Girault and Lefranc [15] who also stated the first formal definition of server-aided verification (SAV).

All existing security models for SAV consider existential forgery attacks [8,15,20,22,24,25], where the adversary, *i.e.*, the malicious server, tries to convince the verifier that an invalid signature is valid. Despite the fundamental theoretical contributions, [15] did not consider attack scenarios in which the malicious signer colludes with the server, *e.g.*, by getting control over the server, in order to tamper with the outcome of the server-aided verification of a signature. The so-called collusion attack was defined by Wu *et al.* in [24,25] together with two SAV schemes claimed to be collusion-resistant. Subsequent works revisited the notion of signer-server collusion [8,21,22]. The most complete and rigorous definition of collusion attack is due to Chow *et al.* [8], who also showed that the protocols in [25] are no longer collusion resistant under the new definition [7,8]. Recently, Cao *et al.* [7] rose new concerns about the artificiality and the expensive communication costs of the SAV in [24]. Wang *et al.* [22] attempted to fix some problems in the security model of [24,25]. The major contribution, however, is due to Chow *et al.* [8], who identified and mitigated the main weaknesses of all previous proposals [24,25,22].

Chow *et al.* [8] showed that the enabler of many attacks against SAV is the absence of an integrity check on the results returned by the server. Integrity however, is not the only concern when outsourcing computations. In this paper, we address for the first time privacy concerns and we introduce the notion of anonymity in the context of SAV of signatures.

1.2 Contributions

The main motivation of this work is the need for formal and realistic definitions in the area of server-aided verification. To this purpose we:

- Introduce a formalism which allows for an intuitive description of *single-round* SAV signature schemes (Section 3);

- Define a security model that includes three new security notions: SAV-*anonymity* (Section 4.3), *extended* existential unforgeability and extended *strong* unforgeability (Section 4.1);

- Describe the *first compiler* to a SAV signature scheme from any signature and a verifiable computation scheme (Section 5). Besides its simplicity, our generic composition identifies *sufficient requirements* on the underlying primitives to achieve security. In particular, we prove that under mild assumptions our compiler provides: extended (existential/strong) unforgeability (Theorem 1); soundness against collusion (Theorem 2); and SAV-anonymity when either the employed verifiable computation is private (Theorem 3) or the signature scheme is adaptive (Theorem 4).

- Apply our generic composition to obtain *new* SAV schemes for the BLS signature [3] (Section 6.1), Waters' signature Wat [23] (Section 6.2) and the *first* SAV for the CL signature by Camenisch and Lysyanskaya [5] (Section 6.3). While preserving efficiency, our proposals achieve better security than previous works (Table 1).

1.3 Paper organisation

Notations and preliminaries are presented in Section 2. Section 3 introduces our formalism for single-round SAV. Section 4 contains our security model. Section 5 presents our compiler and general results about its security. Section 6 describes three new SAV schemes and compares them with previous works. Section 7 concludes the paper.

2 Preliminaries

Throughout the paper, $x \leftarrow A(y)$ denotes the output x of an algorithm A run with input y. If X is a finite set, by $x \xleftarrow{R} X$ we mean x is sampled from the uniform distribution over the set X. The expression $cost(A)$ refers to the computational cost of running algorithm A. For any positive integer n, $[n] = \{1, \ldots, n\}$ and $\mathbb{G}_n$ is a group of order n. A function $f : \mathbb{N} \to \mathbb{R}$ is said to be *negligible* if $f(n) < 1/poly(n)$ for any polynomial $poly(\cdot)$ and any $n > n_0$, for suitable $n_0 \in \mathbb{N}$. Finally, ε denotes a negligible function (implicitly in the security parameter $\lambda \in \mathbb{N}$).

2.1 Signature schemes

Signature schemes [4,5,13] enable one to sign a message in such a way that anyone can verify the signature and be convinced that the message was created by the signer. Formally,

Definition 1 (Signature Scheme). *A signature scheme* $\Sigma = (\mathsf{SetUp}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ *consists of four, possibly randomized, polynomial time algorithms where:*

- $\mathsf{SetUp}(1^\lambda) \rightarrow \mathsf{gp}$*: on input the security parameter* $\lambda \in \mathbb{N}$*, the setup algorithm returns the global parameters* gp *of the scheme, which include a description of the message and the signature spaces* $\mathcal{M}$*,* $\mathcal{S}$*.*
- $\mathsf{KeyGen}(\mathsf{gp}) \rightarrow (\mathsf{pk}, \mathsf{sk})$*: the key generation outputs public-secret key pairs* $(\mathsf{pk}, \mathsf{sk})$*.*
- $\mathsf{Sign}(\mathsf{gp}, \mathsf{sk}, m) \rightarrow \sigma$*: on input a secret key* sk *and a message* $m \in \mathcal{M}$*, the sign algorithm outputs a signature* $\sigma \in \mathcal{S}$ *for* m*.*
- $\mathsf{Verify}(\mathsf{gp}, \mathsf{pk}, m, \sigma) \rightarrow \mathsf{b}$*: The verification algorithm is a deterministic algorithm that given a public key* pk*, a message* $m \in \mathcal{M}$ *and a signature* $\sigma \in \mathcal{S}$*, outputs* $\mathsf{b} = 1$ *for acceptance, or* $\mathsf{b} = 0$ *for rejection.*

In the sequel, we assume that the global parameters gp are input to all the algorithms (a part from SetUp), even when not explicitly stated.

Definition 2 ((In)Valid Signatures). *Let* Σ *be a signature scheme. We say that a signature* $\sigma \in \mathcal{S}$ *is valid for a message* $m \in \mathcal{M}$ *under the key* pk *if* $\mathsf{Verify}(\mathsf{gp}, \mathsf{pk}, m, \sigma) = 1$*. Otherwise, we say that* σ *is invalid.*

In this paper, we refer to (in)valid *signatures* also as (in)valid message-signature *pairs*.

2.2 Verifiable computation

Verifiable computation schemes enable a client to delegate computations to one or more untrusted servers, in such a way that one can efficiently verify the correctness of the result returned by the server [2,12]. Gennaro *et al.* [14] formalised private verification of outsourced computations as:

Definition 3 (Verifiable Computation [14]). *A verifiable computation scheme* $\Gamma = (\mathsf{KeyGen}, \mathsf{ProbGen}, \mathsf{Comp}, \mathsf{Verify})$ *consists of four possibly randomized algorithms where:*

- $\mathsf{KeyGen}(\lambda, f) \rightarrow (\mathsf{pk}, \mathsf{sk})$**:** *given the security parameter* λ *and a function* f*, the key generation algorithm produces a public key* pk*, that encodes the target function* f*, and a secret key* sk*.*
- $\mathsf{ProbGen}(\mathsf{sk}, x) \rightarrow (\omega_x, \tau_x)$**:** *given the secret key* sk *and the input data* x*, the problem generation algorithm outputs a public value* ω_x *and a private value* τ_x*.*
- $\mathsf{Comp}(\mathsf{pk}, \omega_x) \rightarrow \omega_y$**:** *given the public key* pk *and the encoded input* ω_x*, this algorithm computes* ω_y*, which is an encoding of* $y = f(x)$*.*
- $\mathsf{Verify}(\mathsf{sk}, \tau_x, \omega_y) \rightarrow y \cup \perp$**:** *given* sk*,* τ_x *and the encoded result* ω_y*, the verification algorithm returns* y *if* ω_y *is a valid encoding of* $f(x)$*, and* $\perp$ *otherwise.*

A verifiable scheme is efficient if verifying the outsourced computation requires less computational effort than computing the function f on the data x, *i.e.*, $cost(\mathsf{ProbGen}) + cost(\mathsf{Verify}) < cost(f(x))$.

In the remainder of the paper, we often drop the indexes and write $\tau_x = \tau$, $\omega_x = \omega$, $\omega_y = \rho$ and denote by y the output of $\mathsf{Verify}(\mathsf{sk}, \tau, \rho)$.

3 Single-round server-aided verification

In the context of signatures, server-aided verification is a method to improve the efficiency of a resource-limited verifier by outsourcing part of the computation load required in the signature verification to a computationally powerful server. Intuitively SAV equips a signature scheme with:

- An additional $\mathsf{SAV.VSetup}$ algorithm that sets up the server-aided verification and outputs a public component pb (given to the server) and a private one pr (held by the verifier only). [3]

[3] In [8,25] the output of $\mathsf{SAV.VSetup}$ is called **Vstring**.

- An interactive protocol AidedVerify executed between the verifier and the server that outputs: 0 if the input signature is invalid; 1 if the input signature is valid; and $\perp$ otherwise, *e.g.*, when the server returns values that do not match the expected output of the outsourced computation.

In this work, we want to reduce the communication cost of AidedVerify and restrict this to a single-round (two-message) interactive protocol. This choice enables us to describe the AidedVerify protocol as a sequence of three algorithms: SAV.ProbGen (run by the verifier), SAV.Comp (run by the server) and SAV.Verify (run by the verifier). This limitation is less restrictive than it may appear: all the instantiations of SAV signature schemes in [15,17,20,22,24,25,27] are actually single-round SAV. Moreover, our single-round framework assures minimal interactions between the verifier and the server, thus reducing the communication costs.

We define single-round server-aided verification signature schemes as:

Definition 4 (SAV). *A single-round server-aided verification signature scheme is defined by the following possible randomized algorithms:*

$\mathsf{SAV.Init}(1^\lambda) \to \mathsf{gp}$**:** *on input the security parameter $\lambda \in \mathbb{N}$, the initialisation algorithm returns the global parameters* gp *of the scheme, which are input to all the following algorithms, even when not specified.*

$\mathsf{SAV.KeyGen}() \to (\mathsf{pk}, \mathsf{sk})$**:** *the key generation algorithm outputs a secret key* sk *(used to sign messages) and the corresponding public key* pk*.*

$\mathsf{SAV.VSetup}() \to (\mathsf{pb}, \mathsf{pr})$**:** *the server-aided verification setup algorithm outputs a public verification-key* pb *and a private one* pr*.*

$\mathsf{SAV.Sign}(\mathsf{sk}, m) \to \sigma$**:** *given a secret key* sk *and a message m the sign algorithm produces a signature σ.*

$\mathsf{SAV.ProbGen}(\mathsf{pr}, \mathsf{pk}, m, \sigma) \to (\omega, \tau)$ **:** *on input the private verification key* pr*, the public key* pk*, a message m and a signature σ, this algorithm outputs a public-private data pair (ω, τ) for the server-aided verification.*

$\mathsf{SAV.Comp}(\mathsf{pb}, \omega) \to \rho$**:** *on input the public verification key* pb *and ω the outsourced-computation algorithm returns ρ.*

$\mathsf{SAV.Verify}(\mathsf{pr}, \mathsf{pk}, m, \sigma, \rho, \tau) \to \Delta$**:** *the verification algorithm takes as input the private verification-key* pr*, the public key* pk*, m, σ, ρ and τ. The output is $\Delta \in \{0, 1, \perp\}$.*

Intuitively, the output Δ of SAV.Verify has the following meanings:

- $\Delta = 1$: the pair (m, σ) is considered valid and we say that (m, σ) *verifies in the server-aided sense*;
- $\Delta = 0$: the pair (m, σ) is considered invalid and we say that (m, σ) does *not verify in the server-aided sense*;
- $\Delta = \perp$: the server-aided verification has failed, ρ is rejected (not σ), and nothing is inferred about the validity of (m, σ).

Unless stated otherwise, from now on SAV refers to a single-round server-aided signature verification scheme as in Definition 4. Definition 4 implicitly allows to delegate the computation of several inputs, as long as all inputs can be sent in a single round, as a vector ω.

Completeness and efficiency of SAV are defined as follows.

Definition 5 (SAV completeness). *A server-aided verification scheme* SAV *is said to be complete if for all $\lambda \in \mathbb{N}$, $\mathsf{gp} \leftarrow \mathsf{SAV.Init}(1^\lambda)$, for any pair of keys $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{SAV.KeyGen}()$, $(\mathsf{pb}, \mathsf{pr}) \leftarrow \mathsf{SAV.VSetup}()$ and message $m \xleftarrow{R} \mathcal{M}$; given $\sigma \leftarrow \mathsf{SAV.Sign}(\mathsf{sk}, m)$, $(\omega, \tau) \leftarrow \mathsf{SAV.ProbGen}(\mathsf{pr}, \mathsf{pk}, m, \sigma)$ and $\rho \leftarrow \mathsf{SAV.Comp}(\mathsf{pb}, \omega)$, it holds:*

$$\mathsf{Prob}\left[\mathsf{SAV.Verify}(\mathsf{pr}, \mathsf{pk}, m, \sigma, \rho, \tau) = 1\right] > 1 - \varepsilon$$

where the probability is taken over the coin tosses of SAV.Sign*,* SAV.ProbGen*.*

Definition 6 (SAV efficiency). *A server-aided verification scheme* SAV *for a signature scheme $\Sigma = (\mathsf{SetUp}_\Sigma, \mathsf{KeyGen}_\Sigma, \mathsf{Sign}_\Sigma, \mathsf{Verify}_\Sigma)$ is said to be efficient if the computational cost of the whole server-aided verification is less than the cost of running the standard signature verification, i.e.,*

$$\big(cost(\mathsf{SAV.ProbGen}) + cost(\mathsf{SAV.Verify})\big) < cost(\mathsf{Verify}_\Sigma)\ .$$

4 Security model

In server-aided verification there are two kinds of adversaries to be considered: the one that solely controls the server used for the aided-verification, and the one that additionally knows the secret key for signing (signer-server collusion). In the first case, we are mostly concerned about forgeries against the signature scheme, while in the second scenario we want to avoid some kind of repudiation [7]. Existing security models for SAV consider existential unforgeability (EUF) and soundness against collusion (SAC) [8,25]. In this section, we extend the notion of EUF to capture new realistic attack scenarios and we consider for the first time signer anonymity in server-aided verification.

In what follows, the adversary $\mathcal{A}$ is a probabilistic polynomial time algorithm. We denote by q_s (*resp.* q_v) the upper bound on the number of signature (*resp.* verification) queries in each query phase.

4.1 Unforgeability

Intuitively, a SAV signature scheme is unforgeable if a malicious server, taking part to the server-aided verification process, is not able to tamper with the output of the protocol. All the unforgeability notions presented in this section are based on the unforgeability under chosen message and verification attack (UF-ACMV) experiment:

Definition 7. *The unforgeability under chosen message and verification experiment* ($\mathbf{Exp}_{\mathcal{A}}^{\mathsf{UF\text{-}ACMV}}[\lambda]$) *goes as follows:*

Setup. *The challenger $\mathcal{C}$ runs the algorithms* SAV.Init, SAV.KeyGen *and* SAV.VSetup *to obtain the system parameters* gp, *the key pair* $(\mathsf{pk}, \mathsf{sk})$, *and the public-private verification keys* $(\mathsf{pb}, \mathsf{pr})$. *The adversary $\mathcal{A}$ is given* pk, pb, *while* sk *and* pr *are withheld from $\mathcal{A}$.*

Query Phase I. *The adversary can make a series of queries which may be of the following two kinds:*

- sign: $\mathcal{A}$ chooses a message m and sends it to $\mathcal{C}$. The challenger behaves as a signing oracle: it returns the value $\sigma \leftarrow \mathsf{SAV.Sign}(\mathsf{sk}, m)$ and stores the pair (m, σ) in an initially empty list $L \subset \mathcal{M} \times \mathcal{S}$.

- verify: $\mathcal{A}$ begins the interactive (single-round) protocol for server-aided verification by supplying a message-signature pair (m, σ) to its challenger. $\mathcal{C}$ simulates a verification oracle: it runs $\mathsf{SAV.ProbGen}(\mathsf{pr}, \mathsf{pk}, m, \sigma) \rightarrow (\omega, \tau)$, returns ω to $\mathcal{A}$, and waits for a second input. Upon receiving an answer ρ from the adversary, the challenger returns $\Delta \leftarrow \mathsf{SAV.Verify}(\mathsf{pr}, \mathsf{pk}, m, \sigma, \rho, \tau)$.

The adversary can choose its queries adaptively based on the responses to previous queries, and can interact with both oracles at the same time.

Challenge. *$\mathcal{A}$ chooses a message-signature pair (m^*, σ^*) and sends it to $\mathcal{C}$. The challenger computes $(\hat{\omega}, \hat{\tau}) \leftarrow \mathsf{SAV.ProbGen}(\mathsf{pr}, \mathsf{pk}, m^*, \sigma^*)$. The value $\hat{\tau}$ is stored and withheld from $\mathcal{A}$, while $\hat{\omega}$ is sent to the adversary.*

Query Phase II. *In the second query phase, the sign queries are as before, while the verify queries are answered using the same $\hat{\tau}$ generated in the challenge phase, i.e., $\mathcal{A}$ submits only ρ and $\mathcal{C}$ replies with $\Delta \leftarrow \mathsf{SAV.Verify}(\mathsf{pr}, \mathsf{pk}, m^*, \sigma^*, \rho, \hat{\tau})$.*

Forgery. *$\mathcal{A}$ outputs the tuple (m^*, σ^*, ρ^*). The experiment outputs 1 if (m^*, σ^*, ρ^*) is a forgery (see Definition 8), and 0 otherwise.*

Unlike unforgeability for digital signatures, in SAV the adversary can influence the outcome of the signature verification through the value ρ^*. Moreover, $\mathcal{A}$ can perform verification queries. This is a crucial requirement as the adversary cannot run SAV.Verify on its own, since pr and τ are withheld from $\mathcal{A}$. In practice, whenever the output of the server-aided verification is $\perp$ the verifier could abort and stop interacting with the malicious server. In this work, we ignore this case and follow the approach used in [8] and in verifiable computation [14] where the adversary 'keeps on querying' independently of the outcome of the verification queries.

Definition 8 (Forgery). *Consider an execution of the* UF-ACMV *experiment where (m^*, σ^*, ρ^*) is the tuple output by the adversary. We define three types of forgery:*

type-1a forgery: $(m^*, \cdot) \notin L$ *and* $1 \leftarrow \mathsf{SAV.Verify}(\mathsf{pr}, \mathsf{pk}, m^*, \sigma^*, \rho^*, \hat{\tau})$.

type-1b forgery: $(m^*, \sigma^*) \notin L$ *and* $1 \leftarrow \mathsf{SAV.Verify}(\mathsf{pr}, \mathsf{pk}, m^*, \sigma^*, \rho^*, \hat{\tau})$.

type-2 forgery $(m^*, \sigma^*) \in L$ *and* $0 \leftarrow \mathsf{SAV.Verify}(\mathsf{pr}, \mathsf{pk}, m^*, \sigma^*, \rho^*, \hat{\tau})$,

Existential unforgeability for SAV signature schemes is defined for a quite weak adversary: the second query phase is skipped and only type-1a forgeries are considered:

Definition 9 (Existential Unforgeability (EUF) [8]). *A SAV scheme is (ε, q_s, q_v)-existentially unforgeable under adaptive chosen message and verification attacks if* $\mathsf{Prob}\left[\mathbf{Exp}^{\mathsf{UF\text{-}ACMV}}_{\mathcal{A}}[\lambda] = 1\right] < \varepsilon$ *and the experiment* $\mathbf{Exp}^{\mathsf{UF\text{-}ACMV}}_{\mathcal{A}}[\lambda]$ *outputs 1 only on **type-1a forgeries**, and no query is performed in the **Query Phase II**.*

Existential unforgeability for SAV only considers adversaries that generate a signature for a *new* message and make it verify (in the server aided sense). This notion of unforgeability fails to capture some realistic attack scenarios. For instance, consider the case of signed auctions. The adversary is a bidder and wants to keep the price of the goods he is bidding on under a certain threshold. A simple way to achieve this goal is to get control over the server used for the SAV and prevent signatures of higher bids from verifying correctly. This motivates us to *extend* the notion of EUF in [8,25] to also account for malicious servers tampering with the verification outcome of honestly generated message-signature pairs:

Definition 10 (Extended Existential Unforgeability (ExEUF)). *A SAV scheme is (ε, q_s, q_v)-extended existentially unforgeable under adaptive chosen message and verification attacks if* $\varepsilon > \mathsf{Prob}\left[\mathbf{Exp}^{\mathsf{UF\text{-}ACMV}}_{\mathcal{A}}[\lambda] = 1\right]$ *and* $\mathbf{Exp}^{\mathsf{UF\text{-}ACMV}}_{\mathcal{A}}[\lambda]$ *outputs 1 on **type-1a** and **type-2 forgeries**.*

Extended existential unforgeablility deals with a stronger adversary than the one considered in EUF: in ExEUF the adversary can perform two different types of forgeries and has access to an additional query phase (after setting the challenge). Resembling the notion of the strongly unforgeable signatures [4], we introduce *extended strong* unforgeability for SAV:

Definition 11 (Extended Strong Unforgeability (ExSUF)). *A SAV scheme is (ε, q_s, q_v)-extended strong unforgeable under adaptive chosen message and verification attacks if* $\mathsf{Prob}\left[\mathbf{Exp}^{\mathsf{UF\text{-}ACMV}}_{\mathcal{A}}[\lambda] = 1\right] < \varepsilon$ *and* $\mathbf{Exp}^{\mathsf{UF\text{-}ACMV}}_{\mathcal{A}}[\lambda]$ *outputs 1 on **type-1a, type-1b** and **type-2 forgeries**.*

In ExSUF there is no restriction on the pair (m^*, σ^*) chosen by the adversary: it can be a new message (type-1a), a new signature on a previously-queried message (type-1b) or an honestly generated pair obtained in the first Query Phase (type-2).

4.2 Soundness against collusion

In collusion attacks, the adversary controls the server used for the aided verification and holds the signer's secret key. This may happen when a malicious signer hacks the server and wants to tamper with the outcome of a signature verification. As a motivating example consider signed auctions. The owner of a good could take part to the auction (as the malicious signer) and influence its price. For instance, in order to increase the cost of the good, the malicious signer can produce an invalid signature for a high bid (message) and make other bidders overpay for it. To tamper with the verification of the invalid signature, the malicious signer can use the server and make his (invalid) signature verify when the bid is stated. However, in case no one outbids him, the malicious signer can repudiate the signature as it is actually invalid.

We define collusion as in [8], with two minor adaptations: (i) we use our single-round framework, that allows us to clearly state the information flow between $\mathcal{A}$ and $\mathcal{C}$; and (ii) we introduce a second query phase, after the challenge phase (to strengthen the adversary).

Definition 12 (Soundness Against Collusion (SAC)). *Define the experiment* $\mathbf{Exp}^{\mathsf{ACVAuC}}_{\mathcal{A}}[\lambda]$ *to be* $\mathbf{Exp}^{\mathsf{UF\text{-}ACMV}}_{\mathcal{A}}[\lambda]$ *where:*

*- in the **Setup** phase, $\mathcal{C}$ gives to $\mathcal{A}$ all keys except* pr*, and*

- no sign query is performed, and

*- the tuple (m^*, σ^*, ρ^*) output by $\mathcal{A}$ at the end of the experiment is considered **forgery** if $\Delta \leftarrow \mathsf{SAV.Verify}(\mathsf{pr}, \mathsf{pk}, m^*, \sigma^*, \rho^*, \hat{\tau})$ is such that $\Delta \neq \perp$ and $\Delta \neq \mathsf{SAV.Verify}(\mathsf{pr}, \mathsf{pk}, m^*, \sigma^*, \rho, \hat{\tau})$, where $\rho \leftarrow \mathsf{SAV.Comp}(\mathsf{pb}, \hat{\omega})$ is generated honestly.*

A SAV signature scheme is (ε, q_v)-sound against adaptive chosen verification attacks under collusion if $\mathsf{Prob}\left[\mathbf{Exp}^{\mathsf{ACVAuC}}_{\mathcal{A}}[\lambda] = 1\right] < \varepsilon$.

Definition 12 highlights connections between the notions of extended existential unforgeability and soundness against collusion. In particular, it is possible to think of collusion attacks as unforgeability attacks where $\mathcal{A}$ possesses the signing secret key sk (and thus no *sign* query is needed), and a forgery is a tuple for which the output of the server-aided verification does not coincide with the correct one, *e.g.*, if $\sigma^* \leftarrow \mathsf{SAV.Sign}(\mathsf{sk}, m^*)$ then $\mathsf{SAV.Verify}(\mathsf{pr}, \mathsf{pk}, m^*, \sigma^*, \rho^*, \hat{\tau})$ returns 0.

4.3 Anonymity

Anonymous signatures were introduced by Yang *et al.* in [26]. In a nutshell, anonymity (for digital signatures) states that an adversary, who has access to a signature σ and does not hold the corresponding message m, is not able to determine the identity of the signer of σ. Thus, anonymity requires to withhold the pair (m, σ) from the adversary, Otherwise $\mathcal{A}$ could run the verification algorithm of the signature scheme and determine under which public key (among the candidate ones) the given pair is valid. Retaining m from the adversary is a necessary requirement which, however, limits considerably the application scenarios for anonymous signatures. We initiate the study of anonymity in the context of server-aided verification of signatures and provide the first definition of SAV-anonymity.

Consider the running setting of signed auctions. If a malicious server can distinguish whose signature it is performing the aided-verification of, it can easily 'keep out' target bidders from the auction by preventing their signatures from verifying (in the server aided sense). To prevent such an attack, bidders may want to hide their identity from the untrusted server. SAV-anonymity guarantees precisely this: the auctioneer (trusted verifier) learns the identities of the bidders (signers), while the untrusted server is not able to determine whose signature was involved in the SAV.

Definition 13 (SAV-anonymity). *A SAV scheme is* (ε, q_v)*-SAV-anonymous if*

$$\mathsf{Prob}\left[\mathbf{Exp}_{\mathcal{A}}^{\mathsf{SAV\text{-}anon}}[\lambda] = 1\right] < \frac{1}{2} + \varepsilon$$

and $\mathbf{Exp}_{\mathcal{A}}^{\mathsf{SAV\text{-}anon}}[\lambda]$ *is:*

Setup. *The challenger runs the algorithms* SAV.Init, SAV.VSetup *to obtain the system parameters and the verification keys* $(\mathsf{pb}, \mathsf{pr})$*. Then it runs* SAV.KeyGen *twice to generate* $(\mathsf{sk}_0, \mathsf{pk}_0), (\mathsf{sk}_1, \mathsf{pk}_1)$ *and draws* $b \xleftarrow{R} \{0,1\}$*.* $\mathcal{C}$ *gives* pb, $\mathsf{pk}_0, \mathsf{pk}_1$ *to* $\mathcal{A}$ *and retains the secret values* pr, $\mathsf{sk}_0, \mathsf{sk}_1$*.*

Query I. $\mathcal{A}$ *can adaptively perform up to* q_v *partial-verification queries as follows. The adversary sends a pair* (m, i)*,* $i \in \{0,1\}$ *to* $\mathcal{C}$*. The challenger computes* $\sigma \leftarrow \mathsf{SAV.Sign}(\mathsf{sk}_i, m)$*, runs* $\mathsf{SAV.ProbGen}(\mathsf{pr}, \mathsf{pk}_i, m, \sigma) \rightarrow (\omega, \tau)$ *and returns* ω *to* $\mathcal{A}$*.*

Challenge. *The adversary chooses a message* m^* *to be challenged on, and sends it to* $\mathcal{C}$*. The challenger computes* $\sigma \leftarrow \mathsf{SAV.Sign}(\mathsf{sk}_b, m^*)$ *and* $(\omega, \tau) \leftarrow \mathsf{SAV.ProbGen}(\mathsf{pr}, \mathsf{pk}_b, m^*, \sigma)$*; and sends* ω *to the adversary.*

Query II. $\mathcal{A}$ *can perform another query phase, as in Query I.*

Output. *The adversary outputs a guess* $b^* \in \{0,1\}$ *for the identity* b *chosen by* $\mathcal{C}$*. The experiment outputs 1 if* $b^* = b$ *and 0 otherwise.*

The fundamental difference between anonymity for signatures schemes [13,26] and SAV-anonymity lies in the choice of the challenge message m^*. In the former case, it is chosen by the challenger at random, while in SAV we let the adversary select it. This change increases the adversary's power and reflects several application scenarios where $\mathcal{A}$ learns the messages (*e.g.*, bids in signed auctions). We remark that in SAV-anonymity the adversary does not have access to the verification outcome Δ, as this would correspond to having a verification oracle, which is not allowed in the anonymity game for signature schemes [13,26].

5 A compiler for SAV

We present here the first generic compiler for server-aided verification of signatures. Our generic composition method allows to combine any signature scheme Σ with an efficient verifiable computation scheme Γ for a function f involved in the signature verification algorithm, and outputs

$\mathsf{SAV}^{\Gamma}_{\Sigma}$, a single-round server-aided verification scheme for Σ. In particular, our compiler renders the design of SAV schemes more intuitive and modular.

The idea to employ verifiable computation in SAV comes from the following observation. All the attacks presented in [8] succeed because in the target SAV schemes the verifier never checks the validity of the values returned by the server. We leverage the efficiency and security properties of verifiable computation to mitigate such attacks.

5.1 Description of our compiler

Let $\Sigma = (\mathsf{SetUp}_{\Sigma}, \mathsf{KeyGen}_{\Sigma}, \mathsf{Sign}_{\Sigma}, \mathsf{Verify}_{\Sigma})$ be a signature scheme and $\Gamma = (\mathsf{KeyGen}^{\Gamma}, \mathsf{ProbGen}^{\Gamma}, \mathsf{Comp}^{\Gamma}, \mathsf{Verify}^{\Gamma})$ be a verifiable computation scheme.[4] In our generic composition, we identify a computationally-expensive sub-routine of Verify_{Σ} that we refer to as $\mathsf{Ver}_{\mathsf{H}}$ (the *heavy* part of the signature verification); and we outsource $f = \mathsf{Ver}_{\mathsf{H}}$ using the verifiable computation scheme Γ. To ease the presentation, we introduce:

$\mathsf{ProbGen}^{\mathsf{PRE}}$**:** This algorithm prepares the input to $\mathsf{ProbGen}^{\Gamma}$.

$\mathsf{Ver}_{\mathsf{L}}$**:** This algorithm is the computationally *light* part of the signature verification. More precisely, $\mathsf{Ver}_{\mathsf{L}}$ is Verify_{Σ} where $\mathsf{Ver}_{\mathsf{H}}$ is replaced by the output y of Verify^{Γ}. It satisfies: $cost(\mathsf{Ver}_{\mathsf{L}}) < cost(\mathsf{Verify}_{\Sigma})$ and $\mathsf{Ver}_{\mathsf{L}}(\mathsf{pk}_{\Sigma}, m, \sigma, y) = \mathsf{Verify}_{\Sigma}(\mathsf{pk}, m, \sigma)$ whenever $y \neq \perp$.

To give an example, one can split the BLS verification algorithm into $\mathsf{Ver}_{\mathsf{H}}(\mathsf{pk}, m, \sigma) \rightarrow y = (\beta_1, \beta_2)$, which computes the two bilinear pairings $\beta_1 = e(\sigma, g), \beta_2 = e(H(m), \mathsf{pk})$; and $\mathsf{Ver}_{\mathsf{L}}(\mathsf{pk}, m, \sigma, y)$, which performs the equality check $\beta_1 \stackrel{?}{=} \beta_2$. In order to securely outsource $\mathsf{Ver}_{\mathsf{H}}$ to the server, we need to prepare opportune inputs for $\mathsf{ProbGen}^{\Gamma}$. We call this preparatory routine $\mathsf{ProbGen}^{\mathsf{PRE}}$.

Definition 14 ($\mathsf{SAV}^{\Gamma}_{\Sigma}$). *Let Σ, Γ and f be as above. Our generic composition method for single-round server-aided verification signature scheme $\mathsf{SAV}^{\Gamma}_{\Sigma}$ is defined by the following possibly randomized algorithms:*

- $\mathsf{SAV.Init}(1^{\lambda})$*: the initialisation algorithm outputs the global parameters* $\mathsf{gp} \leftarrow \mathsf{SetUp}_{\Sigma}(1^{\lambda})$*, which are implicitly input to all the algorithms.*
- $\mathsf{SAV.KeyGen}()$*: this algorithm outputs* $(\mathsf{pk}_{\Sigma}, \mathsf{sk}_{\Sigma}) \leftarrow \mathsf{KeyGen}_{\Sigma}()$.
- $\mathsf{SAV.Sign}(\mathsf{sk}_{\Sigma}, m)$*: the sign algorithm outputs* $\sigma \leftarrow \mathsf{Sign}_{\Sigma}(\mathsf{sk}_{\Sigma}, m)$.
- $\mathsf{SAV.VSetup}()$*: the verification setup algorithm outputs verification keys* $(\mathsf{pk}^{\Gamma}, \mathsf{sk}^{\Gamma}) \leftarrow \mathsf{KeyGen}^{\Gamma}(\lambda, f)$*, where the function f is described in* gp.
- $\mathsf{SAV.ProbGen}(\mathsf{sk}^{\Gamma}, \mathsf{pk}_{\Sigma}, m, \sigma)$*: this algorithm first runs* $\mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pk}_{\Sigma}, m, \sigma) \rightarrow x$ *to produce an encoding of* pk_{Σ}*, m, σ. Then x is used to compute the output* $(\omega, \tau) \leftarrow \mathsf{ProbGen}^{\Gamma}(\mathsf{sk}^{\Gamma}, x)$.
- $\mathsf{SAV.Comp}(\mathsf{pk}^{\Gamma}, \omega)$*: this algorithm returns* $\rho \leftarrow \mathsf{Comp}^{\Gamma}(\mathsf{pk}^{\Gamma}, \omega)$.
- $\mathsf{SAV.Verify}(\mathsf{sk}^{\Gamma}, \mathsf{pk}_{\Sigma}, m, \sigma, \rho, \tau)$*: the verification algorithm first executes* $\mathsf{Verify}^{\Gamma}(\mathsf{sk}^{\Gamma}, \rho, \tau) \rightarrow y$*; if $y = \perp$, it sets $\Delta = \perp$ and returns. Otherwise, it returns the output of* $\mathsf{Ver}_{\mathsf{L}}(\mathsf{pk}_{\Sigma}, m, \sigma, y) \rightarrow \Delta \in \{0, 1\}$.

Completeness of $\mathsf{SAV}^{\Gamma}_{\Sigma}$. The correctness of $\mathsf{SAV}^{\Gamma}_{\Sigma}$ is a straight-forward computation assuming that Σ is complete and Γ is correct (see the Appendix A for a detailed proof).

Efficiency of $\mathsf{SAV}^{\Gamma}_{\Sigma}$. It is immediate to check that $cost(\mathsf{Verify}_{\Sigma}) = cost(\mathsf{Ver}_{\mathsf{L}}) + cost(\mathsf{Ver}_{\mathsf{H}})$. The $\mathsf{ProbGen}^{\mathsf{PRE}}$ algorithm is just performing encodings of its inputs (usually projections), and does not involve computationally expensive operations.[5] By the efficiency of verifiable computation schemes we have: $cost(\mathsf{Ver}_{\mathsf{H}}) > cost(\mathsf{ProbGen}^{\Gamma}) + cost(\mathsf{Verify}^{\Gamma})$ and thus $cost(\mathsf{Verify}_{\Sigma}) > cost(\mathsf{ProbGen}^{\mathsf{PRE}}) + cost(\mathsf{ProbGen}^{\Gamma}) + cost(\mathsf{Verify}^{\Gamma}) + cost(\mathsf{Ver}_{\mathsf{L}})$, which proves the last claim.

Our generic composition enjoys two additional features: it applies to *any* signature scheme and it allows to reduce the security of $\mathsf{SAV}^{\Gamma}_{\Sigma}$ to the security of its building blocks, Σ and Γ. To demonstrate the first claim, let us set $f = \mathsf{Ver}_{\mathsf{H}} = \mathsf{Verify}_{\Sigma}$ and $\mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pk}_{\Sigma}, m, \sigma) \rightarrow x = (\mathsf{pk}_{\Sigma}, m, \sigma)$. The correctness of Γ implies that $y = \mathsf{Ver}_{\mathsf{H}}(x) = \mathsf{Verify}_{\Sigma}(\mathsf{pk}_{\Sigma}, m, \sigma)$. In this case, $\mathsf{Ver}_{\mathsf{L}}(\mathsf{pk}_{\Sigma}, m, \sigma, y)$ is the function that returns 1 if $y = 1$ and 0 otherwise. We defer the proof of the second claim to the following section.

[4] To improve readability, we put the subscript Σ (*resp.* superscript Γ) to each algorithm related to the signature (*resp.* verifiable computation) scheme.

[5] This claim will become clear after seeing examples of SAV signature schemes.

5.2 Security of our generic composition

The following theorems state the security of the compiler presented in Definition 14. Our approach is to identify sufficient requirements on Σ and Γ to guarantee specific security properties in the resulting $\mathsf{SAV}^{\Gamma}_{\Sigma}$ scheme. To improve readability, all proofs are collected in the Appendix A. We highlight that the results below apply to all our instantiations of the SAV signature schemes presented in Section 6, since these are obtained via our generic composition method.

Theorem 1 (Extended Unforgeability of $\mathsf{SAV}^{\Gamma}_{\Sigma}$). *Let Σ be an $(\varepsilon_{\Sigma}, q_s)$-existentially (resp. strong) unforgeable signature scheme, and Γ an $(\varepsilon^{\Gamma}, q_v)$-secure verifiable computation scheme. Then $\mathsf{SAV}^{\Gamma}_{\Sigma}$ is $(\frac{\varepsilon_{\Sigma}+\varepsilon^{\Gamma}}{2}, q_s, q_v)$-extended existential (resp. strong) unforgeable.*

The proof proceeds by reduction transforming type-1a (*resp.* type-1b) forgeries into existential (*resp.* strong) forgeries against Σ; and type-2 forgeries, into forgeries against the security of Γ.

Theorem 2 (Soundness Against Collusion of $\mathsf{SAV}^{\Gamma}_{\Sigma}$). *Let Σ be a correct signature scheme and Γ an $(\varepsilon^{\Gamma}, q_v)$-secure verifiable computation scheme. Then $\mathsf{SAV}^{\Gamma}_{\Sigma}$ is $(\varepsilon^{\Gamma}, q_v)$-sound against collusion.*

The intuition behind the proof of Theorem 2 is the same as in Theorem 1 for the case of type-2 forgeries.

We present now two independent ways to achieve SAV-anonymity for schemes obtained with our compiler: leveraging either the privacy of the verifiable computation scheme or the adaptibility of the signature scheme.

Theorem 3 (Anonymity of $\mathsf{SAV}^{\Gamma}_{\Sigma}$ from Private Verification). *Let Σ be a correct signature scheme and Γ an $(\varepsilon^{\Gamma}, q_v)$-private verifiable computation scheme. Then $\mathsf{SAV}^{\Gamma}_{\Sigma}$ is $(\varepsilon^{\Gamma}, q_v)$-SAV-anonymous.*

Theorem 3 does not require Σ to be anonymous and SAV-anonymity comes directly from the privacy of the verifiable computation scheme.

Key-homomorphic signatures have been recently introduced by Derler and Slamanig [10]. In a nutshell, a signature scheme provides *adaptibility* of signatures [10] if given a signature σ for a message m under a public key pk, it is possible to publicly create a valid σ' for the same message m under a new public key pk'. In particular, there exists an algorithm Adapt that, given pk, m, σ and a shift amount h, returns a pair (pk', σ') for which $\mathsf{Verify}(\mathsf{pk}', m, \sigma') = 1$ (cf. Definition 16 in [10] for a formal statement). [6]

Theorem 4 (Anonymity of $\mathsf{SAV}^{\Gamma}_{\Sigma}$ from Perfect Adaption). *Let Σ be a signature scheme with perfect adaption and Γ a correct verifiable computation scheme. If the output of $\mathsf{ProbGen}^{\mathsf{PRE}}$ depends only on the adapted values, i.e., for all $\mathsf{pr}, \mathsf{pk}, m, \sigma$ there is a function G such that:*

$$\mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pr}, \mathsf{pk}, m, \sigma) = \mathsf{G}(\mathsf{Adapt}(\mathsf{pk}, m, \sigma, \mathsf{h}), m)$$

for a randomly chosen shift amount h, then $\mathsf{SAV}^{\Gamma}_{\Sigma}$ is unconditionally SAV-anonymous.

Theorem 4 provides a new application of key-homomorphic signatures to anonymity. The proof is inspired to the tricks used in [10], intuitively SAV-anonymity follows from the indistinguishability of the output of Adapt from $(\mathsf{pk}'', \sigma'' \leftarrow \mathsf{Sign}(\mathsf{sk}'', m))$ for a freshly generated key pair $(\mathsf{pk}'', \mathsf{sk}'')$. Many signatures based on the discrete logarithm problem enjoy this property, *e.g.*, BLS [3] and Wat [23].

6 New instantiations of SAV schemes

Our generic composition requires the existence of a verifiable computation scheme for a function $f = \mathsf{Ver}_{\mathsf{H}}$ used in the signature verification algorithm. To the best of the authors' knowledge, there are verifiable computation schemes for arithmetic circuits [9,19] and bilinear pairings [6], but no result is yet known for simpler computations such as hash functions and group exponentiations.

[6] To provide an example, consider the BLS signature scheme [3]. Given $\mathsf{pk} = g^{\mathsf{sk}}$, $m \in \{0,1\}^*$, $\sigma \in \mathbb{G}_p$ and $\mathsf{h} \in \mathbb{Z}_p$, the output of Adapt can be defined as: $\mathsf{pk}' = \mathsf{pk} \cdot g^{\mathsf{h}}$ and $\sigma' = \sigma \cdot H(m)^{\mathsf{h}}$. It is immediate to check that (σ', m) is a valid pair under pk'.

Following previous works' approach, we consider only SAV for pairing-based signatures [8,20,25,27], since bilinear pairings are bottle-neck computations for resource-limited devices.[7]

All our instantiations of SAV schemes are obtained using the compiler in Definition 14. Their security therefore follows from the results of Section 5.2, once shown that that the chosen schemes satisfy the hypothesis of the theorems. For conciseness, we only define the two algorithms $\mathsf{ProbGen}^{\mathsf{PRE}}$ and $\mathsf{Ver}_{\mathsf{L}}$. Appendix B contains thorough descriptions.

6.1 A secure SAV for BLS ($\mathsf{SAV}^{\mathsf{CDS_1}}_{\mathsf{BLS}}$)

The BLS signature by Boneh *et al.* [3] has been widely used for constructing server-aided verification schemes, *e.g.*, Protocols I and II in [25]. Cao *et al.* [7] and Chow *et al.* [8] have shown that all the existing SAV for BLS are neither existentially unforgeable, nor sound against collusion. This motivates us to propose $\mathsf{SAV}^{\mathsf{CDS_1}}_{\mathsf{BLS}}$ (described in Figure 1). As a verifiable scheme for the pairing computation, we employ *'a protocol for public variable A and B'* by Canard *et al.* [6], which we refer to as $\mathsf{CDS_1}$.

$\mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pk}_\Sigma, m, \sigma)$: on input $\mathsf{pk}_\Sigma \in \mathbb{G}_1$, $m \in \{0,1\}^*$ and $\sigma \in \mathbb{G}_1$, the algorithm returns $x = \big((\mathsf{pk}_\Sigma, H(m)), (\sigma, g)\big)$.
$\mathsf{Ver}_{\mathsf{L}}(\mathsf{pk}_\Sigma, m, \sigma, y)$: this algorithm is $\mathsf{Verify}_{\mathsf{BLS}}$ where the computation of the two pairings is replaced with the output $y = (y_1, y_2)$ of $\mathsf{Verify}^{\mathsf{CDS_2}}$. Formally, $\mathsf{Ver}_{\mathsf{L}}$ checks whether $y_1 = y_2$, in which case it outputs $\Delta = 1$, otherwise it returns $\Delta = 0$.

Fig. 1. The core algorithms of $\mathsf{SAV}^{\mathsf{CDS_1}}_{\mathsf{BLS}}$.

By the correctness of the $\mathsf{CDS_1}$ scheme $y_2 = e(\mathsf{pk}_\Sigma, H(m))$ and $y_2 = e(\sigma, g)$, thus $\mathsf{Ver}_{\mathsf{L}}$ has the same output as $\mathsf{Verify}_{\mathsf{BLS}}$. Given that BLS is strongly unforgeable in the random oracle model [3] and that $\mathsf{CDS_1}$ is secure in the generic group model [6], $\mathsf{SAV}^{\mathsf{CDS_1}}_{\mathsf{BLS}}$ is extended strongly unforgeable and sound against collusion. Our SAV scheme for the BLS is not SAV-anonymous: the signer's public key is given to the server for the aided verification. However, SAV-anonymity can be simply gained via the adaptability of BLS [10].

In $\mathsf{SAV}^{\mathsf{CDS_1}}_{\mathsf{BLS}}$ the verifier does not need to perform *any* pairing computation. This is a very essential feature, especially if the verifying device has very limited computational power, *e.g.*, an RFID tag.

6.2 A secure SAV for Wat ($\mathsf{SAV}^{\mathsf{CDS_1}}_{\mathsf{Wat}}$)

Wu *et al.* [25] proposed a SAV for Waters' signature Wat [23], which is neither existentially unforgeable nor sound against collusion. Here we propose $\mathsf{SAV}^{\mathsf{CDS_1}}_{\mathsf{Wat}}$ (described in Figure 2), which is similar to Protocol III in [25], but has strong security guarantees thanks to the verifiable computation scheme for *'public A and B'* $\mathsf{CDS_1}$ [6].

$\mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pk}_\Sigma, m, \sigma)$: given $\mathsf{pk}_\Sigma \in \mathbb{G}_1$, $m \in \{0,1\}^*$ and $\sigma \in \mathbb{G}_1$, select $\mathsf{h} \xleftarrow{R} \mathbb{Z}_p$, compute $(\mathsf{pk'}_\Sigma, \sigma') \leftarrow \mathsf{Adapt}(\mathsf{pk}_\Sigma, m, \sigma, \mathsf{h})$, return $x = (\mathsf{pk'}_\Sigma, m, \sigma')$.
$\mathsf{Ver}_{\mathsf{L}}(\mathsf{pk'}_\Sigma, m, \sigma, y)$: this is $\mathsf{Verify}_{\mathsf{Wat}}$ where the computation of the two pairings is replaced with the outputs y_1, y_2 of $\mathsf{Verify}^{\mathsf{CDS_1}}$. Formally, $\mathsf{Ver}_{\mathsf{L}}$ checks if $y_1 = \mathsf{pk'}_\Sigma \cdot y_2$, in which case it outputs $\Delta = 1$, otherwise it returns $\Delta = 0$.

Fig. 2. The core algorithms of $\mathsf{SAV}^{\mathsf{CDS_1}}_{\mathsf{Wat}}$.

By the correctness of the $\mathsf{CDS_1}$ scheme $y_1 = e(\sigma_1, g)$, and $y_2 = e(H(m), \sigma_2)$. Thus, $\mathsf{Ver}_{\mathsf{L}}$ has the same output as $\mathsf{Verify}_{\mathsf{Wat}}$. Given that $\mathsf{CDS_1}$ is secure in the generic group model [6], and that Wat is existentially unforgeable in the standard model [23] our $\mathsf{SAV}^{\mathsf{CDS_1}}_{\mathsf{Wat}}$ is extended existential unforgeable and sound against collusion. Similarly to Protocol III in [25], $\mathsf{SAV}^{\mathsf{CDS_1}}_{\mathsf{Wat}}$ achieves SAV-anonymity thanks to the perfect adaption of Wat [10].

[7] To give benchmarks, let M_p denote the computational cost of a base field multiplication in $\mathbb{F}_p$ with $\log p = 256$, then computing z^a for any $z \in \mathbb{F}_p$ and $a \in [p]$ costs about $256M_p$, while computing the Optimal Ate pairing on the BN curve requires about $16000M_p$ (results extrapolated from Table 1 in [16]).

6.3 The first SAV for CL ($\mathsf{SAV}^{\mathsf{CDS_2}}_{\mathsf{CL}}$)

The verification of the BLS and the Wat signatures only requires the computation of two bilinear pairings. We want to move the focus to more complex signature schemes that would benefit more of server-aided verification. To this end, we consider scheme A by Camenish and Lysyanskaya [5], which we refer to as CL, where $\mathsf{Verify}_{\mathsf{CL}}$ involves the computation of five bilinear pairings. For verifiability we employ CDS_2, *'a protocol with public constant B and variable secret A'* by Canard *et al.* [6]

Our $\mathsf{SAV}^{\mathsf{CDS_2}}_{\mathsf{CL}}$ scheme is reported in Figure 3.

$\mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pk}_\Sigma, m, \sigma)$: this algorithm simply returns the first two entries of the signature $\sigma = (\sigma_1, \sigma_2, \sigma_3)$, *i.e.*, $x = (\sigma_1, \sigma_2)$.

$\mathsf{Ver}_{\mathsf{L}}(\mathsf{pk}_\Sigma, m, \sigma, y)$: this algorithm is $\mathsf{Verify}_{\mathsf{CL}}$, except for two pairing computations which are replaced with the outcome $y = (\beta_1, \beta_2)$ of $\mathsf{Verify}^{\mathsf{CDS_2}}$. More precisely, the $\mathsf{Ver}_{\mathsf{L}}$ algorithm computes $\alpha_1 = e(\sigma_1, Y)$, $\alpha_2 = e(X, \sigma_1)$ and $\alpha_3 = e(X, \sigma_2)^m$. It then checks whether $\alpha_1 = \beta_1$ and $\alpha_2 \cdot \alpha_3 = \beta_2$. If both of the conditions hold, the algorithm returns $\Delta = 1$, otherwise $\Delta = 0$.

Fig. 3. The core algorithms of $\mathsf{SAV}^{\mathsf{CDS_2}}_{\mathsf{CL}}$.

By the correctness of CDS_2 we have: $y_1 = \beta_1 = e(\sigma, g)$, and $y_2 = \beta_2 = e(H(m), \mathsf{pk}_\Sigma)$. Therefore $\mathsf{Ver}_{\mathsf{L}}$ performs the same checks as $\mathsf{Verify}_{\mathsf{CL}}$ and the two algorithms have the same output. Given that CL is existential unforgeable in the standard model [5] and CDS_2 is secure and private in the generic group model [6], $\mathsf{SAV}^{\mathsf{CDS_2}}_{\mathsf{CL}}$ is extended-existential unforgeable, sound against collusion and SAV-anonymous. Therefore $\mathsf{SAV}^{\mathsf{CDS_2}}_{\mathsf{CL}}$ is an example of a scheme which is SAV-anonymous although the base signature scheme is not anonymous (cf. Lemma 1 in Appendix D).

6.4 Comparison with previous work

Table 1 gives a compact overview of how our SAV schemes compare to previous proposals in terms of unforgeability, soundness under collusion and SAV-anonymity. We report only the highest level of unforgeability that the scheme provides. A yes (*resp.* no) in the table states that the scheme does (*resp.* does not) achieve the property written at the beginning of the row, *e.g.*, Protocol III does not employ a verifiable computation scheme and provides SAV-anonymity. Every scheme or property is followed by a reference paper or the section where the claim is proven.

	Protocol I [25]	Protocol II [25]	$\mathsf{SAV}^{\mathsf{CDS_1}}_{\mathsf{BLS}}$	Protocol III [25]	$\mathsf{SAV}^{\mathsf{CDS_1}}_{\mathsf{Wat}}$	SAV-ZSS [15]	$\mathsf{SAV}^{\mathsf{CDS_2}}_{\mathsf{CL}}$
signature	BLS [3]	BLS [3]	BLS [3]	Wat [23]	Wat [23]	ZSS [27]	CL [5]
verifiability	no	no	CDS_1 [6]	no	CDS_1 [6]	no	CDS_2 [6]
unforgeability	EUF [25]	no [8]	ExSUF (6.1)	no (C.1)	ExEUF (6.2)	EUF [15]	ExEUF (6.3)
collusion resistance	no [8]	no (C.3)	yes (6.1)	no (C.3)	yes (6.2)	no (C.3)	yes (6.3)
anonymity	no (C.4)	no (C.4)	no (6.1)	yes (C.4)	yes (6.2)	no (C.4)	yes (6.3)

Table 1. Comparison among our SAV schemes and previous works: Protocol I (Figure 3 in [25]), Protocol II (Figure 5 in [25]), Protocol III (Figure 4 in [25]), SAV-ZSS [15] (depicted in Figure 1 in [25]).

Regarding efficiency, the computational cost of pairing-based algorithms is influenced by three main parameters: (*i*) the elliptic curve, (*ii*) the field size, and (*iii*) the bilinear pairing. As a result, it is impossible to state that a given algorithm is efficient for all pairings and for all curves, since even the computational cost of the most basic operations (*e.g.*, point addition) variates significantly with the above parameters. For example, CDS_2 provides a 70% efficiency gain[8] for the delegator (verifier) when the employed pairing is the Optimal Ate pairing on the KSS-18 curve [6], but is nearly inefficient when computed on the BN curve [16].

[8] Efficiency gain is the ratio $\big(cost(\mathsf{SAV.ProbGen}) + cost(\mathsf{SAV.Verify})\big)/cost(\mathsf{Verify}_\Sigma)$.

7 Conclusions

In this paper, we provided a framework for single-round server-aided verification signature schemes and introduced a security model which extends previous proposals towards more realistic attack scenarios and stronger adversaries. In addition, we defined the first generic composition method to obtain a SAV for any signature scheme using an appropriate verifiable computation scheme. Our compiler identifies for the first time sufficient requirements on the underlying primitives to ensure the security and anonymity of the resulting SAV scheme. In particular, we showed sufficient conditions to achieve both computational and unconditional SAV-anonymity. Finally, we introduced three new SAV signature schemes obtained via our generic composition method, that simultaneously achieve existential unforgeability and soundness against collusion.

Currently, Canard *et al.*'s is the only verifiable computation scheme for pairings available in the literature. Considering the wide applicability of bilinear pairings in cryptography, a more efficient verifiable computation scheme for these functions would render pairings a server-aided accessible computation to a large variety of resource-limited devices, such as the ones involved in IoT and cloud computing settings.

Acknowledgements We thank Dario Fiore (Assistant Research Professor) for providing useful comments on the contributions of this paper.

References

1. P. Béguin and J. Quisquater. Fast server-aided RSA signatures secure against active attacks. In *Advances in Cryptology - CRYPTO '95*, pages 57–69, 1995.
2. S. Benabbas, R. Gennaro, and Y. Vahlis. Verifiable delegation of computation over large datasets. In *Annual Cryptology Conference*, pages 111–131. Springer, 2011.
3. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. *Journal of Cryptology*, 17(4):297–319, 2004.
4. D. Boneh, E. Shen, and B. Waters. Strongly unforgeable signatures based on computational diffie-hellman. In *International Workshop on Public Key Cryptography*, pages 229–240. Springer, 2006.
5. J. Camenisch and A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In *Annual International Cryptology Conference*, pages 56–72. Springer, 2004.
6. S. Canard, J. Devigne, and O. Sanders. Delegating a pairing can be both secure and efficient. In *International Conference on Applied Cryptography and Network Security*, pages 549–565. Springer, 2014.
7. Z. Cao, L. Liu, and O. Markowitch. On two kinds of flaws in some server-aided verification schemes. *International Journal of Network Security*, 18(6):1054–1059, 2016.
8. S. S. Chow, M. H. Au, and W. Susilo. Server-aided signatures verification secure against collusion attack. *Inf. Security Tech. Report*, 17(3):46 – 57, 2013.
9. C. Costello, C. Fournet, J. Howell, M. Kohlweiss, B. Kreuter, M. Naehrig, B. Parno, and S. Zahur. Geppetto: Versatile verifiable computation. In *Security and Privacy (SP), 2015 IEEE Symposium on*, pages 253–270. IEEE, 2015.
10. D. Derler and D. Slamanig. Key-homomorphic signatures and applications to multiparty signatures. Technical report, IACR Cryptology ePrint Archive 2016, 792, 2016.
11. X. Ding, D. Mazzocchi, and G. Tsudik. Experimenting with server-aided signatures. In *NDSS*, 2002.
12. D. Fiore, R. Gennaro, and V. Pastro. Efficiently verifiable computation on encrypted data. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 844–855. ACM, 2014.
13. M. Fischlin. Anonymous signatures made easy. In *International Workshop on Public Key Cryptography*, pages 31–42. Springer, 2007.
14. R. Gennaro, C. Gentry, and B. Parno. Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In *Annual Cryptology Conference*, pages 465–482. Springer, 2010.
15. M. Girault and D. Lefranc. Server-aided verification: theory and practice. In *International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT*, pages 605–623. Springer, 2005.
16. A. Guillevic and D. Vergnaud. Algorithms for outsourcing pairing computation. In *CARDIS*, pages 193–211. Springer, 2014.
17. F. Guo, Y. Mu, W. Susilo, and V. Varadharajan. Server-aided signature verification for lightweight devices. *The Computer Journal*, page bxt003, 2013.
18. C. H. Lim and P. J. Lee. Server (prover/signer)-aided verification of identity proofs and signatures. In *International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT*, pages 64–78. Springer, 1995.
19. B. Parno, J. Howell, C. Gentry, and M. Raykova. Pinocchio: Nearly practical verifiable computation. In *Security and Privacy (SP), 2013 IEEE Symposium on*, pages 238–252. IEEE, 2013.

20. B. Wang. A server-aided verification signature scheme without random oracles. *International Review on Computers & Software*, 7:3446, 2012.
21. Z. Wang. A new construction of the server-aided verification signature scheme. *Mathematical and Computer Modelling*, 55(1):97–101, 2012.
22. Z. Wang, L. Wang, Y. Yang, and Z. Hu. Comment on wu et al.'s server-aided verification signature schemes. *IJ Network Security*, 10(2):158–160, 2010.
23. B. Waters. Efficient identity-based encryption without random oracles. *In EUROCRYPT 2005, in: Lecture Notes in Computer Science*, 3494(114–127), 2005.
24. W. Wu, Y. Mu, W. Susilo, and X. Huang. Server-aided verification signatures: Definitions and new constructions. In *International Conference on Provable Security*, pages 141–155. Springer, 2008.
25. W. Wu, Y. Mu, W. Susilo, and X. Huang. Provably secure server-aided verification signatures. *Computers & Mathematics with Applications*, 61(7):1705 – 1723, 2011.
26. G. Yang, D. S. Wong, X. Deng, and H. Wang. Anonymous signature schemes. In *International Workshop on Public Key Cryptography*, pages 347–363. Springer, 2006.
27. F. Zhang, R. Safavi-Naini, and W. Susilo. An efficient signature scheme from bilinear pairings and its applications. In *International Workshop on Public Key Cryptography*, pages 277–290. Springer, 2004.

A Collected proofs

This Appendix collects the proofs of the results stated in Section 5.

Correctness of our compiler (Definition 14).
According to Definition 5, a single-round server-aided verification signature scheme is correct if $\mathsf{SAV.Verify}$ outputs 1 with all but negligible probability when all the other algorithms of the scheme are run honestly. This property should hold for any key-tuple and for any message $m \in \mathcal{M}$. Let $(\mathsf{pk}_\Sigma, \mathsf{sk}_\Sigma) \leftarrow \mathsf{SAV.KeyGen}()$ and $(\mathsf{pk}^\Gamma, \mathsf{sk}^\Gamma) \leftarrow \mathsf{SAV.VSetup}()$ be the keys used in the scheme. Let $\sigma \leftarrow \mathsf{SAV.Sign}(\mathsf{sk}_\Sigma, m) = \mathsf{Sign}(\mathsf{sk}_\Sigma, m)$, and $(\omega, \tau) \leftarrow \mathsf{SAV.ProbGen}(\mathsf{sk}^\Gamma, \mathsf{pk}_\Sigma, m, \sigma)$. By the completeness of the VC scheme Γ, $\mathsf{Verify}^\Gamma(\mathsf{sk}^\Gamma, \tau, \mathsf{Comp}^\Gamma(\mathsf{pk}^\Gamma, \omega)) = y \neq \perp$. Finally, by the properties of $\mathsf{Ver_L}$ we have that $\mathsf{Ver_L}(\mathsf{pk}_\Sigma, m, \sigma, y, \tau) = \mathsf{Verify}_\Sigma(\mathsf{pk}, m, \sigma) \rightarrow 1$, since the signature scheme Σ is complete.

Proof of Theorem 1 (Extended Unforgeability of $\mathsf{SAV}^\Gamma_\Sigma$).

Proof. Let $\mathcal{A}$ be an adversary attacking the extended existential unforgeability of the $\mathsf{SAV}^\Gamma_\Sigma$ scheme. In what follows, we construct a reduction that uses a forgery output by $\mathcal{A}$ to break either the existential unforgeability of Σ ($\mathcal{A}_\Sigma$) or the security of Γ ($\mathcal{A}^\Gamma$). Finally, we give an upper bound for the advantage of $\mathcal{A}$ in terms of the advantages of the other two adversaries.

The reduction begins by choosing a value $c \in \{1, 2\}$. If $c = 1$, the reduction ($\mathcal{A}_\Sigma$) starts the EUF game for Σ; if $c = 2$, the reduction ($\mathcal{A}^\Gamma$) starts the verif (security) game for Γ (Experiment 4). This step corresponds to guessing what kind of forgery $\mathcal{A}$ will output (type-1a, or type-2).
Let $c = 1$. The reduction $\mathcal{A}_\Sigma$ starts the EUF game for Σ (described in Experiment 2), and receives pk_Σ from its challenger. $\mathcal{A}_\Sigma$ also generates $(\mathsf{pk}^\Gamma, \mathsf{sk}^\Gamma) \leftarrow \mathsf{SAV.VSetup}()$, and sends to $\mathcal{A}$ the keys pk^Γ and pk_Σ. In the query phase, $\mathcal{A}_\Sigma$ forwards to its challenger all the signature queries received by $\mathcal{A}$, and also stores the transcript in a list L of pairs (m_i, σ_i). $\mathcal{A}_\Sigma$ replies to the verification queries using sk^Γ. Let (m^*, σ^*) be the output of $\mathcal{A}$ in the challenge phase. If $(m^*, \sigma^*) \in L$, $\mathcal{A}_\Sigma$ aborts, as $\mathcal{A}$ is making a type-2 forgery. Otherwise, $\mathcal{A}_\Sigma$ outputs (m^*, σ^*) as an existential forgery to its challenger (and then aborts its interaction with $\mathcal{A}$). By the correctness of the VC scheme Γ, the pair (m^*, σ^*) is part of an extended-existential type-1a forgery against $\mathsf{SAV}^\Gamma_\Sigma$. Thus, $Adv(\mathcal{A} : \text{type-1a}) = Adv(\mathcal{A}_\Sigma) < \varepsilon_\Sigma$, by the existential unforgeability of Σ.
Let $c = 2$. The reduction $\mathcal{A}^\Gamma$ starts the verif security game for the scheme Γ (described in Experiment 4), and receives pk^Γ from its challenger. $\mathcal{A}^\Gamma$ also generates $(\mathsf{pk}_\Sigma, \mathsf{sk}_\Sigma) \leftarrow \mathsf{SAV.KeyGen}()$, and sends to $\mathcal{A}$ the keys pk_Σ and pk^Γ. In the query phase, $\mathcal{A}_\Sigma$ answers all the signature queries using sk_Σ, and stores the transcript, *i.e.*, keeps a list L of queried (m_i, σ_i). When receiving a verification query (m_j, σ_j), $\mathcal{A}^\Gamma$ transforms it into $x_j \leftarrow \mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pk}_\Sigma, m_j, \sigma_j)$, for its challenger. $\mathcal{A}^\Gamma$ then relays the communication, *i.e.*, $\mathcal{A}^\Gamma$ forwards the public output (ω_j) of $\mathsf{ProbGen}^\Gamma$ to $\mathcal{A}$, and $\mathcal{A}$'s reply (ρ_j) to its challenger. Let y_j denote the final output of the challenger to the verification query. If $y = \perp$, $\mathcal{A}^\Gamma$ sends $\Delta = \perp$ to $\mathcal{A}$. Otherwise, $\mathcal{A}^\Gamma$ returns $\Delta \leftarrow \mathsf{Ver_L}(\mathsf{pk}_\Sigma, m, \sigma, y)$. Let (m^*, σ^*)

denote $\mathcal{A}$'s challenge pair. The reduction checks if $(m^*, \sigma^*) \in L$, otherwise it aborts, since $\mathcal{A}$ is submitting a type-1a forgery. If $(m^*, \sigma^*) \in L$, $\mathcal{A}^{\Gamma}$ computes $x^* \leftarrow \mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pk}_{\Sigma}, m^*, \sigma^*)$, sends x^* to its challenger, and returns to $\mathcal{A}$ the public output $\hat{\omega}$ received from its challenger. The second round of queries is handled by $\mathcal{A}^{\Gamma}$ as the first one. Let (m^*, σ^*, ρ^*) be the (type-2) forgery output by $\mathcal{A}$; then $\mathcal{A}^{\Gamma}$ outputs ρ^* to its challenger. By definition of type-2 forgery, it follows that ρ^* is a forgery against the verifiable computation scheme Γ. Thus, $Adv(\mathcal{A} : \text{type-2}) = Adv(\mathcal{A}^{\Gamma}) < \varepsilon^{\Gamma}$, by the security of Γ.
To conclude, we combine the advantages of the two cases ($c \in \{0, 1\}$), and obtain that $\mathsf{SAV}^{\Gamma}_{\Sigma}$ is a $(\frac{\varepsilon_{\Sigma}+\varepsilon^{\Gamma}}{2}, q_s, q_v)$-extended existential unforgeable SAV signature scheme.

It is easy to see that the same proof works for $\mathcal{A}$ an extended strong existential forger, the only change is that for $c = 1$ $\mathcal{A}_{\Sigma}$ starts the SEUF game (described in Experiment 2) and $Adv(\mathcal{A} : \text{type-1a or type-1b}) = Adv(\mathcal{A}_{\Sigma}) < \varepsilon_{\Sigma}$.

Proof of Theorem 2 (Soundness against Collusion of $\mathsf{SAV}^{\Gamma}_{\Sigma}$).

Proof. The proof is done via reduction, in a similar way to the proof of Theorem 1, case $c = 2$. For completeness, we write the detailed proof.

We want here to build a reduction $\mathcal{B}$ that uses a collusion forgery against the scheme $\mathsf{SAV}^{\Gamma}_{\Sigma}$ (produced by an adversary $\mathcal{A}$), to break the security of the VC scheme Γ. The reduction works as follows. $\mathcal{B}$ starts the verif security game for the scheme Γ (Experiment 4), and gets pk^{Γ} from its challenger. $\mathcal{B}$ additionally generates $(\mathsf{pk}_{\Sigma}, \mathsf{sk}_{\Sigma}) \leftarrow \mathsf{SAV.KeyGen}()$, and sends $\mathsf{pk}_{\Sigma}, \mathsf{sk}_{\Sigma}, \mathsf{pk}^{\Gamma}$ to $\mathcal{A}$. During the first query phase, $\mathcal{B}$ transforms $\mathcal{A}$'s verification queries (m, σ) into $x \leftarrow \mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pk}_{\Sigma}, m, \sigma)$, for its challenger. $\mathcal{B}$ then relays the communication, *i.e.*, forwards the public output of $(\omega, \tau) \leftarrow \mathsf{ProbGen}^{\Gamma}(\mathsf{sk}^{\Gamma}, x)$, to $\mathcal{A}$, and $\mathcal{A}$'s the reply, ρ, to its challenger. Let y denote the final output of the challenger to the verification query. If $y = \perp$, $\mathcal{B}$ sends $\Delta = \perp$ to $\mathcal{A}$. Otherwise, $\mathcal{B}$ returns $\Delta \leftarrow \mathsf{Ver}_{\mathsf{L}}(\mathsf{pk}_{\Sigma}, m, \sigma, y)$. Let (m^*, σ^*) denote $\mathcal{A}$'s challenge pair. $\mathcal{B}$ computes $x^* \leftarrow \mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pk}_{\Sigma}, m^*, \sigma^*)$, sends x^* to its challenger, and returns to $\mathcal{A}$ the public output $\hat{\omega}$ received from its challenger. The second round of verification queries is handled by $\mathcal{B}$ with the same strategy as before (this time, using m^* and σ^*). Denote by (m^*, σ^*, ρ^*) the final output of the adversary $\mathcal{A}$. We recall that (m^*, σ^*, ρ^*) is a soundness forgery under collusion if $\mathsf{SAV.Verify}(\mathsf{pr}, \mathsf{pk}, m^*, \sigma^*, \rho^*, \hat{\tau}) \rightarrow \Delta^* \notin \{\perp, \mathsf{SAV.Verify}(\mathsf{pr}, \mathsf{pk}, m^*, \sigma^*, \rho, \hat{\tau})\}$, where $\rho \leftarrow \mathsf{SAV.Comp}(\mathsf{pb}, \hat{\omega})$ is generated honestly. The previous condition implies that:

$$\mathsf{Ver}_{\mathsf{L}}(\mathsf{pk}_{\Sigma}, m^*, \sigma^*, \mathsf{Verify}^{\Gamma}(\mathsf{sk}^{\Gamma}, \rho^*, \tau)) \neq \mathsf{Ver}_{\mathsf{L}}(\mathsf{pk}_{\Sigma}, m^*, \sigma^*, \mathsf{Verify}^{\Gamma}(\mathsf{sk}^{\Gamma}, \rho, \tau))$$

and that $\mathsf{Verify}^{\Gamma}(\mathsf{sk}^{\Gamma}, \rho^*, \tau) \neq \perp$. The two inequalities above imply $\perp \neq \mathsf{Verify}^{\Gamma}(\mathsf{sk}^{\Gamma}, \rho^*, \tau) \neq \mathsf{Verify}^{\Gamma}(\mathsf{sk}^{\Gamma}, \rho, \tau)$. Therefore (x^*, ρ^*) is a valid forgery against the VC scheme Γ. Since we assume Γ to be an ε^{Γ} secure verifiable computation scheme, we derive that $Adv(\mathcal{A}) \leq Adv(\mathcal{B}) < \varepsilon^{\Gamma}$.

Proof of Theorem 3 (Anonymity of $\mathsf{SAV}^{\Gamma}_{\Sigma}$ from Private Verification).

Proof. The proof proceeds by reducing the privacy of the VC scheme Γ to the anonymity of $\mathsf{SAV}^{\Gamma}_{\Sigma}$.

Let the reduction $\mathcal{B}$ initiate the priv game for the VC scheme Γ (described in Experiment 5). $\mathcal{B}$ receives the public key pk^{Γ} from its challenger, and runs $\mathsf{SAV.KeyGen}$ twice to generate two pairs of signing keys $(\mathsf{pk}_0, \mathsf{sk}_0)$ and $(\mathsf{pk}_1, \mathsf{sk}_1)$. Eventually, $\mathcal{B}$ forwards $\mathsf{pk}_0, \mathsf{pk}_1$ and pk^{Γ} to $\mathcal{A}$.

During the query phase of the SAV-anonymity game, $\mathcal{B}$ essentially relays the communication between $\mathcal{A}$ and its challenger. More precisely, upon receiving a query of the form (m, pk_b), from $\mathcal{A}$, the reduction performs the following steps:

(1) it selects sk_b corresponding to the queried identity $b \in \{0, 1\}$,
(2) it produces a valid signature $\sigma \leftarrow \mathsf{SAV.Sign}(\mathsf{sk}_b, m)$,
(3) it computes $x \leftarrow \mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pk}_0, m, \sigma)$,
(4) it starts a (public) verification query on x with its challenger.

The challenger replies to $\mathcal{B}$'s query with ω_x, the public output of the algorithm $\mathsf{SAV.ProbGen}(\mathsf{sk}^{\Gamma}, x)$. $\mathcal{B}$ forwards ω_x as $\omega = \omega_x$ to $\mathcal{A}$. In order to complete its verification query, $\mathcal{B}$ can return a random value ω_y to its challenger, and ignores the challenger's public verification output $\beta \in \{0, 1\}$.

Let m^* denote the challenge message submitted by $\mathcal{A}$. $\mathcal{B}$ prepares its challenge inputs as follows. First, it generates a valid signature of m^* for each identity, *i.e.*, $\sigma_b \leftarrow \mathsf{SAV.Sign}(\mathsf{sk}_b, m^*)$, for $b \in \{0,1\}$. Secondly, it computes $x_b^* \leftarrow \mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pk}_b, m^*, \sigma_b)$. Finally, it provides to its challenger the values x_0^*, x_1^*. The challenger replies with $\omega_{x_b^*}$, according to the private-VC experiment. The reduction concludes the challenge phase by relaying $\hat{\omega} = \omega_{x_b^*}$ to $\mathcal{A}$.

In the second query phase, $\mathcal{B}$ acts as in the first query phase. The final output of $\mathcal{B}$ is the same bit b' output by $\mathcal{A}$.

Since our simulation is perfect, it holds $Adv(\mathcal{A}) = Adv(\mathcal{B}) < \varepsilon^{\Gamma}$.

Proof of Theorem 4 (Anonymity of $\mathsf{SAV}_{\Sigma}^{\Gamma}$ from Perfect Adaption).

Proof. For this proof, we define a sequence of hybrid games, and prove that the case $b = 0$ is indistinguishable from the case $b = 1$. As a matter of notation, W_i denotes the event 'the adversary wins Game i', while $\mathsf{Prob}\,[\mathsf{W}]$ is the probability of event W. The function $\mu : \mathbb{H} \to \mathbb{G}$ is the natural secret-key to public key homomorphism of Σ (implied by perfect adaptivity), *i.e.*, it holds that $\mathsf{pk}_{\Sigma} = \mu(\mathsf{sk}_{\Sigma})$ for any key pair. To highlight the changes between subsequent games, we frame the parts that differ.

As stated by the theorem, $\mathsf{ProbGen}^{\mathsf{PRE}}$ runs Adapt as a subroutine. To ease the presentation for the proof we describe $\mathsf{ProbGen}^{\mathsf{PRE}}$ as a composition of Adapt and a function G:

$$\mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pr}, \mathsf{pk}, m^*, \sigma) = \mathsf{G}(\mathsf{Adapt}(\mathsf{pk}, m^*, \sigma, \mathsf{h} \xleftarrow{R} \mathbb{H}), m^*).$$

Game 0: The original SAV-anonymity game (described in Definition 13), where in challenge phase the challenger runs:

$\mathsf{SAV.ProbGen}(\mathsf{pr}, \mathsf{pk}_b, m^*, \sigma)$: Output (τ, ω) where
$\mathsf{h} \xleftarrow{R} \mathbb{H}$
$(\mathsf{pk}', \sigma') \leftarrow \mathsf{Adapt}(\mathsf{pk}_b, m^*, \sigma, \mathsf{h})$
$x \leftarrow \mathsf{G}(\mathsf{pk}', \sigma', m^*)$, $(\tau, \omega) \leftarrow \mathsf{SAV.ProbGen}(x)$

Note that, with overwhelming probability $\mathsf{pk}' \notin \{\mathsf{pk}_0, \mathsf{pk}_1\}$, *i.e.*, pk' is different from the two public keys involved in the anonymity game.

Game 1: This is the same with Game 0 apart that in the challenge phase the challenger runs the following $\mathsf{SAV.ProbGen}'$ algorithm, instead of $\mathsf{SAV.ProbGen}$:

$\mathsf{SAV.ProbGen}'(\mathsf{pr}, \mathsf{pk}_b, m^*, \sigma)$: Output (τ, ω) where
$\mathsf{h} \xleftarrow{R} \mathbb{H}$, set $\boxed{\mathsf{h}' = \mathsf{sk}_{b\oplus 1} \cdot \mathsf{h}}$
$(\mathsf{pk}', \sigma') \leftarrow \mathsf{Adapt}(\mathsf{pk}_b, m^*, \sigma, \boxed{\mathsf{h}'})$
$x \leftarrow \mathsf{G}(\mathsf{pk}', \sigma', m^*)$, $(\tau, \omega) \leftarrow \mathsf{SAV.ProbGen}(x)$

Transition - Game 0 → Game 1: Under adaptability of signatures, this change is conceptual and $\mathsf{Prob}\,[\mathsf{W}_0]$=$\mathsf{Prob}\,[\mathsf{W}_1]$.

Game 2: This is the same as Game 1, apart that in the challenge phase the challenger replies with signatures generated with the other secret key:

$\mathsf{SAV.ProbGen}'(\mathsf{pr}, \mathsf{pk}_b, m^*, \sigma)$: Output (τ, ω) where
$\mathsf{h} \xleftarrow{R} \mathbb{H}$, $\boxed{\tilde{\sigma} \leftarrow \mathsf{Sign}(\mathsf{sk}_{b\oplus 1}, m^*)}$
$(\mathsf{pk}', \sigma') \leftarrow \mathsf{Adapt}(\boxed{\mathsf{pk}_{b\oplus 1}}, m^*, \tilde{\sigma}, \mathsf{h})$
$x \leftarrow \mathsf{G}(\mathsf{pk}', \sigma', m^*)$, $(\tau, \omega) \leftarrow \mathsf{SAV.ProbGen}(x)$

Transition - Game 1 → Game 2: Also this change in conceptual and $\mathsf{Prob}\,[\mathsf{W}_1]$=$\mathsf{Prob}\,[\mathsf{W}_2]$. To see why, recall that by definition of adaptability the output of $\mathsf{Adapt}(\mathsf{pk}, m, \sigma, \mathsf{h}) \to (\mathsf{pk}', \sigma')$ has the same distribution as $(\mathsf{pk} \cdot \mu(\mathsf{h}), \mathsf{Sign}(\mathsf{sk} + \mathsf{h}, m))$. Thus, in Game 2, σ' is actually a signature for m^* under the public key $\mathsf{pk}' = \mathsf{pk}_b \cdot \big(\mathsf{pk}_{b\oplus 1} \cdot \mu(\mathsf{h})\big)$. Since $\mathbb{H}$ is abelian, we can write pk' also as $\mathsf{pk}' = \mathsf{pk}_{b\oplus 1} \cdot \big(\mathsf{pk}_b \cdot \mu(\mathsf{h})\big) = \mathsf{pk}_{b\oplus 1} \cdot \mu(\mathsf{h}')$, for some $\mathsf{h}' \in \mathbb{H}$. Under adaptability, this change is conceptual: the previous equalities show that σ' is a signature adapted from pk_b but it can also be a signature adapted from $\mathsf{pk}_{b\oplus 1}$. Distinguishing between the two cases implies guessing the shift amount h chosen by the challenger, which leads to unconditional SAV-anonymity.

B Detailed descriptions of our SAV schemes

In this Appendix we present thorough descriptions of the new SAV scheme proposed in this paper (Section 6). The complete explanations of the algorithms in $\mathsf{SAV}^{\mathsf{CDS}_1}_{\mathsf{BLS}}$, $\mathsf{SAV}^{\mathsf{CDS}_1}_{\mathsf{Wat}}$ and $\mathsf{SAV}^{\mathsf{CDS}_2}_{\mathsf{CL}}$ are presented in Figures 4, 5 and 6 respectively.

For consistency, we adopt the multiplicative notation for describing the operation elliptic curve groups.

$\mathsf{SAV.Init}(1^\lambda) = \mathsf{SetUp}_{\mathsf{BLS}}(1^\lambda)$. This algorithm generates the global parameters of the scheme, that include: a Gap Diffie-Hellman bilinear group $(p, g, \mathbb{G}, \mathbb{G}_T, e)$ according to the security parameter λ; and a hash function $H : \{0,1\}^* \to \mathbb{G}$ that maps messages $m \in \mathcal{M} = \{0,1\}^*$ to group elements in $\mathbb{G}$. The output is $\mathsf{gp} = (p, g, H, \mathbb{G}, \mathbb{G}_T, e)$.
$\mathsf{SAV.KeyGen}() = \mathsf{KeyGen}_{\mathsf{BLS}}()$. The key generation algorithm draws a random $s \xleftarrow{R} \mathbb{Z}_p^*$ and outputs $(\mathsf{pk}, \mathsf{sk}) = (g^s, s)$.
$\mathsf{SAV.VSetup}() = \mathsf{KeyGen}^{\mathsf{CDS}_1}()$. This algorithm outputs $\mathsf{pr} = \mathsf{void}$ and $\mathsf{pb} = (p, \mathbb{G}, \mathbb{G}_T, e, g, \hat{\beta})$, where $\hat{\beta} = e(g, g)$.
$\mathsf{SAV.Sign}(\mathsf{sk}, m) = \mathsf{Sign}_{\mathsf{BLS}}(\mathsf{sk}, m)$. The signing algorithm outputs $\sigma = H(m)^s \in \mathbb{G}$.
$\mathsf{SAV.ProbGen}(\mathsf{void}, \mathsf{pk}, m, \sigma)$. This algorithm runs $\mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pk}, m, \sigma) \to \big((\mathsf{pk}, H(m)), (\sigma, g)\big)$ and returns the outputs of $\mathsf{ProbGen}^{\mathsf{CDS}_1}$ on the two pairs $(\mathsf{pk}, H(m))$ and (σ, g). In details, for $(\mathsf{pk}, H(m))$ the problem generator algorithm selects two random values $r_1, r_2 \xleftarrow{R} \mathbb{Z}_p$, computes the points $R_1 = \mathsf{pk}^{r_2^{-1}} g^{r_1}$, $R_2 = H(m)^{r_1^{-1}} g^{r_2}$ and $\hat{U} = \hat{\beta}^{r_1 r_2}$. This process (with fresh randomness) is applied to the pair (σ, g) as well. The final outputs are $\omega = \big((\mathsf{pk}, H(m), R_1^{(1)}, R_2^{(1)}), (\sigma, g, R_1^{(2)}, R_2^{(2)})\big)$ and $\tau = \big((\hat{U}^{(1)}, r_1^{(1)}, r_2^{(1)}), (\hat{U}^{(2)} r_1^{(2)}, r_2^{(2)})\big)$.
$\mathsf{SAV.Comp}(\mathsf{pb}, \omega)$. The algorithm computes the following bilinear pairings: $\alpha_1^{(1)} = e(\mathsf{pk}, H(m))$, $\alpha_2^{(1)} = e(R_1^{(1)}, R_2^{(1)})\big(e(\mathsf{pk}, g) e(g, H(m))\big)^{-1}$, $\alpha_1^{(2)} = e(\sigma, g)$, $\alpha_2^{(2)} = e(R_1^{(2)}, R_2^{(2)})\big(e(\sigma, g) e(g, g)\big)^{-1}$. It returns $\rho = (\rho_1, \rho_2) = \big((\alpha_1^{(1)}, \alpha_2^{(1)}), (\alpha_1^{(2)}, \alpha_2^{(2)})\big)$.
$\mathsf{SAV.Verify}(\mathsf{void}, \mathsf{pk}, m, \sigma, \rho, \tau)$. The verification algorithm first runs $\mathsf{Verify}^{\mathsf{CDS}_1}(\rho_i, \tau_i)$ for $i \in [2]$, *i.e.*, checks whether $\alpha_2^{(i)} = \hat{U}^{(i)} (\alpha_1^{(i)})^{(r_1^{(i)} r_2^{(i)})^{-1}}$ and $\alpha_1 \in \mathbb{G}_T$. If any of the previous checks fails, the verification algorithm returns $\Delta = \perp$ and halts. Otherwise, it sets $y_i = \alpha_1^{(i)}$, for $i \in [2]$ and runs $\mathsf{Ver}_{\mathsf{L}}(\mathsf{pk}, m, \sigma, y)$, which returns $\Delta = 1$ if $y_1 = y_2$, and $\Delta = 0$ otherwise.

Fig. 4. $\mathsf{SAV}^{\mathsf{CDS}_1}_{\mathsf{BLS}}$: Our SAV for the BLS Signature in [3].

$\mathsf{SAV.Init}(1^\lambda) = \mathsf{SetUp}_{\mathsf{CL}}(1^\lambda)$. The setup algorithm generates the global parameters of the scheme, that include a bilinear group $(q, \mathbb{G}, g, \mathbb{G}_T, \hat{g}, e)$.
$\mathsf{SAV.KeyGen}() = \mathsf{KeyGen}_{\mathsf{CL}}()$. The key generation algorithm draws two random values $x, y \xleftarrow{R} \mathbb{Z}_q$, computes $g^x = X$, $g^y = Y$ and returns $\mathsf{pk} = (X, Y)$ and $\mathsf{sk} = (x, y)$.
$\mathsf{SAV.VSetup}() = \mathsf{KeyGen}^{\mathsf{CDS}_2}()$. This algorithm outputs $\mathsf{pr} = \mathsf{void}$ and $\mathsf{pb} = (p, \mathbb{G}, \mathbb{G}_T, e, G, B, \hat{\beta})$, where $G \xleftarrow{R} \mathbb{G}$, $B = g$ and $\hat{\beta} = e(G, B)$.
$\mathsf{SAV.Sign}(\mathsf{sk}, m) = \mathsf{Sign}_{\mathsf{CL}}(\mathsf{sk}, m)$. The sign algorithm picks a random $a \xleftarrow{R} \mathbb{G}$ and outputs the signature $\sigma = (\sigma_1, \sigma_2, \sigma_3) = (a, a^y, a^{x + mxy}) \in \mathbb{G}^3$.
$\mathsf{SAV.ProbGen}(\mathsf{void}, \mathsf{pk}, m, \sigma)$. This algorithm first runs $\mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pk}, m, \sigma) \to (\sigma_2, \sigma_3)$. Then it runs $\mathsf{ProbGen}^{\mathsf{CDS}_2}$ on σ_2 and σ_3. In more details, for $i \in \{2, 3\}$ it selects three random values $r_1^{(i)}, r_2^{(i)}, u^{(i)} \xleftarrow{R} \mathbb{Z}_q$, computes the points $R_1^{(i)} = \sigma_i \cdot G^{r_1^{(i)}}$ and $R_2^{(i)} = \sigma_i^{u^{(i)}} \cdot G^{r_2^{(i)}}$, and calculates $\hat{X}_1^{(i)} = (\hat{\beta})^{r_1^{(i)}}$, $\hat{X}_2^{(i)} = (\hat{\beta})^{r_2^{(i)}}$. The final outputs are $\omega = (R_1^{(2)}, R_2^{(2)}, R_1^{(3)}, R_2^{(3)})$ and $\tau = (u^{(2)}, \hat{X}_1^{(2)}, \hat{X}_2^{(2)}, u^{(3)}, \hat{X}_1^{(3)}, \hat{X}_2^{(3)})$.
$\mathsf{SAV.Comp}(\mathsf{pb}, \omega)$. The algorithm parses $\omega = (R_1^{(2)}, R_2^{(2)}, R_1^{(3)}, R_2^{(3)})$ and returns $\rho = (e(R_1^{(2)}, g), e(R_2^{(2)}, g), e(R_1^{(3)}, g), e(R_2^{(2)}, g))$.
$\mathsf{SAV.Verify}(\mathsf{void}, \mathsf{pk}, m, \sigma, \rho, \tau)$. The verification algorithm first runs $\mathsf{Verify}^{\mathsf{CDS}_2}(\rho, \tau)$, *i.e.*, for $i \in \{2, 3\}$ it checks if $\alpha_2^{(i)} = \hat{X}_2^{(i)} (\alpha_1 (\hat{X}_1^{(i)})^{-1})^u$ and $\alpha_1^{(i)} \in \mathbb{G}_T$. If any of the previous checks fails, the verification algorithm returns $\Delta = \perp$ and halts. Otherwise, the values $y^{(i)} = \beta_1^{(i)} (\hat{X}_1^{(i)})^{-1}$, for $i \in \{2, 3\}$ are used as input for $\mathsf{Ver}_{\mathsf{L}}$. In details, $\mathsf{Ver}_{\mathsf{L}}(\mathsf{pk}, m, \sigma, y = (y^{(2)}, y^{(3)}))$, computes: $\beta_1 = e(\sigma_1, Y)$, $\beta_2 = e(X, \sigma_1 \sigma_2^m)$. If both $\beta_1 = y(1)$ and $\beta_2 = y^{(2)}$, the algorithm returns $\Delta = 1$; otherwise it returns $\Delta = 0$.

Fig. 6. $\mathsf{SAV}^{\mathsf{CDS}_2}_{\mathsf{CL}}$: Our SAV for the CL Signature in [5].

$\mathsf{SAV.Init}(1^\lambda) = \mathsf{SetUp}_{\mathsf{Wat}}(1^\lambda)$. This algorithm generates a bilinear group $(p, g, \mathbb{G}, \mathbb{G}_T, e)$ according to the security parameter λ; selects $n+1$ group elements $V_0, V_1, \ldots V_n \xleftarrow{R} \mathbb{G}$ and defines a function $H : \{0,1\}^n \to \mathbb{G}$ as $H(m) = V_0(\prod_{i=1}^n V_i^{m_i})$. The output is $\mathsf{gp} = (p, g, H, \mathbb{G}, \mathbb{G}_T, e)$.
$\mathsf{SAV.KeyGen}() = \mathsf{KeyGen}_{\mathsf{Wat}}()$. The key generation algorithm draws a random $s \xleftarrow{R} \mathbb{Z}_p^*$ and outputs $(\mathsf{pk}, \mathsf{sk}) = (e(g,g)^s, s)$.
$\mathsf{SAV.VSetup}() = \mathsf{KeyGen}^{\mathsf{CDS}_1}()$. This algorithm outputs $\mathsf{pr} = \mathsf{void}$ and $\mathsf{pb} = (p, \mathbb{G}, \mathbb{G}_T, e, g, \hat{\beta})$, where $\hat{\beta} = e(g,g)$.
$\mathsf{SAV.Sign}(\mathsf{sk}, m) = \mathsf{Sign}_{\mathsf{Wat}}(\mathsf{sk}, m)$. The signing algorithm picks a random $a \xleftarrow{R} \mathbb{Z}_p$ and outputs $\sigma = (\sigma_1, \sigma_2) = (g^s(H(m))^a, g^a) \in \mathbb{G}^2$.
$\mathsf{SAV.ProbGen}(\mathsf{void}, \mathsf{pk}, m, \sigma)$. This algorithm runs $\mathsf{ProbGen}^{\mathsf{PRE}}(\mathsf{pk}, m, \sigma) \to (\mathsf{pk}', \sigma')$ to create a signature for a new public key, *i.e.*, it picks two random values $\mathsf{h}, b \xleftarrow{R} \mathbb{Z}_p$ and sets $\mathsf{pk}' = \mathsf{pk}\hat{\beta}^{\mathsf{h}}$, $\sigma' = (g^{\mathsf{h}}\sigma_1 H(m)^b, \sigma_2 g^b)$. *(By the adaptivity of* Wat *if σ is a valid signature for m under* sk *with randomness a, then σ' is a valid signature for m under* $\mathsf{sk}' + \mathsf{h}$ *with randomness $a + b$).*
Secondly, the problem generation algorithm runs $\mathsf{ProbGen}^{\mathsf{CDS}_1}$ on (σ_1', g) and $(H(m), \sigma_2')$. In details, for each pair (A, B), the algorithm selects two random values $r_1, r_2 \xleftarrow{R} \mathbb{Z}_p$, computes the points $R_1 = A^{r_2^{-1}} g^{r_1}$, $R_2 = B^{r_1^{-1}} g^{r_2}$ and $\hat{U} = \hat{\beta}^{r_1 r_2}$. The final outputs are $\omega = (R_1^{(1)}, R_2^{(1)}, R_1^{(2)}, R_2^{(2)})$ and $\tau = (\mathsf{pk}'\hat{U}^{(1)}, r_1^{(1)}, r_2^{(1)}, \hat{U}^{(2)} r_1^{(2)}, r_2^{(2)})$.
$\mathsf{SAV.Comp}(\mathsf{pb}, \omega)$. The algorithm parses ω as $\big((R_1^{(1)}, R_2^{(1)}), (R_1^{(2)}, R_2^{(2)})\big)$; for each pair (A, B) it computes $\alpha_1 = e(A, B)$ and $\alpha_2 = e(R_1, R_2)\big(e(g, B), e(A, g)\big)^{-1}$. It returns $\rho = (\alpha_1^{(1)}, \alpha_2^{(1)}, \alpha_1^{(2)}, \alpha_2^{(2)})$.
$\mathsf{SAV.Verify}(\mathsf{void}, \mathsf{pk}, m, \sigma, \rho, \tau)$. The verification algorithm parses $\rho = (\rho^{(1)}, \rho^{(2)}) = \big((\alpha_1^{(1)}, \alpha_2^{(1)}), (\alpha_1^{(2)}, \alpha_2^{(2)})\big)$ and $\tau = (\mathsf{pk}', \tau^{(1)}, \tau^{(2)}) = \big((\hat{U}^{(1)}, r_1^{(1)}, r_2^{(1)}), (\hat{U}^{(2)} r_1^{(2)}, r_2^{(2)})\big)$. For $i \in [2]$ it runs $\mathsf{Verify}^{\mathsf{CDS}_2}(\rho^{(i)}, \tau^{(i)})$, *i.e.*, it checks if $\alpha_2^{(i)} = \hat{U}^{(i)}(\alpha_1^{(i)})^{(r_1^{(i)} r_2^{(i)})^{-1}}$ and $\alpha_1 \in \mathbb{G}_T$. If any of the previous checks fails, the verification algorithm returns $\Delta = \perp$ and halts. Otherwise, it returns $y^{(i)} = \alpha_1^{(i)}$ and runs $\mathsf{Ver}_{\mathsf{L}}(\mathsf{pk}, m, \sigma, y)$, which returns $\Delta = 1$ if $y^{(1)} = \mathsf{pk}'\, y^{(2)}$, and $\Delta = 0$ otherwise.

Fig. 5. $\mathsf{SAV}_{\mathsf{Wat}}^{\mathsf{CDS}_1}$: Our SAV for the Wat Signature in [23].

C New attacks against previous works

In this Appendix, we review the main existing works on SAV and provide new attacks against existing schemes.

C.1 (Extended) Existential/Strong Forgeability of [15,25]

Chow *et al.* proved that Protocol II (Figure 5 in [24]) is not existentially unforgeable [8]. In what follows we show that: Protocol III (Figure 4 in [25]) is not existentially unforgeable; Protocol I (Figure 3 in [25]) is not *extended* existentially unforgeable; and SAV-ZSS [15] (depicted in Figure 1 in [25]) is not extended *strongly* unforgeable.

Protocol III is a SAV for the Wat signature. Despite what claimed in [25], this scheme is not existentially unforgeable according to Definition 9. We adapt the notation used in [25] and show a very simple attack strategy to produce type-1a forgeries against Protocol III. Let the adversary select a random message $m^* \xleftarrow{R} \{0,1\}^n$ and two group elements ${\sigma_1}^*, {\sigma_2}^* \xleftarrow{R} \mathbb{G}$. Let $(m^*, \sigma^* = ({\sigma_1}^*, {\sigma_2}^*))$ be the challenge pair. By construction the challenger returns to the adversary $\hat{\omega} = (m^*, \sigma_1', {\sigma_2}^*)$, where $\sigma_1' = {\sigma_1}^* g^r$ for a randomly chosen $r \xleftarrow{R} \mathbb{H}$. The adversary can now use ${\sigma_1}^*$ to compute g^r as $g^r = \frac{\sigma_1'}{{\sigma_1}^*}$. At this point, $\mathcal{A}$ sets $K_2^* = \mathsf{pk}e(g, g^r)$, $K_3^* = 1$ and outputs $(m^*, \sigma^*, \rho^* = (K_2^*, K_3^*))$. This is a type-1a forgery. Indeed by bilinearity we have $K_2^* = \mathsf{pk} \cdot 1 \cdot e(g, g^r) = \mathsf{pk} \cdot K_3^* \cdot K_1^r$. We have thus described a successful strategy to make an un-queried message-signature pair verify in the server-aided sense.

The enabler of our attack against Protocol I and SAV-ZSS is the simplistic definition of the SAV.Verify algorithm: in neither of the schemes the verifier can distinguish between an *invalid* signature and a *wrong* value returned by the server. We adapt the notation in [25] and show a successful attack strategy to produce type-2 forgeries. Let the adversary select a random message $m \xleftarrow{R} \mathcal{M}$ and make a *sign* query on m. Denote by σ the returns signature. According to the unforgeability game the pair (m, σ) is valid. Set $(m^*, \sigma^*) = (m, \sigma)$, and output (m^*, σ^*, ρ^*), where $\rho^* \xleftarrow{R} \mathbb{G}_T$. With overwhelming probability $\rho^* \neq e(H(m^*), \mathsf{pk})$, and thus SAV.Verify returns 0 (on $(m^*, \sigma^*) \in L$). The same attack strategy can be employed against the SAV-ZSS scheme by Girault and Lefranc [15].

We describe an attack strategy to produce extended *strong* forgeries against SAV-ZSS (the same idea applies also against Protocol I). With the notation in [25], let the adversary pick a random message $m \xleftarrow{R} \mathcal{M}$ and make a sign query on m in the first query phase. Let σ be the signature returned by the challenger for message m. $\mathcal{A}$ can set as challenge message to be $m^* = m$ and choose a random $\sigma^* \neq \sigma$. After the challenge phase, $\mathcal{A}$ parses $\hat{\omega}=(\sigma^*, R)$, and outputs ($m^*$, σ^*, $\rho^*=e(\sigma, R)$) at the end of the experiment. It is immediate to check that the adversary's output is a type-1b forgery. Indeed, $(m^*, \sigma^*) \notin L$ and the output of SAV.Verify is 1, since the adversary used the correct σ to produce ρ^* (note that this is not a type-1a forgery since $(m^*, \sigma) \in L$).

C.2 Critical review of previous models for collusion attacks

In the seminal work on SAV, Girault and Lefranc [15] addressed the signer-server collusion scenario as "auxiliary non-repudiation". The first formal definition is due to Wu *et al.* in [24], where collusion is seen as a way to increase the adversary's power, allowing $\mathcal{A}$ to produce valid signatures using the signing key sk. The aim is to make SAV.Verify output 1 (valid) for an invalid pair $(m^*, \bar{\sigma})$, where m^* is a message chosen by $\mathcal{A}$, and $\bar{\sigma}$ is a random *invalid* signature provided by the challenger. This model was criticised by Wang *et al.* [22] in two points. First, the leakage of the signing key sk to the malicious server is considered unrealistic and replaced with a forger's key pair $(\mathsf{pk}_f, \mathsf{sk}_f)$. Secondly, Wang *et al.* suggested to let the adversary output both m^* and the signature σ^* – which is no longer an invalid signature produced by the challenger –. Although the approach proposed in [22] gives an interesting twist to the notion of collusion, we retain that in most practical scenarios, the adversary – *i.e.*, the colluding pair malicious signer-server – actually holds the signing key sk. Therefore we prefer to use Chow *et al.*'s model for collusion [8], which builds on Wu *et al.*'s [24].

C.3 New collusion attacks against the soundness of [15,25]

We present a new attack strategy to break the soundness under collusion in SAV-ZSS [15] and Protocol I [25]. The idea is similar to the one presented at the end of Section 4 for type-1b forgeries against SAV-ZSS. We explain the attack for the Protocol I, the procedure for SAV-ZSS is analogous. The adversary picks a random message m^* and a random signature σ^*, to be the challenge pair. With overwhelming probability σ^* is not a valid signature for m^*. Nonetheless, by the correctness of the scheme $\mathsf{SAV.Verify}(\mathsf{pr}, \mathsf{pk}, m^*, \sigma^*, \rho^*, \hat{\tau})$ outputs 1 whenever $\rho^*=e(\sigma, R)$. The adversary can compute ρ^* using $\hat{\omega}=(\sigma^*, R)$ and generating a valid signature for the challenge message $\sigma \leftarrow \mathsf{SAV.Sign}(\mathsf{sk}, m^*)$. Thus the scheme is not sound under collusion.

Our collusion attack against Protocol II [25] uses a slightly different technique. In order to construct a collusion forgery the adversary can pick m^* and σ^* at random. Let $\hat{\omega} = (m^*, \tilde{\sigma}^*, \mathsf{pk})$ be the value returned by the challenger. The adversary can generate the valid signature $\sigma \leftarrow \mathsf{SAV.Sign}(\mathsf{sk}, m^*)$, compute $\frac{\tilde{\sigma}^*}{\sigma^*} \cdot \sigma = \sigma \cdot g^r = \tilde{\sigma}$ and set $\rho^* = (K_1, K_2) = (e(\tilde{\sigma}, R), e(H(m^*), \mathsf{pk}))$. It is trivial to check that $K_1 = K_2 \cdot \hat{\tau}$, since for the BLS signature $\sigma = H(m^*)^{\mathsf{sk}}$ and $\mathsf{pk} = g^{\mathsf{sk}}$.

Finally, we show that Protocol III [25] is not sound against collusion. Let the adversary choose a random message m^* as the challenge message and set $\sigma^* \leftarrow \mathsf{Sign}_{\Sigma}(\mathsf{sk}, m^*)$, $\rho^* = (K_2^*, K_3^*)$ for $K_2^*, K_3^* \xleftarrow{R} \mathbb{G}_T$. By construction σ^* is a valid signature for m^*, thus the output of the server-aided verification should be $\Delta = 1$. However, since the adversary returns random values for the verification, with non-negligible probability it holds that: $K_2^* \neq \mathsf{pk} \cdot K_3^* \cdot e(g, g)^r$. To conclude, we have $\mathsf{SAV.Verify}(\mathsf{pr}, \mathsf{pk}, m^*, \sigma^*, \rho^*, \hat{\tau}) \rightarrow \Delta = 0$ with overwhelming probability, since Protocol III performs no check on the correctness of the results returned by the server.

C.4 Anonymity of [15,25]

We observe that whenever ω contains σ the SAV is trivially not anonymous: $\mathcal{A}$ can output b^* such that $\mathsf{Verify}(\mathsf{pk}_{b^*}, m^*, \sigma) = 1$.

Since in both Protocol I [25] and SAV-ZSS [15] the value outsourced to the server, ω, contains σ, the schemes are not SAV-anonymous.

In Protocol II [25], ω contains pk, and thus $\mathcal{A}$ can easily win the SAV-anonymity experiment by outputting b^* such that $\mathsf{pk}_{b^*} = \mathsf{pk}$.

Protocol III by Wu *et al.* [25] is SAV-anonymous, in this case anonymity follows from the fact that the verifier adapts the given signature before sending it to the server (Theorem 4).

D Digital Signatures (security notions and schemes)

In what follows, we recall the fundamental definition of a correct signature scheme and give the detailed description of two signature schemes that we turn into $\mathsf{SAV}^{\Gamma}_{\Sigma}$ in the paper, as well as standard security definitions for signature schemes.

Definition 15 (Completeness). *A signature scheme Σ is said to be ε-**complete** if $\forall\, \lambda \in \mathbb{N}$, $\forall \mathsf{gp} \leftarrow \mathsf{SetUp}(1^\lambda)$, all pairs $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}()$ and for all possible messages $m \in \mathcal{M}$, it holds that:*

$$\mathsf{Prob}\left[\mathsf{Verify}\big(\mathsf{gp}, \mathsf{pk}, m, \mathsf{Sign}(\mathsf{gp}, \mathsf{sk}, m)\big) = 1\right] \geq 1 - \varepsilon.$$

D.1 Unforgeability and Anonymity

We present the security notions in a compact notation using experiments and oracles. In particular, $\mathcal{OS}ign$ denotes the signing oracle, which holds the secret key sk and on input a message m returns $\sigma \leftarrow \mathsf{Sign}(\mathsf{gp}, \mathsf{sk}, m)$. The notation $\mathcal{A}^{\mathcal{OS}ign}$ denotes the interaction between the adversary $\mathcal{A}$ and the signing oracle.

We present two flavours of unforgeability: existential and strong.

Definition 16 (Existential Unforgeability [4]). *A digital signature scheme Σ is said to be (ε, q_s)-existential unforgeable* (EUF) *against adaptive chosen message attacks if for any PPT adversary $\mathcal{A}$ it holds that:*

$$\mathsf{Prob}\left[\mathbf{Exp}^{\mathsf{EUF}}_{\mathcal{A}}[\Sigma] = 1\right] < \varepsilon\ .$$

Experiment 1 ($\mathbf{Exp}^{\mathsf{EUF}}_{\mathcal{A}}[\Sigma]$)

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}()$
for $i = 1, \ldots, q_s$
  $x_i \leftarrow \mathcal{A}^{\mathcal{OS}ign(\mathsf{sk},\cdot)}(\mathsf{pk}, \{(x_j, \sigma_j)\}_{j=1}^{i-1})$
  $(m^*, \sigma^*) \leftarrow \mathcal{A}(\mathsf{pk}, \{(x_j, \sigma_j)\}_{j=1}^{q_s})$
if (1)$\mathsf{Verify}(\mathsf{pk}, m^*, \sigma^*) = 1$ and
  (2)$(m^*, \cdot) \notin \{(x_j, \sigma_j)\}_{j=1}^{q_s}$
return 1, else return 0.

Intuitively, existential unforgeability requires that the verification algorithm does not accept signatures that are not generated in an honest way. It is important to notice that the winning condition includes a *new* message: indeed m^* should not be among the queried messages. Strong unforgeability extends EUF to also ensure that the adversary cannot modify (*e.g.*, re-randomising) a signature obtained in the query phase and output a *new* valid signature on the same message [4].

Definition 17 (Strong Existential Unforgeability [4]). *A digital signature scheme Σ is said to be (ε, q_s)-strongly existential unforgeable against adaptive chosen message attacks if for any PPT adversary $\mathcal{A}$ it holds that:*

$$\mathsf{Prob}\left[\mathbf{Exp}^{\mathsf{SEUF}}_{\mathcal{A}}[\Sigma] = 1\right] < \varepsilon\ .$$

Experiment 2 ($\mathbf{Exp}^{\mathsf{SEUF}}_{\mathcal{A}}[\Sigma]$)

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}()$
for $i = 1, \ldots, q_s$
  $x_i \leftarrow \mathcal{A}^{\mathcal{OS}ign(\mathsf{sk},\cdot)}(\mathsf{pk}, \{(x_j, \sigma_j)\}_{j=1}^{i-1})$
  $(m^*, \sigma^*) \leftarrow \mathcal{A}(\mathsf{pk}, \{(x_j, \sigma_j)\}_{j=1}^{q_s})$
if (1)$\mathsf{Verify}(\mathsf{pk}, m^*, \sigma^*) = 1$ and
  (2a)$(m^*, \cdot) \notin \{(x_j, \sigma_j)\}_{j=1}^{q_s}$ or
  (2b)$(m^*, \sigma^*) \notin \{(x_j, \sigma_j)\}_{j=1}^{q_s}$
return 1, else return 0.

The concept of anonymous signatures was introduced in 2006 by Yang *et al.* [26]. As the name suggests, the main feature of anonymous signatures is to hide the identity of the signer when only the signature σ is known. In this case, we modify the signing oracle as follows. $\mathcal{OS}ign$ now holds two secret keys $\mathsf{sk}_0, \mathsf{sk}_1$; on input a message m and an identifier for the identity of the signer, *e.g.*, $b_i \in \{0, 1\}$ $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_{b_i}, m)$.

Definition 18 (Anonymity [26]). *A digital signature scheme Σ is said to be (ε, q_s)-***anonymous** *if for any PPT adversary $\mathcal{A}$ it holds that:*

$$\left| \mathsf{Prob}\left[\mathbf{Exp}^{\text{anon}}_{\mathcal{A}}[\Sigma] = 1\right] - \frac{1}{2} \right| < \varepsilon \ .$$

Experiment 3 ($\mathbf{Exp}^{\text{anon}}_{\mathcal{A}}[\Sigma]$)
$(\mathsf{pk}_0, \mathsf{sk}_0) \leftarrow \mathsf{KeyGen}()$
$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \mathsf{KeyGen}()$
for $i = 1, \ldots, q_s$
$x_i \leftarrow \mathcal{A}^{\mathcal{OS}ign(\mathsf{sk}_0, \mathsf{sk}_1, \cdot, \cdot)}(\mathsf{pk}_0, \mathsf{pk}_1, \{(x_j, \sigma_j)\}_{j=1}^{i-1})$
$b \xleftarrow{R} \{0,1\}, m \xleftarrow{R} \mathcal{M}$
$\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_b, m)$
$b' \leftarrow \mathcal{A}^{\mathcal{OS}ign(\mathsf{sk}_0, \mathsf{sk}_1, \cdot, \cdot)}(\sigma)$
if $b' = b$ output 1, else output 0.

Definition 18 is the one given in [26] for static security. Anonymity holds as long as the challenge message is not revealed to the adversary. Otherwise, the adversary could simply run the public algorithm $\mathsf{Verify}(\mathsf{pk}_1, m, \sigma) \rightarrow \mathsf{b}$ and determine the identity of the signer according to the value of $\mathsf{b} = b'$.

Lemma 1. *The* CL *signature scheme in [5] is not anonymous.*

Proof. We need to show that an adversary $\mathcal{A}$ who possesses the two public keys $\mathsf{pk}_0 = (X_0, Y_0)$ and $\mathsf{pk}_1 = (X_1, Y_1)$ and a signature $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ on an unknown message, has non-negligible probability in determining the identity $b \in \{0,1\}$ of the signer of σ. Consider the equation $e(\sigma_1, Y_0) = e(\sigma_2, g)$, *i.e.*, $e(a, g^{y_0}) = e(a^{y_b}, g)$ for a random value $a \xleftarrow{R} \mathbb{G}$. If the equality does not hold, the adversary outputs the guess $b' = 1$, otherwise, it outputs $b' = 0$. It is immediate that using the previous strategy $\mathcal{A}$ wins the anonymity game with overwhelming probability.

E Security notions in verifiable computation

In what follows, we collect the basic properties of verifiable computation schemes.

Definition 19 (Correctness). *A* VC *scheme is said to be* ***correct*** *if $\forall f$ and $\forall x$, given $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\lambda, f)$, $(\omega_x, \tau_x) \leftarrow \mathsf{ProbGen}(\mathsf{sk}, x)$ and $\omega_y \leftarrow \mathsf{Comp}(\mathsf{pk}, \omega_x)$, then $\mathsf{Verify}(\mathsf{sk}, \tau_x, \omega_y) \rightarrow y$ with $y = f(x) \neq \perp$, holds with all-but negligible probability.*

Below we report the notions of security ($\mathbf{Exp}^{\text{verif}}_{\mathcal{A}}$[VC] [2]) and privacy ($\mathbf{Exp}^{\text{priv}}_{\mathcal{A}}$[VC] [12]) for a verifiable computation scheme. Note that the adopted security models allow for verification queries (which were not considered in the seminal work [14]). Intuitively, a verifiable computation scheme is secure if a malicious server (the *worker*) cannot succeed in persuading the verifier to accept an incorrect output. More formally,

Experiment 4 ($\mathbf{Exp}^{\mathsf{verif}}_{\mathcal{A}}$[VC, f ,$\lambda$])

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\lambda, f)$
for $i = 1, \ldots, \ell = q_v = poly(\lambda)$
$x_i \leftarrow \mathcal{A}(\mathsf{pk}, \{(x_j, \omega_{x_j}, y_j)\}_{j=1}^{i-1})$
$(\omega_{x_i}, \tau_{x_i}) \leftarrow \mathsf{ProbGen}(\mathsf{sk}, x_i)$
$\omega_{y_i} \leftarrow \mathcal{A}(\mathsf{pk}, \{(x_j, \omega_{x_j}, y_j)\}_{j=1}^{i})$
$y_i \leftarrow \mathsf{Verify}(\mathsf{sk}, \tau_{x_i}, \omega_{y_i})$
$\hat{x} \leftarrow \mathcal{A}(\mathsf{pk}, \{(x_j, \omega_{x_j}, y_j)\}_{j=1}^{\ell})$
$(\omega_{\hat{x}}, \tau_{\hat{x}}) \leftarrow \mathsf{ProbGen}(\mathsf{sk}, \hat{x})$
set $\mathsf{aux} = \{\hat{x}, \omega_{\hat{x}}, \mathsf{pk}, \{(x_j, \omega_{x_j}, y_j)\}_{j=1}^{\ell}\}$
for $i = 1, \ldots, \ell = q_v = poly(\lambda)$
$\omega_{y'_i} \leftarrow \mathcal{A}(\mathsf{aux}, \{(\omega_{y'_j}, y'_j)\}_{j=1}^{i-1})$
$y'_i \leftarrow \mathsf{Verify}(\mathsf{sk}, \tau_{\hat{x}}, \omega_{y'_i})$
$\omega^*_{\hat{y}} \leftarrow \mathcal{A}(\mathsf{aux}, \{(\omega_{y'_j}, y'_j)\}_{j=1}^{\ell})$
$y^* \leftarrow \mathsf{Verify}(\mathsf{sk}, \tau_{\hat{x}}, \omega^*_{\hat{y}})$
if $y^* \neq \perp$ and $y^* \neq f(x)$
return 1, else return 0.

Definition 20 (Security). *A verifiable computation scheme Γ is (ε, q_v)-secure for a function f if for any probabilistic polynomial time adversary $\mathcal{A}$ it holds that:*

$$\mathsf{Prob}\left[\mathbf{Exp}^{\text{verify}}_{\mathcal{A}}[\Gamma, f, \lambda] = 1\right] \leq \varepsilon \ .$$

The notion of privacy for a verifiable computation scheme essentially states that if the algorithm ProbGen is run on two different inputs, the corresponding two public outputs are indistinguishable to a malicious server. More formally,

Definition 21 (Private). *A verifiable computation scheme Γ is (ε,q_v)-private for a function f if for any probabilistic polynomial time adversary $\mathcal{A}$ it holds that:*

$$\mathsf{Prob}\left[\mathbf{Exp}^{\mathrm{priv}}_{\mathcal{A}}[\mathsf{VC},\, f,\, \lambda] = 1\right] \leq \tfrac{1}{2} + \varepsilon.$$

The privacy experiment reported below is an adaptation to our notation of the definition given by Fiore *et al.* in [12]. We define a function **Bool** to simulate the *public verification output* of a VC scheme, *i.e.*, $\mathbf{Bool}(y \neq \perp)$ returns 1 if y differs from the rejection value $\perp$, and 0 otherwise.

Experiment 5 ($\mathbf{Exp}^{\mathsf{priv}}_{\mathcal{A}}[\mathsf{VC},\, f,\, \lambda]$)

$b \xleftarrow{R} \{0,1\}$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\lambda, f)$
for $i = 1, \ldots, \ell = q_v = poly(\lambda)$
  $x_i \leftarrow \mathcal{A}(\mathsf{pk}, \{(x_j, \omega_{x_j}, \beta_j)\}_{j=1}^{i-1})$
  $(\omega_{x_i}, \tau_{x_i}) \leftarrow \mathsf{ProbGen}(\mathsf{sk}, x_i)$
  $\omega_{y_i} \leftarrow \mathcal{A}(\mathsf{pk}, \{(x_j, \omega_{x_j}, \beta_j)\}_{j=1}^{i})$
  $y_i \leftarrow \mathsf{Verify}(\mathsf{sk}, \tau_{x_i}, \omega_{y_i})$
  $\beta_i \leftarrow \mathbf{Bool}(y_i \neq \perp)$
$(\hat{x}_0, \hat{x}_1) \leftarrow \mathcal{A}(\mathsf{pk}, \{(x_j, \omega_{x_j}, \beta_j)\}_{j=1}^{\ell})$
$(\omega_{\hat{x}_0}, \tau_{\hat{x}_0}) \leftarrow \mathsf{ProbGen}(\mathsf{sk}, \hat{x}_0)$
$(\omega_{\hat{x}_1}, \tau_{\hat{x}_1}) \leftarrow \mathsf{ProbGen}(\mathsf{sk}, \hat{x}_1)$
set $\mathsf{aux} = \{\hat{x}_0, \hat{x}_1, \omega_{\hat{x}_b}, \mathsf{pk}, \{(x_j, \omega_{x_j}, \beta_j)\}_{j=1}^{\ell}\}$
for $i = 1, \ldots, \ell = q_v = poly(\lambda)$
  $x'_i \leftarrow \mathcal{A}(\mathsf{aux}, \{(x'_j, \omega_{x'_j}, \beta'_j)\}_{j=1}^{i-1})$
  $(\omega_{x'_i}, \tau_{x'_i}) \leftarrow \mathsf{ProbGen}(\mathsf{sk}, x'_i)$
  $\omega_{y'_i} \leftarrow \mathcal{A}(\mathsf{aux}, \{(x'_j, \omega_{x'_j}, \beta'_j)\}_{j=1}^{i})$
  $y_i \leftarrow \mathsf{Verify}(\mathsf{sk}, \tau_{x_i}, \omega_{y_i})$
  $\beta_i \leftarrow \mathbf{Bool}(y_i \neq \perp)$
$b' \leftarrow \mathcal{A}(\mathsf{aux}, \{(x'_j, \omega_{x'_j}, \beta'_j)\}_{j=1}^{\ell})$
  if $b' = b$ output 1, else output 0.