Practical Signatures from the Partial Fourier Recovery Problem Revisited: A Provably-Secure and Gaussian-Distributed Construction

Xingye Lu[1][0000-0002-3595-044X], Zhenfei Zhang[2], and Man Ho Au[1]

[1] The Hong Kong Polytechnic Univerisity, Hong Kong
xingye.lu@connect.polyu.hk, mhaau@polyu.edu.hk
[2] Onboard Security, Wilmington, Massachusetts, USA
zzhang@onboardsecurity.com

Abstract. In this paper, we present a new lattice-based signature scheme, PASS$_G$, based on signatures from the partial Fourier recovery problem PASS$_{RS}$ introduced by Hoffstein et al. in 2014. Same as PASS$_{RS}$, security of our construction relies on the average-case hardness of a special kind of Short Integer Solution (SIS) problem and the hardness of partial Fourier recovery problem. PASS$_G$ improves PASS$_{RS}$ in two aspects. Firstly, unlike PASS$_{RS}$, PASS$_G$ comes with a reduction proof and is thus provably secure. Secondly, we adopt rejection sampling technique introduced by Lyubashevsky in 2008 to reduce the signature size and improve the efficiency. More concretely, signatures of PASS$_G$ are Gaussian-distributed and is more space efficient. We also present another security parameter set based on best known attack using BKZ 2.0 algorithm introduced by Chen and Nguyen in 2011.

Keywords: Lattice-based cryptography · Digital signature · Partial Fourier Recovery problem.

1 introduction

In 2014, Hoffstein et al. [9] presented a signature scheme called PASS$_{RS}$. As a candidate of practical post-quantum signature schemes, the security of PASS$_{RS}$ is based on a special hard problem known as partial Fourier recovery. The problem requires recovery of a ring element with small norm given an incomplete description of its Chinese remainder representation. Even though there is no known reduction from standard lattice problems to the partial Fourier recovery problem, [9] shows that there is a relationship between this problem and the Short Integer Solution (SIS) problem. By assuming the average-case hardness of a special SIS problem which is called Vandermonde-SIS, the security of PASS$_{RS}$ is said to rest on the hardness of Vandermonde-SIS. However, no security reduction between PASS$_{RS}$ and Vandermonde-SIS is provided in [9].

In this paper, we present PASS$_G$, an efficient lattice-based signature scheme based on PASS$_{RS}$ that provides provable security along with more secure parameter sets comparing with the original PASS$_{RS}$.

1.1 Related Work

Early candidates of lattice-based signature schemes, such as GGH signature scheme [8], lack security proofs and have been broken subsequently due to transcript attacks.

The seminal work of Gentry Peikert and Vaikuntanathan [7], known as the GPV framework, combines a hash-and-sign paradigm with a pre-image sampling function. The signature schemes obtained through this fashion enjoys a provable security based on the hardness of the SIS problem. In the GPV framework, the efficiency of a signature scheme (in terms of both speed and size) depends heavily on the preimage sampling function and the quality of secret basis produced by the trapdoor generating function. Improving performance of these functions becomes the research objective for the following studies. To the best of our knowledge, the most efficient construction following this direction while admitting a security proof is due to Micciancio and Peikert [13].

Besides GPV framework adopting “hash-and-sign” techniques, there are also lattice-based signature schemes built through Fiat-Shamir heuristics. Lyubashevsky and Micciancio [12] first presented a lattice-based one-time signature scheme based on the ring-SIS problem. Based on [12], Lyubashevsky [10] then proposed a lattice-based interactive identification scheme and converted the scheme into a signature scheme using Fiat-Shamir heuristics. In the scheme, an abortion technique is used to protect the secret key from leakage. This abortion techniques, usually known as rejection sampling, has flourished modern lattice based signatures. For example, by rejecting to a Gaussian distribution [11] or a Bimodal Gaussian distribution (BLISS) [4], one is able to reduce both the rejection rate and the size of the signatures. State-of-the-art following this direction is Dilithium [5], whose hardness is based on the learning with error problem over modular lattices.

Different from these previous lattice-based signatures schemes, Hoffstein et al. [9] proposed PASS$_{RS}$ based on the partial Fourier recovery problem. It adopts the same aborting technique used in [10] to decouple the signature from the secret key. Although the time efficiency of PASS$_{RS}$ is comparable with BLISS, we note that there are still rooms for improvement. First of all, PASS$_{RS}$ does not admit a formal reduction proof. Moreover, cryptanalysis has been developing very rapidly during the past 2 years due to a new model [1] of analyzing the cost of BKZ 2.0 lattice reduction algorithm [3]. As a consequence, the security level of the original PASS$_{RS}$ will be significantly reduced. It is fair to say PASS$_{RS}$ may not be secure if the originally suggested parameters are adopted. To solve these problems, we present a new signature scheme PASS$_G$

Our Contribution: Comparing with PASS$_{RS}$, our contributions can be summarized as follow:

- We apply the rejection sampling technique from [11] to PASS$_{RS}$ to construct a new scheme known as PASS$_G$.
- which features reduced signature size thanks to the use of rejection sampling.

- We further provide several sets of security parameters for our new scheme that are robust against new analysis.

2 Preliminary

2.1 Notation

Elements in $\mathbb{Z}_q$ are represented by integers in $[-\frac{q}{2}, \frac{q}{2})$. We use cyclotomic polynomial rings $\mathbb{Z}_q[x]/(x^N + 1)$ with N being a power of 2 and q being a prime congruent to $1 \mod 2N$. An element $\mathbf{a} \in R_q$ is represented as a polynomial $\mathbf{a} = a_0 + a_1\mathbf{x} + a_2\mathbf{x}^2 + \cdots + a_{N-1}\mathbf{x}^{N-1}$ with coefficients $a_i \in \mathbb{Z}_q$. We can also use vector $[a_0, a_1, a_2, \cdots, a_{N-1}]^T$ to represent polynomial $\mathbf{a}$. We use $\star$ to denote the multiplication on R_q and $\odot$ to denote component-wise multiplication of vectors. For any β with $\gcd(\beta, q) = 1$, Fermat's little theorem says $\beta^{q-1} = 1(\mod q)$. Since $q = rN + 1$, we have $\beta^{rN} = 1 \bmod q$. We can define a ring homomorphism mapping $\mathbf{f} \to \mathbf{f}(\beta^{\mathbf{r}})$ for any $\mathbf{f} \in R_q$. For any $\mathbf{f}_1, \mathbf{f}_2 \in R_q$,

$$(\mathbf{f}_1 + \mathbf{f}_2)(\beta^r) = \mathbf{f}_1(\beta^r) + \mathbf{f}_2(\beta^r) \text{ and } (\mathbf{f}_1 \star \mathbf{f}_2)(\beta^r) = \mathbf{f}_1(\beta^r) \odot \mathbf{f}_2(\beta^r)$$

For distribution $\mathcal{D}$, $x \xleftarrow{\$} \mathcal{D}$ means uniformly sampling x according to distribution $\mathcal{D}$. $\|\mathbf{v}\|_1$ is the ℓ_1 norm of vector $\mathbf{v}$ and $\|\mathbf{v}\|$ is the ℓ_2 norm of $\mathbf{v}$.

The continuous normal distribution over $\mathbb{R}^N$ centered at $\mathbf{v}$ with standard deviation σ is defined as $\rho^N_{\mathbf{v},\sigma}(\mathbf{x}) = (\frac{1}{\sqrt{2\pi\sigma^2}})^N e^{\frac{-\|\mathbf{x}-\mathbf{v}\|^2}{2\sigma^2}}$. For simplicity, when $\mathbf{v}$ is the zero vector, we use $\rho^N_\sigma(\mathbf{x})$.

The discrete normal distribution over $\mathbb{Z}^N$ centered at $\mathbf{v} \in \mathbb{Z}^N$ with standard deviation σ is defined as $\mathcal{D}^N_{\mathbf{v},\sigma}(\mathbf{x}) = \frac{\rho^N_{\mathbf{v},\sigma}(\mathbf{x})}{\rho^N_{\mathbf{v},\sigma}(\mathbb{Z}^N)}$.

Lemma 1 (Rejection Sampling [4]). *Let V be an arbitrary set, and $h : V \to \mathbb{R}$ and $f : \mathbb{Z}^m \to \mathbb{R}$ be probability distributions. If $g_v : \mathbb{Z}^m \to \mathbb{R}$ is a family of probability distribution indexed by all $v \in V$ with the property that*

$$\exists M \in \mathbb{R} \text{ such that } \forall v \in V, \forall \mathbf{z} \in \mathbb{Z}^m, \Pr[M \cdot g_v(\mathbf{z}) \geq f(\mathbf{z})] \geq 1 - \varepsilon.$$

Then the output distribution of the following algorithm $\mathcal{A}$:

1.$v \xleftarrow{\$} h$; 2. $\mathbf{z} \xleftarrow{\$} g_v$; 3. output $(\mathbf{z}, v)$ with probability $\min\left(\frac{f(\mathbf{z})}{M \cdot g_v(\mathbf{z})}, 1\right)$.
is within statistical distance $\frac{\varepsilon}{M}$ of

1. $v \xleftarrow{\$} h$; 2. $\mathbf{z} \xleftarrow{\$} f$; 3. output $(\mathbf{z}, v)$ with probability $\frac{1}{M}$.
The probability of algorithm $\mathcal{A}$ output something is at least $\frac{1-\varepsilon}{M}$.

Lemma 2 ([11]).

1. *For any $k > 0$, $\Pr[\|\mathbf{z}\| > k\sigma\sqrt{N}; \mathbf{z} \xleftarrow{\$} \mathcal{D}^N_\sigma] < k^N e^{\frac{N}{2}(1-k^2)}$;*
2. *For any vector $\mathbf{v} \in \mathbb{R}^N$, $\sigma, r > 0$, $\Pr[|\langle\mathbf{z}, \mathbf{v}\rangle| > r; \mathbf{z} \xleftarrow{\$} \mathcal{D}^N_\sigma] \leq 2\exp(-\frac{r^2}{2\|\mathbf{v}\|^2\sigma^2})$.*

2.2 Digital Signatures

A digital signature scheme consists of three algorithms, namely, KeyGen, $\mathsf{Signing}$, $\mathsf{Verification}$, described as follows.

- $\mathsf{KeyGen}(1^\lambda) \to (\mathsf{sk}, \mathsf{pk})$: This key generation algorithm generates private signing key sk and public verification key pk.
- $\mathsf{Signing}(\mathsf{sk}, \mu) \to \sigma$: On input signing key sk and message μ, the signing algorithm outputs signature σ on μ.
- $\mathsf{Verification}(\mu, \sigma, \mathsf{pk}){\to}$ *accept/reject*: On input message μ, signature σ and verification key pk, the verification algorithm outputs accept if σ is a signature on μ. otherwise, it outputs reject.

Security of a digital signature scheme can be defined by a Game held between a challenger $\mathcal{C}$ and a probabilistic polynomial-time forger $\mathcal{F}$. Game consists of three phases, namely, *Setup*, *Query* and *Output*.

- *Setup.* The challenger $\mathcal{C}$ runs KeyGen algorithm and obtains private signing key and public verification key pair $(\mathsf{sk}, \mathsf{pk})$. $\mathcal{C}$ sends verification key pk to the forger $\mathcal{F}$.
- *Query.* Forger $\mathcal{F}$ sends message μ_i to challenger $\mathcal{C}$. $\mathcal{C}$ signs μ_i using sk and returns the corresponding signature σ_i to $\mathcal{F}$. Forger $\mathcal{F}$ repeats the process n times where n is polynomial in λ and finally obtains a list of message and signature pair $((\mu_1, \sigma_1)$,(μ_2, σ_2),$\cdots$,$(\mu_n, \sigma_n))$.
- *Output.* The forger $\mathcal{F}$ outputs a forgery (μ^*, σ^*). $\mathcal{F}$ wins Game if

$$(\mathsf{Verification}(\mu^*, \sigma^*, \mathsf{pk}) \to \mathit{accept}) \wedge ((\mu^*, \sigma^*) \notin \{(\mu_1, \sigma_1), (\mu_2, \sigma_2), \cdots, (\mu_n, \sigma_n)\}).$$

Definition 1. *A signature scheme (*KeyGen*,* $\mathsf{Signing}$*,* $\mathsf{Verification}$*) is said to be strong unforgeable if for any polynomial-time forger* $\mathcal{F}$*, the probability of* $\mathcal{F}$ *winning* Game *is negligible.*

2.3 Hardness Assumption

Before introducing the hard problem in our construction, we first introduce the *partial Fourier recovery* problem which requires recovering a signal from a restricted number of its Fourier coefficients.

Let ω be the primitive Nth root of -1 modulo q. We define the discrete Fourier transform over $\mathbb{Z}_q$ to be the linear transformation $\mathcal{F}\mathbf{f} = \hat{\mathbf{f}} : \mathbb{Z}_q^N \to \mathbb{Z}_q^N$ given by $(\mathcal{F})_{i,j} = \omega^{ij}$. The Fourier transform matrix $\mathcal{F}$ is a Vandermonde matrix. Let $\mathcal{F}_\Omega$ be the restriction of $\mathcal{F}$ to the set of t rows specified by an index set, Ω, $(\mathcal{F}_\Omega)_{ij} = \omega^{\Omega_i j}$. The partial Fourier recovery problem is that, given an evaluation $\hat{\mathbf{f}}|_\Omega \in \mathbb{Z}_q^t$, find $\mathbf{x}$ with small norm such that $\hat{\mathbf{x}}|_\Omega = \hat{\mathbf{f}}|_\Omega (\mod q)$. The solution $\mathbf{x}$ is required to be small since one can easily find a large $\mathbf{x}$ such that $\hat{\mathbf{x}}|_\Omega = \hat{\mathbf{f}}|_\Omega$. This problem has been well studied and considered to be hard in general.

We note that to date, there is no known reduction from lattice-based hard problem to *partial Fourier recovery* problem. However, finding a short preimage by a given evaluation and a transform matrix $\mathbf{F}_\Omega$ is known to be related to solving the Short Integer Solution (SIS) and the Inhomogeneous Short Integer Solution (ISIS) problem, two average-case hard problems which are frequently used in lattice-based cryptography constructions. So we define a new problem called Vandermonde-SIS problem. Here we assume that the hardness of SIS problem is not relied on the structure of the public matrix and the Vandermonde-SIS problem is hard in average-case. The security of our proposed signature scheme is based on the assumed average-case hardness of the Vandermonde-SIS problem.

Definition 2 (Vandermonde $-$ $\mathbf{SIS}^{\mathcal{K}}_{q,t,N,\beta}$ problem). *Given a Vandermonde matrix $\mathbf{F}_\Omega \in \mathbb{Z}_q^{t\times N}$ drawn according to some distribution $\mathcal{K}$, find a non-zero $\mathbf{v} \in \mathbb{Z}_q^N$ such that $\mathbf{F}_\Omega \mathbf{v} = \mathbf{0}$ and $\|\mathbf{v}\| \le \beta$.*

The distribution $\mathcal{K}$ here refers to randomly samples t rows from discrete Fourier transform matrix $\mathcal{F}$.

3 Construction

In this section, we describe the construction of PASS_G in details. Our construction involves the following algorithms:

KeyGen: This algorithm generates polynomial $\mathbf{f} \in R_q$ with each coefficient independently and uniformly sampled from $\{-1, 0, 1\}$ as the secret key. The corresponding public key is $\hat{\mathbf{f}}|_\Omega = \mathbf{F}_\Omega \mathbf{f}$. As described in section 2.3, $\mathbf{F}_\Omega$ is the restriction of $\mathbf{F}$ to the set of t rows. Thus, $\mathbf{F}_\Omega$ can be generated by randomly picking t rows from the original Fourier transform matrix $\mathbf{F}$.

$\mathsf{Signing}(\mathbf{f}, \mu)$: To sign message μ, the signer first randomly samples polynomial $\mathbf{y}$ from discrete normal distribution $\mathcal{D}_\sigma^N$ and computes $\hat{\mathbf{y}}|_\Omega = \mathbf{F}_\Omega \mathbf{y}$. The signer then computes challenge $\mathbf{c} = \mathsf{FormatC}(\mathsf{Hash}(\hat{\mathbf{y}}|_\Omega, \mu))$ where $\mathsf{FormatC}$ and Hash are two public algorithms such that:

$$\mathsf{Hash} : \mathbb{Z}_q^t \times \{0,1\}^* \to \{0,1\}^\ell, \mathsf{FormatC} : \{0,1\}^\ell \to \{\mathbf{v} : \mathbf{v} \in \{-1,0,1\}^N, \|\mathbf{v}\|_1 \le \kappa\}.$$

Finally, the signer computes $\mathbf{z} = \mathbf{f} \star \mathbf{c} + \mathbf{y}$ and outputs $(\mathbf{z}, \mathbf{c})$ with probability $\min(\frac{\mathcal{D}_\sigma^N(\mathbf{z})}{M\mathcal{D}^N_{\mathbf{f}\star\mathbf{c},\sigma}(\mathbf{z})}, 1)$ where $M = \exp(\frac{28\alpha+1}{2\alpha^2})$ and $\sigma = \alpha \cdot \kappa\sqrt{N}$.

$\mathsf{Verification}(\mu, \mathbf{z}, \mathbf{c}, \mathbf{F}_\Omega, \hat{\mathbf{f}}|_\Omega)$: The verifier accepts the signature if and only if $\|\mathbf{z}\| \le k\sigma\sqrt{N}$ and $\mathbf{c} = \mathsf{FormatC}(\mathsf{Hash}(\hat{\mathbf{z}}|_\Omega - \hat{\mathbf{f}}|_\Omega \odot \hat{\mathbf{c}}|_\Omega, \mu))$.

In the signing procedure, $\mathbf{z}$ is distributed according to $\mathcal{D}^N_{\mathbf{f}\star\mathbf{c},\sigma}$. Thus, for any $\mathbf{z}^* \in \mathbb{R}^N$, we have:

$$\begin{aligned}\Pr[\mathbf{z} = \mathbf{z}^*] = \mathcal{D}^N_{\mathbf{f}\star\mathbf{c},\sigma} = \frac{\rho_{\mathbf{f}\star\mathbf{c},\sigma}(\mathbf{z}^*)}{\rho_\sigma(\mathbb{Z}^N)} &= \frac{1}{\rho_\sigma(\mathbb{Z}^N)} \exp(-\frac{\|\mathbf{z}^* - \mathbf{f}\star\mathbf{c}\|^2}{2\sigma^2}) \\ &= \mathcal{D}_\sigma^N \exp(-\frac{-2\langle \mathbf{z}^*, \mathbf{f}\star\mathbf{c}\rangle + \|\mathbf{f}\star\mathbf{c}\|^2}{2\sigma^2})\end{aligned}$$

We have:

$$\frac{\mathcal{D}_\sigma^N}{\mathcal{D}_{\mathbf{f}\star\mathbf{c},\sigma}^N} = \frac{\mathcal{D}_\sigma^N}{\mathcal{D}_\sigma^N \exp(-\frac{-2\langle \mathbf{z}^*, \mathbf{f}\star\mathbf{c}\rangle + \|\mathbf{f}\star\mathbf{c}\|^2}{2\sigma^2})} = \exp(\frac{-2\langle \mathbf{z}^*, \mathbf{f}\star\mathbf{c}\rangle + \|\mathbf{f}\star\mathbf{c}\|^2}{2\sigma^2})$$

According to Lemma 2, when $r = 14\|\mathbf{v}\|\sigma$, with probability at least $1 - 2^{-128}$ we have $\langle \mathbf{z}^*, \mathbf{f}\star\mathbf{c}\rangle > -14\|\mathbf{f}\star\mathbf{c}\|\sigma$. Then, with probability at least $1 - 2^{-128}$, we have:

$$\exp(\frac{-2\langle \mathbf{z}^*, \mathbf{f}\star\mathbf{c}\rangle + \|\mathbf{f}\star\mathbf{c}\|^2}{2\sigma^2}) < \exp(\frac{28\|\mathbf{f}\star\mathbf{c}\|\sigma + \|\mathbf{f}\star\mathbf{c}\|^2}{2\sigma^2}).$$

Assume $\sigma = \alpha \cdot \kappa\sqrt{N}$. Then,

$$\exp(\frac{28\|\mathbf{f}\star\mathbf{c}\|\sigma + \|\mathbf{f}\star\mathbf{c}\|^2}{2\sigma^2}) \leq \exp(\frac{28\kappa\sqrt{N}\sigma + (\kappa\sqrt{N})^2}{2\sigma^2}) = \exp(\frac{28\alpha + 1}{2\alpha^2}).$$

According to Lemma 1, if we reject $\mathbf{z}$ with probability $\min(\frac{\mathcal{D}_\sigma^N(\mathbf{z})}{M\mathcal{D}_{\mathbf{f}\star\mathbf{c},\sigma}^N(\mathbf{z})}, 1)$ where $M = \exp(\frac{28\alpha+1}{2\alpha^2})$. The distribution of $\mathbf{z}$ should be identical to $\mathbf{y}$.

Theorem 1. *Assume there is a polynomial-time forger who can successfully forge a PASS$_G$ signature with non-negligible probability δ by making at most s queries to the signing oracle and h queries to the random oracle* $\mathsf{FormatC}\circ\mathsf{Hash}$. *Then, there exits a polynomial-time algorithm which can solve the* **Vandermonde−SIS**$^{\mathcal{K}}_{q,t,N,\beta}$ *problem for $\beta = 2k\sigma\sqrt{N} + 2\kappa\sqrt{N}$ with probability $\frac{\delta^2}{2(h+s)}$.*

We remark that details of the security proof are omitted from this version due to page limit and can be found in the full version.

4 Practical Instantiation

In this section, we present a practical instantiation with parameters chosen according to the lattice reduction algorithm BKZ 2.0. This gives us an approach to analyse the security of PASS$_G$ under best known attack. Two sets of parameters with 128-bit security will be presented. Based on the two sets of parameters, we can estimate the rejection rate and signature size of our PASS$_G$.

Table 1 gives two sets of parameters. Both sets provides 128 bit security against quantum attackers. The first set of parameters provides a similar security level as the original PASS$_{RS}$ signature scheme, and is performance oriented. The second set is security oriented and has a larger build in margin. This is to account for future advance in cryptanalysis.

The best known lattice attack against our scheme is to look for the unique shortest vector within a lattice spanned via the basis:

$$\mathbf{B} = \begin{bmatrix} q\mathbf{I}_t & 0 & 0 \\ \mathbf{F}_\Omega & \mathbf{I}_N & 0 \\ \hat{\mathbf{f}}|_\Omega & 0 & 1 \end{bmatrix}$$

	Parameter 1	Parameter 2
N	512	1024
$q \equiv 1 \mod 2N$	$2^{16}+1$	$2^{16}+1$
$t = \lvert\omega\rvert$	256	512
k	13.3	13.3
σ	2000	1800
κ s.t. $2^{\kappa} \cdot \binom{N}{\kappa} \geq 2^{256}$	44	36
$M = \exp(\frac{2\tau\kappa\sigma+\kappa^2}{2\sigma^2})$	≈ 7.4	≈ 7.4
Lattice strength	1.0035	1.0017
public key size $(\log_2 q + 2)t$	832 Bytes	1664 Bytes
signature length $\approx (\log_2 \sigma + 2)N + \min(\kappa \log_2 N, N)$	882 Bytes	1709 Bytes

Table 1. PASS$_{RS}$ Signature Scheme Parameter

where $\mathbf{I}_t$ is a t dimensional identity matrix. This lattice has a unique shortest vector $\langle 0, \mathbf{f}, 1\rangle$ with an l_2 norm of approximately $\sqrt{2N/3+1}$. On the other hand, it has been shown in [6] that the ability to locate a unique shortest vector in a lattice depends on the root Hermite factor of the lattice, which is the n-th root of

$$\frac{\text{Gaussian expected length}}{l_2 \text{ norm of the target vector}}$$

where $n = (N+t+1)$ is the dimension of the lattice. We known that the Gaussian expected length of this lattice is $\sqrt{\frac{N+t+1}{2\pi e}} q^{\frac{t}{N+t+1}}$. This results in

$$\left(\frac{\sqrt{\frac{N+t+1}{2\pi e}} q^{\frac{t}{N+t+1}}}{\sqrt{2N/3+1}} \right)^{\frac{1}{N+t+1}}$$

With $t \approx N/2$, this quantity is $\approx \left(\sqrt{9/(8\pi e)} q^{\frac{1}{3}} \right)^{\frac{2}{3N}}$.

For the parameter sets that we are suggesting, this yields 1.0035 and 1.0017, respectively. Applying the latest results of estimating the cost of the BKZ 2.0 algorithm with (quantum) sieving [3, 1, 2], we estimate the cost to recover this shortest vector requires at least 2^{129} and 2^{198} operations.

Acknowledgement We appreciate the anonymous reviewers for their valuable suggestions. Part of this work was supported by the National Natural Science Foundation of China (Grant No. 61602396, U1636205), and from the Research Grants Council of Hong Kong (Grant No. 25206317).

Reference

1. E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. Post-quantum key exchange - A new hope. In *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016.*, pages 327–343, 2016.

2. S. Bai, T. Laarhoven, and D. Stehle. Tuple lattice sieving. Cryptology ePrint Archive, Report 2016/713, 2016. `https://eprint.iacr.org/2016/713`.
3. Y. Chen and P. Q. Nguyen. BKZ 2.0: Better lattice security estimates. In D. H. Lee and X. Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2011.
4. L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky. Lattice signatures and bimodal gaussians. In R. Canetti and J. A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 40–56. Springer, 2013.
5. L. Ducas, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehle. Crystals – dilithium: Digital signatures from module lattices. Cryptology ePrint Archive, Report 2017/633, 2017. `https://eprint.iacr.org/2017/633`.
6. N. Gama and P. Q. Nguyen. Predicting lattice reduction. In N. P. Smart, editor, *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*, pages 31–51. Springer, 2008.
7. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In C. Dwork, editor, *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*, pages 197–206. ACM, 2008.
8. O. Goldreich, S. Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. In B. S. K. Jr., editor, *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, volume 1294 of *Lecture Notes in Computer Science*, pages 112–131. Springer, 1997.
9. J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, and W. Whyte. Practical signatures from the partial fourier recovery problem. In I. Boureanu, P. Owesarski, and S. Vaudenay, editors, *Applied Cryptography and Network Security - 12th International Conference, ACNS 2014, Lausanne, Switzerland, June 10-13, 2014. Proceedings*, volume 8479 of *Lecture Notes in Computer Science*, pages 476–493. Springer, 2014.
10. V. Lyubashevsky. Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*, pages 598–616, 2009.
11. V. Lyubashevsky. Lattice signatures without trapdoors. In Pointcheval and Johansson [14], pages 738–755.
12. V. Lyubashevsky and D. Micciancio. Asymptotically efficient lattice-based digital signatures. In R. Canetti, editor, *Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008.*, volume 4948 of *Lecture Notes in Computer Science*, pages 37–54. Springer, 2008.
13. D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In Pointcheval and Johansson [14], pages 700–718.
14. D. Pointcheval and T. Johansson, editors. *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*. Springer, 2012.