IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 10, 2018, accepted December 13, 2018, date of publication January 1, 2019,
date of current version January 11, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2889242

An Efficient Strong Designated Verifier Signature Based on $\mathcal{R}$−SIS Assumption

JIE CAI[1], HAN JIANG[2], PINGYUAN ZHANG[1], ZHIHUA ZHENG[3], GUANGSHI LYU[1], AND QIULIANG XU[2]

[1]School of Mathematics, Shandong University, Jinan 250100, China
[2]School of Software, Shandong University, Jinan 250101, China
[3]College of Information Science and Engineering, Shandong Normal University, Jinan 250358, China

Corresponding author: Han Jiang (jianghan@sdu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61572294, Grant 61602287, and Grant 11771252, in part by the State Key Program of National Natural Science of China under Grant 61632020, in part by the Natural Science Foundation of Shandong Province under Grant ZR2017MF021, in part by the Major Innovation Project of Science and Technology, Shandong, under Grant 2018CXGC0702, in part by the Fundamental Research Funds of Shandong University under Grant 2017JC019, and in part by the Primary Research & Development Plan of Shandong Province under Grant 2018GGX101037.

ABSTRACT The designated verifier signature (DVS), introduced by Jakobsson *et al.*, has the property that only the designated verifier can verify the generated signature. In order to prevent an eavesdropper to get the signature on-line before the designated verifier receives it, they also proposed strong designated verifier signature (SDVS). In this paper, according to an efficient SDVS proposed by Saeednia *et al.*, we present a post-quantum SDVS in the random oracle model based on lattice assumption. The unforgeability is based on the hardness of the average-case hard problem $\mathcal{R}-\mathrm{SIS}_{q,n,m,\beta}$, which is at least as hard as worst-case SVP_{γ} over ideal lattices. In addition, compared with existing lattice-based SDVS schemes, our scheme cuts by more than 50 percent repetitions and the size of signature is shorter with 256 bits security.

INDEX TERMS Designated verifier signature, lattice, post-quantum, SIS problem.

I. INTRODUCTION

With the development of digital signature schemes, more and more signature schemes with special characteristics are considered, such as blind signature, ID-based signature, group (ring) signature etc. In the cases of private bidding and auctions, secret ballot elections etc, there is a question that how to solve the contradiction between reliability and privacy. Designated verifier signature scheme provided the answer.

In 1996, the designated verifier signature (DVS) was first introduced by Jakobsson *et al.* [1]. It needs to satisfy a particular property that only designated verifier can verify the generated signature. Although the designated verifier can produce a simulated signature which is indistinguishable with the signer's, he can't convince others that the signer is the real producer for some signatures.

Unfortunately, the first proposed DVS scheme can't prevent an on-line eavesdropper to get the signature before it is received by designated verifier. And the signature is able to be verified by a third party. Thus, a definition called strong designated verifier signature (SDVS) against this attack was also proposed in [1]. In a SDVS scheme, verification step needs the private key of verifier, hence no one except designated verifier can verify it.

A. RELATED WORK

1) SDVS SCHEME BASED ON DISCRETE LOGARITHM PROBLEM

In [1], Jakobsson *et al.* provided two feasible techniques for making DVS to be a SDVS in transcripts. One way is to use a probabilistically encrypted with the public key of intended verifier; the other is to choose the symmetry encryption of a session key. However, the latter one inevitably brings an additional complex operation. In 2003, Saeednia *et al.* (SKM, for short) [2] designed the first efficient SDVS which was based on a merged applications of the Schnorr signature [3] and the Zheng signcryption schemes [4], without using any encryption or other operations. Thus, this scheme becomes a basic framework in designing SDVS schemes.

Then many other SDVS were provided [5]–[9]. Specifically, in 2004, Laguillaumie and Vergnaud [9] gave some new security definitions including unforgeability, untransferability and privacy of signer's identity (undelegateability). In 2007, Li *et al.* [8] showed undelegateability of [9] was so strong that no SDVS existed and maybe it was a controversial definition. Hence we don't consider this property in our scheme until a standard definition for protecting privacy of signer's identity is developed.

Unfortunately, the schemes described above are based on discrete logarithm problem, which can't resist against quantum adversaries. Hence more and more cryptographers begin to design post-quantum cryptographic schemes.

2) LATTICE-BASED SIGNATURES WITH GAUSSIAN SAMPLING AND UNIFORM SAMPLING

Generally speaking, the post-quantum cryptography systems mainly include lattice-based, code-based, multivariate cryptosystems and homology-based on supersingular elliptic curves cryptography.

Among of them, lattice-based cryptography has been widely studied. In recent years, many efficient lattice-based signature schemes were proposed [10]–[12]. From the viewpoint of improvement tendency, cryptographers focus on how to shorten the size of signature and times of rejection sampling. They usually use compression technique to shorten the signature size, where one can sign a message with high bits of a random number. In order to lower the repetition, people mainly utilize rejection sampling lemma and filtering technique.

Rejection sampling lemma (see [12]) was first provided in 2012, and the author gave a signature scheme with Gaussian sampling. In addition, the rejection probability was defined by $\min(f(z)/Mg_v(z), 1)$, where f, g were gaussian distribution, and $v, z, M \in \mathbb{R}$. It is easy to see a low rejection probability is depended on a small M. In 2013, Ducas et.al. proposed bimodal gaussian (see [11]) to reduce the number M.

However, in 2016, it has been proved that, with discrete Gaussian sampling technique, these schemes could lead to a lot of potential side-channel attacks, even complete leakage of private key [13], [14]. Although, one can design almost perfect implementations to protect against some side-channel attacks (see [15]), the intricacies make it an area where one can easily make mistakes.

To make schemes resist above attacks, one may use filtering technique with uniform sampling (see [16], [17]). The aim of rejection sampling aspect is to protect the secret key. The idea is the signer can select to output signatures by simply checking whether those signatures fall in a fixed range or not. Simply speaking, if we want to get a special number $c = a + b$ which can't reveal anything about a secret number $a \in [-B, B]$ (here B presents a non-negative bound), where $b \leftarrow_R [-5B, 5B]$ is uniformly chosen, the range of c must satisfies $c \in [-4B, 4B]$. Otherwise, we refresh b to make the distribution of c independent on a. Rückert (see [18]) extended it to polynomial rings and gave a reject aborting equation $e^{1/\Phi}$, where $\Phi \in \mathbb{N}^+$. In a concrete scheme, Φ is related to the size of signature more or less. Hence, determining its value needs to balance both of them.

3) LATTICE-BASED SDVS SCHEMES

As far as we know, The first lattice-based SDVS scheme [19] was proposed by Wang et.al. in 2012. According to the framework of SKM, they utilized the Bonsai trees and pre-image sampling function primitives to construct the SDVS. Its unforgeability and nontransferability were based on SIS problem and LWE problem respectively, which were proved in the random oracle model.

In 2013, Li *et al.* proposed a post-quantum SDVS [20] according to lattice-based signature scheme [21]. The security is based on SIS problem in the standard model, and they also use pre-image sampling function. In 2016, Noh and Jeong [22] provided a SIS-based SDVS scheme following from [19], and its security was reduced to the same hard problems with [19]. It is proved in the standard model.

However, all of these schemes have several disadvantages listed as follows:

- Gaussian sampling was used in their schemes, which is unusual to resist side-channel attack.
- They were designed in regular lattices instead of ideal lattice. Hence, this will inevitably bring larger size of public key and signature.
- They used pre-image sampling function and Bonsai trees, which will result in having fairly complex operations and large parameters.
- Since they focused on pure theoretical research, they didn't provide specific parameters of a real implementation in their schemes. In addition, no detailed comparisons were shown with other lattice-based SDVS schemes.

B. OUR CONTRIBUTION

In this paper, we put forward a new efficient SDVS scheme that is based on $\mathcal{R}-\mathrm{SIS}_{q,n,m,d}$ problem in ideal lattice with uniform sampling. Notice that our design is totally different from above lattice-based SDVS in the aspect of constructions of hard problem and sampling methods. In addition, we propose a new lemma (Lemma 1) to support the correctness of our design and proof.

- **Lower repetition and shorter size of signature.** The repetition of our scheme is 1.28 and the size of the signature is 42721 bits (16448 bits can be done using the technology in [10]) with 256-bit security. Obviously, our scheme has shorter signature size and repetition. There are several reasons for this:
  1) Our scheme is the first SDVS over ideal lattice ($\mathcal{R}-$SIS problem), and we don't use Bonsai trees and pre-image sampling. Hence we reduce the size of pk, signature and communication cost.
  2) We use a similar Fiat-Shamir framework [23] which is always used in many lattice-based signature schemes [10]–[12], [16], [17] to improve their efficiency. So our SDVS is efficient based on this framework.
- **Resisting side-channel attacks.** We utilize uniform sampling instead of Gaussian sampling which can effectively resist side-channel attacks [13]–[15].
- **Giving detailed parameters.** We provide the detailed parameters to show the lower size of pk, signature

and communication cost in our SDVS. Moreover, we also give comparisons with above lattice-based SDVS scheme.

C. ORGANIZATION OF THE PAPER

We firstly introduce some definitions of SDVS, describe the major design ideas of SKM lattices briefly and provide some necessary hard problems and lemmas in Section II. Then we show our detailed lattice-based SDVS scheme, its security proof and comparisons of parameter in Section III. Finally we present a conclusion and further work in Section IV.

II. PRELIMINARIES

A. STRONG DESIGNATED VERIFIER SIGNATURE

A SDVS scheme consists of four algorithms between signer (Alice) and a designated verifier (Bob). The specific definition is as follows:

Definition 1: Given an integer n, a SDVS with security parameter n is defined by the following:

- **Setup:** it is a probabilistic algorithm which takes n as input. The outputs are the public parameters (PK_a, SK_a) and (PK_b, SK_b) which belong to signer and designated verifier respectively;
- **Sign:** it is a probabilistic (deterministic) algorithm which takes a triple (μ, SK_a, PK_b) containing a message, a signing sk and a verifying pk as inputs. The output is a designated verifier signature σ of message μ;
- **Verify:** it is a deterministic algorithm which takes a quadruple $(\sigma, \mu, PK_a, SK_b)$ containing a bit string, a message, a signing pk and a verifying sk as inputs, and tests whether σ is a valid designated signature of μ with the keys (PK_a, SK_a, PK_b, SK_b).
- **Simulation:** it is a probabilistic algorithm which takes a quadruple (μ, PK_a, SK_b, PK_b) as inputs. Anyone and generate an indistinguishable signatures form those generated by the triple (μ, SK_a, PK_b).

A SDVS must satisfy the following secure properties.

1) **correctness:** a properly formed designated verifier signature must be accepted by the verifying algorithm. That is, for all valid (PK_a, SK_a, PK_b, SK_b) and a message μ, the equation holds:

$$\text{Verify}_{PK_a,PK_b,SK_b}(\text{Sign}_{PK_a,PK_b,SK_a}(\mu)) = \text{accept}.$$

2) **unforgeability:** here we give a brief game of existential unforgeable against adaptive chosen message attack (EUF-CMA) [8] between a polynomially bounded adversary $\mathcal{A}$ and a challenger $\mathcal{C}$.
   - The challenger $\mathcal{C}$ constructs valid pk and sk,
   $$(PK_a, PK_b, SK_a, SK_b) \leftarrow \text{setup}(1^n),$$
   where n is the security parameter. Then $\mathcal{C}$ sends (PK_a, PK_b) to the adversary $\mathcal{A}$.
   - $\mathcal{A}$ queries the signing oracle q_s times (which is polynomially bounded in n) at any time for message μ_i. The challenger $\mathcal{C}$ answers his queries by providing $\sigma_i = \text{Sign}(PK_a, PK_b, SK_a, \mu_i)$.
   - At the end of the game, we say that the adversary is success if he outputs a new signature σ^* for message μ^* satisfying correctness equation and $\mu^* \neq \mu_i$.

   For any polynomial time adversary $\mathcal{A}$ running above game in time t, we say that a SDVS scheme is (t, ε) EUF-CMA secure (unforgeability) if the below equation holds:
   $$\Pr[\text{Verify}_{SDVS,\mathcal{A}}^{EUF-CMA}(\sigma^*, \mu^*) = \text{accept}] \leq \varepsilon,$$
   where $\varepsilon > 0$ is a negligible function of secure parameter n.
3) **untransferability:** we also provide a game involving a challenger $\mathcal{C}$ and a distinguisher $\mathcal{D}$. $\mathcal{C}$ provides Sign and Simulation algorithms to simulate the attack environment for the distinguisher $\mathcal{D}$, then $\mathcal{D}$ tries to distinguish that a given output comes from the signer or designated verifier.
   - The challenger $\mathcal{C}$ produces valid pk and sk,
   $$(PK_a, PK_b, SK_a, SK_b) \leftarrow \text{setup}(1^n),$$
   where n is the security parameter. Then $\mathcal{C}$ sends (PK_a, PK_b) to $\mathcal{D}$, and the left keys are kept secret.
   - The distinguisher $\mathcal{D}$ queries the signatures for any message μ_i. The challenger $\mathcal{C}$ answers them by providing $\sigma_i = \text{Sign}(PK_a, PK_b, SK_a, \mu_i)$.
   - The distinguisher queries a new message μ^*. $\mathcal{C}$ tosses a coin $b \leftarrow_R \{0, 1\}$. If $b = 0$, he runs Sign algorithm and returns $\sigma^* = \text{Sign}(PK_a, PK_b, SK_a, \mu^*)$. Otherwise, he runs Simulation algorithm and returns $\sigma^* = \text{Simulation}(PK_a, PK_b, SK_b, \mu^*)$.
   - After receiving the challenging signature σ^*, $\mathcal{D}$ can query new messages expect for μ^*.
   - At the end of this game, $\mathcal{D}$ outputs a bit b' and wins it if $b = b'$.

   The advantage of $\mathcal{D}$ is defined as:
   $$\text{Adv}_{SDVS,\mathcal{D}}^{CMA} = |\Pr[b = b'] - 1/2|$$
   We say that a SDVS scheme is untransferability against a (t, q_s) adaptively chosen message distinguisher $\mathcal{D}$ if the value of the above equation is negligible after querying q_s signatures in time t.

In our paper, we will prove our scheme satisfies all of the above secure properties according to these formal definitions.

B. SKM DESIGNATED VERIFIER SCHEME

The SKM scheme is based on DL problem, they assume: a large prime p with a prime factor q of $p-1$, a generator $g \in \mathbb{Z}_p^*$ with order q and a hash function h with values in $\mathbb{Z}_q$. And all the initially common parameters are shared between the participants Bob and Alice.

Each participant i chooses his secret key $x_i \in \mathbb{Z}_q$ and publishes the corresponding public key $y_i = g^{x_i} \bmod p$.

1) SIGNATURE GENERATION

To sign a message μ for Bob, Alice selects two random values $k \in \mathbb{Z}_q$, $t \in \mathbb{Z}_p^*$ and computes

$$\begin{aligned} c &= y_b^k \, mod \, p, \\ r &= h(c, \mu), \\ s &= kt^{-1} - rx_a \, mod \, q. \end{aligned}$$

The triple (r, s, t) is the signature of the message μ.

2) VERIFICATION

Bob checks the correctness of equation $h((g^s y_a^r)^{tx_b} \, mod \, p, \mu) = r$.

Obviously, the above verification equation contains the private key of Bob, then only he can verify it. In addition, even if anyone else who gets this secret key can behave the same way as Bob to calculate the equation, he cannot show or prove the signature actually comes from Alice. Apparently Bob is able to produce indistinguishable transcripts.

3) TRANSCRIPT SIMULATION

Bob has the ability to simulate the signature. For example, he selects $s' \in \mathbb{Z}_q$, $r' \in \mathbb{Z}_q^*$ at random and computes

$$\begin{aligned} c &= g^{s'} y_a^{r'} modp, \\ r &= h(c, \mu), \\ l &= r' r^{-1} modq, \\ s &= s' l^{-1} modq, \\ t &= l x_b^{-1} modq. \end{aligned}$$

These values are substituted in the expression $(g^s y_a^r)^{tx_b} \, mod \, p$ to calculate c and get $h(c, \mu) = r$.

4) SECURITY

If an adversary can generate a valid signature without Alice's or Bob's secret keys, then he will have the ability to solve Diffie-Hellman problem $g^{x_a x_b}$ in polynomial time (see [2]).

C. LATTICES

Notation: We choose the quotient ring $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$, where q is a polynomial-size prime number, n is a power of 2 and elements in ring $\mathbb{Z}_q$ are the integers in the range $[-q/2, q/2]$. t^{-1} represents an invertible element in $\mathcal{R}_q$. The statement $x \leftarrow_R D$ shows that x is chosen uniformly at random from the finite set D. We will write D_k to denote all elements $\omega \in \mathcal{R}_q$ such that $\|\omega\|_\infty \leq k$. Particularly, B_k means $\omega \in \{-1, 0, 1\}^m$ such that $\|\omega\|_1 \leq k$. We denote two random variables X, Y over a discrete domain D, and define the statistical distance of them as $\Delta(X, Y) = 1/2 \sum_{a \in D} |Pr[X = a] - Pr[Y = a]|$.

The bold capital letters are matrices and bold small letters are vectors, while normal fonts for integers and real. All vectors are column-vectors unless otherwise noted. For a vector $\mathbf{v}$ (a matrix $\mathbf{S}$), we denote by $\mathbf{v}^T$ ($\mathbf{S}^T$) its transpose, by $\|\mathbf{v}\|$ its Euclidean norm (ℓ_2 norm), and by $\|\mathbf{v}\|_\infty$ its infinity norm. We let the ℓ_2 norm of the matrix is $\|\mathbf{S}\| = \max \|\mathbf{s}_i\|$ instead of the minimum of eigenvalue [24], where $\mathbf{s}_i$ is each column vector in $\mathbf{S}$. $h : \{0, 1\}^* \rightarrow \{-1, 0, 1\}^m$ is a cryptographic hash function hashing onto B_k (see [10], [12]).

Lattices are formally defined as discrete additive subgroups of $\mathbb{R}^m$. We often represent them as $\mathcal{L} = \mathbf{B}\mathbb{Z}^n$, $n \leqslant m$, where $\mathbf{B}$ is a basis. In cryptography, integral lattices, i.e. subgroups of $\mathbb{Z}^m$ are usually considered.

One of the most common hard problems about lattice is shortest vector problem (SVP). In fact, there are three variants of SVP, depending on whether find the shortest vector (search SVP), compute its length (optimization SVP), or decide if it is shorter than some given number (decisional SVP). And the three above variants are essentially equivalent.

Particularly important to lattice cryptography is approximation problem SVP_γ.

Definition 2: Given a basis $\mathbf{B}$ of n-dimensional lattice and $\gamma = \gamma(n), \gamma \neq 1$, find $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{v}\| \leq \gamma \cdot min\|\mathbf{v}\|$, which is called search approximate shortest vector problem (SVP_γ).

Similarly, approximate problems also have three versions. However, they are not equivalent, and whether the search version is not harder than the optimization version is an open question. Usually, the decisional version is denoted GapSVP_γ. The security of our scheme can be reduced to the decision version.

D. HARD PROBLEMS IN OUR SCHEME

1) HARD PROBLEM OVER RING

Generally speaking, lattice-based cryptographic schemes have large keys sizes, which mainly because the private and public keys matrices have large dimension and every entry in them is independent. Hence, People are beginning to think about ways to reduce this independence. For example, the matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ can be generated by choosing its first column $\mathbf{a}_0$ uniformly at random form $\mathbb{Z}_q^n$ and the left $n - 1$ columns, $\mathbf{a}_1, \ldots, \mathbf{a}_{n-1}$ are the coefficient representation of the polynomial $\mathbf{a}_0 \mathbf{x}^i$ in the ring $\mathbb{Z}_q[x]/(x^n+1)$. The generation of column $\mathbf{a}_n$ is the same as the first one. Repeat the previous process and get the final matrix.

The ring $\mathcal{R}_q$ is also considered as the sub-ring of anti-circulant square matrices where each ring element $r \in \mathcal{R}_q$ can be regarded as a linear transformation$x \mapsto r \cdot x$ over the coefficient embedding of $\mathcal{R}_q$. By constructing $\mathbf{A}$ like this, $\mathbf{As}$ is equivalent to polynomial multiplications and additions in the ring $\mathbb{Z}_q[x]/(x^n + 1)$. In 2006, references [25] and [26] introduced a ring variant of SIS independently.

2) SPECIFIC HARD PROBLEM OVER RING

The construction of our scheme is based on $\mathcal{R}-\mathrm{SIS}_{q,n,m,d}$ which is a variant of $\mathcal{R}-\mathrm{SIS}_{q,n,m,\beta}$ problem (see [12]). Always we suppose $m \geq 2n$, then a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ will contain n linearly independent columns over $\mathbb{Z}_q$ with high probability which is up to $e^{-\Omega(n)}$ when q is a prime of size at least $2m$. First we give definition of $\mathcal{R}-$SIS problem.

Definition 3 [11]: Let $\mathcal{R}$ be some ring and $\mathcal{K}$ be some distribution over $\mathcal{R}_q^{n\times m}$, where $\mathcal{R}_q$ is the quotient ring $\mathcal{R}/(q\mathcal{R})$. Given a random matrix $\mathbf{A} \in \mathcal{R}_q^{n\times m}$ following the distribution $\mathcal{K}$, find a non-zero vector $\mathbf{v} \in \mathcal{R}_q^m$ such that $\mathbf{Av} = \mathbf{0}$ and $\|\mathbf{v}\| \le \beta$, which is denoted $\mathcal{R}-\mathrm{SIS}^{\mathcal{K}}_{q,n,m,\beta}$ problem.

Then $\mathcal{R}-\mathrm{SIS}^{\mathcal{K}}_{q,n,m,d}$ problem has a limitation $\mathbf{s} \in \{-d,\ldots,0,\ldots,d\}^m$ such that $\mathbf{As} = \mathbf{t}$. Lyubashevsky [12] has proven the decision $\mathrm{SIS}_{q,n,m,d}$ problem is harder with increase of d, and there exists a polynomial-time reduction from $\mathrm{SIS}_{q,n,m,d}$ decision problem to the $\ell_2-\mathrm{SIS}_{q,n,m,\beta}$ problem under conditions $m = 2n$ and $4d\beta \le q$.

In [26], it was shown that if the ring $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$, where q is a polynomial-size prime number, n is a power of 2, then average case $\mathcal{R}-\mathrm{SIS}^{\mathcal{K}}_{q,1,m,\beta}$ problem is as hard as the worst case $\tilde{\mathcal{O}}(\sqrt{n}\beta)-$SVP problem for all lattices that are ideals in $\mathcal{R}$ where $\mathcal{K}$ is the uniform distribution over $\mathcal{R}_q^{1\times m}$.

In order to make our constructing correct and efficient, we provide a new lemme in the next part.

E. A NEW LEMMA FOR THE DESIGN OF OUR SCHEME

Here, we give the below lemma to show the conclusion over ring $\mathcal{R}_q^{2\times m}$ still holds. We provide the following lemma to ensure the security of our scheme. Now we show the necessity of constructing it, and then give a proof in detail.

- **The design of square matrix is necessary.** Since there are operations of matrix multiplication in our scheme, we need to design a square matrix to support multiplicative property.
- **The efficiency must kept.** We don't want to increase the computation with the increase of its dimension. Hence, we fill a general matrix $\mathbf{A}_1$ with zero matrix to get a square form directly. Notice that doing like this, the actual calculation is $\mathbf{A}_1\mathbf{V}_1$, and the expected result is attained.
- **The security must be ensured.** By proving the lemma, we can easily see that there is no change of the problem itself. Furthermore, the norm of new solution to SIS problem is equal to the original one. It means that this special square matrix doesn't impact on our security assumption.

Lemma 1: If the ring $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$, where q is a polynomial-size prime number, n is a power of 2 and $m = 2n$, then $\mathcal{R}-\mathrm{SIS}^{\mathcal{K}}_{q,2,m,\beta}$ problem is as hard as the $\tilde{\mathcal{O}}(\sqrt{n}\beta)-$SVP problem for all lattices that are ideals in $\mathcal{R}$ where $\mathcal{K}$ is the uniform distribution over $\mathcal{R}_q^{2\times m}$.

Proof: We suppose $\mathbf{A}_1 \in \mathcal{R}_q^{1\times m}$ and $\mathbf{v}_1,\cdots,\mathbf{v}_n \in \mathcal{R}_q^m$ satisfy $\mathbf{A}_1\mathbf{v}_i = \mathbf{0} \mod q$, $\|\mathbf{v}_i\|_2 \le \beta (i = 1,\cdots,n)$. We denote

$$\mathbf{A} = \begin{bmatrix}\mathbf{A}_1^{n\times m}\\ \mathbf{0}^{n\times m}\end{bmatrix}, \quad \mathbf{V}_1^{m\times n} = \left[\mathbf{v}_1,\cdots,\mathbf{v}_n\right],$$

and

$$\mathbf{V} = \left[\mathbf{V}_1^{m\times n}, \mathbf{0}^{m\times n}\right],$$

then, we verify that the value of $\mathbf{AV} \mod q$ is zero matrix or not. According to the multiplicative principle of block matrices, we get

$$\begin{aligned}\mathbf{AV} &= \begin{bmatrix}\mathbf{A}_1^{n\times m}\\ \mathbf{0}^{n\times m}\end{bmatrix}\left[\mathbf{V}_1^{m\times n}, \mathbf{0}^{m\times n}\right]\\ &= \begin{bmatrix}(\mathbf{A}_1\mathbf{V}_1)^{n\times n} & \mathbf{0}^{n\times n}\\ \mathbf{0}^{n\times n} & \mathbf{0}^{n\times n}\end{bmatrix}.\end{aligned}$$

Since we have the known condition $\mathbf{A}_1\mathbf{v}_i = \mathbf{0} \mod q$, then we get

$$\begin{aligned}\mathbf{A}_1\left[\mathbf{v}_1,\cdots,\mathbf{v}_n\right] &= \left[\mathbf{A}_1\mathbf{v}_1,\cdots,\mathbf{A}_1\mathbf{v}_n\right]\\ &= \mathbf{A}_1\mathbf{V}_1\\ &= \mathbf{0} \mod q\end{aligned}$$

Hence, $\mathbf{AV} = \mathbf{0} \mod q$ holds. By definition, $\|\mathbf{V}\| = \max\|\mathbf{v}_i\|$, where $i = 1,\cdots,2n$. However, according to the construction of $\mathbf{V}$, the values of i from $n+1$ to $2n$ are 0. Then we have $\|\mathbf{V}\| = \max\|\mathbf{v}_i\| = \|\mathbf{V}_1\| = \beta$. Since it doesn't change the length of the shortest vector, its security also can be reduced to $\tilde{\mathcal{O}}(\sqrt{n}\beta)-$SVP problem without a loss of problem gap. We finish our proof.

With the above proof and analysis, the unforgeability of our scheme can be reduced to $\mathcal{R}-\mathrm{SIS}_{q,n,m,d}$ problem, which ensures the problem our design based on is also hard.

F. FILTERING TECHNIQUE OVER RING

In our scheme, we use uniform distribution over ring, and the rejection sampling aspect is simply check whether the individual coefficients of signature fall in a fixed range.

Lemma 2: [18] Let $m = \Omega(n)$, $\mathbf{a},\mathbf{b} \in \mathbb{Z}^m$ with arbitrary $\mathbf{a} \in \{\mathbf{v} \in \mathbb{Z}^m : \|\mathbf{v}\|_\infty \le A\}$ and random $\mathbf{b} \leftarrow_R \{\mathbf{v} \in \mathbb{Z}^m : \|\mathbf{v}\|_\infty \le B\}$. Given $B \ge \Phi mA$ for $\Phi \in \mathbb{N}^+$, we have $Pr[\|\mathbf{a}-\mathbf{b}\|_\infty \le B - A] > \frac{1}{e^{1/\Phi}} - o(1)$.

This lemma tells us that if we choose random vector $\mathbf{b}$ appropriately, the norm of $\mathbf{a}-\mathbf{b}$ is constrained in a expected range with high probability. Thus it can protect the secret vector (usually $\mathbf{a}$). In our scheme, there is an important signature process $\mathbf{z} = \mathbf{S}_a\mathbf{r} + \mathbf{kt}^{-1}$, in which the signature $\mathbf{z}$ can be fell within a range to hide the secret key $\mathbf{S}_a$, as long as $\mathbf{kt}^{-1}$ is reasonably assigned.

Besides, the final probability inequation in this lemma is actually a formula of repetitions. If we want get a secure domain for the signature $\mathbf{z}$, we must repeat this process $e^{1/\Phi}$ times. In addition, the value of Φ affects the size of signature, thus how to determine it is an emphatic problem (see Fig.1).

III. OUR CONSTRUCTION

In this section, we firstly go into details about our post-quantum protocol in which it contains key-generation, signing, verification, simulation algorithms. Then we provide the security proof according to our formal security definitions. Finally, we list the parameters in our scheme.

Particularly, in the key-generation phase of our scheme, we need construct a square matrix public key $\mathbf{A}$, which can't add extra calculations. Hence, we use a obvious method that is filling the square matrix with $\mathbf{A} \in \mathcal{R}_q^{n\times m}$ and $\mathbf{0}^{n\times m}$.

Furthermore, the security of this structure is still proved (see detailed Lemma 1). In signing and verification phases, we using filtering technique (Lemma 2) over ring to get an efficient scheme, which can resist side-channel attacks and has lower repetition 1.28.

In order to shorten the signature size in Table 1, we utilize a form of Module-SIS problem, then the final result is 16448 bits.

A. OUR SCHEME

1) KEY GENERATION

We now briefly sketch the key generation algorithm of our designated verifier signature scheme. Here we firstly give a description on regular lattice, then show a ring setting on ideal lattice. There are two secret matrices $\mathbf{S}_a$, $\mathbf{S}_b \in D_d^{m\times m}(D = \mathbb{Z})$ with small coefficients. The reason we choose such high dimensions $(m \times m)$ is that it can keep matrix multiplications running smoothly. The public key consists of the matrices $\mathbf{A}, \mathbf{Y}_a, \mathbf{Y}_b \in \mathbb{Z}_q^{m\times m}$ such that $\mathbf{A}^T\mathbf{S}_a \, mod\, q = \mathbf{Y}_a$, $\mathbf{A}\mathbf{S}_b \, mod\, q = \mathbf{Y}_b$ respectively. Notice that $\mathbf{A}$ is also a square matrix, and other schemes always choose uniformly at random $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$. Nevertheless, this will not increase the actually computational capacity by the proof of *lemma 1*. In ring variants of our scheme, we have $\mathbf{A} \in \mathcal{R}_q^{2\times m}, \mathbf{S}_i(i = a, b) \in \mathcal{R}_q^m$. In the following algorithm, KeyGen, SigKey, VerKey, and RO represent key generation, signing key, verification key and random oracle respectively.

KeyGen:	
SigKey:	$\mathbf{S}_i \leftarrow_R \{-d, \ldots, 0, \ldots, d\}^{m\times m}(i = a, b)$
VerKey:	$\mathbf{A} \leftarrow_R \mathbb{Z}_q^{m\times m}$, $\mathbf{Y}_a \leftarrow \mathbf{A}^T\mathbf{S}_a$, $\mathbf{Y}_b \leftarrow \mathbf{A}\mathbf{S}_b$
RO:	$h : \{0, 1\}^* \rightarrow \{\mathbf{r} : \mathbf{r} \in \{-1, 0, 1\}^m, \parallel \mathbf{r} \parallel_1 \leq \eta\}$, η is the Hamming weight of $\mathbf{r}$.

$(\mathbf{S}_a, \mathbf{Y}_a)$ is Alice's secret key and $(\mathbf{S}_b, \mathbf{Y}_b)$ belongs to Bob.

2) SIGNATURE GENERATION

Let β be a integer such that $\|\mathbf{S}_a\mathbf{r}\|_\infty < \beta$ with high probability over the choices of $\mathbf{S}_a \leftarrow D_d^{m\times m}$ and $\mathbf{r} \leftarrow B_\eta$. Then Alice computes

Sign:
1. $\mathbf{t} \leftarrow_R D_\gamma^m(\gamma \leq q)$
2. if $\mathbf{t}$ is not reversible, then goto 1.
3. $\mathbf{k} \leftarrow_R D_\gamma^m$
4. $\mathbf{c} = \mathbf{Y}_b^T\mathbf{k} \, mod\, q$
5. $\mathbf{r} = h(\mathbf{c}, \mu)$
6. $\mathbf{z} = \mathbf{S}_a\mathbf{r} + \mathbf{k}\mathbf{t}^{-1}$
7. if $\parallel \mathbf{z} \parallel_\infty \geq \gamma - \beta$ or $\parallel \mathbf{S}_a\mathbf{r} \parallel_\infty > \beta$, then goto 3.
8. output the signature $(\mathbf{r}, \mathbf{z}, \mathbf{t})$ of message μ.

Notice that there are two rejecting steps, step 2 and step 7. We now compute the probability step 2 and step 7 will not result in a restart.

About step 2, we will refer to [27] for the invertibility of parameter $\mathbf{t}$. We give a simple description

Input : parameters N, σ, q and B_γ
Output : $\mathbf{t}$
1. $\mathbf{t} \leftarrow T(\sigma + 1, \sigma)$
2. **if** $\mathbf{t}$ is not invertible mod q then goto step 1 **end if**
3. **if** $\parallel \mathbf{t} \parallel_1 \geq B_\gamma$ then goto step 1 **end**
4. **return** $\mathbf{t}$

Here, $T(\sigma + 1, \sigma)$ is a trinary polynomials of degree less than N, where there are $\sigma + 1$ positive coefficients and σ negative coefficients. If $\sigma = 205, \gamma = 40$, the above process can be completed in $48.9ms$ (see [27]). Hence we do not consider the probability of repetition in this step any longer.

About step 7, the probability $\|\mathbf{z}\|_\infty \geq \gamma - \beta(\gamma > 1/2)$ can be computed by considering each coefficient separately. Suppose each coefficient of $\mathbf{S}_a\mathbf{r}$ is δ, then the corresponding coefficient of $\mathbf{z}$ will fall within $-\gamma + \beta + 1$ and $\gamma - \beta - 1$ when the coefficient of $\mathbf{k}\mathbf{t}^{-1}$ falls within $-\gamma + \beta + 1 - \delta$ and $\gamma - \beta - 1 - \delta$. The size of this range is $2(\gamma - \beta) - 1$ and the coefficient of $\mathbf{k}\mathbf{t}^{-1}$ have $2\gamma - 1$. Thus, the probability that every coefficient of $\mathbf{k}\mathbf{t}^{-1}$ is in the good range is

$$(\frac{2(\gamma - \beta) - 1}{2\gamma - 1})^m = (1 - \frac{\beta}{\gamma - 1/2})^m \approx e^{-m\beta/\gamma}$$

About β in step 7, $\|\mathbf{S}_a\mathbf{r}\|_\infty \leq d\eta$, then $\beta \leq d\eta$. And by the *lemma 2*, β must satisfy the inequations $\Phi m\beta \leq \gamma$.

3) VERIFICATION

Bob verities the equations

Verify:
1. $h(\mathbf{c}, \mu) = h(\mathbf{S}_b^T(\mathbf{A}^T\mathbf{z} - \mathbf{Y}_a\mathbf{r})\mathbf{t} \, mod\, q, \mu)$
2. $\|\mathbf{z}\|_\infty \geq \gamma - \beta$

It is easy to see that the private key of Bob makes the verification equation can be computed by him only.

4) TRANSCRIPT SIMULATION

Bob simulates the signature as follows. He randomly chooses $\mathbf{z}'$ and $\mathbf{r}'$. Let

$$\mathbf{S}_b^T(\mathbf{A}^T\mathbf{z} - \mathbf{Y}_a\mathbf{r})\mathbf{t} = \mathbf{c} = \mathbf{S}_b^T(\mathbf{A}^T\mathbf{z}' - \mathbf{Y}_a\mathbf{r}') \, mod\, q$$

We get equations

$$\mathbf{z} = \mathbf{z}'\mathbf{t}^{-1},$$
$$\mathbf{r} = \mathbf{r}'\mathbf{t}^{-1}.$$

Compared to SKM designated verifier scheme, an important part of the constructed signature, $(\mathbf{z}, \mathbf{r})$, doesn't contain Bob's secret key here. Even so, it does not affect Bob's ability. Rather, we can see that anybody who gets the value of $\mathbf{t}$ may produce a distinguishable view with Bob's. This way, it satisfies strong designated verifier scheme requirements defined above.

B. SECURITY

1) CORRECTNESS

Suppose Bob gets the signature $\sigma = (\mathbf{r}, \mathbf{z}, \mathbf{t})$ form Alice, if the condition $\|\mathbf{z}\|_\infty \geq \gamma - \beta$ holds, then he computes

$$\begin{aligned}\mathbf{S}_b^T(\mathbf{A}^T\mathbf{z} - \mathbf{Y}_a\mathbf{r})\mathbf{t} &= \mathbf{S}_b^T\mathbf{A}^T\mathbf{z}\mathbf{t} - \mathbf{S}_b^T\mathbf{Y}_a\mathbf{r}\mathbf{t} \\ &= \mathbf{S}_b^T\mathbf{A}^T\mathbf{z}\mathbf{t} - \mathbf{S}_b^T\mathbf{A}^T\mathbf{S}_a\mathbf{r}\mathbf{t} \\ &= \mathbf{S}_b^T\mathbf{A}^T(\mathbf{z} - \mathbf{S}_a\mathbf{r})\mathbf{t} \\ &= \mathbf{Y}_b^T\mathbf{k} \mod q. \end{aligned} \tag{1}$$

Hence, the below equation holds,

$$\text{Verify}_{\mathbf{Y}_a,\mathbf{Y}_b,\mathbf{S}_b}(\text{Sign}_{\mathbf{Y}_a,\mathbf{Y}_b,\mathbf{S}_a}(\mu)) = \text{accept}.$$

2) UNFORGEABILITY

Theorem 1: If an adversary $\mathcal{A}$ can generate a new valid signature σ^* by the game of EUF-CMA in time t, then he may have the ability to solve the $\mathcal{R}$−SIS$_{q,n,m,d}$ search problem in polynomial time.

Proof: We now prove that our scheme is (t, ε) EUF-CMA secure (unforgeability).

Assume a PPT attacker $\mathcal{A}$ has an ability to produce a signature $\sigma^* = (\mathbf{r}^*, \mathbf{z}^*, \mathbf{t}^*)$ which can be correctly verified at the end of the EUF-CMA game, then he can compute the following equation.

$$\begin{aligned}\mathbf{S}_b^T(\mathbf{A}^T\mathbf{z}^* - \mathbf{Y}_a\mathbf{r}^*)\mathbf{t}^* &= (\mathbf{S}_b^T\mathbf{A}^T\mathbf{z}^* - \mathbf{S}_b^T\mathbf{Y}_a\mathbf{r}^*)\mathbf{t}^* \\ &= (\mathbf{Y}_b^T\mathbf{z}^* - \mathbf{S}_b^T\mathbf{Y}_a\mathbf{r}^*)\mathbf{t}^* \, mod q \end{aligned} \tag{2}$$

As a matter of fact, the attacker can continue to calculate the above equation, i.e.,

$$\begin{aligned}(\mathbf{Y}_b^T\mathbf{z}^* - \mathbf{S}_b^T\mathbf{Y}_a\mathbf{r}^*)\mathbf{t}^*(\mathbf{t}^*)^{-1} - \mathbf{Y}_b^T\mathbf{z}^* &= \mathbf{Y}_b^T\mathbf{z}^* - \mathbf{S}_b^T\mathbf{Y}_a\mathbf{r}^* - \mathbf{Y}_b^T\mathbf{z}^* \\ &= -\mathbf{S}_b^T\mathbf{Y}_a\mathbf{r}^* mod q, \end{aligned} \tag{3}$$

In fact, he can simplify $-\mathbf{S}_b^T\mathbf{Y}_a\mathbf{r}^*$ further to $-\mathbf{Y}_b^T\mathbf{S}_a\mathbf{r}^*$.

We note $\mathbf{W} = -\mathbf{Y}_b^T\mathbf{S}_a\mathbf{r}^* \, mod \, q$, and so long as $\|\mathbf{S}_a\mathbf{r}^*\| \leq \beta$ $(0 < \beta < d\eta$ is polynomial in $n)$, thereupon, he gets a solution for $\mathcal{R}$−SIS$_{q,n,m,d}$ search problem.

To further discuss security, the Lemma 1 provides the possibility which is polynomial-time reduction form this average-case hard problem to the worst-case hard problem.

Summing up the above analysis, we get

$$\begin{aligned}&\Pr[\text{Verify}_{SDVS,\mathcal{A}}^{EUF-CMA}(\sigma^*, \mu^*) = \text{accept}] \\ &\quad = \Pr[\mathbf{W} = -\mathbf{Y}_b^T\mathbf{S}_a\mathbf{r}^* \mod q \mid \|\mathbf{S}_a\mathbf{r}^*\| \leq \beta] \\ &\quad \leq \varepsilon. \end{aligned}$$

3) UNTRANSFERABILITY

Theorem 2: The above scheme is untransferability against a (t, q_s) adaptively chosen message distinguisher $\mathcal{D}$, where q_s is the times of querying signatures in time t from challenger $\mathcal{C}$.

Proof: According to the definition of untransferability game between the distinguisher $\mathcal{D}$ and challenger $\mathcal{C}$, we now prove the advantage of $\mathcal{D}$ is negligible. That is the equation $\text{Adv}_{SDVS,\mathcal{D}}^{CMA} = |\Pr[b = b'] - 1/2| < \varepsilon$ holds.

Suppose distinguisher $\mathcal{D}$ has adaptively queried q_s signatures, then he queries a new message μ^*. $\mathcal{C}$ tosses a coin $b \leftarrow_R \{0, 1\}$. If $b = 0$, he runs Sign algorithm and returns $\sigma^* = \text{Sign}(PK_a, PK_b, SK_a, \mu^*)$. Otherwise, he runs Simulation algorithm and returns $\sigma^* = \text{Simulation}(PK_a, PK_b, SK_b, \mu^*)$. After receiving the challenging signature σ^*, $\mathcal{D}$ can query new messages expect for μ^*.

At the end of game, we will compute the advantage of $b = b'$. Firstly, we prove the following distributions are identical. Then we give the result. We let the left of vertical bar represent the case $b = 0$ (Sign algorithm), and the right part is the case $b = 1$ (Simulation algorithm). Then we compute the probabilities of these cases:

$\mathbf{k}, \mathbf{t} \in D_\gamma^m$	$\mathbf{z}', \mathbf{r}' \in D_\gamma^m$
$\mathbf{r} = h(\mathbf{Y}_b^T\mathbf{k} \, mod \, q, \mu)$	$\mathbf{r} = h(\mathbf{S}_b^T(\mathbf{A}^T\mathbf{z}' - \mathbf{Y}_a\mathbf{r}') mod \, q, \mu)$
$\mathbf{z} = \mathbf{S}_a\mathbf{r} + \mathbf{k}\mathbf{t}^{-1}$	$\mathbf{z} = \mathbf{z}'\mathbf{t}^{-1}$
	$\mathbf{t} = \mathbf{r}'\mathbf{r}^{-1}$

Let $(\tilde{\mathbf{r}}, \tilde{\mathbf{z}}, \tilde{\mathbf{t}})$ be a randomly chosen signature in the set where all valid signatures. Then we have the following probability distribution equations:

$$\begin{aligned}&Pr[(\mathbf{r}, \mathbf{z}, \mathbf{t}) = (\tilde{\mathbf{r}}, \tilde{\mathbf{z}}, \tilde{\mathbf{t}})] \\ &\quad = \Pr_{\mathbf{k};\mathbf{t}\neq\mathbf{0}}\begin{bmatrix}\mathbf{r} = h(\mathbf{Y}_b^T\mathbf{k} mod \, q, \mu) = \tilde{\mathbf{r}} \\ \mathbf{t} = \tilde{\mathbf{t}} \\ \mathbf{z} = \mathbf{S}_a\mathbf{r} + \mathbf{k}\mathbf{t}^{-1} = \tilde{\mathbf{z}}\end{bmatrix} \\ &\quad = \frac{1}{\gamma^m(\gamma^m - 1)} \end{aligned} \tag{4}$$

$$\begin{aligned}&Pr[(\mathbf{r}, \mathbf{z}, \mathbf{t}) = (\tilde{\mathbf{r}}, \tilde{\mathbf{z}}, \tilde{\mathbf{t}})] \\ &\quad = \Pr_{\mathbf{z}';\mathbf{r}'\neq\mathbf{0}}\begin{bmatrix}\mathbf{r} = h(\mathbf{S}_b^T(\mathbf{A}^T\mathbf{z}' - \mathbf{Y}_a\mathbf{r}') \, mod \, q, \mu) = \tilde{\mathbf{r}} \\ \mathbf{t} = \mathbf{r}'\mathbf{r}^{-1} = \tilde{\mathbf{t}} \\ \mathbf{z} = \mathbf{z}'\mathbf{r}\mathbf{r}'^{-1} = \tilde{\mathbf{z}}\end{bmatrix} \\ &\quad = \frac{1}{\gamma^m(\gamma^m - 1)} \end{aligned} \tag{5}$$

which means that both distributions of probabilities are the same.

Since the probability is the same in the two case, we can see distinguisher $\mathcal{D}$ can't distinguish the signature query about message μ^* at the end of this game. That is to say, the below equation holds.

$$\text{Adv}_{SDVS,\mathcal{D}}^{CMA} = |\Pr[b = b'] - 1/2| < \varepsilon.$$

C. PARAMETERS

1) PARAMETERS OF OUR SCHEME

We let $m = 2n$ to ensure that there exists a polynomial-time reduction from solving the SIS$_{q,n,m,d}$ decision problem to the ℓ_2−SIS$_{q,n,m,\beta}$ problem. η satisfies $2^\eta \cdot C_m^\eta \geq 2^{256}$ for which main reason is that (generally) one only needs random oracle output λ bits for obtaining signatures with λ bits security. According to the signature size discussion, smaller Φ is better, but it can increase the repetitions. Thus, taking into consideration of these characteristics, we set $\Phi = 4$. A simple analysis is given in appendix I later (see, Fig. 1). Since $\eta = 31$, $\beta \leq d\eta$, we let $d = 1$ so that making the

TABLE 1. Parameters for 256 bits security.

Parameters	Relationship	Value
q	prime	8380417
n	power of 2	1024
m	$= 2n$	2048
η	$2^{\eta} \cdot C_m^{\eta} \geq 2^{256}$	31
Φ	$-$	4
$e^{-1/\Phi}$	$-$	≈ 0.78
d	$-$	1
β	$\leq d\eta$	31
γ	$\geq m\log(\Phi\beta)$	14242
secret key size (bit)	$\approx m^2\log(2d+1)$	$2^{22.7}$
public key size (bit)	$\approx m^2\log(q)$	$2^{26.5}$
signature size (bit)	$< 3\gamma - \log(\beta)$	**42721**
repetition	$e^{1/\Phi}$	**1.28**

value of β small enough, and then the signature size is also sufficiently small.

The sizes of secret key and public key are in regular lattice of our scheme, and if the secret key and public key are chosen in ideal lattice, they exactly are $m\log(2d+1)$ and $m\log q$. See the table below for more details. Apparently the signature size of our scheme is a little larger than the other general lattice-based schemes in ideal lattices because of an extra parameter t.

2) IMPROVED PARAMETERS

From Table 1, we can see the sizes of the *sk*, *pk* and *signature* in our scheme typically rely on the parameter n. Notice that our scheme doesn't use module lattices or any other compression techniques. If we utilize compression method of [10], the signature length is small enough to use in practice. Ducas *et al.* [10] presented the Module-SIS problem, where $k, l \geq 1$ ($k, l \in \mathbb{Z}$) and $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n+1)$ (they choose $k = l = 4, n = 256$ which is similar with the ring case $k = l = 1$ and $n = 1024$) to ensure the same security with 256 bits. Our construction is actually based on the case $k = l = 1$. Ultimately, the signature length is 16448 bits which is small enough, and the approximate value of *pk* is $2^{13.5}$ bits.

We state any method which can reduce the size of parameter n under a certain security must reduce the sizes of the *sk*, *pk* and *signature* in our scheme.

3) THE COMPARISONS

The size of our scheme is clearly larger than SKM based on discrete logarithm problem. That is because lattice-based schemes basically need choose a large parameter to ensure security. Thus we don't give a contrast of sizes for those parameters anymore.

Additionally, since SDVS schemes [20], [22] are proved the security in standard model which include more complex operations, here we only show comparable parameters except repetition in the following table with them.

Actually, in SDVS schemes Wang *et al.* [19], Li *et al.*[20], and Boyen [21] must choose large parameters to use pre-image sampling function and Bonsai trees with Gaussian sampling. For example, they need to choose $m \gg 2n$, which result in large signature size. In addition, we know that as signature size increases, the repetition M also increases with Gaussian sampling (see [11]). Since our scheme is based on $\mathcal{R}-$SIS assumption with uniform sampling, our results of signature size and repetition are better than others.

TABLE 2. Performance comparisons with 256 bits security.

Scheme	Hard problem	Model	signature size (bit)	Repetition
Wang [19]	LWE,SIS	RO	3.3×10^6	2.72
Noh [22]	LWE,SIS	standard	9.7×10^4	–
Li [20]	SIS	standard	1.3×10^7	–
Ours	$\mathcal{R}-$SIS	RO	1.6×10^4	1.28

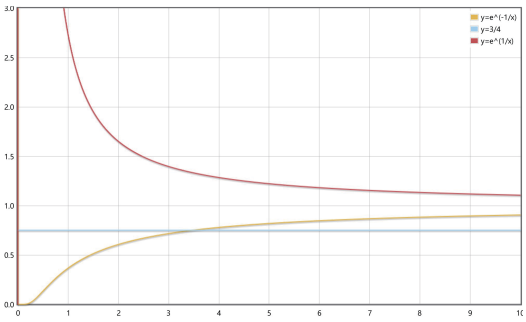

FIGURE 1. Acceptation probability and repetition functions.

IV. CONCLUSION AND FURTHER WORK

Conclusion: In this paper, according to the first SDVS scheme (SKM), we show an efficient lattice-based designated verifier signature. Our scheme has shorter signature size and lower repetition compared with other known lattice-based SDVS schemes.

Further Work: We are certain that the sizes of parameters in our scheme can be as short as existing lattice-based ones. However, there are several meaningful points that need to be focused on in the design aspect.

1) The generations of *pk* for Alice and Bob are a little different, $\mathbf{A}^T\mathbf{S}_a \bmod q = \mathbf{Y}_a$, $\mathbf{AS}_b \bmod q = \mathbf{Y}_b$ respectively. We want to design them in the same form if we can.
2) The definition of *strong* designated verifier scheme is only qualified in SKM and ours. The privacy of signers identity (non-delegate-ability) is also a meaningful definition SDVS (see [9]). We find the latter is actually show a description of witness indistinguishable of knowledge for the signer. In the next stage we will constructs a lattice-based witness indistinguishable of knowledge protocol to reach the aim.
3) If the above failed, we continue to explore new frameworks to design SDVS. And we try to give a proof that one SDVS based on a combination of a signature protocol and signcryption can not possibly satisfy the above requirements.

APPENDIX

We show the acceptation probability and repetition functions in Fig. 1. Without loss of generality, we denote x and y represent independent and dependent variables respectively. We can see that the probability y is decreased first, and then increase with increased x (repetition is opposite). If you just see it from probability and repetition, the value of x is as bigger as better. And in that case, probability and repetition are close to 1.

Nonetheless, the size of our signature increases with the increase of variable x. The expression can be simplified $\log(2^{2055}x - 2^5)$. Of course, people want to x, the smaller the better, in order to shorten the size. For above reasons, we must make a trade off. So we only consider the part in which y is more than 0.75 and less than 1.5. At this point, x need satisfy condition $x \geq 4$ and $x = 4$ should be most appropriate.

REFERENCES

[1] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Zaragoza, Spain, 1996, pp. 143–154.
[2] S. Saeednia, S. Kremer, and O. Markowitch, "An efficient strong designated verifier signature scheme," in *Proc. 6th Int. Conf. ICISC*, Seoul, South Korea, 2003, pp. 40–54.
[3] C. P. Schnorr, "Efficient signature generation by smart cards," *J. Cryptol.*, vol. 4, no. 3, pp. 161–174, 1991.
[4] Y. Zheng, "Digital signcryption or how to achieve cost(signature & encryption) ≪ cost(signature) + cost(encryption)," in *Proc. 17th Annu. Int. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA, 1997, pp. 165–179.
[5] Q. Huang, G. Yang, D. S. Wong, and W. Susilo, "Efficient strong designated verifier signature schemes without random oracles or delegatability," IACR Cryptol. ePrint Arch., Santa Barbara, CA, USA, Tech. Rep. 2009/518, 2009, p. 518. [Online]. Available: http://eprint.iacr.org/2009/518
[6] J. Ki, J. Y. Hwang, D. Nyang, B.-H. Chang, D. H. Lee, and J.-I. Lim, "Constructing strong identity-based designated verifier signatures with self-unverifiability," *ETRI J.*, vol. 34, no. 2, pp. 235–244, Apr. 2012.
[7] J. G. Li, N. Qian, X. Y. Huang, and Y. C. Zhang, "Certificate-based strong designated verifier signature scheme," *Chin. J. Comput.*, vol. 35, no. 8, pp. 1579–1587, Aug. 2012.
[8] Y. Li, W. Susilo, Y. Mu, and D. Pei, "Designated verifier signature: Definition, framework and new constructions," in *Proc. 4th Int. Conf. UIC*, Hong Kong, 2007, pp. 1191–1200.
[9] F. Laguillaumie and D. Vergnaud, "Designated verifier signatures: Anonymity and efficient construction from *any* bilinear map," in *Proc. 4th Int. Conf. SCN*, Amalfi, Italy, Sep. 2004, pp. 105–119.
[10] L. Ducas, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-dilithium: Digital signatures from module lattices," IACR Cryptol. ePrint Arch., Santa Barbara, CA, USA, Tech. Rep. 2017/633, 2017, p. 633. [Online]. Available: http://eprint.iacr.org/2017/633
[11] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, "Lattice signatures and bimodal Gaussians," in *Proc. 33rd Annu. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA, 2013, pp. 40–56.
[12] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Proc. 31st Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Cambridge, U.K., 2012, pp. 738–755.
[13] L. G. Bruinderink, A. Hülsing, T. Lange, and Y. Yarom, "Flush, Gauss, and reload—A cache attack on the BLISS lattice-based signature scheme," in *Proc. 18th Int. Conf. CHES*, Santa Barbara, CA, USA, 2016, pp. 323–345.
[14] P. Pessl, "Analyzing the shuffling side-channel countermeasure for lattice-based signatures," in *Proc. 17th Int. Conf. Cryptol. (INDOCRYPT)*, Kolkata, India, 2016, pp. 153–170.
[15] D. Micciancio and M. Walter, "Gaussian sampling over the integers: Efficient, generic, constant-time," IACR Cryptol. ePrint Arch., Santa Barbara, CA, USA, Tech. Rep. 2017/259, 2017, p. 259. [Online]. Available: http://eprint.iacr.org/2017/259
[16] V. Lyubashevsky, "Lattice-based identification schemes secure under active attacks," in *Proc. 11th Int. Workshop Pract. Theory Public-Key Cryptogr. (PKC)*, Barcelona, Spain, 2008, pp. 162–179.
[17] V. Lyubashevsky, "Fiat-shamir with aborts: Applications to lattice and factoring-based signatures," in *Proc. 15th Int. Conf. Theory Appl. Cryptol. Inf. Secur. (ASIACRYPT)*, Tokyo, Japan, 2009, pp. 598–616.
[18] M. Rückert, "Lattice-based blind signatures," in *Proc. 16th Int. Conf. Theory Appl. Cryptol. Inf. Secur. (ASIACRYPT)*, Singapore, 2010, pp. 413–430.
[19] F. Wang, Y. Hu, and B. Wang, "Lattice-based strong designate verifier signature and its applications," *Malaysian J. Comput. Sci.*, vol. 25, no. 1, pp. 11–22, Jan. 2012.
[20] I. X. Li, Y. J. Zheng, and M. I. Xu, "Lattice-based strong designated verifier signature scheme," *J. Cell Commun. Signaling*, vol. 34, no. 10, pp. 2363–2366, Oct. 2013.
[21] X. Boyen, "Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more," in *Public Key Cryptography—PKC*, P. Q. Nguyen and D. Pointcheval, Eds. Berlin, Germany: Springer, 2010, pp. 499–517.
[22] G. Noh and I. R. Jeong, "Strong designated verifier signature scheme from lattices in the standard model," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 6202–6214, Feb. 2017.
[23] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Advances in Cryptology—CRYPTO*. Santa Barbara, CA, USA: Springer, 1986, pp. 186–194.
[24] D. Micciancio, "Almost perfect lattices, the covering radius problem, and applications to ajtai's connection factor," *SIAM J. Comput.*, vol. 34, no. 1, pp. 118–169, Jan. 2003, doi: 10.1137/S0097539703433511.
[25] C. Peikert and A. Rosen, "Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices," in *Proc. TCC*, New York, NY, USA, 2006, pp. 145–166.
[26] V. Lyubashevsky and D. Micciancio, "Generalized compact knapsacks are collision resistant," in *Proc. ICALP*, Venice, Italy, 2006, pp. 144–155.
[27] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang, "Choosing parameters for ntruencrypt," in *Proc. Cryptographers' Track RSA Conf. (CT-RSA)*, San Francisco, CA, USA, 2017, pp. 3–18.

JIE CAI received the master's degree from the School of Mathematics, Shandong University, Jinan, China, in 2012, where she is currently pursuing the Ph.D. degree in mathematics and information security. Her research interest includes information security and cryptography, especially post-quantum cryptography based on lattices.

HAN JIANG received the master's and Ph.D. degrees from the School of Computer Science and Technology, Shandong University, Jinan, China, in 2005 and 2008, respectively. He is currently a Lecturer with Shandong University. His current research interest includes cryptography and information security, especially secure multi-party computation. He is a member of CACR.

PINGYUAN ZHANG received the master's degree from the School of Mathematics, Shandong University, Jinan, China, in 2015, where he is currently pursuing the Ph.D. degree in mathematics and information security. His research interest includes information security and cryptography, especially post-quantum cryptography based on lattices. He is a member of CACR.

ZHIHUA ZHENG was born in 1962. She is currently an Associate Professor with Shandong Normal University. Her current research interests include cryptography algorithms and protocols.

GUANGSHI LYU received the Ph.D. degree in 2004 under the supervision of Prof. J. Liu. He is currently a Mathematician and a Professor of mathematics with Shandong University. His current research interests include analytic number theory, particularly in the subfields of automorphic L-functions, and multiplicative number theory.

QIULIANG XU received the master's and Ph.D. degrees from Shandong University, Jinan, China, in 1985 and 1999, respectively. He is currently a Professor and a Ph.D. Supervisor with Shandong University, where he has been since 1985. He is also Syndic of the Chinese Association for Cryptologic Research. His current research interests include public key cryptography and multi-party secure computation. He holds several Science Foundations and the Key Program of China.