Hindawi
Security and Communication Networks
Volume 2019, Article ID 9678095, 8 pages
https://doi.org/10.1155/2019/9678095

Research Article

ID-Based Strong Designated Verifier Signature over $\mathscr{R}$-SIS Assumption

Jie Cai,[1] **Han Jiang**,[2] **Pingyuan Zhang**,[1] **Zhihua Zheng**,[3] **Hao Wang**,[3] **Guangshi Lü**,[1] **and Qiuliang Xu**[2]

[1]*School of Mathematics, Shandong University, Ji'nan, Shandong, China*
[2]*School of Software, Shandong University, Ji'nan, Shandong, China*
[3]*School of Information Science and Engineering, Shandong Normal University, Ji'nan, Shandong, China*

Correspondence should be addressed to Han Jiang; jianghan@sdu.edu.cn

Received 23 April 2019; Accepted 18 June 2019; Published 15 July 2019

Academic Editor: Clemente Galdi

In this paper, we propose an ID-based strong designated verifier signature (SDVS) over $\mathscr{R}$–SIS assumption in the random model. We remove pre-image sampling function and Bonsai trees such complex structures used in previous lattice-based SDVS schemes. We only utilize simple rejection sampling to protect the security of our scheme. Hence, we will show our design has the shortest signature size comparing with existing lattice-based ID-based SDVS schemes. In addition, our scheme satisfies anonymity (privacy of signer's identity) proved in existing schemes rarely, and it can resist side-channel attacks with uniform sampling.

1. Introduction

The first designated verifier signature scheme was proposed by Jakobsson, Sako, and Impagliazzo [1] in 1996. This signature scheme satisfies that only the designated verifier can verify correctness of generated signatures and he can't convince others to believe in the validity of these signatures. The main reason for satisfying this property is that the designated verifier can generate an indistinguishable transcript from the real signatures. In [1], they also provided a notion of strong designated verifier signature (SDVS) to resist an online eavesdropper's attack. In a SDVS, anyone can create an identical transcript which is indistinguishable from real signatures. Generally speaking, a SDVS needs to satisfy unforgeability and untransferability which were provided by Saeednia, Kremer, and Markowitch in [2] formally. In [3], Laguillaumie and Vergnaud added a property, that is, privacy of signer's identity (anonymity), which means any adversary can't distinguish Alice's signature for Bob from Cindy's signature for Bob without Bob's secret key.

An advantage of identity-based scheme is that the verifier doesn't need to generate his public key setup before receiving authenticated message from signer. In [4], Susilo, Zhang, and Mu first introduced the notion of identity-based SDVS (ID-based SDVS). They gave an efficiently generic construction of such schemes which were based on bilinear Diffie-Hellman assumption.

2. Related Work

2.1. Classical ID-Based SDVS Schemes. Several classical ID-based SDVS have been provided since the first general construction is introduced in [4]. In [5], Huang et al. proposed a short ID-based SDVS based on bilinear pairing. Their contributions of paper are not merely their shorter signature size, but having two security proofs in random model and in standard model. In addition, the scheme of [5] has anonymity compared with [4]. Recently, Blazy et al. provided an ID-based SDVS [6] under CDH assumption in the standard model.

However, classical ID-based SDVS schemes can't resist against quantum adversaries. Hence, people try to design postquantum ID-based SDVS schemes. With the collection of postquantum algorithms by NIST, lattice-based cryptography is widely studied.

2.2. Lattice-Based ID-Based SDVS Schemes. As far as we know, there are two main postquantum schemes both based on lattice hard problems. The first lattice-based ID-based SDVS was proposed by Noh et al. [7]. They used pre-image sampling function and Bonsai trees (see [8]) with large parameters to protect the security. Soon Wang et al. proposed a more efficient scheme [9]. The security of this scheme was based on the hardness of LWE and its unforgeability can be reduced to SIS problem in the random model. At the same time, they showed the signature size ($3m \log q$) is shorter than any other already existing SDVS scheme.

However, above schemes that used Gaussian sampling are unusual to resist side-channel attack [10–12], and the authors only gave the proofs of unforgeability and untransferability without anonymity.

2.3. Our Contribution. In this paper, we propose an efficient ID-based SDVS based on SIS problem over ring in the random model, and our design has advantages as follows:

(1) *Shorter signature size and lower rejection time*. The signature size of our scheme approximately equals $2m \log q + m$. Since $q \gg 2$ holds in practical application, it is easy to see our result is better than $3m \log q$ [9]. The main reason for this is that we don't utilize pre-image sampling function and Bonsai trees such complex structures. Then we needn't choose too large parameters to protect the existence and security of scheme. About efficiency, we use filtering technique (see [13]) to make the rejection 1.28 lower than others.

(2) *Resisting side-channel attacks*. The common methods of existing sampling over lattice-based signature are Gaussian sampling (see [14–16]) and uniform sampling (see [13, 17, 18]). It has been proved that these schemes with Gaussian sampling lead to side-channel attacks easily [10–12]. Hence we choose uniform sampling to resist them efficiently.

(3) *Satisfying anonymity*. Although anonymity was introduced in [3] long ago, being proved in existing schemes is very rare indeed. Our scheme satisfies three properties of unforgeability, untransferability, and anonymity. In addition, anonymity can be reduced to solving SIS problem.

Organization of the Paper. We will show the basic notations, relative lattice hard problem assumption and rejection sampling used in our scheme, and detailed definitions of ID-based SDVS and security model in Section 3. Then we propose our ID-based SDVS scheme in detail in Section 4. In Section 5, we provide the proof of security. In Section 6, we present the relationship of our parameters to ensure the existence and security of our scheme. Finally, we give a conclusion and further work in Section 7. Data availability, conflicts of interest, and funding statement can be seen in the last three sections, respectively.

3. Preliminaries

3.1. Notations. We note ring $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$, where q is a prime number and n is a power of 2 positive number. The bold small (capital) letters are vectors (matrices), and the normal letters are integers or real. The ℓ_p norm of a vector $\mathbf{x}$ is denoted by $\|\mathbf{x}\|_p$ ($p = 1, 2, \infty$). $\mathcal{D}_\gamma$ means a uniform distribution in which an element $\mathbf{x} \xleftarrow{\$} \mathcal{R}_q$ is chosen randomly such that $\|\mathbf{x}\|_\infty \leq \gamma$. An invertible element in distribution $\mathcal{D}_\gamma$ is represented by $\mathbf{x}^{-1}$. An element in $\mathcal{R}_q^{n\times m}$ is $\mathbf{X} = \{\mathbf{x}_1 \dots \mathbf{x}_m\}$, $m \geq n \log q$. We note $h : \{0,1\}^* \longrightarrow \{\mathbf{r} : \mathbf{r} \in \{-1, 0, 1\}^m, \|\mathbf{r}\|_1 \leq \iota\}$ is a hash function. Function H maps $\{0,1\}^*$ to $\mathcal{R}_q^{m\times m}$, which is derived by using AES128-ECB [19, 20].

3.2. Rejection Sampling. In previous part of our paper, we have shown that using Gaussian sampling can cause serious side-channel attack; then we just provide uniform sampling in this part.

The method of uniform sampling is usually called filtering technique [17, 18]. Its core idea is the signer needs to output a secure signature by choosing its proper range, and its main aim is making such a good output uniform to protect his secret key. In [13], Rückert provided a form over polynomial rings.

Lemma 1 (see [13]). *Given two sets* $\mathcal{S}_1 = \{\mathbf{a} \in \mathbb{Z}^m \mid \|\mathbf{a}\|_\infty \leq A\}$ *and* $\mathcal{S}_2 = \{\mathbf{b} \in \mathbb{Z}^m \mid \|\mathbf{b}\|_\infty \leq B, B \geq \Phi m A, \Phi \in \mathbb{N}^+\}$, *and if given any* $\mathbf{a} \in \mathcal{S}_1$, $\mathbf{b} \xleftarrow{\$} S_2$, *then we have* $Pr[\|\mathbf{a} - \mathbf{b}\|_\infty \leq B - A] > e^{-1/\Phi} - o(1)$.

Usually, $\mathbf{a}$ contains information of secret key and signature form is $\mathbf{a} - \mathbf{b}$. According to above lemma, we can see that the output $\mathbf{a} - \mathbf{b}$ is indistinguishable with uniform distribution if and only if it is constrained in the range $B - A$. Further, if the signature is in this range, $\mathbf{a}$ doesn't leak any information about the secret key.

More importantly, this lemma tells us that the signature size is dependent on three parameters Φ, m, and A. In principle, the smaller these chosen parameters, the better. Unfortunately, a smaller value of Φ can cause a larger rejection time ($\approx e^{1/\Phi}$); hence we must find a tradeoff for it. In our scheme, the chosen parameter A (replaced by υ) is smaller than any other existing ones, which makes our signature size the shortest.

3.3. Lattice Assumption. There are two important average-case problems, SIS and LWE, in lattices which can be reduced to the worst-case problems GapSVP and SIVP [21, 22]. A formal form of SIS problem is always denoted $\ell_2 - \mathrm{SIS}_{q,n,m,\beta}$. Here we list its form over ring, which is at least as hard as worst-case problem SVP_Γ on ideal lattices (see [23]).

Definition 2 (see [14]). 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 nonzero vector $\mathbf{v} \in \mathcal{R}_q^m$ such that

$\mathbf{Av} = \mathbf{0}$ and $\|\mathbf{v}\|_2 \le \beta$ $(0 < \beta \le q \cdot poly(n))$, which is denoted $\mathscr{R} - \mathrm{SIS}^{\mathscr{K}}_{q,n,m,\beta}$ problem.

Compared with SIS, $\mathscr{R}$–SIS is more compact and more efficient. In order to ensure existing of a sufficiently short solution, the dimension m in $\mathscr{R}$–SIS is approximate $\log q$ instead of $n \log q$ in SIS problem. Furthermore, one can compute $\mathbf{Av}$ in quasilinear time with fast Fourier transform (FFT).

Besides, $\mathscr{R}$–SIS and its associated cryptographic functions also can be proved at least as hard as certain lattice (called ideal lattice over ring $\mathscr{R}$) problems in the worst case. In [23], Peikert and Rosen provided that $\mathscr{R}$–SIS is at least as hard as worst-case SVP_Γ ($\Gamma = O\sqrt{\log n}$) on ideal lattice in $\mathscr{R}$, where $\mathscr{R} = \mathscr{O}_K$ is the ring of algebraic integers in any number field K. Particularly, the fastest time in known (quantum) algorithms to solve SIS_Γ problem on ideal lattice is exponential $2^{\Omega(n)}$. Indeed, now it seems that the additional algebraic structure of ideal lattices does not bring any advantages to solving this problem.

3.4. An Equivalent Construction of Random Matrix $\mathbf{A}$. Since our design has many matrix multiplications, we need to find an equivalent square matrix to satisfy their multiplicability. Moreover, in [16], Lyubashevsky showed that if $m \ge 2n$, there are n linearly independent columns in a random matrix $\mathbf{A} \in \mathscr{R}_q^{n \times m}$ with probability $e^{-\Omega(n)}$, when q is a prime of size bigger than $2m$.

In order to construct an efficient lattice-based SDVS scheme, we have introduced this idea in [24], so we provide it in brief here.

Lemma 3. *If* $\mathbf{A}_1 \in \mathscr{R}_q^{n \times m}$, $m = 2n$, $\mathbf{X}_1 \in \mathscr{R}_q^{m \times m}$ *satisfies* $\mathbf{A_1 X_1} = \mathbf{0} \mod q$, *then we construct a new matrix*

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_1^{n \times m} \\ \mathbf{0}^{n \times m} \end{bmatrix} \in \mathscr{R}_q^{m \times m} \tag{1}$$

, *and we have* $\mathbf{AX} = \mathbf{0} \mod q$, *where* $\mathbf{X} = \mathbf{X_1}$.

Proof. According to the multiplicability of the partitioned matrix, we can compute the below equation,

$$\mathbf{AX} = \begin{bmatrix} \mathbf{A}_1^{n \times m} {\mathbf{X}_1}^{m \times m} \\ \mathbf{0}^{n \times m} {\mathbf{X}_1}^{m \times m} \end{bmatrix} = \mathbf{0} \mod q. \tag{2}$$

This lemma shows that such a square matrix has two advantages for our scheme as follows:

(i) Don't change the security. Notice that the new square matrix $\mathbf{A}$ has the same solution as the common form $\mathbf{A}_1 \in \mathscr{R}_q^{n \times m}$ based on SIS assumption. Hence, they have equivalent security.

(ii) Don't change the efficiency. Although the dimension of matrix is increased, it doesn't cause extra computation by filling zero matrix in original one. □

3.5. Definitions of ID-Based SDVS. An ID-based SDVS scheme contains five polynomial time algorithms (Setup, Extract, Sign, Verf, and Sim) between two participants Alice (signer) and Bob (designated verifier). Every participant has his identity ID_A (ID_B). Generally, there exists a private key generator (PKG) to provide a secret key S_{ID_A} (S_{ID_B}) for each participant during an extract algorithm. The detailed descriptions of these algorithms are shown as follows.

Definition 4. Given a security parameter $\lambda = poly(n)$, an ID-based SDVS is defined by algorithms:

(1) *Setup*: It is a probabilistic algorithm inputting the security parameter λ and outputting system parameters (sp) and master key (mk). That is,

$$(sp, mk) \longleftarrow \mathrm{Setup}(\lambda). \tag{3}$$

(2) *Extract*: It is a deterministic (probabilistic) algorithm inputting sp, mk, and participant's identity $ID_i \in \{0,1\}^*$ and outputting relative secret key S_{ID_i}. Actually, the identity ID_i is often considered public key of participant, and ID_A (ID_B) belongs to Alice (Bob) in two-party schemes. Specifically,

$$S_{ID_i} \longleftarrow \mathrm{Extract}(sp, mk, ID_i). \tag{4}$$

(3) *Sign*: It is a deterministic (probabilistic) algorithm inputting signer's secret key S_{ID_A}, designated verifier's public key ID_B, and message μ. Then it outputs a signature σ.

$$\sigma \longleftarrow \mathrm{Sign}\left(S_{ID_A}, ID_B, \mu\right). \tag{5}$$

(4) *Verf*: It is a deterministic algorithm inputting message μ and relatively received signature σ from signer Alice, S_{ID_B} and ID_A. The designated verifier Bob verifies whether the following equation is correct or not:

$$(True, \perp) \longleftarrow \mathrm{Verf}\left(S_{ID_B}, ID_A, \mu, \sigma\right) \tag{6}$$

(5) *Sim*: It is a probabilistic algorithm inputting a quadruple $(S_{ID_B}, ID_A, ID_B, \mu)$. Anyone can generate an indistinguishable signatures generated by the triple (S_{ID_A}, ID_B, μ).

Security Model

(1) *Correctness*: For all valid Sign (S_{ID_A}, ID_B, μ), the designated verifier always gets the following result:

$$\mathrm{Verf}\left(S_{ID_B}, ID_A, \mu, \mathrm{Sign}\left(S_{ID_A}, ID_B, \mu\right)\right) = True. \tag{7}$$

(2) *Unforgeability*: We provide a game between a PPT adversary $\mathscr{A}$ and a challenger $\mathscr{C}$ to define existential unforgeability against adaptive chosen message attack (EUF-CMA). In addition, we denote that ID_i and ID_j are signer and designated verifier ID, respectively.

(i) *Setup*. The challenger $\mathscr{C}$ runs the following algorithm to generate sp and mk.

$$(sp, mk) \longleftarrow \text{Setup}(\lambda). \tag{8}$$

(ii) *Extraction queries*. The adversary $\mathscr{A}$ can query the secret key of signer with ID_i. Then $\mathscr{C}$ runs Extract (sp, mk, ID_i) to answer him. That is, $\mathscr{A}$ can get S_{ID_i}.

(iii) *Sign queries*. When $\mathscr{A}$ obtains S_{ID_i}, he queries a signature σ with message μ and designated verifier ID_j. Then $\mathscr{C}$ answers him with a correct signature by algorithm Sign (S_{ID_i}, ID_j, μ).

(iv) *Output*. At the end of this game, the adversary $\mathscr{A}$ is able to generate a new signature σ^* with message μ^*, ID_{i^*} and ID_{j^*} satisfying necessary conditions:

(1) ID_{i^*} and ID_{j^*} have never been requested in *Extraction queries* step.

(2) Message μ^* related with ID_{i^*} and ID_{j^*} has never been requested in *Sign queries* step.

(3) The signature σ^* with message μ^*, ID_{i^*} and ID_{j^*} is valid.

Then, we provide a formal security description of EUF-CMA. We say the ID-based SDVS scheme is (t, ϵ) EUF-CMA secure, if the following probability is negligible for any PPT adversary $\mathscr{A}$ runs above game in time t.

$$\Pr\left[\text{Verf}\left(ID_{i^*}, ID_{j^*}, \mu^*, \sigma^*\right) = True\right] \leq \epsilon, \tag{9}$$

where $\epsilon > 0$ is a negligible function of secure parameter λ.

(3) *Untransferability*: This property simply means that any PPT adversary $\mathscr{A}$ can't distinguish the real signature and simulated one in below game between $\mathscr{A}$ and challenger $\mathscr{C}$.

(i) *Setup*. The challenger $\mathscr{C}$ runs algorithm Setup(λ) to generate sp and mk.

(ii) *Sign and Verf queries*. The PPT adversary $\mathscr{A}$ queries for Sign and Verf queries adaptively for chosen message μ_i. The challenger $\mathscr{C}$ answers him by running algorithms Sign(S_{ID_A}, ID_B, μ_i) and Verf$(S_{ID_B}, ID_A, \mu_i, \sigma_i)$. Notice that the identities of two participants are fixed and the parameter i is form 1 to $q_s = poly(n)$ in this step.

(iii) *Challenge*. After q_s signing and verifying queries, $\mathscr{A}$ chooses a new massage μ^* to query $\mathscr{C}$. $\mathscr{C}$ tosses a coin randomly and chooses $b \overset{\$}{\leftarrow} \{0, 1\}$. When $b = 0$, he runs $\sigma^* \longleftarrow$ Sign (S_{ID_A}, ID_B, μ^*) correctly; otherwise he runs $\sigma^* \longleftarrow \text{Sim}(S_{ID_B}, ID_A, ID_B, \mu^*)$ to answer adversary's request.

(iv) *Output*. At the end of this game, the adversary $\mathscr{A}$ outputs $b' \in \{0, 1\}$. If $b = b'$ holds, the adversary succeeds in the game.

Formally, for any PPT adversary, he has a correct guess after q_s quests in t time with negligible probability; then we say this ID-based SDVS is (t, q_s) untansferable. That is,

$$\left|\Pr\left[b = b'\right] - \frac{1}{2}\right| < \epsilon. \tag{10}$$

(4) *Anonymity*: To be accurate, any adversary can't distinguish the real signer's identity form given ID_{A_0} and ID_{A_1} for a designated verifier's identity ID_B. It is similar with witness indistinguishable property actually. The detailed description of game is shown as follows.

(i) *Setup*. The challenger $\mathscr{C}$ runs algorithm Setup(λ) to generate sp and mk.

(ii) *Extraction queries*. The adversary $\mathscr{A}$ can query the secret key of signer with ID_i. Then $\mathscr{C}$ runs Extract (sp, mk, ID_i) to answer him.

(iii) *Sign and Verf queries*. $\mathscr{A}$ queries the signature with message μ for the signer ID_i and designated verifier ID_j. Then $\mathscr{C}$ outputs a signature σ and returns $True$ or $\perp$ if $\mathscr{A}$ inputs (μ, σ).

(iv) *Challenge*. The adversary $\mathscr{A}$ outputs a message μ^* with signer's possible identities ID_{A_0}, ID_{A_1} and designated verifier's identity ID_B to challenger $\mathscr{C}$ satisfying necessary conditions:

(1) ID_{A_0}, ID_{A_1}, and ID_B have never been requested in *Extraction queries* step.

(2) Message μ^* (or pair (μ^*, σ^*)) has never been requested in *Sign and Verf queries* step with ID_{A_0}, ID_{A_1}, and ID_B.

After receiving μ^*, $\mathscr{C}$ tosses a coin randomly, chooses $b \overset{\$}{\leftarrow} \{0, 1\}$, and computes Sign $(S_{ID_{A_b}}, ID_B, \mu^*)$ returned to $\mathscr{A}$.

(v) *Output*. At the end of this game, the adversary $\mathscr{A}$ outputs $b' \in \{0, 1\}$. If $b = b'$ holds, the adversary succeeds in the game.

Hence, for any PPT adversary, he has a correct guess after q_s quests in t time with negligible probability; then we say this ID-based SDVS satisfies property of (t, q_s) privacy of signer's identity. That is,

$$\left|\Pr\left[b = b'\right] - \frac{1}{2}\right| < \epsilon. \tag{11}$$

4. Our ID-Based SDVS Scheme

In this part, we will provide our detailed construction. Then we get an efficient ID-based SDVS scheme over $\mathscr{R}$–SIS assumption. Always we assume Alice is the signer and Bob is designated verifier.

4.1. Setup. Let n be the rank of lattice, and PKG chooses $\mathbf{A} \overset{\$}{\leftarrow} \mathscr{R}_q^{m \times m}$. There is a low norm solution of $\mathscr{R}$–SIS problem $\mathbf{X} \in \mathscr{R}_q^{m \times m}$ such that $\mathbf{AX} = \mathbf{0} \mod q$. We can see $\mathbf{X}$ is indeed the mk.

4.2. Extract. Let $H : \{0,1\}^* \longrightarrow \mathscr{R}_q^{m\times m}$ generated by using AES128-ECB [19, 20] be a mapping and $h : \{0,1\}^* \longrightarrow \{\mathbf{r} : \mathbf{r} \in \{-1,0,1\}^m, \|\mathbf{r}\|_1 \leq \iota\}$ be a hash function. In addition, we denote ID_A (ID_B) is Alice's (Bob's) identity. Then, PKG computes $H(ID_i) = \mathbf{H}_i$ $(i = A, B)$ to be seen as the participant's public key. Since $\mathbf{H}_i \in \mathscr{R}_q^{m\times m}$, $\mathbf{X} \in \mathscr{R}_q^{m\times m}$, PKG can generate the secret keys by computing $\mathbf{X}\cdot\mathbf{H}_A = \mathbf{S}_A \mod q$ and $\mathbf{H}_B \cdot \mathbf{X} = \mathbf{S}_B \mod q$. Simply speaking,

$$\mathbf{S}_i \longleftarrow \text{Extract}\left(n, H, \mathbf{X}, ID_i\right) \quad (i = A, B). \tag{12}$$

4.3. Sign. Alice executes the following steps to sign a signature for message μ.

(1) $\mathbf{t} \overset{\$}{\leftarrow} \mathscr{D}_\gamma(\gamma < q)$

(2) if $\mathbf{t}$ is not reversible, then go to step (1).

(3) $\mathbf{k} \overset{\$}{\leftarrow} \mathscr{D}_\gamma$

(4) $\mathbf{c} = \mathbf{H}_B \cdot \mathbf{k} \mod q$

(5) $\mathbf{r} = h(\mathbf{c}, \mu)$

(6) $\mathbf{z} = \mathbf{S}_A \cdot \mathbf{r} + \mathbf{k} \cdot \mathbf{t}^{-1}$

(7) if $\|\mathbf{z}\|_\infty \geq \gamma - \upsilon$ or $\|\mathbf{S}_A \cdot \mathbf{r}\|_\infty \geq \upsilon$, then go to step (3).

(8) output signature $(\mathbf{r}, \mathbf{z}, \mathbf{t})$ of message μ.

Notice that there are two loop conditions in step (1) and step (7). Thus, it is necessary for us to evaluate their efficiencies.

(i) *About step (1).* In [25], Hoffstein et al. proposed a method to search an invertible polynomial $\mathbf{t}$ within 48.9 ms. Their instance is that $\mathbf{t}$ satisfies $\|\mathbf{t}\|_1 \leq 40$ in a trinary polynomial set $T(206, 205)$, where 206 and 205 are numbers of positive coefficients and negative coefficients, respectively. Since such an invertible $\mathbf{t}$ is contained in set $\mathscr{D}_\gamma$, we can also find it in 48.9 ms.

(ii) *About step (7).* This step is the key to compute the repetition using filtering technique (see [13]). In order to utilize their result, we require that the inequation $m\Phi\upsilon \leq \gamma$ must be satisfied. Hence we get the repetition is approximately $e^{1/\Phi}$. Obviously, we can see that $e^{1/\Phi}$ is a monotonically decreasing function with variable $\Phi \in \mathbb{N}^+$, and the bigger value of Φ seemingly is better. However, two of composition parts of signature are $\mathbf{z}$ and $\mathbf{t}$, and their size is $m\log(\gamma - \upsilon) + m\log\gamma$ which is positively correlated with parameter Φ. Hence, choosing bigger Φ is not wise. Then we get the optimal solution $\Phi = 4$ by observing the following expression,

$$\Phi = \min_{0.75 \leq e^{-1/\Phi'} \leq 1} \Phi', \tag{13}$$

where $1 \leq \Pr[\|\mathbf{z}\|_\infty \leq \gamma - \upsilon] = e^{-1/\Phi'} \leq 0.75$. Furthermore, the repetition is $e^{1/\Phi} \approx 1.28$.

4.4. Verf. When receiving signature $\sigma = (\mathbf{r}, \mathbf{z}, \mathbf{t})$ from signer Alice, Bob verifies whether the following equation is correct or not:

(1) $h(\mathbf{c}, \mu) = h(\mathbf{H}_B\mathbf{z}\mathbf{t} - \mathbf{S}_B\mathbf{H}_A\mathbf{r}\mathbf{t} \mod q, \mu)$

(2) $\|\mathbf{z}\|_\infty \leq \gamma - \upsilon$

4.5. Sim. If one gets a quadruple $(\mathbf{S}_B, ID_A, ID_B, \mu)$, he chooses two random elements $\mathbf{z}'$ ($\|\mathbf{z}'\|_\infty \geq \gamma - \upsilon$) and $\mathbf{r}'$ to compute $\mathbf{z}'\mathbf{t}^{-1} = \mathbf{z}$ and $\mathbf{r}'\mathbf{t}^{-1} = \mathbf{z}$. Hence, he can also compute the following equation,

$$\mathbf{H}_B\mathbf{z}\mathbf{t} - \mathbf{S}_B\mathbf{H}_A\mathbf{r}\mathbf{t} = \mathbf{c} = \mathbf{H}_B\mathbf{z}' - \mathbf{S}_B\mathbf{H}_A\mathbf{r}', \tag{14}$$

which is an indistinguishable signature with Alice's.

5. Security

In this part, we will show our scheme satisfies three properties including unforgeability, untransferability, and anonymity (privacy of signer's identity) according to security model in Section 2.

5.1. Correctness. After receiving the signature $(\mathbf{r}, \mathbf{z}, \mathbf{t})$ of message μ, designated verifier verifies the condition $\|\mathbf{z}\|_\infty \leq \gamma - \upsilon$ and computes the value of hash function as follows.

$$\begin{aligned} h(\mathbf{c}, \mu) &= h\left(\mathbf{H}_B\left(\mathbf{z} - \mathbf{S}_A\mathbf{r}\right)\mathbf{t} \mod q, \mu\right) \\ &= h\left(\mathbf{H}_B\mathbf{z}\mathbf{t} - \mathbf{H}_B\mathbf{S}_A\mathbf{r}\mathbf{t} \mod q, \mu\right) \\ &= h\left(\mathbf{H}_B\mathbf{z}\mathbf{t} - \mathbf{H}_B\mathbf{X}\mathbf{H}_A\mathbf{r}\mathbf{t} \mod q, \mu\right) \\ &= h\left(\mathbf{H}_B\mathbf{z}\mathbf{t} - \mathbf{S}_B\mathbf{H}_A\mathbf{r}\mathbf{t} \mod q, \mu\right). \end{aligned} \tag{15}$$

Then the following equation holds.

$$\text{Verf}\left(\mathbf{S}_B, ID_A, \mu, \text{Sign}\left(\mathbf{S}_A, ID_B, \mu\right)\right) = True. \tag{16}$$

5.2. Unforgeability

Theorem 5. *If there is a PPT adversary $\mathscr{A}$ that has ability to succeed in (t, ϵ) EUF-CMA game, then he can solve SIS problem over $\mathscr{R}_q^{m\times m}$.*

Proof. Suppose EUF-CMA game proceeds as required between $\mathscr{A}$ and challenger $\mathscr{C}$. When $\mathscr{A}$ finishes *Extraction* and *Sign* queries in time t, he outputs a new signature $(\sigma^* = (\mathbf{r}^*, \mathbf{z}^*, \mathbf{t}^*), \mu^*)$ with two new identities ID_{i^*} and ID_{j^*} satisfying the following conditions:

(1) ID_{i^*} and ID_{j^*} have never been requested in *Extraction queries* step.

(2) Message μ^* related with ID_{i^*} and ID_{j^*} has never been requested in *Sign queries* step.

(3) The signature σ^* with message μ^*, ID_{i^*}, and ID_{j^*} is valid.

If Verf (Sign $(ID_{i^*}, ID_{j^*}, \mu^*)) = True$ holds, then $\mathscr{A}$ can compute

$$\begin{aligned}&\mathbf{H}_{j^*}\left(\mathbf{z}^* - \mathbf{S}_{i^*}\mathbf{r}^*\right)\mathbf{t}^*\left(\mathbf{t}^*\right)^{-1} - \mathbf{H}_{j^*}\mathbf{z}^* \\ &\quad = \mathbf{H}_{j^*}\mathbf{z}^* - \mathbf{H}_{j^*}\mathbf{S}_{i^*}\mathbf{r}^* - \mathbf{H}_{j^*}\mathbf{z}^* = -\mathbf{H}_{j^*}\mathbf{S}_{i^*}\mathbf{r}^* \\ &\qquad\qquad\qquad\qquad \bmod q.\end{aligned} \tag{17}$$

In addition, the equation $\|\mathbf{z}^*\|_\infty \le \gamma - \upsilon$ holds, which means $\|\mathbf{S}_{i^*}\mathbf{r}^*\|_\infty \le \upsilon$ is satisfied. We can easily see that the adversary gets a solution of SIS problem for a random element $\mathbf{H}_{j^*} \in \mathscr{R}_q^{m\times m}$. □

5.3. Untransferability

Theorem 6. *Our ID-based SDVS is (t, q_s) untransferability.*

Proof. The adversary $\mathscr{A}$ and challenger $\mathscr{C}$ play untransferable game as required. After q_s signing and verifying queries, $\mathscr{A}$ chooses a new massage μ^* to query $\mathscr{C}$. $\mathscr{C}$ chooses $b \xleftarrow{\$} \{0,1\}$, and if $b = 0$, $\mathscr{C}$ computes $\sigma^* \longleftarrow \mathrm{Sign}(\mathbf{S}_A, ID_B, \mu^*)$ to answer $\mathscr{A}$. That is,

$$\begin{aligned}&\mathbf{t}^*, \mathbf{k}^* \xleftarrow{\$} \mathscr{D}_\gamma, \\ &\mathbf{r}^* = h\left(\mathbf{H}_B \cdot \mathbf{k}^* \mod q, \mu^*\right), \\ &\mathbf{z}^* = \mathbf{S}_A \cdot \mathbf{r}^* + \mathbf{k}^* \cdot \left(\mathbf{t}^*\right)^{-1},\end{aligned} \tag{18}$$

output signature $(\mathbf{r}^*, \mathbf{z}^*, \mathbf{t}^*)$ of message μ^*.

Otherwise, $\mathscr{C}$ runs $\sigma^* \longleftarrow \mathrm{Sim}(\mathbf{S}_B, ID_A, ID_B, \mu^*)$ to answer adversary's request. That is,

$$\begin{aligned}&\mathbf{z}', \mathbf{r}' \xleftarrow{\$} \mathscr{D}_\gamma, \\ &\mathbf{r}^* = h\left(\left(\mathbf{H}_B\mathbf{z}' - \mathbf{S}_B\mathbf{H}_A\mathbf{r}'\right) \bmod q, \mu^*\right), \\ &\mathbf{z}^* = \mathbf{z}'\left(\mathbf{t}^*\right)^{-1}, \\ &\mathbf{t}^* = \mathbf{r}'\left(\mathbf{r}^*\right)^{-1},\end{aligned} \tag{19}$$

output signature $(\mathbf{r}^*, \mathbf{z}^*, \mathbf{t}^*)$ of message μ^*. Now we compute the probabilities of above two signatures σ^* distributions.

$$\begin{aligned}&Pr\left[\left(\mathbf{r}^*, \mathbf{z}^*, \mathbf{t}^*\right) \mid b = 0\right] \\ &\quad = Pr\left[\mathbf{t}^*, \mathbf{k}^* \ne 0 \mid \mathbf{t}^*, \mathbf{k}^* \xleftarrow{\$} \mathscr{D}_\gamma\right] = \frac{1}{\gamma^m\left(\gamma^m - 1\right)}. \\ &Pr\left[\left(\mathbf{r}^*, \mathbf{z}^*, \mathbf{t}^*\right) \mid b = 1\right] \\ &\quad = Pr\left[\mathbf{z}', \mathbf{r}' \ne 0 \mid \mathbf{z}', \mathbf{r}' \xleftarrow{\$} \mathscr{D}_\gamma\right] = \frac{1}{\gamma^m\left(\gamma^m - 1\right)}.\end{aligned} \tag{20}$$

Hence, the advantage of guessing $b = b'$ for $\mathscr{A}$ is negligible, and we can obtain

$$\left|\Pr\left[b = b'\right] - \frac{1}{2}\right| < \epsilon. \tag{21}$$

□

5.4. Anonymity

Theorem 7. *If the PPT adversary $\mathscr{A}$ can distinguish the signer's identity from given ID_{A_0} and ID_{A_1} for a designated verifier's identity ID_B, then he can distinguish the different solutions of SIS problem over $\mathscr{R}_q^{m\times m}$.*

Proof. Here, we also suppose that $\mathscr{A}$ and $\mathscr{C}$ interact with each other as defined of secure model. After Extraction, Sign, and Verf queries are finished, the adversary $\mathscr{A}$ outputs a message μ^* with signer's possible identities ID_{A_0}, ID_{A_1} and designated verifier's identity ID_B to challenger $\mathscr{C}$ satisfying the above elements that have not been queried.

After receiving μ^*, $\mathscr{C}$ tosses a coin randomly, chooses $b \xleftarrow{\$} \{0,1\}$, and computes Sign $(S_{ID_{A_b}}, ID_B, \mu^*)$ returned to $\mathscr{A}$. If $\mathscr{A}$ can guess b correctly, this means he can compute the probability as follows.

$$\begin{aligned}Pr\left[b = b'\right] &= \left|Pr\left[\mathscr{D}\left(\mathbf{H}_B\mathbf{z}^*\mathbf{t}^* - \mathbf{S}_B\mathbf{H}_{A_0}\mathbf{r}^*\mathbf{t}^*\right)\right]\right. \\ &\quad \left. - Pr\left[\mathscr{D}\left(\mathbf{H}_B\mathbf{z}^*\mathbf{t}^* - \mathbf{S}_B\mathbf{H}_{A_1}\mathbf{r}^*\mathbf{t}^*\right)\right]\right| \\ &= \left|Pr\left[\mathscr{D}\left(\mathbf{S}_B\mathbf{H}_{A_0}\mathbf{r}^*\mathbf{t}^*\right)\right] - Pr\left[\mathscr{D}\left(\mathbf{S}_B\mathbf{H}_{A_1}\mathbf{r}^*\mathbf{t}^*\right)\right]\right| \\ &= \left|Pr\left[\mathscr{D}\left(\mathbf{H}_B\mathbf{X}\mathbf{H}_{A_0}\mathbf{r}^*\mathbf{t}^*\right)\right]\right. \\ &\quad \left. - Pr\left[\mathscr{D}\left(\mathbf{H}_B\mathbf{X}\mathbf{H}_{A_1}\mathbf{r}^*\mathbf{t}^*\right)\right]\right| \\ &= \left|Pr\left[\mathscr{D}\left(\mathbf{H}_B\mathbf{S}_{A_0}\mathbf{r}^*\mathbf{t}^*\right)\right] - Pr\left[\mathscr{D}\left(\mathbf{H}_B\mathbf{S}_{A_1}\mathbf{r}^*\mathbf{t}^*\right)\right]\right| \\ &= \left|Pr\left[\mathscr{D}\left(\mathbf{H}_B\mathbf{S}_{A_0}\mathbf{r}^*\right)\right] - Pr\left[\mathscr{D}\left(\mathbf{H}_B\mathbf{S}_{A_1}\mathbf{r}^*\right)\right]\right|\end{aligned} \tag{22}$$

We consider $\mathbf{S}_{A_0}\mathbf{r}^*$ and $\mathbf{S}_{A_1}\mathbf{r}^*$ as different solutions of SIS problem with $\mathbf{H}_B \in \mathscr{R}_q^{m\times m}$. Since the result of final equation is negligible, $Pr[b = b'] \le \epsilon$ holds. □

6. Parameters

Except for m, n, q, there are several main parameters for evaluating our signature efficiency, which are ι, Φ, υ, and γ. We will describe them one by one.

(i) Parameter ι. Generally, one wants to get λ bit security signature; then he will assume the output of hash function is also λ bit (see [15, 16]). So the parameter ι satisfies condition $2^\iota \cdot C_m^\iota \ge 2^{256}$.

(ii) Parameter Φ. It is chosen according to the actual situations. Firstly, it must make the value of $e^{-1/\Phi}$ be in the range $[0.75, 1]$. In this case, the chosen value satisfying $e^{-1/\Phi} = 1(\approx 1)$ is the best one. Secondly, it can't enlarge the signature size $m + m\log(\gamma - \upsilon) + m\log\gamma$. To sum up, we show the final equation,

$$\Phi = \min_{0.75 \le e^{-1/\Phi'} \le 1} \Phi'. \tag{23}$$

(iii) Parameters υ and γ. In order to utilize the result [13], we get the condition $m\Phi\upsilon \le \gamma$ directly. In addition,

Table 1: Parameters of our ID-based SDVS over $\mathscr{R}$–SIS.

Parameters	Relationship
n	rank of lattice
q	a prime number
m	$2n$
γ	$< q$
υ	$\gamma/4m$
ι	$2^{\iota} \cdot C_m^{\iota} \geq 2^{256}$
Φ	4
Signature size	$2m \log q + m$
Repetition	$e^{1/\Phi} \approx 1.28$

since choosing bigger γ means that we can get a larger signature, we let γ equal $m\Phi\upsilon$. Besides, according to the definition of $\mathscr{D}_{\gamma}$, we can easily see $\gamma < q$. So $\gamma = m\Phi\upsilon < q$ holds.

Comparison of Signature Size. Here we give a comparison with [9] about signature size, and our result is better than theirs ($3m \log q$). Furthermore, we can see that the signature size of our design is the shortest among any other existing ID-based SDVS schemes over ideal lattice. The detailed parameters can be seen in Table 1. Based on what we have discussed in those parameters, we provide the final size of our signature as follows:

$$\begin{aligned} & m \log 2 + m \log (\gamma - \upsilon) + m \log \gamma \\ & = m + m \log \left(\gamma - \frac{\gamma}{4m} \right) + m \log \gamma \\ & \leq m + m \log \left(q - \frac{q}{4m} \right) + m \log q \\ & \leq m + m \log q + m \log q \leq 3m \log q. \end{aligned} \tag{24}$$

7. Conclusion and Further Work

Conclusion. In this paper, we provide an ID-based SDVS scheme over ideal lattice. Our scheme has the shortest signature size $2m \log q + m$ and satisfies three properties unforgeability, untransferability, and anonymity proved in the random oracle. Moreover, we use uniform sampling to resist side-channel attacks in our design, and the repetition approximate 1 means our scheme has a relatively high efficiency.

Further Work. We consider the quantum random oracle. As far as we know, in existing lattice-based signature schemes, only TESLA [26] has proved its security in the quantum random oracle. Hence, our further work is to use their method to give a proper proof in the quantum random oracle for our scheme.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China [grant numbers 61572294, 61602287, 11531008, and 11771252]; the State Key Program of National Natural Science of China [grant number 61632020]; the Natural Science Foundation of Shandong Province [grant number ZR2017MF021]; the Major Innovation Project of Science and Technology, Shandong [grant number 2018CXGC0702]; the Fundamental Research Funds of Shandong University [grant number 2017JC019]; the Primary Research & Development Plan of Shandong Province [grant number 2018GGX101037]; the National Innovation Demonstration Zone Development and Construction Fund Project of Shandong Peninsula [grant number S190101010001]; the Innovative Research Team in University by Ministry of Education [grant number IRT16R43]; and Taishan Scholars Project.

References

[1] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," in *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques - Advances in Cryptology - EUROCRYPT '96*, vol. 1070, pp. 143–154, Saragossa, Spain, May 1996.

[2] S. Saeednia, S. Kremer, and O. Markowitch, "An efficient strong designated verifier signature scheme," in *Proceedings of the 6th International Conference, Information Security and Cryptology - ICISC '03*, vol. 2971, pp. 40–54, Seoul, Korea, November 2003.

[3] F. Laguillaumie and D. Vergnaud, "Designated verifier signatures: anonymity and efficient construction from any bilinear map," in *Proceedings of the 4th International Conference of Security in Communication Networks, SCN '04*, Revised Selected Papers, pp. 105–119, Amalfi, Italy, September 2004.

[4] W. Susilo, F. Zhang, and Y. Mu, "Identity-based strong designated verifier signature schemes," in *Proceedings of the 9th Australasian Conference, Information Security and Privacy, ACISP '04*, pp. 313–324, Sydney, Australia, July 2004.

[5] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "Short (identity-based) strong designated verifier signature schemes," in *Proceedings of the 2nd International Conference of Information Security Practice and Experience, ISPEC '06*, pp. 214–225, Hangzhou, China, April 2006.

[6] O. Blazy, E. Conchon, P. Germouty, and A. Jambert, "Efficient id-based designated verifier signature," in *12th International Conference on Availability, Reliability and Security*, pp. 44:1–44:8, Reggio Calabria, Italy, August 2017.

[7] G. Noh, J. Y. Chun, and I. R. Jeong, "Identity-based strong designated verifier signature scheme from lattices," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 23, no. 1, pp. 45–56, 2013.

[8] F. Wang, Y. Hu, and B. Wang, "Lattice-based strong designate verifier signature and its applications," *Malaysian Journal of Computer Science*, vol. 25, no. 1, pp. 11–22, 2012.

[9] F. H. Wang, H. U. Yu-Pu, and C. X. Wang, "Identity-based strong designate verifier signature over lattices," *Journal of*

China Universities of Posts and Telecommunications, vol. 21, no. 6, pp. 52–60, 2014.

[10] 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 *Proceedings of the Cryptographic Hardware and Embedded Systems – CHES '16*, B. Gierlichs and A. Y. Poschmann, Eds., pp. 323–345, Springer, Berlin, Germany, 2016.

[11] P. Pessl, "Analyzing the shuffling side-channel countermeasure for lattice-based signatures," in *Proceedings of the Progress in Cryptology – INDOCRYPT '16*, O. Dunkelman and S. K. Sanadhya, Eds., pp. 153–170, Springer International Publishing, Cham, Switzerland, 2016.

[12] D. Micciancio and M. Walter, "Gaussian sampling over the integers: efficient, generic, constant-time," in *Proceedings of the 37th Annual International Cryptology Conference - Advances in Cryptology - CRYPTO '17*, vol. 10402, pp. 455–485, California, Calif, USA, August 2017.

[13] M. Rückert, "Lattice-based blind signatures," in *Proceedings of the 16th International Conference on the Theory and Application of Cryptology and Information Security - Advances in Cryptology - ASIACRYPT '10*, vol. 6477 of *Lecture Notes in Computer Science*, pp. 413–430, Singapore, December 2010.

[14] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, "Lattice signatures and bimodal gaussians," in *Proceedings of the 33rd Annual Cryptology Conference - Advances in Cryptology - CRYPTO '13*, Proceedings, Part I, pp. 40–56, California, Calif, USA, August 2013.

[15] L. Ducas, T. Lepoint, V. Lyubashevsky et al., "CRYSTALS - dilithium: digital signatures from module lattices," IACR Cryptology ePrint Archive, 633, 2017, http://eprint.iacr.org/2017/633.

[16] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques - Advances in Cryptology - EUROCRYPT '12*, pp. 738–755, Cambridge, UK, April 2012.

[17] V. Lyubashevsky, "Lattice-based identification schemes secure under active attacks," in *Proceedings of the 11th International Workshop on Practice and Theory in Public-Key Cryptography - Public Key Cryptography - PKC '08*, vol. 4939, pp. 162–179, Barcelona, Spain, March 2008.

[18] V. Lyubashevsky, "Fiat-shamir with aborts: applications to lattice and factoring-based signatures," in *Proceedings of the 15th International Conference on the Theory and Application of Cryptology and Information Security - Advances in Cryptology - ASIACRYPT '09*, vol. 5912, pp. 598–616, Tokyo, Japan, December 2009.

[19] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange - a new hope," in *Proceedings of the 25th USENIX Security Symposium, USENIX Security '16*, pp. 327–343, Texas, Tex, USA, August 2016, https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/alkim.

[20] J. W. Bos, C. Costello, L. Ducas et al., "Take off the ring! practical, quantum-secure key exchange from LWE," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1006–1018, Vienna, Austria, October 2016.

[21] "Advances in Cryptology - CRYPTO 2013," in *Proceedings of the 33rd Annual Cryptology Conference, R. Canetti and J. A. Garay, Eds.*, vol. 8042 of *Proceedings, Part I, Lecture Notes in Computer Science*, Springer, California, Calif, USA, August 2013.

[22] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC '05)*, pp. 84–93, ACM, Maryland, Md, USA, May 2005.

[23] C. Peikert and A. Rosen, "Lattices that admit logarithmic worst-case to average-case connection factors," in *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pp. 478–487, ACM, California, Calif, USA, June 2007.

[24] J. Cai, H. Jiang, P. Zhang, Z. Zheng, G. Lyu, and Q. Xu, "An efficient strong designated verifier signature based on R-sis assumption," *IEEE Access*, vol. 7, pp. 3938–3947, 2019.

[25] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang, "Choosing parameters for ntruencrypt," in *Proceedings of the Cryptographers' Track at the RSA Conference - Topics in Cryptology - CT-RSA '17*, pp. 3–18, California, Calif, USA, 2017.

[26] E. Alkim, N. Bindel, J. A. Buchmann et al., "Revisiting TESLA in the quantum random oracle model," in *Proceedings of the 8th International Workshop - Post-Quantum Cryptography, PQCrypto '17*, pp. 143–162, The Netherlands, June 2017.