Oblivious Transfer from weakly Random Self-Reducible Public-Key Cryptosystem

Claude Crépeau *, Raza Ali Kazmi *

McGiLL University
crepeau@cs.mcgill.ca, raza-ali.kazmi@mail.mcgill.ca

Abstract. In this work, we define a new notion of *weakly Random-Self-Reducibile* cryptosystems and show how it can be used to implement secure Oblivious Transfer. We also show that two recent (Post-quantum) cryptosystems (based on Learning with errors and Approximate Integer GCD) can be considered as weakly Random-Self-Reducible.

1 Introduction

An oblivious transfer is a protocol by which a sender transfers one of many pieces of information to a receiver, but remains oblivious as to which piece has been transferred. The early implementations of Oblivious Transfer of Rabin [1], and Even, Goldreich and Lempel [2] were very innovative but did not offer very strong security. The very first OT protocols that may be considered secure were introduced by Ficher, Micali and Rackoff [3], and Berger, Peralta and Tedrick [4].

Later, two methodologies where introduced. A first set of results by Brassard, Crépeau and Robert [18] relied on *Random-Self-Reducibility* (**RSR** for short) of certain number theoretic assumptions such as the Quadratic Residuosity assumption, the RSA assumption or the Discrete log assumption. These results were not extended to very general computational assumptions because the **RSR** property, which was at the heart of the construction, is not very common. In a second set of results by Goldreich, Micali and Wigderson [19], secure Oblivious Transfer protocols were constructed from the generic assumption that (enhanced)[1] Trap-door One-Way permutations exist.

Unfortunately, all constructions that are used to implement secure OT under either of these methodologies fall apart when faced with a quantum computer [5]: none of the so-called Post-Quantum Cryptosystems can directly implement secure OT under these methodologies. Nevertheless, some small modifications to the GMW methodology have led to proposals for OT under the Learning with error LWE assumption [6]. Similarily, Dowsley, van de Graaf, Müller-Quade and Nascimento [7] as well as Kobara, Morozov and Overbeck [8] have proposed Oblivious Transfer protocols based on assumptions related to the McEliece public-key cryptosystem [9]. Both of these papers use generalization of the GMW methodology. However both of them also require an extra computational assumption on top of McEliece's to conclude security. Those were the first proposals for OT protocols believed secure against a quantum computer[2].

* Supported in part by Québec's FQRNT, Canada's NSERC, CIFAR, and QuantumWorks.

[1] The enhanced property is not very restrictive, but some examples of candidates Trap-door One-Way permutations seem to escape it [20].

[2] Earlier results accomplished a similar security level using only a One-Way function and Quantum Communication. The motivation of the papers cited above and of the current work is to avoid quantum communication altogether [10].

More recently, a new methodology has been proposed by Peikert, Vaikuntanathan and Waters [6] using the notion of dual-mode cryptosystems. Their approach can be instantiated using a couple number theoretic assumptions, and LWE in the Post-Quantum case. However, this methodology does not seems to extend to any other post-quantum assumptions such as Approximate Integer GCD, for instance.

In this chapter, we first formalize the results by Brassard, Crépeau and Robert [18] which relied on the **RSR** property of certain number theoretic assumptions (we now have five candidates) in order to introduce a new notion of weakly random-self-reducible encryption scheme **wRSR**. We then show how it is possible to construct a secure Oblivious Transfer under the sole assumption that a secure **wRSR** encryption scheme exists. We show that encryption schemes from two (Post-Quantum) computational assumptions, LWE [17] and AIGCD [13], have this weaker property. We hope that in the future, our methodology may be used for various new computational assumptions as well.

2 Previous work

Random Self-Reducible Encryption Scheme

Informally speaking an encryption scheme is Random-Self-Reducible (**RSR**) if an arbitrary ciphertext c may be efficiently transformed to a uniformly distributed ciphertext c' by a user who only knows the public-key from that system. Moreover, upon learning the decryption m' of c', the user is able to efficiently compute m, the decryption of c, from knowledge of the relation between c and c'.

RSR encryption schemes are generally implemented from a homomorphic encryption scheme. Notice however that the **RSR** property is very strong in its uniformity requirement. Homomorphic encryption schemes may fail to satisfy that extra constraint completely. It is worth mentioning that a fully homomorphic circuit private encryption scheme (see [12–16]) is inherently a **RSR** encryption scheme. However, to guarantee that the homomorphic property is used properly extra work would be required, using Zero-knowledge proofs for instance. In the end, this approach also works but the overhead is similar to ours, while the computational assumptions to obtain fully homomorphic encryption schemes are significantly stronger than ours (see section 6.4).

OT from Random-Self-Reducible encryption schemes

Brassard, Crépeau and Robert [18] showed how zero-knowledge protocols may be combined with Random-Self-Reducible assumptions such as Quadratic Residuosity or RSA to obtain a secure 1-out-of-n OT. The latter has the following structure: a sender encrypts n secret messages using its own public-key cryptosystem; the receiver, upon reception of these n encryptions, picks one of them at its choosing and randomizes it using the **RSR** property of the cryptosystem; the sender receives a ciphertext that could equally come from any of the original encryptions; its decryption is obtained from the sender and returned to the receiver; the receiver obtains its chosen message from the decrypted message and the randomness involved in its self-reduction. Zero-knowledge proofs are used to make sure the receiver constructed the random ciphertext properly.

OT from trap-door one-way permutations

In an effort to obtain OT from a more general assumption, an alternate approach was introduced by Goldreich, Micali and Wigderson [19]. Suppose the sender knows the trap-door to a one-way permutation. The receiver constructs two messages from the domain of the permutation, one using the one-way algorithm, the other sampling directly from the image. Using the trap-door, the sender will find the pre-image of both of these elements and use them to transmit two messages. The receiver who knows only one pre-image, is able to recover only one of the two messages. Zero-knowledge proofs are used to make sure the receiver does not know the pre-image of both.

It was realized many years after the fact that not all trap-door one-way permutations could be used in the above protocol, because it is not always easy to sample from the image without knowing a pre-image [20]. Thus, the notion of *enhanced* trap-door one-way permutation was introduced to remedy to this difficulty. Worth noticing is the work of Haitner [21] who weakened the requirements to implement OT using a collection of dense trapdoor permutations.

Bit Commitments and Zero-Knowledge protocols

Under the assumption that we have a One-Way Function, it is possible to get a statistically binding, computationally concealing Bit Commitment scheme by the general constructions of Håstad, Impegliazzo, Levin and Luby's [22] and Naor [23]. These constructions and their proofs of security are also valid when the adversary is a quantum computer.[3] In this paper, ZK protocols will be used to prove that certain values are constructed properly from a public-key. Invoking general techniques developed in [24] and [25], we can prove any relation among committed bits in a computational zero-knowledge fashion.

Both parties may publish a public-key using a similar computational assumption, use its own to construct a Bit Commitment Scheme and prove arbitrary polynomially verifiable statements about its commitments.

Compairasion with Homomorphic Cryptosystems

The notions of **RSR** and **wRSR** cryptosystems are in some sense similar to that of Homomorphic Cryptosystems. Part of the **wRSR** properties are usually implemented using the Homomorphic property of their related cryptosystem. However, contrary to general constructions such as Fully Homomorphic Cryptosystems where *two* homomorphic operations are necessary, **wRSR** relies on a single operation. Moreover, **wRSR** does not need the cryptosystem to tolerate application of several successive homomorphic operations in a row, which is typical of constructions for Fully Homomorphic Encryptions. As a result, and although we use similar assumptions (LWE [17] and AIGCD [13]) as constructions for Fully Homomorphic Encryptions, the versions of these assumptions we need are actually *weaker* than theirs. In the end, it is more likely that our assumptions are hard.

[3] Under the same assumption, it is also possible to get a computationally binding, statistically concealing, Bit Commitment scheme by the general construction of Haitner, Nguyen, Ong, Reingold,and Vadhan [26]. However their proof technique does not appear to extend to quantum adversaries.

3 Background material

Notations

We denote a vector v by lower-case bold letters $\mathbf{v}$ and matrices by upper-case bold letters $\mathbf{V}$. We denote the Euclidean norm of a vector $\mathbf{v}$ by $\|\mathbf{v}\|_2$, the largest entry (in absolute value) of a vector or a matrix is denoted by $\|\mathbf{v}\|_\infty$ or $\|\mathbf{V}\|_\infty$ and $\lfloor x \rceil$ denote the nearest integer to x. We denote ϵ the empty string.

Gaussian distribution and standard tail inequality

For any $\beta \geq 0$ the *Gaussian distribution* with mean 0 is the distribution on $\mathbb{R}$ having density function $D_\beta(x) = \frac{1}{\beta}\exp(-\pi(x/\beta)^2)$, for all $x \in \mathbb{R}$.

A random variable with normal distribution, lies within $\pm\frac{t\cdot\beta}{\sqrt{2\pi}}$ of its mean, except with probability at most $\frac{1}{t}\cdot\exp(-t^2/2)$.

For any integer $q \geq 2$, the *discrete Gaussian distribution* $\overline{\psi}_\beta(q)$ over $\mathbb{Z}_q$ with mean 0 and standard deviation $\pm\frac{q\cdot\beta}{\sqrt{2\pi}}$ is obtained by drawing $y \leftarrow D_\beta$ and outputting $\lfloor q\cdot y \rceil \pmod q$.

$\binom{2}{1}$-Oblivious Transfer

A One-out-of-Two Oblivious Transfer denoted as $\binom{2}{1}$-OT, is a protocol in which a sender inputs two ordered bits b_0, b_1 and a receiver inputs a choice bit c. The protocol sends b_c to the receiver, without the sender learning c, while the receiver learns nothing other than b_c. A full definition of the security of oblivious transfer can be obtained from the work of [20].

4 Random Self-Reducible Encryption Scheme

In this section we formalize the definition of **RSR** encryption schemes. We further show that two number theoretic schemes satisfy this property.

Definition 1 *Let $\xi = (KeyGen, Enc, Dec, \mathcal{M}, \mathcal{C})$ be a public-key cryptosystem and λ be the security parameter. The cryptosystem ξ is random-self-reducible if there exists a set $\widehat{\mathcal{M}}$, a pair of probabilistic polynomial-time algorithms $(\mathcal{S}, \mathcal{S}')$, together with a polynomial-time algorithm $\widehat{Dec}$, such that for a key pair $(sk, pk) \leftarrow KeyGen(1^\lambda)$ and uniformly picked string $\mathbf{R}$ from $\widehat{\mathcal{M}}$,*

1. *$\mathcal{S}_{pk} : \widehat{\mathcal{M}} \times \mathcal{C} \to \mathcal{C}$, $\mathcal{S}'_{pk} : \widehat{\mathcal{M}} \times \widehat{\mathcal{M}} \to \mathcal{M}$, and $\widehat{Dec}_{sk} : \mathcal{C} \to \widehat{\mathcal{M}}$,*
2. *$\mathcal{S}_{pk}(\mathbf{R}, c)$ is uniformly distributed over $\mathcal{C}$, for all $c \in \mathcal{C}$,*
3. *$\mathcal{S}'_{pk}(\mathbf{R}, \widehat{Dec}_{sk}(\mathcal{S}_{pk}(\mathbf{R}, Enc_{pk}(m)))) = m$, for all messages $m \in \mathcal{M}$.*

Examples of RSRCryptosystem There are several cryptosystems that satisfy **RSR** property for example the RSA [27], Micali-Goldwasser [28], Paillier cryptosystems [32], Elgamal [29], Elliptic curve [30] are all random self-reducible. We give details of the first two:

Goldwasser-Micali Cryptosystem Let (x, n) and (p, q) denote the public/private keys and (Enc, Dec) denote the encryption/decryption algorithms.

1. $\widehat{\mathcal{M}} = \{0, 1\}$, $\widehat{Dec} = Dec$
2. $\mathcal{S}_{pk}(\mathbf{R}, Enc(b)) = Enc(\mathbf{R}) \cdot Enc(b) \bmod n = Enc(\mathbf{R} \oplus b)$, where bit $\mathbf{R}$ is uniformly chosen.
3. $\mathcal{S}'_{pk}(\mathbf{R}, b) = \mathbf{R} \oplus b$.

Semantically secure RSA Cryptosystem Let (e, n) and d denote the public/private keys and $\left(Enc := \left(lsb^{-1}(b)\right)^e \bmod n, Dec := lsb(m^d \mod n)\right)$ denote the encryption/decryption algorithms, where $lsb^{-1}(b)$ is a random element r in $\mathbb{Z}_n^*$ such that $lsb(r) = b$.

1. $\widehat{\mathcal{M}} = \mathbb{Z}_n^*$, $\widehat{Dec}(m) = m^d \mod n$
2. $\mathcal{S}_{pk}(\mathbf{R}, Enc(b)) = \mathbf{R}^e \cdot Enc(b) \bmod n = \left(\mathbf{R} \cdot lsb^{-1}(b)\right)^e \bmod n$ where $\mathbf{R}$ is uniformly chosen from the message space $\widehat{M}$.
3. $\mathcal{S}'_{pk}(\mathbf{R}, m) = lsb\left(\mathbf{R}^{-1} \cdot m \mod n\right)$.

5 $\binom{2}{1}$-OT from a RSR Public-Key Cryptosystem

Let $\xi = (KeyGen, Enc, Dec, \mathcal{M}, \mathcal{C})$ be a **RSR** public-key cryptosystem and λ be the security parameter. Let $(sk, pk) \leftarrow KeyGen(1^\lambda)$ be sender's private and public-keys. The sender encodes his bits so that $Enc_{pk}(b_0)$ and $Enc_{pk}(b_1)$ are semantically secure encryptions of b_0, b_1.

Protocol 1 $\binom{2}{1}$-OT from **RSR** Cryptosystem.

1: The sender computes $c_0 \leftarrow Enc_{pk}(b_0)$ and $c_1 \leftarrow Enc_{pk}(b_1)$.
2: The sender sends the ordered pair (c_0, c_1) to the receiver.
3: The receiver picks a string $\mathbf{R}$ uniformly from $\mathcal{C}$ and computes $c \leftarrow \mathcal{S}_{pk}(\mathbf{R}, c_i)$ for its choice bit i and sends c to the sender.
4: The sender computes $\widehat{m} \leftarrow \widehat{Dec}_{sk}(c)$ and sends $\widehat{m}$ to the receiver.
5: The receiver obtains the bit $b_i \leftarrow \mathcal{S}'_{pk}(\mathbf{R}, \widehat{m})$.

Correctness

We first observe that this protocol correctly computes $\binom{2}{1}$-OT.

$$\mathcal{S}'_{pk}(\mathbf{R}, \widehat{m}) = \mathcal{S}'_{pk}(\mathbf{R}, \widehat{Dec}_{sk}(c)) = \mathcal{S}'_{pk}(\mathbf{R}, \widehat{Dec}_{sk}(\mathcal{S}_{pk}(\mathbf{R}, c_i)))$$
$$= \mathcal{S}'_{pk}(\mathbf{R}, \widehat{Dec}_{sk}(\mathcal{S}_{pk}(\mathbf{R}, Enc_{pk}(b_i)))) = b_i \text{ by definition 1.}$$

Theorem 1 *Protocol* 1 *is a secure oblivious transfer in the semi-honest model.*

Proof. We will present a simulator for each party. These simulators are given the local input (which also includes the security parameter λ) and the local output of the corresponding party. The following schematic depiction of the information flow in protocol 1 may be useful towards the constructions of the simulators.

Sender		*Receiver*
input $\left((b_0, b_1), 1^\lambda\right)$		input $\left(i, 1^\lambda\right)$
$(sk, pk) \leftarrow KeyGen(1^\lambda)$	$\xrightarrow{pk}$	
$c_0 := Enc_{pk}(b_0), c_1 := Enc_{pk}(b_1)$	$\xrightarrow{(c_0, c_1)}$	
	$\xleftarrow{c}$	$c := \mathcal{S}_{pk}(\mathbf{R}, c_i)$
$\widehat{m} \leftarrow \widehat{Dec}_{sk}(c)$	$\xrightarrow{\widehat{m}}$	
output ϵ		output $b_i := \mathcal{S}'_{pk}(\mathbf{R}, \widehat{m})$

Simulator for the sender's view: We will first present a simulator for the sender's view. On input $\left((b_0, b_1), 1^\lambda, \epsilon\right)$, this simulator uniformly picks c' from $\mathcal{C}$ and outputs $\left((b_0, b_1), 1^\lambda, c'\right)$. Clearly this output distribution is identical to the view of the sender in the real execution. This hold because c' is uniformly distributed over the ciphertext space $\mathcal{C}$. Therefore, the receiver's security is perfect.
Simulator for the receiver's view: On input $\left(i, b_i, 1^\lambda\right)$, this simulator generates $(sk', pk') \leftarrow KeyGen(1^\lambda)$ as in protocol 1. It computes $c'_i \leftarrow Enc_{pk'}(b_i)$ and $c'_{1-i} \leftarrow Enc_{pk'}(b)$ (for some $b \in \mathcal{M}$) The simulator then picks a string $\mathbf{R}'$ uniformly. It then computes $c' \leftarrow \mathcal{S}_{pk'}(\mathbf{R}', c'_i)$ and $\widehat{m}' \leftarrow \widehat{Dec}_{sk'}(c')$. The simulator outputs $\left(i, 1^\lambda, pk', c'_0, c'_1, \widehat{m}'\right)$. Note that except for c'_{1-i}, this output distribution is identical to the view of the receiver in the real execution. Moreover, since ξ is a semantically secure encryption scheme, it is impossible to distinguish between the encryption of b_{1-i} and b for any probabilistic polynomial time adversary except with negligible probability. Therefore, the sender's security is computational.
Malicious adversaries: Of course we are not only interested in the semi-honest case but also to the situation with malicious adversaries. To handle these cases, zero-knowledge proofs are used by the sender to demonstrate that c_0, c_1 are well formed encryptions and by the receiver to demonstrate that c is indeed constructed from a single c_i and not a combination of both. We leave it as an exercise to demonstrate the full result including zero-knowledge proofs [20]:

Theorem 2 *Protocol* 1 *may be compiled to a secure oblivious transfer in the malicious model.*

Proof (see [20, 24]).

6 weakly Random Self-Reducible Encryption

The current state of affairs is that we don't know of any **RSR** cryptosystem believed to be resistant to quantum attacks. The **RSR** property may be considered too strong in its uniformity requirement of the output of $\mathcal{S}$. One can weaken this property to statistical indistinguishability for some pair of probabilistic polynomial distributions and can still obtain a secure OT protocol provided we have cryptosystems satisfying this weaker property.

In this section we define the notion of *weakly Random-Self-Reducibile* public-key cryptosystem. Informally speaking a *public-key cryptosystem* is weakly Random-Self-Reducible if it is possible efficiently (using the public key) to re-encrypt a ciphertext c_i in a way to make it unrecognizable, regardless of the plaintext it carries. After obtaining decryption of the re-encrypted ciphertext $\widehat{c}$, it is possible to recover the plaintext hidden by the original encryption c_i. We accept that the unrecognizability property be statistical indistinguishability instead of perfect indistinguishability as in **RSR** .

Our definition is motivated by the fact that many post-quantum encryption schemes use random errors in the process of encrypting the plaintext. Many of these schemes provide a fair amount of flexibility in choosing the size of the error for a fixed pair of public and private keys. Due to this flexibility, one can easily convert these cryptosystem into a **wRSR** scheme. The encryption algorithm Enc involves relatively small errors, while the re-encryption process uses relatively large errors that will hide the original error. The definition is formally stated below.

Definition 2 *A public-key cryptosystem* $\xi = (KeyGen, Enc, Dec, \mathcal{M}, \mathcal{C})$ *is weakly random-self-reducible if there exist sets* $\widehat{\mathcal{M}}, \widehat{\mathcal{C}}$*, a pair of probabilistic polynomial-time algorithms* $(\mathcal{S}, \mathcal{S}')$*, together with a probabilistic polynomial-time algorithm* $\widehat{Dec}$*, and a probabilistic-polynomial time distribution* χ *on* $\widehat{\mathcal{C}}$ *such that for all* $c_1, c_2 \in \mathcal{C}$*, key pair* $(sk, pk) \leftarrow KeyGen\left(1^{\lambda}\right)$ *and* $\mathbf{R} \xleftarrow{\chi} \widehat{\mathcal{C}}$*:*

1. $\mathcal{S}_{pk} : \widehat{\mathcal{C}} \times \mathcal{C} \to \widehat{\mathcal{C}}$, $\mathcal{S}'_{pk} : \widehat{\mathcal{C}} \times \widehat{\mathcal{M}} \to \mathcal{M}$ *and* $\widehat{Dec}_{sk} : \widehat{\mathcal{C}} \to \widehat{\mathcal{M}}$,
2. $\mathcal{S}_{pk}(\mathbf{R}, c_1)$ *and* $\mathcal{S}_{pk}(\mathbf{R}, c_2)$ *are statistically indistinguishable,*
3. $\mathcal{S}'_{pk}\Big(\mathbf{R}, \widehat{Dec}_{sk}\left(\mathcal{S}_{pk}(\mathbf{R}, Enc_{pk}\left(m\right))\right)\Big) = m$*, for all messages* $m \in \mathcal{M}$*.*

Note that **RSR** is the sub-case of **wRSR** where $\widehat{\mathcal{M}} = \mathcal{C}$, χ is the uniform distribution over $\widehat{\mathcal{C}}$ and $S_{pk}(\mathbf{R}, c)$ is uniformly distributed over $\mathcal{C}$. In section 6.1 we show that one can construct a weakly Random-Self-Reducible encryption schemes based on the Approximate Integer GCD assumption [17] or the Learning with Errors assumption [13].

6.1 Instantiation of wRSR public-key Cryptosystems

In this section we provide concrete instantiations of **wRSR** schemes from two different post-quantum assumptions.

1. Approximate Integer GCD problem (**AIGP**)[13].
2. Learning with Errors (**LWE**)[34].

More precisely we show that one can easily construct a **wRSR** from the cryptosystems presented in [13, 17]. Please note that for these encryption schemes, operation ($a \mod n$) means mapping integer a into the interval $[-\lfloor n/2 \rfloor, \lfloor n/2 \rfloor]$, (where n is an odd positive integer).

6.2 Approximate Integer GCD problem

Let p be a large η-bit odd integer and x_i's are defined as follows

$$x_i = q_i p + r_i, \;\; 0 \leq i \leq \tau$$

where x_i is a γ-bit number which is much larger than p and r_i is a ρ-bit error-term which is much smaller than p in absolute value. W.l.o.g. assume that x_0 is the largest of them, and that x_0 is odd. Under the Approximate Integer GCD assumption the function

$$f_x(s, z, b) = \left(2\overline{z} + b + 2\sum_{i=1}^{\tau} x_i s_i\right) \bmod x_0$$

is one-way for anyone who does not know p, where $b \in \{0,1\}$, $\mathbf{s} \in \{0,1\}^\tau$ is a random binary vector and $\overline{z}$ is a random error term of appropriate size (see below).

6.3 public-key Cryptosystem from AIGCD Problem

Van Dijk, Gentry, Halevi and Vaikuntanathan constructed a fully homomorphic encryption scheme based on the problem of finding an approximate integer gcd [13]. The construction below has many parameters, controlling things like the number of integers in the public-key and the bit-length of the various components. Specifically, we use the following five parameters (all polynomial in the security parameter λ):

- η is the bit-length of the secret key p.
- γ is the bit-length of the integers x_i in the public-key.
- ρ is the bit-length of the noise r_i.
- ρ' is the bit-length of the random error z.
- τ is the number of integers in the public-key, (contrary to the other parameters, this is *not* a bit-size.)

These parameters must be set under the following constraints:

- $\rho \in \omega(\log \lambda)$, to protect against brute-force attacks on the noise.
- $\rho' = \Omega(\rho + \log \tau)$ (τ is a polynomial is λ, e.g $\tau = \lambda$).
- $\eta \geq \rho \cdot \Theta(\lambda \log^2 \lambda)$ and should satisfy $2^{\eta-2} > 2^{\rho'} + \tau \cdot 2^{\rho}$, to avoid sums of errors passing $p/2$.
- $\gamma \in \omega(\eta^2 \log \lambda)$, to thwart various lattice-based attacks on the underlying approximate-gcd problem.
- $\tau \geq \gamma + \omega(\log \lambda)$, in order to use the leftover hash lemma in the reduction to approximate gcd.

The public-key is the vector $\mathbf{x} = (x_0, x_1, \ldots, x_\tau)$ and the private key is the η bit integer p. To encrypt a bit $b \in \{0,1\}$ under the public-key $\mathbf{x}$.

- $Enc_{\mathbf{x}}(b)$
  1. Pick uniformly a random bit string $s_1, \cdots, s_\tau$ and pick uniformly a $\overline{\rho}$-bit error-term $\overline{z}$.
  2. Output the ciphertext $c \leftarrow \left(2\overline{z} + b + 2\sum_{i=1}^{\tau} x_i s_i\right) \bmod x_0$.

- $Dec_p(c)$
  1. $c' \leftarrow c \bmod p$.
  2. Output bit $b \leftarrow c' \bmod 2$.

The decryption works, provided the overall distance to the nearest multiple of p does not exceed $p/2$, that is $2(\overline{z} + \sum_{i=1}^{\tau} r_i s_i)$ is less than $p/2$ in absolute value. For the above choice of parameters this will always be the case. We rely on the work of [13] to assess that the resulting cryptosystem is a semantically secure encryption scheme.

6.4 weakly RSR based on Approximate Integer GCD

The cryptosystem based on **AIGCD** can easily be converted to a **wRSR** encryption scheme. Keeping the same notations as above we set

- $\rho = 2\sqrt{\lambda}$ (is the size of r_i's in the public key), $\overline{\rho} = \rho/2$ (size of the error term $\overline{z}$ in Enc).
- $\rho' = 2\rho$ (size of the error term $\mathcal{Z}$ in $\mathcal{S}_{pk}$)
- $\eta = \Theta(\lambda)$ (size of the private key). This parameter is smaller than suggested in [13].
- $\gamma \in \omega(\eta^2 \log \lambda)$. This parameter is smaller than suggested in [13].
- $\tau = \gamma + \rho$ (number of x_i's in public-key $\mathbf{x}$).
- $\mathcal{I} = \left\{[-2^{\rho'}, -2^{\rho'-1}] \cup [2^{\rho'-1}, 2^{\rho'}]\right\} \cap \mathbb{Z}$.
- $\mathcal{R}' = \left\{2\mathcal{Z} + 2\sum_{i=1}^{\tau} x_i w_i \bmod x_0 : \mathcal{Z} \in \mathcal{I}, w_i \in \{0,1\}\right\}$.

- $\widehat{\mathcal{M}} = \{0,1\}$ and $\widehat{\mathcal{C}} = \mathcal{C} \times \widehat{\mathcal{M}}$.
- The distribution χ is induced by picking $\mathbf{r} \xleftarrow{uniform} \mathcal{R}'$, $e \xleftarrow{uniform} \widehat{\mathcal{M}}$ and outputting $\mathbf{R} = (\mathbf{r}, e)$.
- $\mathcal{S}_{pk}(\mathbf{R}, c) := (\mathbf{r} + e + c) \bmod x_0$.
- $\widehat{Dec_{sk}} := Dec_{sk}$.
- $\mathcal{S}'_{pk}(\mathbf{R}, \hat{b}) := (e + \hat{b}) \bmod 2$.

wRSR Encryption Scheme from AIGCD

wRSR Properties(Semi-Honest Case). The scheme clearly satisfies the first and the third properties for the above choice of parameters. For the second property let

$$\mathcal{S}_{pk}(\mathbf{R}, c) = \left(2\mathcal{Z} + e + 2\sum_{i=1}^{\tau} x_i w_i\right) + c \bmod x_0$$
$$\mathcal{S}_{pk}(\mathbf{R}, c') = \left(2\mathcal{Z} + e' + 2\sum_{i=1}^{\tau} x_i w_i\right) + c' \bmod x_0.$$

Since $c, c' \in \mathcal{C}$, there exist $\overline{\rho}$ bit integers $\overline{z}, \overline{z}'$, vectors $\mathbf{s}, \mathbf{s}' \in \{0,1\}^{\tau}$ and bits $b, b' \in \{0,1\}$ such that

$$c = \left(2\overline{z} + b + 2\sum_{i=1}^{\tau} x_i s_i\right) \bmod x_0 \;\;\&\;\; c' = \left(2\overline{z}' + b' + 2\sum_{i=1}^{\tau} x_i s'_i\right) \bmod x_0$$

Note that $\mathcal{S}_{pk}(\mathbf{R}, c)$ and $\mathcal{S}_{pk}(\mathbf{R}, c')$ are perfectly indistinguishable if $\mathbf{r} + b + e$ and $\mathbf{r} + b' + e$ lie in the interval $\mathcal{I}$. Also note that both $\mathbf{r} + b + e$ and $\mathbf{r} + b' + e$ can at most be $2^{\rho'+1} + 2^{\overline{\rho}+1} + \tau \cdot 2^{\rho+2} + 2$ in the absolute value and are guaranteed to lie in $\mathcal{I}$ as far as $\mathcal{Z}$ or $\mathcal{Z}'$ do not lie in

$$\mathbb{Z} \cap \left\{[-2^{\rho'}, (2^{\overline{\rho}+1} + \tau 2^{\rho+2} + 2) - 2^{\rho'}] \cup [2^{\rho'} - (2^{\overline{\rho}+1} + \tau 2^{\rho+2} + 2), 2^{\rho'}]\right\}.$$

Note that $\overline{\rho}$ is $\rho/2$ bits, $\rho = 2\sqrt{\lambda}$ and $\tau = \tilde{O}(\lambda^2)$. The probability of $\mathcal{Z}$ or $\mathcal{Z}'$ lie in this interval is

$$2 \times \left(\frac{2^{\overline{\rho}+1} + \tau \cdot 2^{\rho+1} + 2}{2^{2\rho-1}}\right) = \left(\frac{2^{\sqrt{\lambda}+1} + \tau \cdot 2^{2\sqrt{\lambda}+1} + 2}{2^{4\sqrt{\lambda}-3}}\right) < 2^{-\sqrt{\lambda}} \cdot \tau$$

which is negligible in the security parameter λ. Hence, $\mathcal{S}_{pk}(\mathbf{R}, c)$ and $\mathcal{S}_{pk}(\mathbf{R}, c')$ are statistically indistinguishable.

6.5 Learning with Errors (LWE)

Let $n, q \geq 2$ be positive integers and χ be a distribution on $\mathbb{Z}_q$. For a uniformly chosen vector $\mathbf{s} \in \mathbb{Z}_q^n$ we obtained a distribution $A_{\mathbf{s},\chi}$ on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ by choosing a vector $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random and a noise $x \leftarrow \chi$ and outputting $\left(\mathbf{a}, \mathbf{a}^T\mathbf{s} + x\right)$.

Definition (LWE). For an integer $q = q(n)$ and a distribution χ on $\mathbb{Z}_q$, the goal of the (average case) **LWE** problem is defined as follows : given m independent samples from $A_{\mathbf{s},\chi}$ (for some uniformly chosen fixed vector $\mathbf{s} \in \mathbb{Z}_q^n$) output $\mathbf{s}$ with non-negligible probability. The **Decision** version LWE problem denoted as $\mathbf{distLWE}_{n,m,q,\chi}$ is to distinguish (with non-negligible advantage) from the m samples chosen according to $A_{\mathbf{s},\chi}$, from m samples chosen uniformly from $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

In [34] Regev proved that the search version LWE is at least as hard quantumly approximating certain lattice problems in the worst case. Formally Regev proved the following theorem.

Theorem 3 *Let n, q be integers and $\alpha \in (0,1)$ be such that $q > 2\sqrt{n}$. If there exists an efficient algorithm that solves LWE then there exists an efficient quantum algorithm that approximates the decision version of the shortest vector problem* ($\mathbf{GAPSVP}_\gamma$) *and the shortest independent vectors problem* (**SIVP**) *to within $\tilde{O}(n/\alpha)$ in the worst case.*

6.6 A Simple BGN-Type Cryptosystem

The BGN-Type cryptosystem is a semantically secure public-key cryptosystem, whose security is equivalent to the hardness of the LWE problem [17].

- n is the security parameter and $c = c(n) > 0$ be any function of n.
- $q > 2^{20}(c+4)^3 n^{3c+4} \log^5 n$ is a prime modulus.
- The message space is the set $\mathcal{M} = \{\mathbf{B} \in \mathbb{Z}_2^{m \times m} : \ m = \lfloor 8n \log q \rfloor\}$.
- $\beta = \frac{1}{27n^{1+(3c/2)}\sqrt{qm}\log n \log q}$ specify a discrete normal distribution $\overline{\psi}_\beta(q)$ over $\mathbb{Z}_q$.

The public-key is a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and the private key is a matrix $\mathbf{T} \in \mathbb{Z}_q^{m \times m}$, such that

- $\mathbf{A}$ is statistically close to uniform distribution over $\mathbb{Z}_q^{m \times n}$.
- $\mathbf{T} \cdot \mathbf{A} \mod q = \mathbf{0}$ and $\mathbf{T}$ is invertible over $\mathbb{Z}$.
- The Euclidean norm of all the rows in $\mathbf{T}$ is bounded by $O(n \log q)$.

To encrypt a binary $m \times m$ matrix $\mathbf{B}$ under the public-key $\mathbf{A}$:

- $Enc_{pk}(\mathbf{B})$
  1. Pick a matrix $\mathbf{S} \in \mathbb{Z}_q^{n \times m}$ uniformly and an error matrix $\mathbf{X} \in \mathbb{Z}_q^{m \times m}$ with each entry in $\mathbf{X}$ is chosen independently according to the distribution $\overline{\psi}_\beta(q)$.
  2. Output the ciphertext $\mathbf{C} \leftarrow \mathbf{AS} + \mathbf{2X} + \mathbf{B} \pmod q \in \mathbb{Z}_q^{m \times m}$.
- $Dec_{sk}(\mathbf{C})$
  1. Set $\mathbf{D} \leftarrow \mathbf{TCT}^t \mod q = \mathbf{T}(\mathbf{2X} + \mathbf{B})\mathbf{T}^t \mod q$.
  2. Output the plaintext $\mathbf{B} \leftarrow \mathbf{T}^{-1}\mathbf{D}\left(\mathbf{T}^t\right)^{-1} \pmod 2 \in \mathbb{Z}_2^{m \times m}$.

To see that the decryption works, recall that $\mathbf{T} \cdot \mathbf{A} \mod q = \mathbf{0}$, therefore $\mathbf{TCT}^t \equiv \mathbf{T}(\mathbf{2X} + \mathbf{B})\mathbf{T}^t \mod q$. Moreover, for the above choice of parameters each entry in $\mathbf{T}(\mathbf{2X} + \mathbf{B})\mathbf{T}^t$ will be much smaller than $q/2$ in the absolute value with overwhelming probability [17]. Hence, we have $\mathbf{T}(\mathbf{2X} + \mathbf{B})\mathbf{T}^t \mod q = \mathbf{T}(\mathbf{2X} + \mathbf{B})\mathbf{T}^t$ over the integers.

6.7 weakly Random-Self-Reducible from LWE

Due to space limitation the **wRSR** encryption scheme from LWE is describe in appendix A.

7 Conclusion and open problem

In this work we introduced a new notion of a **weakly Random Self-Reducible** public key cryptosystem and a general methodology to obtain secure oblivious transfer under this assumption. We also show that **wRSR** schemes can be constructed from post-quantum assumptions presented in [13, 17]. We conclude with two open problems related to our work.

McEliece Assumption: Construct a weakly Random-Self-Reducible encryption from McEliece assumption [9].
NTRU Assumption: Construct a weakly Random-Self-Reducible encryption from NTRU assumption [36].

References

1. Michael Oser Rabin. *How to exchange secrets by oblivious transfer*. Technical Memo TR81, Aiken Computation Laboratory, Harvard University, (1981).
2. Shimon Even, Oded Goldreich and Abraham Lempel. *A randomized protocol for signing contracts*. Communications of the ACM, volume 28, issue 6, pages 637 – 647 (1985).
3. Michael J. Fischer, Silvio Micali and Charles Rackoff. *A secure protocol for the oblivious transfer*. Journal of Cryptology, volume 9, issue 3, pages 191 – 195 (1996).
4. Richard Berger, Rene Peralta, and Tom Tedrick. *A provably secure oblivious transfer protocol*. In EUROCRYPT, pages 379 – 386 (1984).
5. Peter W Shor. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. SIAM Journal on Computing, volume 26, issue 5, pages 1484 – 1509 (1997).
6. Christopher Peikert, Vinod Vaikuntanathan and Brent Waters. *A Framework for Efficient and Composable Oblivious Transfer*. In CRYPTO, pages 554 – 571 (2008).
7. Rafael Dowsley, Jeroen van de Graaf, Jörn Müller-Quade and Anderson C. A. Nascimento. *Oblivious Transfer Based on the McEliece Assumptions*. In proceedings of the 3rd international conference on Information Theoretic Security. Lecture Notes in Computer Science Volume 5155, pages 107 – 117 (2008).
8. Kazukuni Kobara, Kirill Morozov and Raphael Overbeck. *Coding-Based Oblivious Transfer*. In Mathematical Methods in Computer Science. Lecture Notes in Computer Science, volume 5393, pages 142 – 156 (2008).
9. Robert J. McEliece. *A public-key cryptosystem based on algebraic coding theory*. Technical memo, California Institute of Technology (1978).
10. Claude Crépeau. *Quantum Oblivious Transfer*. Journal of Modern Optics, special issue on Quantum Communication and Cryptography, volume 41, number 12, pages 2445 – 2454 (1994).
11. Nick Howgrave-Graham. *Approximate integer common divisors*. In CaLC, pages 51– 66 (2001).
12. Craig Gentry. *Fully homomorphic encryption using ideal lattices*. In STOC, pages 169 – 178 (2009).
13. Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. *Fully Homomorphic Encryption over the Integers*. In EUROCRYPT, pages 24 – 43 (2010).
14. Zvika Brakerski and Vinod Vaikuntanathan. *Efficient Fully Homomorphic Encryption from (Standard) LWE*. In FOCS, pages 97 – 106 (2011).
15. Zvika Brakerski and Vinod Vaikuntanathan. *Fully homomorphic encryption from ring-LWE and security for key dependent messages*. In CRYPTO, pages 505 – 524 (2011).

16. Craig Gentry and Shai Halevi. *Fully homomorphic encryption without squashing using depth-3 arithmetic circuits.* In FOCS, pages 107 – 109 (2011).

17. Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. *A simple BGN-Type Cryptosystem from Learning with Errors.* In EUROCRYPT, pages 506 – 522 (2010).

18. Gilles Brassard, Claude Crépeau and Jean-Marc Robert. *All-or-nothing disclosure of secrets.* In CRYPTO, pages 224 – 238 (1986).

19. Oded Goldreich, Silvio Micali, and Avi Wigderson. *How to play any mental game or a completeness theorem for protocols with honest majority.* In STOC, pages 218 – 229 (1987).

20. Oded Goldreich. *Foundations of Cryptography.* Volume I & II. Cambridge University Press, 2001 – 2004.

21. Iftach Haitner. *Semi-honest to Malicious Oblivious Transfer - The Black-Box Way.* In TCC, pages 412 – 426 (2008).

22. Johan Håstad, Russell Impagliazzo, Leonid A. Levin and Michael Luby. *A Pseudo-Random Generator From Any One-Way Function.* SIAM Journal on Computing, volume 28, number 4, pages 12 – 24 (1993).

23. Moni Naor. *Bit Commitment Using Pseudorandomness.* Journal of Cryptology, volume 4, number 2, pages 151 – 158 (1991).

24. Gilles Brassard and Claude Crépeau. *Zero-knowledge simulation of Boolean circuits.* In CRYPTO, pages 223 – 233 (1986).

25. Claude Crépeau, Jeroen van de Graaf and Alain Tapp. *Committed Oblivious Transfer and Private Multi-Party Computation.* In CRYPTO, pages 110 – 123 (1995).

26. Iftach Haitner and Minh-Huyen Nguyen and Shien Jin Ong and Omer Reingold, and Salil Vadhan. *Statistically Hiding Commitments and Statistical Zero-Knowledge Arguments from Any One-Way Function.* SIAM Journal on Computing, volume 39 , issue 3, pages 1153 – 1218 (2009).

27. Ron Rivest, Adi Shamir, and Leonard Adleman. *A method for obtaining digital signatures and public-key cryptosystems.* Communications of the ACM, volume 21, issue 2, pages 120 – 126 (1978).

28. Shafi Goldwasser and Silvio Micali. *Probabilistic encryption.* Journal of Computer and System Sciences, volume 28, issue 2, pages 270 – 299 (1984).

29. Taher ElGamal. *A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.* IEEE Transactions on Information Theory, volume 31, issue 4, pages 469 – 472 (1985).

30. Lawrence C. Washington.

31. lliptic Curves: Number Theory and Cryptography. Discrete Mathematics and Its Applications, 2003.

32. Pascal Paillier. *Public-key cryptosystems based on composite degree residuosity classes.* In EUROCRYPT, pages 538 – 554 (1999).

33. Christopher Peikert and Vinod Vaikuntanathan. *Noninteractive Statistical Zero-Knowledge Proofs for Lattice Problems.* In CRYPTO, pages 17 – 21 (2008).

34. Oded Regev. *On lattices, learning with errors, random linear codes, and cryptography.* In STOC, pages 84 – 93 (2005).

35. Claude Crépeau. *Equivalence between two flavours of oblivious transfer.* In CRYPTO, pages 350 – 354 (1987).

36. Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman *NTRU: A Ring Based Public Key Cryptosystem.* In Algorithmic Number Theory (ANTS III), pages 267 – 288 (1998).

A weakly Random-Self-Reducible from LWE

The encryption scheme is very similar to the BGN-Type cryptosystem (section 6.6). The main constraints on the parameters are given by the correctness requirement and hardness requirements (β should be large enough such that we can invoke above theorem).

- $q \in \left(2^{4(\log n)^2-1}, 2^{4(\log n)^2}\right)$ is a prime modulus.
- Entries of the error matrix $\mathbf{X}$ in Enc_{pk} are chosen independently according to $\overline{\psi}_\beta(q)$, where

$$\beta = \frac{2^{-2(\log n)^2}}{20m \cdot (\log_2 n - 1) \cdot (20n \log_2 q)^2}.$$

- $\mathcal{I} = \left\{[-2^{3(\log n)^2}, -2^{3(\log n)^2-1}] \cup [2^{3(\log n)^2-1}, 2^{3(\log n)^2})]\right\} \cap \mathbb{Z}$.
- $\mathcal{R}' = \{\mathbf{AW} + 2\mathbf{X} \bmod q : \mathbf{X} \in \mathcal{I}^{m\times m}, \mathbf{W} \in \mathbb{Z}_q^{n\times m}\}$.

These parameters yield an approximation factor of $\tilde{O}(n/\alpha) = \tilde{O}(n^{O(\log n)})$, for lattice problems such as ($\mathbf{GAPSVP}_\gamma$). The best known algorithms for ($\mathbf{GAPSVP}_\gamma$) for $\gamma = \tilde{O}(n^{O(\log n)})$, runs in $2^{\tilde{\Omega}(n)}$.

- $\widehat{\mathcal{M}} = \mathcal{M}$, $\widehat{\mathcal{C}} = \mathcal{C} \times \widehat{\mathcal{M}}$.
- The distribution χ on $\widehat{\mathcal{C}}$ is induced by picking $\mathbf{r} \xleftarrow{uniform} \mathcal{R}'$, $\mathbf{B}' \xleftarrow{uniform} \widehat{\mathcal{M}}$ and outputting $\mathbf{R} = (\mathbf{r}, \mathbf{B}')$.
- $\mathcal{S}_{pk}(\mathbf{R}, \mathbf{C}) := (\mathbf{r} + \mathbf{B}' + \mathbf{C}) \bmod q$.
- $\widehat{Dec}_{sk} := Dec_{sk}$.
- $\mathcal{S}'_{pk}\left(\mathbf{R}, \widehat{\mathbf{B}}\right) := \left(\mathbf{B}' + \widehat{\mathbf{B}}\right) \bmod 2$.

wRSR Encryption Scheme from LWE

Theorem 4 *Let $n > 339$ be any integer, $q \in \left(2^{4(\log n)^2-1}, 2^{4(\log n)^2}\right)$ be any prime and $\beta = \frac{2^{-2(\log n)^2}}{20m\cdot(\log_2 n-1)\cdot(20n\log_2 q)^2}$. Then $\widehat{Dec}_{sk}$ correctly decrypts with overwhelming probability. Furthermore the above* **LWE** *construction is a* **wRSR** *encryption scheme.*

Proof $\widehat{Dec}_{sk}(\mathcal{S}_{pk}(\mathbf{R}, \mathbf{C}))$ will decrypt to $(\mathbf{B} + \mathbf{B}') \bmod 2$, as long as

$$\|\mathbf{T}(2(\mathbf{X} + \mathbf{X}') + (\mathbf{B} + \mathbf{B}'))\mathbf{T}^t\|_\infty < q/2.$$

With overwhelming probability every entry of $\mathbf{T}(\mathbf{X})$ and $\mathbf{T}(\mathbf{B} + \mathbf{B}')$ is at most $40\beta q(\log_2 n - 1)n \log_2 q$ and $40n \log_2 q$. Therefore with overwhelming probability

$$\|\mathbf{T}(2(\mathbf{X} + \mathbf{X}') + (\mathbf{B}' + \mathbf{B}))\mathbf{T}^t\|_\infty < m(40n \log_2 q)^2 \cdot \left(\beta q(\log_2 n) + 2^{3(\log n)^2}\right).$$

from tail inequality $\beta q(\log_2 n) < 2^{2(\log n)^2}$, with overwhelming probability and $m = \lfloor 8n \log q \rfloor$ and $\log q = 4(\log n)^2$, therefore

$$\|\mathbf{T}(2(\mathbf{X}+\mathbf{X}')+(\mathbf{B}'+\mathbf{B}))\mathbf{T}^t\|_\infty < n^3(16\log n)^6 \cdot \left(2^{2(\log n)^2}+2^{3(\log n)^2}\right).$$

But $(40n)^6 \log_2 n \cdot \left(2^{2(\log n)^2}+2^{3(\log n)^2}\right) < q/2$ for all $n > 339$, hence

$$\|\mathbf{T}(2(\mathbf{X}+\mathbf{X}')+(\mathbf{B}'+\mathbf{B}))\mathbf{T}^t\|_\infty < 2^{n-1} < \tfrac{q}{2}.$$

wRSR Properties (**Semi-Honest Case**). The scheme clearly satisfies the first property. The scheme also satisfies the third property whenever $\widehat{Dec}_{sk}$ is correct, which will be the case with overwhelming probability for above choice of parameters. To prove the construction satisfies the second property let $\mathcal{S}_{pk}(\mathbf{R},\mathbf{C}) = \mathbf{AW}+\mathbf{E}+2\mathbf{Z}+\mathbf{C} \mod q$, and $\mathcal{S}_{pk}(\mathbf{R}',\mathbf{C}') = \mathbf{AW}'+\mathbf{E}'+2\mathbf{Z}'+\mathbf{C}' \mod q$. Since, $\mathbf{C}$ and $\mathbf{C}'$ are in the ciphertext space, there exist matrices $\mathbf{S},\mathbf{S}' \in \mathbb{Z}_q^{n\times m}$, $\mathbf{B},\mathbf{B}' \in \mathbb{Z}_2^{m\times m}$ and $\mathbf{X},\mathbf{X}' \in \mathbb{Z}_q^{m\times m}$, such that

$$\mathbf{C} = \mathbf{AS}+\mathbf{B}+2\mathbf{X} \mod q \text{ and } \mathbf{C}' = \mathbf{AS}'+\mathbf{B}'+2\mathbf{X}' \mod q$$

note that as far as each entry in $2(\mathbf{Z}+\mathbf{X})+(\mathbf{E}+\mathbf{B})$ and $2(\mathbf{Z}'+\mathbf{X}')+(\mathbf{E}'+\mathbf{B}')$ lie in the interval $\mathcal{I}$, $\mathcal{S}_{pk}(\mathbf{R},\mathbf{C})$ and $\mathcal{S}_{pk}(\mathbf{R}',\mathbf{C}')$ remain perfectly indistinguishable. The probability that each entry in $2(\mathbf{Z}+\mathbf{X})+(\mathbf{E}+\mathbf{B})$ and $2(\mathbf{Z}'+\mathbf{X}')+(\mathbf{E}'+\mathbf{B}')$ does not lies in $\mathcal{I} = \{[-2^{3(\log n)^2}, -2^{3(\log n)^2-1}] \cup [2^{3(\log n)^2-1}, 2^{3(\log n)^2})]\} \cap \mathbb{Z}$ is

$$\left(\frac{2^{3(\log n)^2}-(2^{3(\log n)^2}+\|\mathbf{X}\|_\infty+2)}{2^{3(\log n)^2-1}} + \frac{2^{3(\log n)^2}-(2^{3(\log n)^2}+\|\mathbf{X}'\|_\infty+2)}{2^{3(\log n)^2-1}}\right) = \frac{\|\mathbf{X}\|_\infty+\|\mathbf{X}'\|_\infty+4}{2^{3(\log n)^2-1}}.$$

Furthermore with overwhelming probability $\|\mathbf{X}\|_\infty$ and $\|\mathbf{X}'\|_\infty$ are at most $2^{2(\log n)^2}$, therefore with overwhelming probability

$$\frac{\|\mathbf{X}\|_\infty+\|\mathbf{X}'\|_\infty+4}{2^{3(\log n)^2-1}} = \frac{2^{2(\log n)^2+1}+4}{2^{3(\log n)^2-1}} < 2^{-(\log n)^2+1}$$

which is negligible in n. Therefore $\mathcal{S}_{pk}(\mathbf{R},\mathbf{C})$ and $\mathcal{S}_{pk}(\mathbf{R}',\mathbf{C}')$ are statistically indistinguishable.