Noninteractive Zero Knowledge Proof System for NP from Ring LWE

Wenping Ma

School of Telecommunication Engineering, Xidian University

wp_ ma@mail.xidian.edu.cn

A hash function family is called correlation intractable if for all sparse relations, it hard to find, given a random function from the family, an input output pair that satisfies the relation. Correlation intractability (CI) captures a strong Random Oracle like property of hash functions. In particular, when security holds for all sparse relations, CI suffices for guaranteeing the soundness of the Fiat-Shamir transformation from any constant round, statistically sound interactive proof to a non-interactive argument.

In this paper, based on the method proposed by Chris Peikert and Sina Shiehian, we construct a hash family that is computationally correlation intractable for any polynomially bounded size circuits based on Learning with Errors Over Rings (RLWE) with polynomial approximation factors and Short Integer Solution problem over modules (MSIS), and a hash family that is somewhere statistically intractable for any polynomially bounded size circuits based on RLWE. Similarly, our construction combines two novel ingredients: a correlation intractable hash family for log depth circuits based on RLWE, and a bootstrapping transform that uses leveled fully homomorphic encryption (FHE) to promote correlation intractability for the FHE decryption circuit on arbitrary circuits. Our construction can also be instantiated in two possible modes, yielding a NIZK that is either computationally sound and statistically zero knowledge in the common random string model, or vice-versa in common reference string model. The proposed scheme is much more efficient.

1 Introduction

A zero knowledge proof system [GMR85] is a protocol by which a prover can convince a verifier that a particular statement is true, while revealing nothing more than fact. Such a system is noninteractive zero knowledge proof [BDMP88] (NIZK) if both parties have access to some common string, and the prover just sends a single message to the verifier. Since the introduction of NIZK, several works have constructed such protocols for arbitrary NP languages based on various cryptographic structure, and used them in a series of important cryptographic applications.

The Fiat-Shamir Transform [FS86] is an important tool for designing non interactive argument schemes. A central question in the foundational study of cryptography regards the security of this transformation is for which protocols and hash families does the Fiat-Shamir transform preserve soundness? Under what assumptions can we prove this?

A recent line of research [KRR17, CCRR18, HL18, CCH$^+$19] develops a framework for instantiating the Fiat-Shamir transform [FS86], which removes interaction from a public coin protocol by replacing each random verifier message with a hash of the transcript so far. These works show that if the hash function satisfies a property call correlation intractability [CGH98], then the Fiat Shamir transform can be applied soundly to many interactive protocols, including some zero knowledge ones. Roughly speaking, a hash family H is correlation intractable for a relation R, given a hash key k, it is hard to find an input-output pair $(x, H_k(x)) \in R$. In the context of Fiat-Shamir, this ensures that a cheating prover cannot find a message that hashes to a verifier message that admits an accepting transcript.

The works [CCRR18, HL18, CCH$^+$19] construct correlation intractable hash functions for various sparse relations, and use them to soundly instantiate the Fiat-Shamir transform, obtaining NIZK proofs for all of NP. Of particular interest is the beautiful work of [CCH$^+$19], which shows that for this purpose, it suffices to have correlation intractability for arbitrary polynomial time computations, i.e., for the special class of efficiently searchable relations. These are relations where each input has at most a single output that is computable within some desired polynomial time bound.

The hash families constructed in [CCRR18, CCH$^+$19] are proved to be correlation intractable under various lattice related assumptions. However, these assumptions are somehow non-standard, involving either optimal hardness (e.g., of LWE with uniform error in an interval) against polynomial time attacks [CCRR18, CCH$^+$19], or the existence of circularly secure FHE [CCH$^+$19]. Although the latter assumption seems tantalizingly close to plain LWE (and remains the only known way of obtaining FHE that supports unbounded as opposed to just leveled, homomorphic computations), none of these assumptions are known to be supported by the hardness of LWE, nor the conjectured worst case hardness of lattice problems.

Chris Peikert and Sina Shiehian showed there exists a noninteractive zero knowledge proof system for any NP language, based on the plain LWE problem[PS19]. They finally solve central open problem of basing NIZK for NP on worst case lattice assumptions. They constructed a correlation intractable hash family for bounded circuits is obtained by combining two new ingredients: (1) a correlation intractable hash family for bounded circuits is obtained on plain SIS/LWE, where in particular for log depth circuits the associated approximation factor is a polynomial; (2) a bootstrapping transform that uses fully homomorphism encryption to promote CI for the FHE decryption circuits to CI for arbitrary bounded circuits.

In this paper, using some new techniques recently introduced by Chris Peikert and Sina Shiehian [PS19], we construct a hash family that is correlation intractable for any polynomially bounded size circuits based on RLWE. Similarly, our construction combines two novel ingredients: a correlation intractable hash family for log depth circuits based on RLWE, and a bootstrapping transform that uses leveled FHE to promote correlation intractability for the FHE decryption circuit on arbitrary circuits. Our construction can also be instantiated in two possible modes, yielding a NIZK that is either computationally sound and statistically zero knowledge in the common random string model, or vice-versa in common reference string model. Because power of two cycotomic rings are very convenient to use, the proposed hash family is much more efficient.

2 Preliminaries

For each positive integer a, we denote the set $\{0, 1, \cdots, a-1\}$ by Z_a.

For a set A, we denote by $a \xleftarrow{\$} A$ that a is drawn uniformly from A. If χ is a probability distribution, then $a \leftarrow \chi$ means that a is drawn at random according to the probability distribution χ.

Logarithms are in base 2, unless specified otherwise.

For a positive integer a and $x \in \mathbb{Q}$, we define $x \bmod a$ as the unique element x' in the interval $[-\frac{a}{2}, \frac{a}{2})$ satisfying $x' = x \bmod a$.

For a $x \in \mathbb{Q}$, we denote by $\lceil x \rceil$ the smallest integer greater than or equal to x, and by $\lfloor x \rfloor$ the largest positive integer less than or equal to x.

Unless specifically stated, all vectors will be column vectors. We denote column vectors by bold lower case letters, e.g., $\mathbf{v}$, and matrices by bold upper-case letters, e.g., $\mathbf{A}$. For a vector $\mathbf{v}$ (or matrix $\mathbf{A}$), we denote by $\mathbf{v}^T$ (or $\mathbf{A}^T$) its transpose. For a vector $\mathbf{v}$, we write $\mathbf{v}[i]$ to denote the i-th entry (coordinate) of $\mathbf{v}$; for a matrix $\mathbf{A}$ we write a_{ij} to denote the entry in row i, column j.

The Kronecker product $\mathbf{A} \otimes \mathbf{B}$ of two matrixes (or vectors) $\mathbf{A}$ and $\mathbf{B}$ is obtained by replacing each entry $a_{i,j}$ of $\mathbf{A}$ with the block $a_{ij}\ \mathbf{B}$.

We denote by R the ring $Z[x]/(x^d+1)$ and R_q the ring $R/(q \cdot R)$, where d is a power of 2. Regular font letters denote elements in R or R_q (which includes elements in Z and Z_q) and bold lower case letters represent vectors with coefficients in R or R_q. We often equate elements in polynomial rings with their coefficient vectors. In particular, we will use R_2 to denote the set of R elements with binary coefficients, e.g., when sometimes, it may denote those vectors that have 0/1 coordinates. We write the dot product of $\mathbf{u}, \mathbf{v} \in R^n$ as $< \mathbf{u}, \mathbf{v} >= \sum_{i=1}^{n} u[i] \cdot v[i] \in R$. We use $||r||$ for $r \in R$ refers to the Euclidean norm of r's coefficient vector. We say $\gamma_R = \max\{\|a \cdot b\|/(\|a\| \cdot \|b\|) : a, b \in R\}$ is the expansion factor of R. The value of γ_R is at most $\sqrt{d}$ by Cauchy-Schwarz. For $a \in R$, a mod q means each coefficient of a reduced into the range $[-\frac{q}{2}, \frac{q}{2})$.

We use the standard asymptotic notation to describe the order of growth of functions: for any positive real valued functions $f(n)$ and $g(n)$ we write $f = O(g)$if there exists two constants a, b such that $f(n) \leq a \cdot g(n)$ for all $n \geq b$; $f = o(g)$ if $lim_{n \to \infty} \frac{f(n)}{g(n)} = 0$;$f = \omega(g)$ if $g = o(f)$. Wa say that a function $\mu(\lambda)$ is negligible if $\mu(\lambda) = O(\lambda^{-c})$ for every constant c.

2.1 Learning With Errors over Rings

We recall the Leaning With Errors over Rings (RLWE) problem introduced by Vadim Lyubashevsky, Chris Peikert and Oded Regev , and their hardness based on worst case lattice problems [LPR12].

Definition 1. For security parameter λ, let $f(x) = x^d + 1$ where $d = d(\lambda)$ is a power of 2. Let $q = q(\lambda) \geq 2$ be an integer. Let $R = Z[x]/(f(x))$ and $R_q = R/(q \cdot R)$. Let $\chi = \chi(\lambda)$ be a distribution over R. The $\text{RLWE}_{d,q,\chi}$ problem is to distinguish the following two distributions: in the first distribution, one samples $(a_i, b_i) \in R_q^2$ uniformly. In the second distribution, one first draws $s \leftarrow R_q$ uniformly and then samples $(a_i, b_i) \in R_q^2$ by sampling $a_i \leftarrow R_q$ uniformly, $e_i \leftarrow \chi$, and setting $b_i = a_i \cdot s + e_i$. The $\text{RLWE}_{d,q,\chi}$ assumption is that the $\text{RLWE}_{d,q,\chi}$ problem is infeasible.

Theorem 1. for any d that is a power of 2, ring $R = Z[x]/(x^d + 1)$, prime integer $q = 1 \bmod d$, and $B = \omega(\sqrt{d \log d})$, there is an efficiently samplable distribution χ that outputs elements of R of length a most B with overwhelming probability, such that if there exists an efficient algorithm that solves $\text{RLWE}_{d,q,\chi}$, then there is an efficient quantum algorithm for solving $d^{\omega(1)} \cdot (q/B)$ approximate worst case SVP for ideal lattices over R.

2.2 Module Short Integer Solution

We recall the Leaning With Errors over Rings (RLWE) problem introduced by Adeline Langlois and Damien Stehle, which generalizes both SIS and R-SIS, and their hardness based on worst case lattice problems[LS15].

Definition 2. The problem M-SIS$_{q,m,\beta}$ is as follows: Given $a_1, \cdots, a_m \in R_q^k$ chosen independently from the uniform distribution, find $z_1, \cdots, z_m \in R$ such that $\sum_{i=1}^{m} a_i \cdot z_i = 0 \bmod q$, and $0 < \|z\| \leq \beta$, where $z = (z_1, \cdots, z_m)^T \in R^m$.

Theorem 2. For any $k \geq 1$ and $\epsilon(N) = N^{-\omega(1)}$, there is a probabilistic polynomial time reduction from solving Mod-GIVP$_\gamma^{\eta_\epsilon}$ in polynomial time (in the worst case, with high probability) to solving M-SIS$_{q,m,\beta}$ in polynomial time with non-negligible probability, for any $m(N)$, $q(N)$, $\beta(N)$ and $\gamma(N)$ such that $\gamma \geq \beta\sqrt{N}\cdot\omega(\sqrt{\log N})$, $q \geq \beta\sqrt{N}\cdot\omega(\log N)$ and $m, \log q \leq poly(N)$.

2.3 Leveled Fully Homomorphic Encryption

Fully Homomorphic Encryption (FHE) was introduced by Craig Gentry, we recall the notion of leveled FHE and its desired properties[Gen09].

Throughout this section we use λ to indicate the security parameter. In addition, all schemes in this paper encryption bit-by bit and therefore our definitions only refer to this case.

A homomorphic encryption scheme HE = (HE.Keygen, HE.Enc, HE.Dec, HE.Eval) is a quadruple of PPT algorithms as follows.

Key generation: The algorithm $(pk, evk, sk) \leftarrow \text{HE.Keygen}(1^\lambda)$ takes a unary representation of the security parameter and outputs a public encryption key pk, a public evalution key evk and a secret decryption key sk.

Encryption: The algorithm $c \leftarrow \text{HE.Enc}_{\text{pk}}(\mu)$ takes the public key pk and a single bit message $\mu \in \{0,1\}$ and outputs a ciphertext c.

Decryption: The algorithm $\mu^* \leftarrow \text{HE.Dec}_{sk}(c)$ takes the secret key sk and a ciphertext c and outputs a message $\mu^* \in \{0,1\}$.

Homomorhic evaluation: The algorithm $c_f \leftarrow \text{HE.Eval}_{evk}(f, c_1, \cdots, c_l)$ takes the evaluation key evk, a function $f : \{0,1\}^l \rightarrow \{0,1\}$ and a set of l ciphertexts $c_1, \cdots, c_l$, and outputs a ciphertext c_f. In this work, f will be represented by an arithmetic circuit over $GF(2)$.

Definition 3. A scheme **HE** is **IND-CPA** secure if for any polynomial time adversary $\mathcal{A}$ it holds that

$$\begin{aligned} \mathbf{Adv_{CPA}}[\mathcal{A}] &= |\mathbf{Pr}[\mathcal{A}(\mathbf{pk}, \mathbf{evk}, \mathbf{HE}.\mathbf{Enc_{pk}}(\mathbf{0}) = \mathbf{1}] \\ &\quad -[\mathcal{A}(\mathbf{pk}, \mathbf{evk}, \mathbf{HE}.\mathbf{Enc_{pk}}(\mathbf{1}) = \mathbf{1}]| \\ &= \mathbf{negl}(\lambda), \end{aligned}$$

where $(\mathbf{pk}, \mathbf{evk}, \mathbf{sk}) \leftarrow \mathbf{HE.Keygen(1^\lambda)}$.

Definition 4. (compactness) A homomorphic scheme HE is compact if there exist a polynomial $s = s(k)$ such that the output length of HE.Eval$(\cdot, \cdot)$ is at most s bits long regardless of f of the number of inputs.

Definition 5. (fully homomorphic encryption) A scheme HE is fully homomorphic if it is both compact and homomorphic for the class of all arithmetic circuits over $GF(2)$.

Based on RLWE, Zvika Brakerski, Craig Gentry and Vinod Vaikuntanathan constructed leveled fully homomorphic encryption schemes (capable of evaluating arbitrary polynomial size circuits)[BGV11]. Using their constructions, we will construct correlation intractable hash function for arbitrary polynomial size circuits.

2.4 Correlation Intractability

We recall the definitions of correlation intractability proposed in [CCH+19, PS19], in their computational and statistical versions.

Definition 6. We say that a relation $R \subset X \times Y$ is searchable in size S if there exists a function $f : X \to Y$ that is implementable as a Boolean circuit of size S, such that if $(x, y) \in R$ then $y = f(x)$.

Definition 7. Let $\mathcal{R} = \{R_\lambda\}$ be a relation class. A hash function family (Gen, Hash) is correlation intractable for $\mathcal{R}$ if for every non-uniform polynomial size adversary $\mathcal{A} = \{A_\lambda\}$ there exists a negligible function $v(\lambda)$ such that for every $R_\lambda \in \mathcal{R}$

$$\Pr_{\substack{k \leftarrow \mathrm{Gen}(1^\lambda) \\ x = A_\lambda(k)}} [(x, \mathrm{Hash}(k, x)) \in R_\lambda] \leq v(\lambda).$$

Definition 8. Let $\mathcal{R} = \{R_\lambda\}$ be a relation class. A hash function family (Gen,Hash) with a fake key generation algorithm StatGen is somewhere statistically correlation intractable for $\mathcal{R}$ if

1. StatGen $(1^\lambda, z)$, where z is an auxiliary input, outputs a key k,

2. there exists a negligible function $v(\lambda)$ and a class of auxiliary inputs $\mathcal{Z} = \{\mathcal{Z}_\lambda\}$ such that

1) the distribution ensembles $\{\mathrm{StatGen}(1^\lambda, z_\lambda)\}$ and $\{\mathrm{Gen}(1^\lambda)\}$ are computationally indistinguishable for every sequence of $z_\lambda \in \mathcal{Z}_\lambda$, and

2) for every $R_\lambda \in \mathcal{R}$ there exists $z_R \in \mathcal{Z}_\lambda$ such that

$$\Pr_{k \leftarrow \mathrm{StatGen}(1^\lambda, z_\lambda)} [\exists\, x, s.t. (x, \mathrm{Hash}(k, x)) \in R] \leq v(\lambda),$$

we call z_R the intractability guarantee for R_λ.

2.5 Noninteractive Zero Knowledge Arguments (and Proofs)

The following preliminaries are taken from [PS19].

Definition 9. A noninteractive zero knowledge (NIZK) argument system Π for an NP relation R is a tuple of PPT algorithms (Setup, Prove, Verify) having the following interfaces:

1. Setup $(1^n, 1^\lambda)$, given a statement length n and a security parameter λ, outputs a string σ,

2. Prove (σ, x, ω), given a string and a statement witness pair $(x, \omega) \in R$, output a proof π,

3. Verify (σ, x, π), given a string σ, a statement x, and a proof π, either accepts or rejects.

The proof system Π must satisfy the following requirements for every polynomial function $n = n(\lambda)$. $\mathcal{L}(R)$ denotes the language $\{x : \exists\, \omega, s.t. (x, \omega) \in R\}$ and R_n denotes the set $R \bigcap (\{0,1\}^n \times \{0,1\}^*)$.

1. Completeness: for every $(x, \omega) \in R$ and $\lambda \in N$, Verify (σ, x, π) accepts with probability 1, over the choice of $\sigma \leftarrow \mathrm{Setup}(1^{|x|}, 1^\lambda)$ and $\pi \leftarrow \mathrm{Prover}(\sigma, x, \omega)$.

2. Soundness: For every $x_n \in \{0,1\}^n \setminus \mathcal{L}(R)$ and every polynomial size $P^* = P^*_\lambda$, there is a negligible function v such that

$$\Pr_{\substack{\sigma \leftarrow \mathrm{Setup}(1^n, 1^\lambda) \\ \pi \leftarrow P^*_\lambda(\sigma)}} [V(\sigma, x_n, \pi) = 1] \leq v(\lambda).$$

3. Statistical zero knowlwdge: there exists a PPT simulator S such that for every $(x, \omega) \in R$, the following two distribution ensembles are statistically indistinguishable:

$$\big(S(1^\lambda, x)\big)_\lambda \overset{s}{\rightarrow} \big\{\big(\sigma, \mathrm{Prover}(\sigma, x, \omega)\big) : \sigma \leftarrow \mathrm{Setup}\big(1^{|x|}, 1^\lambda\big)\big\}_\lambda.$$

If the distribution are computationally indistributionable, then Π is said to be computational zero knowledge.

A NIZK argument system can also satisfy various stronger properties. We list some important variants below.

1. Common random string: Setup$(1^n, 1^\lambda)$ simply outputs a uniformly random string.

2. Statistical soundness: there exists a negligible function $v(\lambda)$ such that for any $n \in N$

$$\Pr_{\sigma \leftarrow \text{Setup}(1^n, 1^\lambda)} [\exists\ (x, \pi^*) s.t. \text{Verify}(\sigma, x, \pi^*) \text{accepts}\ \Lambda\ x \notin L] \leq v(\lambda).$$

3. Adaptive soundness: for every non uniform polynomial size "cheating" prover $P^* = P^*_\lambda$ there exists a negligible function $v(\lambda)$ such that for any $n \in N$,

$$\Pr_{\substack{\sigma \leftarrow \text{Setup}(1^n, 1^\lambda) \\ (x, \pi*) \leftarrow P^*_\lambda(\sigma)}} [\text{Verify}(\sigma, x, \pi^*) \text{accepts}\ \Lambda\ x \notin L] \leq v(\lambda).$$

4. Adaptive (computational) zero knowledge: there exists a PPT simulator $S = (S_1, S_2)$ such that for every non uniform polynomial size "cheating" verifier $V^* = (V_1^*, V_2^*)$, for every $n \in N$ the probabilities

$$\Pr[V_2^*(\sigma, x, \pi, \varsigma) = 1, (x \in L)].$$

In the following two experiments differ only by negl(λ):

1. in the "real" experiment, $\sigma \leftarrow$ Setup$(1^{|x|}, 1^\lambda)$, $(x, \omega, \varsigma) \leftarrow V_1^*(\sigma)$, $\pi \leftarrow$ Prove(σ, x, ω);

2. in the "simulation" experiment, $(\sigma, \tau) \leftarrow S_1(1^\lambda)$, $(x, \omega, \varsigma) \leftarrow V_1^*(\sigma)$, $\pi \leftarrow S_2(\sigma, x, \tau)$.

3 New Fully Homomorphic commitments

3.1 Gadgets Matrixes

For a positive integer modulus q, let $l = \lceil \log q \rceil$, the "gadger" vector over Z_q [MP12, PS19] is defined as

$$\mathbf{g}^T = (1, 2, 4, \cdots, 2^{l-1}) \in Z_q.$$

For every $u \in Z_q$, there is an efficiently computable binary vector $\mathbf{g}^{-1}[u] \in \{0, 1\}^l$ such that $< \mathbf{g}, \mathbf{g}^{-1}[u] >= u \bmod q$. Specifically, $\mathbf{g}^{-1}[u]$ corresponds to the binary representation of u in $\{0, 1, \cdots, q-1\}$.

Let $\mathbf{J}^T = (1, 1, \cdots, 1) \in Z_q^d$ be an all 1 column vector of length d.

Let $\mathbf{a}^T = (a_0, a_1, \cdots, a_{d-1}) \in Z_q^d$, in this paper, we define the inner product of a and J as $< \mathbf{J},\ \mathbf{a}^T >= a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} \in R_q$.

We define the function $\mathbf{g}^{-1} \otimes \mathbf{J} : R_q \to \{0, 1\}^{d \cdot l}$, which applies $\mathbf{g}^{-1}$ to each coordinate and appends the results. That is to say, if $x \in R_q$, we decomposes x into its bit representation, Namely, write $x = \sum_{j=0}^{\lfloor \log q \rfloor} 2^j \cdot u_j$, where all of the vectors u_j are in R_2^n, and output $(g^{-1} \otimes \mathbf{J}[x])^T = (u_0, u_1, \cdots, u_{\lfloor \log q \rfloor}) \in R_2^{\lceil \log q \rceil}$. Because we equate the elements in R with their coefficient vectors, we have $g^{-1} \otimes J[x] \in \{0, 1\}^{d \cdot l}$.

If we define $\mathbf{J}^T = (1, 1, \cdots, 1) \in Z_q^{d \cdot n}$ be an all 1 vector of length $d \cdot n$, we define the function $g^{-1} \otimes \mathbf{J} : R_q^n \to \{0, 1\}^{d \cdot n \cdot l}$ similarly, that is to say, for every $x \in R_q^n$, we decomposes x into its bit representation. Namely, write $x = \sum_{j=0}^{\lfloor \log q \rfloor} 2^j \cdot u_j$, where all of the vectors u_j are in R_2^n, and output $(\mathbf{g}^{-1} \otimes \mathbf{J}[x])^T = (u_0, u_1, \cdots, u_{\lfloor \log q \rfloor}) \in R_2^{n \cdot \lceil \log q \rceil}$.

For a dimension n, the two gadget matrix are defined as

$$\mathbf{G}_2 = \mathbf{I}_2 \otimes \mathbf{g}^T \in Z_q^{2 \times (2l)},$$

$$\bar{\mathbf{G}} = I_2 \otimes \mathbf{g}^T \otimes\ \mathbf{J} \in R_q^{2 \times (2dl)}.$$

Obviously, if a column vector $\mathbf{x} \in \{0, 1\}^{2ld}$, $\bar{\mathbf{G}} \cdot \mathbf{x} = (u(x), v(x)^T$, where $u(x), v(x) \in R_q$.

In the following, we define two functions:

$\mathbf{G}_2^{-1} = \mathbf{I}_2 \otimes \mathbf{g}^{-1} : Z_q^2 \to \{0, 1\}^{2l}$, which applies $\mathbf{g}^{-1}$ to each coordinate and appends the results. This has the essential property, which is also reflective of the mixed product property, that for every $\mathbf{u} \in Z_q^2$, $\mathbf{G}_2 \cdot \mathbf{G}_2^{-1}[\mathbf{u}] = \mathbf{u}$.

$\bar{\mathbf{G}}^{-1} = \mathbf{I}_2 \otimes \mathbf{g}^{-1} \otimes \mathbf{J} : R_q^2 \to \{0, 1\}^{2dl}$ as follows, for every $(u(x), v(x)) \in R_q^2$, $\bar{\mathbf{G}}^{-1}[(u(x), v(x))^T] = (\mathbf{g}^{-1} \otimes \mathbf{J}[u(x)], \mathbf{g}^{-1} \otimes \mathbf{J}[v(x)])^T$. This also has the essential property, which is also reflective of the mixed product property, that is for every $(u(x), v(x)) \in R_q^2$, $\bar{\mathbf{G}} \cdot \bar{\mathbf{G}}^{-1}[(u(x), v(x))^T] = (u(x), v(x))^T$.

3.2 New Homomorphic commitments

Here we use the relevant homomorphic properties of gadgets, which were exploited in [GSW13, BGG+14, BV14, AP14, GVW15, PS19], to construct the fully homomorphic commitments.

Let $\mathbf{A} \in R_q^{2 \times m}$ be an arbitrary matrix for some dimension m. Let $\mathbf{C}_i = \mathbf{A}\mathbf{R}_i + x_i \mathbf{G}_2$ for some matrix $\mathbf{R}_i \in R^{m \times (2l)}$ and scalar $x_i \in Z_q$ for $i = 1, 2$. We view $\mathbf{C}_i$ as a commitment to x_i under randomness $\mathbf{R}_i$. Observe that these commitments satisfy the following:

$$\mathbf{G}_2 - \mathbf{C}_1 = \mathbf{A} \cdot (-\mathbf{R}_i) + (1 - x_1)\mathbf{G}_2,$$

$$\begin{aligned} C_\times &= \mathbf{C}_1 \times \bar{\mathbf{G}}^{-1}[\mathbf{C}_2] = \mathbf{A}(\mathbf{R}_1 \cdot \bar{\mathbf{G}}^{-1}[\mathbf{C}_2]) + x_1 \cdot \mathbf{G}_2 \cdot \bar{\mathbf{G}}^{-1}[\mathbf{A}\mathbf{R}_2 + x_2\mathbf{G}_2] \\ &= \mathbf{A}(\mathbf{R}_1 \cdot \bar{\mathbf{G}}^{-1}[\mathbf{C}_2] + x_1\mathbf{R}_2) + (x_1 \cdot x_2)\mathbf{G}_2. \end{aligned}$$

In particular, if the committed values x_i are restricted to bits, then we can implement NAND gate ($\mathrm{NAND}(x, y) = 1 - x \cdot y$) using the above two homomorphic operations, and then we can homomorphically evaluate any booean circuit.

We also need another homomorphic property. Suppose we have a commitment

$$\mathbf{C} = \mathbf{A}\mathbf{R} + \mathbf{x}^t \otimes \mathbf{G}_2 = \mathbf{A} \cdot \mathbf{R} + \mathbf{x}^t \otimes \mathbf{I}_2 \otimes \mathbf{g}^t.$$

It is easy to prove that for the matrix $\bar{\mathbf{G}} \in Z_q^{2\times 2dl}$, there exists a vector $\mathbf{m}_{\bar{\mathbf{G}}} \in R_2^{4dl^2}$ such that for every vector $\mathbf{x} \in Z_q^{2dl}$. we have $\mathbf{x}^t \otimes \mathbf{I}_2 \otimes g^t \cdot \mathbf{m}_{\bar{\mathbf{G}}} = \bar{\mathbf{G}} \cdot \mathbf{x}$, then

$$\mathbf{C}_{\bar{\mathbf{G}}} = \mathbf{C} \cdot \mathbf{m}_{\bar{\mathbf{G}}} = \mathbf{A} \cdot \mathbf{r}_{\bar{\mathbf{G}}} + \bar{\mathbf{G}} \cdot \mathbf{x}.$$

We view $\mathbf{C}_{\bar{\mathbf{G}}}$ as a "quasi-commitment" to $\bar{\mathbf{G}} \cdot \mathbf{x} \in R_q^2$, under randomness $\mathbf{r}_{\bar{\mathbf{G}}}$, which is small if $\mathbf{R}$ is small.

We summarize all of the above in the following fully homomorphic commitment scheme.

Construction for fully homomorphic commitment scheme

The fully homomorphic commitment (FHC) scheme is parameterized by q and m, and is defined as follows.

1. FHC.Gen chooses a uniformly random $\mathbf{A} \leftarrow R_q^{2\times m}$, where $m \geq 4l$.

2. $\mathrm{Com}(\mathbf{A}, \mathbf{x} \in Z_q^S; \mathbf{R} \leftarrow R^{m\times 2Sl})$ outputs a commitment $\mathbf{C} = \mathbf{A}\mathbf{R} + \mathbf{x}^t \otimes \mathbf{G}_2 \in R_q^{2\times 2Sl}$. If the randomness of $\mathbf{R}$ is not provided explicitly, it is chosen uniformly from $R_2^{m\times 2Sl}$.

3. $\mathrm{CircuitEval}(C, \mathbf{C} \in R_q^{2\times 2Sl}; \mathbf{R} \in R^{m\times 2Sl})$. For a Boolean circuit $C : \{0,1\}^t \rightarrow \{0,1\}^L$, deterministically outputs a commitment matrix $\mathbf{C}_C \in R_q^{2\times 2Ll}$ and additionally an integer matrix $\mathbf{R}_C \in R^{m\times 2Ll}$.

4. $\mathrm{QuasiEval}(\bar{\mathbf{G}} \in Z_q^{2\times 2dl}, \mathbf{C} \in R_q^{2\times 4dl^2}; \mathbf{R} \in R^{m\times 4dl^2})$ deterministically output a quasi commitment vector $\mathbf{C}_{\bar{\mathbf{G}}} \in R_q^2$ and additionally an integral matrix $\mathbf{r}_{\bar{\mathbf{G}}} \in R^m$.

Proposition: the above fully homomorphic commitment scheme satisfies the following properties:

1. By the leftover hash lemma, for any $\mathbf{x} \in Z_q^{\mathrm{poly}(m)}$ the distribution of $(\mathbf{A}, \mathbf{C})$ has $\mathrm{negl}(m)$ statistical distance from uniformly random, where $\mathbf{A} \leftarrow \mathrm{Gen}(1^m)$ and $\mathbf{C} \leftarrow \mathrm{Com}(\mathbf{A}, \mathbf{x})$.

2. For any Boolean circuit $C : \{0,1\}^S \rightarrow \{0,1\}^L$ of depth h, any $\mathbf{x} \in \{0,1\}^S$, any $\mathbf{A} \in R_q^{2\times m}$ and $\mathbf{R} \in R^{m\times 2Sl}$, for commitment $\mathbf{C} = \mathrm{Com}(\mathbf{A}, \mathbf{x}; \mathbf{R})$

we have

$$\mathrm{CircuitEval}(C, \mathbf{C}; \mathbf{R}) = \mathrm{Com}(\mathbf{A}, C(x); \mathbf{R}_C),$$

where $\mathbf{R}_C \in R^{m\times 2Ll}$ is the additional output $\mathrm{Com}(\mathbf{A}, C(x); \mathbf{R}_C)$, and $\|R_C\| = ||R|| \cdot d^{O(h)}$.

3. For any $\mathbf{x} \in \{0,1\}^{2dl}$, any $\mathbf{A} \in R_q^{2\times m}$ and any $\mathbf{R} \in R^{m\times 4dl^2}$, for commitment $\mathbf{C} = \mathbf{AR} + \mathbf{x}^t \otimes \mathbf{G}_2$ we have

$$\mathrm{QuasiEval}(\bar{\mathbf{G}}, \mathbf{C}; \mathbf{R}) = \mathbf{A} \cdot \mathbf{r}_{\bar{\mathbf{G}}} + \bar{\mathbf{G}} \cdot \mathbf{x},$$

where $\mathbf{r}_{\bar{\mathbf{G}}} \in R^m$ is the additional output of $\mathrm{QuasiEval}(\bar{\mathbf{G}}, \mathbf{C}; \mathbf{R})$, and $\|\mathbf{r}_{\bar{\mathbf{G}}}\| \leq \|\mathbf{R}\| \cdot (2dl)^2$.

4 Correlation-Intractable Hashing from MSIS and RLWE

4.1 Construction for Circuits

The hash family CIH=(Gen, Hash) with fake key generation algorithm StatGen is parameterized by an arbitrary circuit size $S = S(\lambda) = poly(\lambda)$ and depth $h = h(\lambda) \leq S(\lambda)$. Let $U(C, x) = C(x)$ denote a universal circuit with depth h and size S.

1. $\mathrm{Gen}(1^\lambda)$: generate $\mathbf{A} \leftarrow$FHC.Gen and $\mathbf{C} \leftarrow \mathrm{Com}(\mathbf{A}, 0^{S(\lambda)})$, choose a uniformly random $\mathbf{a} \leftarrow R_q^2$, and output the hash key $\mathbf{k} = (\mathbf{a}, \mathbf{C})$.

2. $\mathrm{StatGen}(1^\lambda.C)$: given a circuit C of size S, choose a uniformly random $\overline{\mathbf{A}} \leftarrow R_q^m$ and $\overline{a}(x) \leftarrow R_q$, choose $s(x) \leftarrow R_q$, $\overline{\mathbf{e}} \leftarrow \chi^m$ and $e \leftarrow \chi$, where χ is an RLWE error distribution. Let

$$A = \begin{bmatrix} \overline{\mathbf{A}} \\ s(x) \cdot \overline{\mathbf{A}} + \overline{\mathbf{e}} \end{bmatrix} \in R_q^{2\times m}, a = \begin{bmatrix} \overline{a}(x) \\ s(x) \cdot \overline{a}(x) + e - \left\lfloor \frac{q}{2} \right\rfloor \cdot J \end{bmatrix} \in R_q^2,$$

here we define $J = 1 + x + x^2 + \cdots + x^{d-1} \in R_q$.

Compute $\mathbf{C} \leftarrow \mathrm{Com}(\mathbf{A}, C)$ and output the hash key $\mathbf{k} = (\mathbf{a}, \mathbf{C})$.

3. $\mathrm{Hash}(\mathbf{k} = (\mathbf{a}, \mathbf{C}), x)$: let circuit $U_x(\cdot) = U(\cdot, x)$, and output

$$\bar{\mathbf{G}}^{-1}[a + \mathrm{QuasiEval}(\bar{\mathbf{G}}, \mathrm{CircuitEval}(U_x, \mathbf{C}))] \in \{0,1\}^{2dl}.$$

4.2 Correlation Intractability

In the following, we prove that the construction is computationally correlation intractable under an appropriate MSIS assumption and RLWE assumption, and statistically correlation intractable under an appropriate RLWE assumption.

Theorem 3. Assuming the hardness of MSIS for a sufficiently large β, the construction above is correlation intractable for the class of functions with output length $2dl$ that can be implemented by size S depth h Boolean circuits.

Proof. Let $Adv = \{A_\lambda\}$ be any non-uniform polynomial size adversary, and fix any sequence of functions $\{f_\lambda\}$, where f_λ has output length $2dl$ and can be implemented by a circuit C_λ of size $S = S(\lambda)$ and depth $h = h(\lambda)$. To show the construction above is correlation intractable with respect to f, we first define a hybrid experiment and show that it is statistically indistinguishable from the real experiment. Then we show that in this hybrid, it is hard for an adversary to break correlation intractability against $\{f_\lambda\}$.

In the hybrid experiment we merely modify how $\mathbf{C} \leftarrow \mathrm{Com}(\mathbf{A}, C)$ for $C = C_\lambda$ is generated. By item 1 of Proposition, this experiment is within statistical distance $\mathrm{negl}(\lambda)$ from the real one, so Adv's success probability can differ by at most this much between the real and hybrid experiments.

We now show that under hardness hypothesis, $v(\lambda) = \Pr_k[x = A_\lambda(k) : \mathrm{Hash}(k, x) = f(x)]$ is a negligible function that depends only on Adv. To do this we use Adv to construction a non uniform polynomial size attacker $S = \{S_\lambda\}$ against MSIS that also has success probability $v(\lambda)$, as follows.

The attacker S_λ, given an MSIS instance $\mathbf{A}' = [\mathbf{a}|\mathbf{A}] \in R_q^{2\times(m+1)}$, generates $\mathbf{C} \leftarrow Com(\mathbf{A}, C)$ and retains the commitment randomness $\mathbf{R} \in R_2^{m\times 2Sl}$. It defines a hash key $\mathbf{k} = (\mathbf{a}, \mathbf{C})$ and let $x = A_\lambda(\mathbf{k})$. If $\mathrm{Hash}(\mathbf{k}, x) = f(x)$, then lets $(\mathbf{C}_x, \mathbf{R}_x) = \mathrm{CircuitEval}(U_x, \mathbf{C}; \mathbf{R})$ and then lets $\mathbf{r}_x$ be the additional output of $\mathrm{QuasiEval}(\bar{\mathbf{G}}, \mathbf{C}_x; R_x)$. It output $\mathbf{z}_x = (1, \mathbf{r}_x) \in R^{m+1}$ as the nonzero MSIS solution.

We now analyze S_λ. First observe that the distribution of the hash key $\mathbf{k}$ it provides to A_λ is exactly as in the hybrid experiment, by the uniform distribution of the MSIS instance $\mathbf{A}' = [\mathbf{a}|\mathbf{A}]$. We claim that $\mathbf{z}_x = (1, \mathbf{r}_x)$ is a valid MSIS solution whenever $\mathrm{Hash}(\mathbf{k}, x) = f(x)$. To see this, observe that this condition implies that

$$\begin{aligned}
\bar{\mathbf{G}} \cdot f(x) &= \bar{\mathbf{G}} \cdot \mathrm{Hash}(\mathbf{k}, x) \\
&= \mathbf{a} + \mathrm{QuasiEval}(\bar{\mathbf{G}},\ \mathrm{CircuitEval}\ (U_x, \mathbf{C})) \\
&= \mathbf{a} + (\mathbf{A}\mathbf{r}_x + \bar{\mathbf{G}} \cdot f(x)) \\
&= \mathbf{A}'\mathbf{z}_x + \bar{\mathbf{G}} \cdot f(x)
\end{aligned}$$

and that $\|\mathbf{z}_x| \leq \beta$, therefore $\mathbf{A}'\mathbf{z}_x = 0$, and $\mathbf{z}_x$ satisfies the norm bound, as desired. □

Theorem 4. Assuming the hardness of RLWE. Construction is somewhere statistically correlation intractable for the class of functions with output length $2dl$ that can be implemented by size S depth h boolen circuits; each circuits serves as the intractability guarantee for itself.

Proof. First, it follows immediately from RLWE assumption that the output of $\mathrm{Gen}(1^\lambda)$ and $\mathrm{Gen}(1^\lambda, C_\lambda)$ are computationally indistinguishable for any sequence of circuits C_λ of size S.

Now fix any sequence of functions $\{f_\lambda\}$, where f_λ has single bit output length and can be implemented by a circuit of size $S = S(\lambda)$ and depth $h = h(\lambda)$. we will show that

$$\Pr_{k \leftarrow \mathrm{StatGen}(1^\lambda, f_\lambda)} [\exists\, x, s.t. \mathrm{Hash}(k, x) = f(x)] \leq v(\lambda),$$

where $v(\lambda)$ is a negligible function.

Using the notation from StateGen, let $\mathbf{A}' = [\mathbf{a}|\mathbf{A}] \in R_q^{2\times(m+1)}$ and let $\overline{\mathbf{A}'} = [\overline{\mathbf{a}}, \overline{\mathbf{A}}] \in R_q^{m+1}$ be its first row. Similarly, let $\mathbf{e}' = (e, \overline{\mathbf{e}}) \in R^{m+1}$. For any hash input x, define $\mathbf{r}_x$ and $\mathbf{z}_x = (1, \mathbf{r}_x) \in R^{m+1}$ exactly as in the proof of theorem above. Now, notice that if $\mathrm{Hash}(\mathbf{k}, x) = f(x)$, then as above we have

$$\bar{\mathbf{G}} \cdot f(x) = \mathbf{A}'\mathbf{z}_x + \bar{\mathbf{G}} \cdot f(x).$$

This implies that

$$\begin{bmatrix} \overline{\mathbf{A}}' \cdot \mathbf{z}_x \\ s(x) \cdot \overline{\mathbf{A}}' \cdot \ \mathbf{z}_x + \mathbf{e}' \cdot \mathbf{z}_x \end{bmatrix} = \begin{bmatrix} 0 \\ \lfloor \frac{q}{2} \rfloor \cdot J \end{bmatrix},$$

and hence $< \mathbf{e}', \mathbf{z}_x >= \lfloor \frac{q}{2} \rfloor \cdot J$, it is impossible. □

4.3 Correlation Intractable Hashing for all Circuits

In this subsection let $L = L(\lambda)$, $S = S(\lambda)$ and $h = h(\lambda)$ be arbitrary poly(λ)-bound functions, and define the relation class $R_{L,S,d} = \{\mathcal{R}_{\lambda,L,S,d}\}$, where $\mathcal{R}_{\lambda,L,S,d} = \{R_f = \{(x, f(x))\}\}$ is the set of all efficiently searchable relations whose search functions f can be computed by a circuit with output length $L(\lambda)$, size $S(\lambda)$, and depth $h(\lambda)$.

Let FHE be a leveled fully homomorphic encryption scheme instantiated to support a circuit class $C = \{C_\lambda\}$ of depth at most $h = h(\lambda)$, and let $U_\lambda(C, x) = C(x)$ denote a universal circuit for circuits $C \in C_\lambda$, with decryption circuit having size $S_{\mathrm{Dec}}(\lambda)$ and logarithmic depth $h_{\mathrm{Dec}}(\lambda) = O(\log \lambda)$.

Let CIH=(Gen,Hash) be a hash function family with fake-key generation algorithm StatGen for circuit size $S = L \cdot S_{\mathrm{Dec}}(\lambda)$ and depth $d = d_{\mathrm{Dec}}(\lambda)$. Define a new hash family CIH* =(Gen*,Hash*) with fake key generation algorithm StatGen* as follows:

1. $\text{Gen}^*(1^\lambda)$: generate $k \leftarrow$GIH.Gen(1^λ) and $(sk, ek) \leftarrow$FHE.Gen(1^λ). Generate $c \leftarrow$Enc(pk, D) for some arbitrary "dummy" circuit $D \in C_\lambda$, and output hash key $k' = (k, ek, c)$.

2. $\text{StatGen}^*(1^\lambda, C)$: generate $(sk, ek) \leftarrow$FHE.Gen(1^λ) and $k \leftarrow$StatGen$(1^\lambda$, FHE.Dec$(sk, \cdot))$. Generate $c \leftarrow$Enc$(pk, C)$and output hash key $k' = (k, ek, c)$.

3. $\text{Hash}^*(k' = (k, ek, c), x)$: let circuit $U_x(\cdot) = U_\lambda(\cdot, x)$ and out hash value Hash$(k$, Eval(ek, U_x, c).

Theorem 5. Assuming the hardness of RLWE for poly(n) bounded χ and suitable q, and the CPA security of FHE. The hash family CIH* =(Gen*,Hash*) with fake key generation algorithm StatGen*instantiated with FHE and CIH is correlation intractable with respect to $R_{L,S,d}$ (respectively, somewhere statistically correlation intractable with respect to $R_{L,S,d}$, where for each $R_f \in R_{L,S,d}$ the intractability guarantee is f).

Proof. First, it follows immediately from the CPA security of FHE that the output of Gen(1^λ) and Gen$(1^\lambda, C_\lambda)$ are computationally indistinguishable for any sequence of circuits C_λ of size S.

The rest of the proof is similar to the proof of the theorem in [PS19] and will not be described here. □

Using the leveled FHE scheme based on RLWE that has jointly pseudorandom evaluation keys and ciphertexts [BGV11], we get the following corollary.

Corollary 1. Assuming the hardness of RLWE, there exists a somewhere statistically correlation intractable hash family with pseudorandom hash keys for $R_{L,S,d}$, where for each $R_f \in R_{L,S,d}$ the intractability guarantee is f.

5 Noninteractive Zero Knowledge for NP

We are now ready to instantiate the noninteractive zero knowledge protocol from [CCH$^+$19, PS19] with our correlation intractable hash function. We first recall the following theorem.

Theorem 6 (CCH$^+$19)**.** Assuming the existence of

1. a lossy public key encryption scheme with uniformly random lossy public keys (respectively, an ordinary CPA secure public key encryption scheme),

2. a hash family with (psedo) random keys which is CI for all circuits of output length $L(\lambda) \geq \lambda^c$ for some constant $c > 0$ and size bounded by some sufficiently large $S(\lambda) = poly(\lambda)$ (respectively, a hash family that is

somewhere statistically correlation intractable of all such circuits, where the intractability guarantee for each circuit is itself).

There exists an adaptively sound, statistically zero knowledge noninteractive argument system with common random string for any NP language (respectively, a statistically sound, adaptively zero knowledge noninteractive proof system with common reference string).

Theorem 7. Assuming the hardness of RLWE, for any NP language there exists

1. an adaptively sound, statistically zero knowledge noninteractive argument system having a common random string,
2. a statistically sound, adaptively zero knowledge noninteractive proof system having a common reference string.

The proof of the theorem is similar to the proof of the theorem in [PS19], it will not be described here.

References

- [BDMP88] M.Blum, A.De Santis, S.Micali, and G.Persiano. Noninteractive zero-knowledge. SIAM J. Comput., 20(6):1084-1118,1911. Preliminary version in STOC 1988.

- [BFM88] M.Blum, P.Feldman, and S.Micali. Non interactive zero knowledge and its applications (extended abstract). In STOC, pp. 103-112, 1988.

- [BGV11] ZvIka Brakerski, Craig Gentry and Vinod Vaikuntanathan. Fully Homomorphic encryption without bootstrapping. Electronic Colloquium on Computational Complexity, Report No. 111(2011).

- [BLP$^+$13] Z.Brakerski, A.Langlois, C.Peikert, O.Regev, and D.Stehle. Classical hardness of learning with errors. In STOC, pp. 575-584, 2013.

- [CCH$^+$19] R.Canetti, Y.Chen, J.Holmgren, A.Lombardi, G.Rothblum, and D.Wichs. Fiat-Shamir: From practice to theory, In STOC,2019.To appear.

- [CCHLRR18] Ran Canetti, Yilei Chen, Justin Holmgren, Alex Lombardi, Guy N.Rothblum and Ron D. Rothblum. Fiat-Shamir from simpler assumptions. IACR Cryptology ePrint Archive, 2018.

- [CCRR18] Ran Canetti, YileI Chen, Leonid Reyzin, and R.D.Rothblum. Fiat Shamir and correlation intractability from strong KDM secure encryption. In EUROCRYPT. pp. 91-122, 2018.

- [CGH98] R.Canetti, O.Goldreich, and S.Halevi. The random oracle methodology, revisited. J.ACM, 41(4):557-594, 2004. Preliminary version in STOC 1998.

- [CLW19] Ran Canetti, Alex Lombardi, Daniel Wichs. Fiat-Shamir: From Practice to theory, Part 11-NIZK and Correlation intractability from circular secure FHE.May 1,2009.

- [FS86] A.Fiat and A.Shamir. How to prove yourself: Practical solutions to identification and signature problems. In CRYPTO, pages 186-194,1986.

- [FLS90] U.Feige, D.Lapidot, and A.Shamir. Multiple noninteractive zero knowledge proofs under general assumptions. SIAM J.Comput., 29(10):1-28,1999.Preliminary version in FOCS 1990.

- [Gen09] C.Gentry. A fully homomorphic encryption scheme. Ph.D.Thesis, Stanford University, 2009. http://crypto.stanford.edu/craig.

- [GMR85] S.Goldwasser, S.Micali, and C.Rackoff. The knowledge complexity of interactive proofsystems. SIAM J.Comput., 18(1):186-208, 1989. Preliminary version in STOC 1985.

- [GO94] O.Goldreich and Y.Oren. Definitions and properties of zero knowledge proof systems.J.Cryptology. 7(1):1-32, 1994.

- [GOS06] J.Groth, R.Ostrovsky, and A.Sahai. Perfect non-interactive zero knowledge for NP. In EUROCRYPT, pp. 339-358, 2006.

- [GSW13] C.Gentry, A.Sahai, and B.Waters. Homomorphic encryption from learning with errors: Conceptually- Simpler, asymptotically-faster, attribute based. In CRYPTO, pp.75-92, 2013.

- [HL18] J.Holmgren and A.Lombardi. Cryptographic hashing from strong one way functions. In FOCS, pp. 850-858, 2018.

- [KRR17] Y.T.Kalai, G.N.Rothblum, and R.D.Rothblum. From obfuscation to the security of Fiat-Shamir for proofs. InCRYPTO, pp. 224-251, 2017.

- [KW18] S.Kim and D.J.Wu. Multi-theorme preprocessing NIZKs from lattices. In Crypto, pp. 733-765, 2018.

- [LPR12] Vadim Lyubashevsky, Chris Peikert and Oded Regev. On Ideal Lattices and Learning with errors over rings. In EUROCRYPT, volume 6110 of Lecture Notes in Computer Science, pages 1-23,2010.

- [LS15] Adeline Langlois. Damien Stehle. Worst case to average case reductions for module lattices. Des. Codes Cryptogr. pp. 565-599, 2015.

- [MP12] D.Micciancio and O.Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In RUROCRYPT, pp. 700-718, 2012.

- [MR04] D.Micciancio and O.Regev. Worst case to average case reductions based on Gaussian measures. SIAM J.Comput., 37(1):267-302, 2007.Preliminary version in FOCS 2004.

- [MV90] M.Micciancio and S. P. Vadhan. Public key cryptosystems provably secure against chosen ciphertext attacks. In STOC, pp. 427-437, 1990.

- [MW03] D.Micciancio and S.P.Wadhan. Statistical zero knowledge proofs with efficient provers:Lattice problems and more. In Crypto, pp.282-298, 2003.

- [Pei09] C.Peikert. Public key cryptosystems from the worst case shortest vector problem. In STOC, pp. 333-342, 2009.

- [PRS17] C.Peikert, O.Regev, and N.Stephems-Davidowitz. Pseudorandomness of Ring LWE for any ring and modulus. In STOC, pp. 461-473, 2017.

- [PS19] Chris Peikert and Sina Shiehian. Noninteractive zero knowledge for NP from learning with Errors. IACR Cryptology ePrint Archive, 2019.

- [PV08] C.Peikert and V.Vaikuntanathan. Noninteractive statistical zero-knowledge proofs for lattice problems. In CRYPTO, pp. 536-553, 2008.

- [PVW08] C.Peikert, V.Vaikuntanathan, and B.Waters. A framework for efficient and composable oblivious transfer. In CRYPTO, pp.554-571, 2008.

- [SW14] A.Sahai and B.Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In STOC, pp. 475-484, 2014.