# Transitive Signature Schemes for Undirected Graphs from Lattices

**Geontae Noh[1] and Ik Rae Jeong[2*]**
[1] Department of Information Security, Seoul Cyber University
60, Solmae-ro 49-gil, Gangbuk-gu, Seoul, 01133, Korea
[e-mail: gnoh@iscu.ac.kr]
[2] CIST (Center for Information Security Technologies), Korea University
145 Anam-ro, Seongbuk-gu, Seoul, 02841, Korea
[e-mail: irjeong@korea.ac.kr]
*Corresponding author: Ik Rae Jeong

*Received September 13, 2017; revised November 25, 2018; accepted January 27, 2019; published June 30, 2019*

## Abstract

In a transitive signature scheme, a signer wants to authenticate edges in a *dynamically growing* and *transitively closed* graph. Using transitive signature schemes it is possible to authenticate an edge $(i,k)$, if the signer has already authenticated two edges $(i,j)$ and $(j,k)$. That is, it is possible to make a signature on $(i,k)$ using two signatures on $(i,j)$ and $(j,k)$. We propose the first transitive signature schemes for undirected graphs from lattices. Our first scheme is provably secure in the random oracle model and our second scheme is provably secure in the standard model.

***Keywords:*** Lattice-based cryptography, transitive signature, undirected graphs

---

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2017R1C1B5076610).

**http://doi.org/10.3837/tiis.2019.06.030** **ISSN : 1976-7277**

# 1. Introduction

In 2002, Silvio Micali and Ronald L. Rivest introduced the concept of transitive signatures [1]. In a transitive signature scheme, a signer wants to authenticate edges in a *dynamically growing* and *transitively closed* graph. The signer with the knowledge of a secret key can generate two signatures $\sigma_{i,j}$ on $(i, j)$ and $\sigma_{j,k}$ on an edge $(j,k)$, then anyone without the knowledge of the secret key can derive a signature $\sigma_{i,k}$ on $(i,k)$ from $\sigma_{i,j}$ and $\sigma_{j,k}$. This property of transitive signatures could be useful in applications such as a military chain-of-command (for directed graphs) and administrative domains (for undirected graphs).

Constructing a transitive signature scheme for directed graphs still remains an open problem. In 2003, Susan Rae Hohenberger even showed that constructing a transitive signature scheme for directed graphs may be very hard [2]. Actually, there exist only transitive signature schemes for *directed trees* (not for directed graphs) [3][4][5][6][7]. In this paper, we only take an interest in constructing a transitive signature scheme for *undirected graphs*.

In an undirected graph, we assume that there are $\mathrm{k}$ nodes. Then we observe that there may exist $O(\mathrm{k}^2)$ edges. With a standard signature scheme, naturally, a signer has to generate $O(\mathrm{k}^2)$ signatures. With a transitive signature scheme, however, a signer only needs to generate $O(\mathrm{k})$ signatures [1]. Therefore, the transitive signature scheme can be efficient and useful in the environments.

## 1.1 Related Works

### 1.1.1 Transitive Signatures

In 2002, Silvio Micali and Ronald L. Rivest proposed the first transitive signature scheme for undirected graphs [1]. In 2004, Siamak Fayyaz Shahandashti et al. proposed a transitive signature scheme for undirected graphs [8]. Their scheme is based on bilinear maps. Since then, Mihir Bellare and Gregory Neven proposed transitive signature schemes for undirected graphs [9][10]. The securities of their schemes are based on the hardness of RSA assumption, factoring, DLP, GDH (Gap Diffie-Hellman) assumption, respectively. Mihir Bellare and Gregory Neven also constructed a simple generic transformation from a *stateful* transitive signature scheme to a *stateless* transitive signature scheme with a pseudorandom function [10]. The signing algorithm in the transformed stateless transitive signature scheme is deterministic because the pseudorandom function is used.

### 1.1.2 Lattice-based Cryptosystems

To date, there exist many transitive signature schemes for undirected graphs, but there exists no transitive signature scheme for undirected graphs from lattices. Lattice-based cryptosystems have some advantages compared to other cryptosystems based on the hardness of factoring, DLP, and so on. First, lattice-based cryptosystems are based on the worst-case hardness assumptions, but other cryptosystems are based on the average-case hardness assumptions. Next, lattice-based cryptosystems have the potential to resist quantum computing attacks, but other cryptosystems are insecure against quantum computing attacks [11]. Finally, lattice-based cryptosystems require less computational cost than other cryptosystems. With these in mind, there are proposed many lattice-based cryptosystems such as standard signatures [12][13][14][15][16], (hierarchical) identity-based signatures [15][17], group signatures [18], ring signatures [19][20], designated verifier signatures [21], homomorphic signatures [22][23], public key encryptions [16], (hierarchical) identity-based encryptions [12][13][24][25][26], homomorphic encryptions [27], and so on.

### 1.1.3 Homomorphic Signatures

Transitive signatures are related to homomorphic signatures formalized by Robert Johnson et al. in 2002 [28]. In a homomorphic signature scheme, a signer wants to authenticate data and anyone without the knowledge of the secret can generate a valid signature for computing on signed data. In 2011, Dan Boneh and David Mandell Freeman proposed two linearly homomorphic signature schemes from lattices [22][23].

### 1.2 Our Contributions

We propose two transitive signature schemes for undirected graphs from lattices. The first scheme is provably secure in the random oracle model and the second scheme is provably secure in the standard model.

Our transitive signature schemes are *stateful*. In 2012, Abhishek Banerjee et al. proposed pseudorandom functions from lattices [29]. With the pseudorandom functions from lattices, our stateful transitive signature schemes can be transformed into *stateless* transitive signature schemes [10].

All existing transitive signature schemes are insecure against quantum computing attacks. Therefore, we propose the first transitive signature schemes that have the potential to resist quantum computing attacks. Our first transitive signature scheme which is motivated by Craig Gentry et al.'s signature scheme from lattices [12] is provably secure in the random oracle model. To design our transitive signature scheme, we use a signature value in Craig Gentry et al.'s signature scheme that has a particular coset of $q$-ary lattices [12]. Our second transitive signature scheme is provably secure in the standard model. To make our transitive signature scheme secure in the standard model, we use the idea of the $k$-time signature scheme from lattices by Dan Boneh and David Mandell Freeman [22] and a signature value that has a particular coset of $q$-ary lattices [12].

## 2. Preliminaries

### 2.1 Notations

Let $n$ be a security parameter. We denote integers, real numbers, the ring of integers modulo $q \geq 2$ by $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{Z}_q$, respectively. We denote matrices by upper-case letters (e.g., $A$) and vectors by lower-case letters (e.g., $v$). We denote the Euclidean norms of $v$ by $\|v\|$. We use standard big-$O$ notation. For all integer $c > 0$, we say that a function $f(n) = O(n^{-c}) : \mathbb{Z} \to \mathbb{R}^+$ is negligible in $n$. If $q \in \Theta(n^c)$, for all integer $c > 0$, we say $q = \text{poly}(n)$. If $v$ is selected from a distribution $\mathcal{D}$ at random, we denote $v \leftarrow \mathcal{D}$. We denote a concatenation of $v_1$ and $v_2$ by $v_1 | v_2$. Let $\text{Round}(v)$ be the function that rounds the coordinates of its argument vector $v$ to the nearest integers.

### 2.2 Lattices

In this paper, we will be interested in $m$-dimensional integer lattices which are defined as follows:

**Definition 2.1**. Given any basis $B = \{b_1, \cdots, b_m\} \subset \mathbb{Z}^m$, an $m$-dimensional integer lattice $\Lambda$ and a dual lattice $\Lambda^*$ of $\Lambda$ are defined as follows:

$$\Lambda = \{B \cdot z = \sum_{i=1}^{m} z_i b_i : z \in \mathbb{Z}^m\} \subseteq \mathbb{Z}^m, \tag{1}$$

$$\Lambda^* = \{x \in \mathbb{Z}^m : \forall y \in \Lambda, \langle x, y \rangle \in \mathbb{Z}\} \subseteq \mathbb{Z}^m. \tag{2}$$

In particular, we will use $q$-ary lattices and their cosets which are defined as follows:

**Definition 2.2**. Given any uniformly random matrix $A \in \mathbb{Z}_q^{n \times m}$, a zero vector $0 \in \mathbb{Z}_q^n$, and any syndrome $u \in \mathbb{Z}_q^n$, a $q$-ary lattice $\Lambda_q^{\perp}(A)$ and a coset $\Lambda_q^u(A)$ of $\Lambda_q^{\perp}(A)$ are defined as follows:

$$\Lambda_q^{\perp}(A) = \{v \in \mathbb{Z}^m : A \cdot v = 0 (\text{mod}\, q)\} \subseteq \mathbb{Z}^m, \tag{3}$$

$$\Lambda_q^u(A) = \{v \in \mathbb{Z}^m : A \cdot v = u\ (\text{mod}\, q)\} \subseteq \mathbb{Z}^m. \tag{4}$$

#### 2.2.1 Gaussian Distributions

We recall Gaussian distributions.

**Definition 2.3** (Gaussian function). Let $\mathcal{H}$ be a $d$-dimensional subspace of $\mathbb{R}^m$. For $m \geq 1$, $s > 0$, $x \in \mathcal{H}$, and $c \in \mathcal{H}$, a Gaussian function $\rho_{\mathcal{H},s,c}(x)$ is defined as follows:

$$\rho_{\mathcal{H},s,c}(x) = \exp(-\pi \| x - c \|^2 / s^2). \tag{5}$$

**Definition 2.4** (Continuous distribution). Let $\mathcal{H} =$ span$(\Lambda \subset \mathcal{H})$. For $x \in \Lambda$, a continuous distribution $\mathcal{D}_{\mathcal{H},s,c}(x)$ with density function is defined as follows:

$$\mathcal{D}_{\mathcal{H},s,c}(x) = \frac{\rho_{\mathcal{H},s,c}(x)}{\int_{x \in \mathcal{H}} \rho_{\mathcal{H},s,c}(x)\, dx}. \tag{6}$$

**Definition 2.5** (Discrete distribution). Let $\mathcal{H} =$ span $(\Lambda \subset \mathcal{H})$. For $x \in \Lambda$, a discrete distribution $\mathcal{D}_{\Lambda,s,c}(x)$ with density function over $\Lambda$ is defined as follows:

$$\mathcal{D}_{\Lambda,s,c}(x) = \frac{\mathcal{D}_{\mathcal{H},s,c}(x)}{\mathcal{D}_{\mathcal{H},s,c}(\Lambda)}. \tag{7}$$

For convenience, $\rho_{\mathcal{H},s,0}(x)$ and $\mathcal{D}_{\mathcal{H},s,0}(x)$ are abbreviated as $\rho_{\mathcal{H},s}(x)$ and $\mathcal{D}_{\mathcal{H},s}(x)$, respectively.

**Definition 2.6** (Gaussian parameter). Let $\Lambda^*$ be a dual lattice of $\Lambda$. For $\varepsilon > 0 \in \mathbb{R}$, a Gaussian parameter $\eta_\varepsilon(\Lambda)$ is the smallest $s$ such that $\rho_{\mathcal{H},1/s}(\Lambda^* \setminus \{0\}) \le \varepsilon$.

### 2.2.2 Trapdoor Generation

We will use the trapdoor generation algorithm $\text{GenTrap}(1^n, 1^m, q)$ which is as follows:

**Theorem 2.7** (Trapdoor generation) [16]. Given any integers $n \ge 1$, $m = O(n \log q)$, and $q \ge 2$, the trapdoor generation algorithm $\text{GenTrap}(1^n, 1^m, q)$ outputs a uniformly random matrix $A \in \mathbb{Z}_q^{n \times m}$ and a trapdoor matrix $T \leftarrow \mathcal{D}_{\mathbb{Z},\omega(\sqrt{\log n})}^{\overline{m} \times nl}$ of $\Lambda_q^\perp(A)$, where $m = \overline{m} + nl$, $\overline{m} = O(nl)$, $l = O(\log n)$, and the rank of $A$ is $n$.

### 2.2.3 Gaussian Pre-image Sampling

We will use the Gaussian pre-image sampling algorithm $\text{SampleD}(A, T, u, s)$ which is as follows:

**Theorem 2.8** (Gaussian pre-image sampling) [16]. Given any uniformly random matrix $A \in \mathbb{Z}_q^{n \times m}$, any trapdoor matrix $T \leftarrow \mathcal{D}_{\mathbb{Z},\omega(\sqrt{\log n})}^{\overline{m} \times nl}$ of $\Lambda_q^\perp(A)$, any syndrome $u \in \mathbb{Z}_q^n$, and large enough $s = O(\sqrt{n \log q})$, the Gaussian pre-image sampling algorithm $\text{SampleD}(A, T, u, s)$ outputs a vector $v$. The statistical distance between the distribution of $v$ and $\mathcal{D}_{\Lambda_q^u(A), s \cdot \omega(\sqrt{\log n})}$ is negligible in $n$.

### 2.2.4 Gaussian Domain Sampling

We will use the Gaussian domain sampling algorithm $\text{SampleDom}(1^m, s)$ which is as follows:

**Theorem 2.9** (Gaussian domain sampling) [12]. Given any positive integer $m$ and large enough $s$, the Gaussian domain sampling algorithm $\text{SampleDom}(1^m, s)$ outputs a vector $v \leftarrow \mathcal{D}_{\mathbb{Z},s}^m$.

### 2.2.5 Hard Problems

The securities of our constructions are based on the SIS problem and k-SIS problem, respectively. The SIS problem is defined as follows:

**Definition 2.10** (SIS problem) [30][12]. Given any uniformly random matrix $A \in \mathbb{Z}_q^{n \times m}$, the $\text{SIS}_{q,m,\beta}$ problem is to find a non-zero vector $v \in \mathbb{Z}^m$ such that $A \cdot v = 0 \pmod q$ and $\| v \| \le \beta$.

The advantage $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{SIS}}(n)$ of an algorithm $\mathcal{A}$ in the $\mathrm{SIS}_{q,m,\beta}$ problem is the probability that $\mathcal{A}$ solves the $\mathrm{SIS}_{q,m,\beta}$ problem.

The $\mathrm{k}$-$\mathrm{SIS}$ problem is defined as follows:

**Definition 2.11** ($\mathrm{k}$-$\mathrm{SIS}$ problem) [22]. Given any uniformly random matrix $A \in \mathbb{Z}_q^{n\times m}$ and $\mathrm{k}$ vectors $v_1,\cdots,v_{\mathrm{k}} \leftarrow \mathcal{D}_{\Lambda_q^{\perp}(A),s}$ such that $A\cdot v_1 = \cdots = A\cdot v_{\mathrm{k}} = 0(\bmod q)$, the $\mathrm{k}$-$\mathrm{SIS}_{q,m,\beta,s}$ problem is to find a non-zero vector $v \in \mathbb{Z}^m$ such that $A\cdot v = 0(\bmod q)$, $\| v \| \le \beta$, and $v$ is not in $\mathbb{Q}$-span $(\{v_1,\cdots,v_{\mathrm{k}}\})$.

The advantage $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{k-SIS}}(n)$ of an algorithm $\mathcal{A}$ in the $\mathrm{k}$-$\mathrm{SIS}_{q,m,\beta,s}$ problem is the probability that $\mathcal{A}$ solves the $\mathrm{k}$-$\mathrm{SIS}_{q,m,\beta,s}$ problem.

The SIS problem for $q \ge \beta\cdot\sqrt{n}\cdot\omega(\sqrt{\log n})$ is hard assuming worst-case hardness of approximating the SIVP on lattices [30][12]. The $\mathrm{k}$-$\mathrm{SIS}$ problem for $\mathrm{k} = O(n/\log n)$ is hard assuming average-case hardness of the SIS problem [22][31].

### 2.2.6 Useful Lemmas

In this paper, we will use the following lemmas:

**Lemma 2.12** [30][13][16]. For $\varepsilon \in \{0,1\}$, $s \ge \eta_{\varepsilon}(\Lambda_q^{\perp}(A))$ for some uniformly random matrix $A \in \mathbb{Z}_q^{n\times m}$, $c \in span(\Lambda_q^{\perp}(A))$, and $x \leftarrow \mathcal{D}_{\Lambda,s,c}$, the probability of $\| x \| \ge s\cdot\sqrt{m}$ is negligible in $n$ and the probability of $x = c$ is negligible in $n$.

**Lemma 2.13** [22]. Let $q$ be an odd prime, let $m \ge O(n\log q)$, and let $s > \omega(\sqrt{\log m})$. Given an instance $(A, v_1,\cdots,v_{\mathrm{k}}) \in \mathbb{Z}_q^{n\times m}\times\mathbb{Z}^{m\times \mathrm{k}}$ of the $\mathrm{k}$-$\mathrm{SIS}_{q,m,\beta,s}$ problem for any $\beta$, $(A, v_1 \,(\bmod 2),\cdots,v_{\mathrm{k}} \quad (\bmod 2)) \in \mathbb{Z}_q^{n\times m}\times\mathbb{Z}_2^{m\times \mathrm{k}}$ is statistically indistinguishable from uniform.

**Lemma 2.14** [22]. Let $m$ be an integer and $\mathrm{k} < m$ an integer. The probability that the rank of a uniformly random matrix $V \in \mathbb{Z}_2^{m\times \mathrm{k}}$ is not $\mathrm{k}$ is at most $1/2^{m-k}$.

**Lemma 2.15** [22]. Let $m \ge O(n\log q)$, let $\mathrm{k}\cdot\omega(\log n) < \min(s, m^{1/4})$, and let $(A, v_1,\cdots,v_{\mathrm{k}}) \in \mathbb{Z}_q^{n\times m}\times\mathbb{Z}^{m\times \mathrm{k}}$ be an instance of the $\mathrm{k}$-$\mathrm{SIS}_{q,m,\beta,s}$ problem for any $\beta$. There exist only $(\pm v_1,\cdots,\pm v_{\mathrm{k}})$ such that the non-zero vectors of length at most $1.1\cdot s\cdot\sqrt{m/2\pi}$ in $\mathbb{Q}$-span $(\{v_1,\cdots,v_{\mathrm{k}}\})$.

### 2.3 Definitions for Transitive Signatures

We define transitive signatures. A transitive signature scheme $\mathrm{TS} = \{\mathrm{TS.Gen}, \mathrm{TS.Sign}, \mathrm{TS.Vrfy}, \mathrm{TS.Comp}\}$ is specified as follows:

- $\mathrm{TS.Gen}(1^n)$ : On input the security parameter $1^n$, output a public key $pk$ and a secret key $sk$.
- $\mathrm{TS.Sign}(sk,(i,j))$ : On input the secret key $sk$ and the edge $(i,j)$, output a signature $\sigma_{i,j}$ on the edge $(i,j)$.
- $\mathrm{TS.Vrfy}(pk,(i,j),\sigma_{i,j})$ : On input the public key $pk$, the edge $(i,j)$, and the signature $\sigma_{i,j}$ on the edge $(i,j)$, output a bit 1 if $\sigma_{i,j}$ is valid and output a bit 0 otherwise.
- $\mathrm{TS.Comp}(pk,(i,j,k),\sigma_{i,j},\sigma_{j,k})$ : On input the public key $pk$, the signature $\sigma_{i,j}$ on $(i,j)$, the signature $\sigma_{j,k}$ on $(j,k)$, output a valid signature $\sigma_{i,k}$ on $(i,k)$.

Transitive signatures basically have to satisfy *correctness*, *transitivity*, and *transitive unforgeability under chosen-edge attacks*. First, we define that a transitive signature scheme $\mathrm{TS}$ is correct if, for any valid signature $\sigma_{i,k}$ on the edge $(i,k)$ (generated with the $\mathrm{TS.Sign}(sk,(i,k))$ algorithm) or for any valid combined signature $\sigma_{i,k}$ on $(i,k)$ (generated with the $\mathrm{TS.Comp}(pk,(i,j,k), \sigma_{i,j},\sigma_{j,k})$ algorithm), the $\mathrm{TS.Vrfy}(pk,(i,k),\sigma_{i,k})$ algorithm outputs a bit 1 with all but negligible probability.

Next, we define that a transitive signature scheme $\mathrm{TS}$ is transitive if, for two signatures $\sigma_{i,j}$ on $(i,j)$ and $\sigma_{j,k}$ on the edge $(j,k)$, anyone without the knowledge of the secret key can derive a signature $\sigma_{i,k}$ on $(i,k)$ which is indistinguishable from another signature $\sigma'_{i,k}$ on $(i,k)$ (generated with the $\mathrm{TS.Sign}(sk,(i,k))$ algorithm).

Finally, we define that a transitive signature scheme $\mathrm{TS}$ is transitively unforgeable under chosen-edge attacks if, in the following game $\mathrm{Game}^{\mathrm{TU}}_{\mathrm{TS},\mathcal{F}}(n)$ between an algorithm $\mathcal{A}$ and a forger $\mathcal{F}$, the advantage $\mathrm{Adv}^{\mathrm{TU}}_{\mathrm{TS},\mathcal{F}}(n)$ of $\mathcal{F}$ is negligible.

- **Setup**: $\mathcal{A}$ runs the $\mathrm{TS.Gen}(1^n)$ algorithm to get $(pk,sk)$. $\mathcal{A}$ sends $pk$ to $\mathcal{F}$.
- **Signing queries**: $\mathcal{F}$ sends the edge $(i,j)$ to $\mathcal{A}$. $\mathcal{A}$ runs the $\mathrm{TS.Sign}(sk,(i,j))$ algorithm to get $\sigma_{i,j}$ and sends it to $\mathcal{F}$.
- **Output**: $\mathcal{F}$ outputs the edge $(i^*,j^*)$ and the signature $\sigma_{i^*,j^*}$. If the $\mathrm{TS.Vrfy}(pk,(i^*,j^*),\sigma_{i^*,j^*})$ algorithm outputs a bit 1 and the edge $(i^*,j^*)$ is not in the transitive closure of previously signed edges, then $\mathcal{F}$ wins the game $\mathrm{Game}^{\mathrm{TU}}_{\mathrm{TS},\mathcal{F}}(n)$.

The advantage $\mathrm{Adv}^{\mathrm{TU}}_{\mathrm{TS},\mathcal{F}}(n)$ of $\mathcal{F}$ in the game $\mathrm{Game}^{\mathrm{TU}}_{\mathrm{TS},\mathcal{F}}(n)$ is the probability that $\mathcal{F}$ wins the game $\mathrm{Game}^{\mathrm{TU}}_{\mathrm{TS},\mathcal{F}}(n)$.

### 2.4 Chameleon Hash Function

In the *Proof of Theorem 4.3*, we will use a chameleon hash function proposed by David Cash et al. in 2010 [13]. David Cash et al.'s chameleon hash function $\mathrm{H}(\cdot,\cdot):\{0,1\}^* \times \{0,1\}^m \to \{0,1\}^n$ has the following properties:

1. Trapdoor property: Given $\mathrm{H}(i,r_i)$ and $j \neq i$, one with the knowledge of the trapdoor information can sample $r_j$ such that $\mathrm{H}(i,r_i) = \mathrm{H}(j,r_j)$.
2. Collision-resistance property: It is hard to compute two pairs $(i,r_i)$ and $(j,r_j)$ without the knowledge of the trapdoor information such that $\mathrm{H}(i,r_i) = \mathrm{H}(j,r_j)$ and $(i,r_i) \neq (j,r_j)$.

David Cash et al.'s chameleon hash function $\mathrm{H}(\cdot,\cdot)$ is collision-resistant assuming the $\mathrm{SIS}_{q,m,\beta}$ problem.

## 3. Our Construction for Undirected Graphs in the Random Oracle Model

We construct a transitive signature scheme for undirected graphs in the random oracle model. Our scheme involves the following parameters:

- A security parameter is $n$.
- The dimension of signatures is $m = \overline{m} + nl$, where $\overline{m} = O(nl)$ and $l = O(\log n)$.
- $q = \mathrm{poly}(n)$.
- A Gaussian parameter is $s = O(n^c \sqrt{\log n}) \cdot \omega(\sqrt{\log n})$, where $c$ is constant.

We construct our scheme $\mathrm{TS}_1 = \{\mathrm{TS}_1.\mathrm{Gen}, \mathrm{TS}_1.\mathrm{Sign}, \mathrm{TS}_1.\mathrm{Vrfy}, \mathrm{TS}_1.\mathrm{Comp}\}$ as follows:

- $\mathrm{TS}_1.\mathrm{Gen}(1^n)$: On input the security parameter $1^n$:
    1. Compute $(A,T)$ using the GenTrap algorithm, where $A \in \mathbb{Z}_q^{n\times m}$ and $T \leftarrow \mathcal{D}^{\overline{m}\times nl}_{\mathbb{Z},\omega(\sqrt{\log n})}$.
    2. Choose a hash function $\mathrm{H}(\cdot):\{0,1\}^* \to \mathbb{Z}_q^n$.
        i. Note that the security analysis will view $\mathrm{H}(\cdot)$ as a random oracle.
    3. Output a public key $pk = (A, \mathrm{H}(\cdot))$ and a secret key $sk = T$.

- $\mathrm{TS}_1.\mathrm{Sign}(sk,(i,j))$: On input the secret key $sk = T$ and the edge $(i,j)$:
  1. If state $St(i)$ is empty, compute $h_i = \mathrm{H}(i) \in \mathbb{Z}_q^n$, sample $v_i \leftarrow \mathcal{D}_{\Lambda_q^{h_i}(A),s}$ using the Gaussian pre-image sampling algorithm $\mathsf{SampleD}$ in the Theorem 2.8, and set $St(i) = v_i$.
  2. If state $St(j)$ is empty, compute $h_j = \mathrm{H}(j) \in \mathbb{Z}_q^n$, sample $v_j \leftarrow \mathcal{D}_{\Lambda_q^{h_j}(A),s}$ using the Gaussian pre-image sampling algorithm $\mathsf{SampleD}$ in the Theorem 2.8, and set $St(j) = v_j$.
  3. Compute $\sigma_{i,j} = v_i - v_j$ with states $St(i) = v_i$ and $St(j) = v_j$.
  4. Output a signature $\sigma_{i,j}$.
- $\mathrm{TS}_1.\mathrm{Vrfy}(pk,(i,j),\sigma_{i,j})$: On input the public key $pk = (A, \mathrm{H}(\cdot))$, the edge $(i,j)$, and the signature $\sigma_{i,j}$:
  1. Compute $h_i = \mathrm{H}(i) \in \mathbb{Z}_q^n$ and $h_j = \mathrm{H}(j) \in \mathbb{Z}_q^n$.
  2. Output a bit 1 if $\| \sigma_{i,j} \| \le s \cdot \sqrt{2m}$ and $A \cdot \sigma_{i,j} = h_i - h_j \pmod q$, and output a bit $0$ otherwise.
- $\mathrm{TS}_1.\mathrm{Comp}(pk,(i,j,k),\sigma_{i,j},\sigma_{j,k})$ : On input the public key $pk = (A, \mathrm{H}(\cdot))$, the signature $\sigma_{i,j}$ on $(i,j)$, the signature $\sigma_{j,k}$ on $(j,k)$:
  1. Compute $\sigma_{i,k} = \sigma_{i,j} + \sigma_{j,k}$.
  2. Output a signature $\sigma_{i,k}$.

## 3.1 Correctness

We show that our scheme $\mathrm{TS}_1$ is correct.

**Theorem 3.1**. Our scheme $\mathrm{TS}_1$ is correct.

*Proof of Theorem 3.1*. The $\mathrm{TS}_1.\mathrm{Sign}(sk,(i,j))$ algorithm can sample $v_i$ and $v_j$ such that $\| v_i \| \le s \cdot \sqrt{m}$, $\| v_j \| \le s \cdot \sqrt{m}$, $A \cdot v_i = h_i \pmod q$, and $A \cdot v_j = h_j \pmod q$. That is, $A \cdot \sigma_{i,j} = A \cdot (v_i - v_j) = h_i - h_j \pmod q$ and $\| \sigma_{i,j} \| = \| v_i - v_j \| \le s \cdot \sqrt{2m}$.

The $\mathrm{TS}_1.\mathrm{Comp}(pk,(i,j,k),\sigma_{i,j},\sigma_{j,k})$ algorithm can compute $\sigma_{i,j} + \sigma_{j,k} = (v_i - v_j) + (v_j - v_k) = v_i - v_k$ such that $\| v_i \| \le s \cdot \sqrt{m}$, $\| v_k \| \le s \cdot \sqrt{m}$, $A \cdot v_i = h_i \pmod q$, and $A \cdot v_k = h_k \pmod q$. That is, $A \cdot \sigma_{i,k} = A \cdot (v_i - v_k) = h_i - h_k \pmod q$ and $\| \sigma_{i,k} \| = \| v_i - v_k \| \le s \cdot \sqrt{2m}$.

Therefore, our scheme $\mathrm{TS}_1$ is correct. □

### 3.2 Transitivity

We show that our scheme $\mathrm{TS}_1$ is transitive for undirected graphs.

**Theorem 3.2**. Our scheme $\mathrm{TS}_1$ is transitive for undirected graphs.

*Proof of Theorem 3.2*. The $\mathrm{TS}_1.\mathrm{Comp}(pk,(i,j,k),\sigma_{i,j},\sigma_{j,k})$ algorithm computes as follows:

$$\sigma_{i,k} = \sigma_{i,j} + \sigma_{j,k} = v_i - v_j + v_j - v_k = v_i - v_k. \tag{8}$$

A combined signature $\sigma_{i,k}$ on the edge $(i,k)$ generated with the $\mathrm{TS}_1.\mathrm{Comp}(pk,(i,j,k),\sigma_{i,j},\sigma_{j,k})$ is indistinguishable from $\sigma'_{i,k}$ on the edge $(i,k)$ generated with the $\mathrm{TS}_1.\mathrm{Sign}(sk,(i,k))$.

On the other hand, $\sigma_{i,j}$ can be easily made from $\sigma_{j,i}$ as follows:

$$\sigma_{i,j} = -\sigma_{j,i} = -(v_j - v_i) = v_i - v_j. \tag{9}$$

Therefore, our scheme $\mathrm{TS}_1$ is transitive for undirected graphs. □

### 3.3 Transitive Unforgeability

We show that our scheme $\mathrm{TS}_1$ is transitively unforgeable under chosen-edge attacks in the random oracle model.

**Theorem 3.3**. Our scheme $\mathrm{TS}_1$ is transitively unforgeable under chosen-edge attacks in the random oracle model if the $\mathrm{SIS}_{q,m,\beta}$ problem for $\beta = s\cdot\sqrt{4m}$ is hard.

*Proof of Theorem 3.3*. Let $\mathrm{H}(\cdot)$ be a random oracle controlled by $\mathcal{A}$. Then we can construct $\mathcal{A}$ attacking the $\mathrm{SIS}_{q,m,\beta}$ problem for $\beta = s\cdot\sqrt{4m}$ if there exists a forger $\mathcal{F}$ mounting transitive forgery attacks on $\mathrm{TS}_1$ as follows:

- **Setup**: On input an instance $A \in \mathbb{Z}_q^{n\times m}$ of the $\mathrm{SIS}_{q,m,\beta}$ problem:
  1. $\mathcal{A}$ sends $pk = A$ to $\mathcal{F}$.
- $\mathrm{H}$ **-queries**: On input the $i$-th node $i$:
  1. $\mathcal{A}$ samples $v_i \leftarrow \mathcal{D}_{\mathbb{Z},s}^m$ using the $\mathrm{SampleDom}(1^m, s)$ algorithm.
  2. $\mathcal{A}$ computes $h_i = A\cdot v_i \in \mathbb{Z}_q^n$.
  3. $\mathcal{A}$ sends $h_i$ to $\mathcal{F}$.
  4. $\mathcal{A}$ adds a tuple $\{i, v_i, h_i\}$ to the hash table.

- **Signing queries**: On input the edge $(i, j)$ :
  1. If $i$ already appears on the hash table, $\mathcal{A}$ looks up $\{i, v_i, h_i\}$ in the hash table. Otherwise, $\mathcal{A}$ queries $i$ to the H **-queries** phase to get $\{i, v_i, h_i\}$.
  2. If $j$ already appears on the hash table, $\mathcal{A}$ looks up $\{j, v_j, h_j\}$ in the hash table. Otherwise, $\mathcal{A}$ queries $j$ to the H **-queries** phase to get $\{j, v_j, h_j\}$.
  3. $\mathcal{A}$ computes $\sigma_{i,j} = v_i - v_j$ .
  4. $\mathcal{A}$ sends $\sigma_{i,j}$ to $\mathcal{F}$ .
     i. Note that the number of signing queries is $Q = \text{poly}(n)$ .
- **Output**: Assume that $\mathcal{F}$ output a forged signature $\sigma_{i^*,j^*}$ on the edge $(i^*, j^*)$ . $\mathcal{A}$ proceeds as follows:
  1. $\mathcal{A}$ takes $\{i^*, v_{i^*}, h_{i^*}\}$ and $\{j^*, v_{j^*}, h_{j^*}\}$ from the hash table.
  2. $\mathcal{A}$ computes $z = \sigma_{i^*,j^*} - v_{i^*} + v_{j^*}$ .
     i. Note that the probability of $\sigma_{i^*,j^*} = v_{i^*} - v_{j^*}$ is negligible in $n$ by **Lemma 2.12**.
     ii. The Euclidean norm of $z$ is $\| z \| \leq s \cdot \sqrt{4m} = \beta$.
  3. $\mathcal{A}$ outputs $z$ as a solution to the $\text{SIS}_{q,m,\beta}$ problem.

The advantage $\text{Adv}^{\text{TU}}_{\text{TS}_1,\mathcal{F}}(n)$ of $\mathcal{F}$ in the game $\text{Game}^{\text{TU}}_{\text{TS}_1,\mathcal{F}}(n)$ is computed as follows:

$$\text{Adv}^{\text{SIS}}_{\mathcal{A}} \geq \text{Adv}^{\text{TU}}_{\text{TS}_1,\mathcal{F}}. \tag{10}$$

□

## 4. Our Construction for Undirected Graphs in the Standard Model

We construct a transitive signature scheme for undirected graphs in the standard model. Our scheme involves the following parameters:

- A security parameter is $n$ .
- The dimension of signatures is $m = \overline{m} + nl$ , where $\overline{m} = O(nl)$ and $l = O(\log n)$ .
- $q = \text{poly}(n)$ is an odd prime.
- A Gaussian parameter is $s = O(n^c \sqrt{\log n}) \cdot \omega(\sqrt{\log n})$ , where $c$ is constant.
- The number of nodes is $\text{k} = O(n / \log n)$ .

We construct our scheme $\text{TS}_2 = \{\text{TS}_2.\text{Gen}, \text{TS}_2.\text{Sign}, \text{TS}_2.\text{Vrfy}, \text{TS}_2.\text{Comp}\}$ as follows:

- $\text{TS}_2.\text{Gen}(1^n)$ : On input the security parameter $1^n$ :
  1. Compute $(A, T)$ using the GenTrap algorithm, where $A \in \mathbb{Z}^{n \times m}_{2q}$ and

$T \leftarrow \mathcal{D}_{\mathbb{Z},\omega(\sqrt{\log n})}^{\overline{m}\times nl}$.

2. Choose a hash function $\mathrm{H}(\cdot,\cdot):\{0,1\}^* \times \{0,1\}^m \to \{0,1\}^n$.
3. Output a public key $pk = (A, \mathrm{H}(\cdot,\cdot))$ and a secret key $sk = T$.

- $\mathrm{TS}_2.\mathrm{Sign}(sk,(i,j))$: On input the secret key $sk = T$ and the edge $(i,j)$:
  1. If state $St(i)$ is empty, choose $r_i \leftarrow \{0,1\}^m$, compute $h_i = \mathrm{H}(i, r_i) \in \{0,1\}^n$, sample $v_i \leftarrow \mathcal{D}_{\Lambda_{2q}^{q\cdot h_i}(A),s}$ using the Gaussian pre-image sampling algorithm $\mathrm{SampleD}$ in the Theorem 2.8, and set $St(i) = (v_i, r_i)$.
  2. If state $St(j)$ is empty, choose $r_j \leftarrow \{0,1\}^m$, compute $h_j = \mathrm{H}(j, r_j) \in \{0,1\}^n$, sample $v_j \leftarrow \mathcal{D}_{\Lambda_{2q}^{q\cdot h_j}(A),s}$ using the Gaussian pre-image sampling algorithm $\mathrm{SampleD}$ in the Theorem 2.8, and set $St(j) = (v_j, r_j)$.
  3. Compute $v_{i,j} = v_i - v_j$ with states $St(i) = (v_i, r_i)$ and $St(j) = (v_j, r_j)$.
  4. Output a signature $\sigma_{i,j} = (v_{i,j}, r_i, r_j)$.
- $\mathrm{TS}_2.\mathrm{Vrfy}(pk,(i,j),\sigma_{i,j})$: On input the public key $pk = (A, \mathrm{H}(\cdot,\cdot))$, the edge $(i,j)$, and the signature $\sigma_{i,j} = (v_{i,j}, r_i, r_j)$:
  1. Compute $h_i = \mathrm{H}(i, r_i) \in \{0,1\}^n$ and $h_j = \mathrm{H}(j, r_j) \in \{0,1\}^n$.
  2. Output a bit 1 if $\| v_{i,j} \| \le 1.1 \cdot s \cdot \sqrt{m/\pi}$ and $A \cdot v_{i,j} = q \cdot h_i - q \cdot h_j \pmod{2q}$, and output a bit $0$ otherwise.
- $\mathrm{TS}_2.\mathrm{Comp}(pk,(i,j,k),\sigma_{i,j},\sigma_{j,k})$: On input the public key $pk = (A, \mathrm{H}(\cdot,\cdot))$, the signature $\sigma_{i,j} = (v_{i,j}, r_i, r_j)$ on the edge $(i,j)$, the signature $\sigma_{j,k} = (v_{j,k}, r_j, r_k)$ on the edge $(j,k)$:
  1. Compute $v_{i,k} = v_{i,j} + v_{j,k}$.
  2. Output a signature $\sigma_{i,k} = (v_{i,k}, r_i, r_k)$.

### 4.1 Correctness

We show that our scheme $\mathrm{TS}_2$ is correct.

**Theorem 4.1**. Our scheme $\mathrm{TS}_2$ is correct.

*Proof of Theorem 4.1*. The $\mathrm{TS}_2.\mathrm{Sign}(sk,(i,j))$ algorithm can sample $v_i$ and $v_j$ such that $\| v_i \| \le 1.1 \cdot s \cdot \sqrt{m/2\pi}$, $\| v_j \| \le 1.1 \cdot s \cdot \sqrt{m/2\pi}$, $A \cdot v_i = q \cdot h_i \pmod{2q}$, and $A \cdot v_j = q \cdot h_j \pmod{2q}$. That is, $A \cdot v_{i,j} = A \cdot (v_i - v_j) = q \cdot h_i - q \cdot h_j \pmod{2q}$ and $\| v_{i,j} \| = \| v_i - v_j \| \le 1.1 \cdot s \cdot \sqrt{m/\pi}$.

The $\mathrm{TS}_2.\mathrm{Comp}(pk,(i,j,k),\sigma_{i,j},\sigma_{j,k})$ algorithm can compute $v_{i,j}+v_{j,k}=(v_i-v_j)+(v_j-v_k)=v_i-v_k$ such that $\|v_i\|\le 1.1\cdot s\cdot\sqrt{m/2\pi}$, $\|v_k\|\le 1.1\cdot s\cdot\sqrt{m/2\pi}$, $A\cdot v_i=q\cdot h_i \pmod{2q}$, and $A\cdot v_k=q\cdot h_k \pmod{2q}$. That is, $A\cdot v_{i,k}=A\cdot(v_i-v_k)=q\cdot h_i-q\cdot h_k \pmod{2q}$ and $\|v_{i,k}\|=\|v_i-v_k\|\le 1.1\cdot s\cdot\sqrt{m/\pi}$.

Therefore, our scheme $\mathrm{TS}_2$ is correct. □

### 4.2 Transitivity

We show that our scheme $\mathrm{TS}_2$ is transitive for undirected graphs.

**Theorem 4.2**. Our scheme $\mathrm{TS}_2$ is transitive for undirected graphs.

*Proof of Theorem 4.2*. The $\mathrm{TS}_2.\mathrm{Comp}(pk,(i,j,k),\sigma_{i,j},\sigma_{j,k})$ algorithm computes as follows:

$$v_{i,k}=v_{i,j}+v_{j,k}=v_i-v_j+v_j-v_k=v_i-v_k. \tag{11}$$

A combined signature $\sigma_{i,k}$ on $(i,k)$ generated with the $\mathrm{TS}_2.\mathrm{Comp}(pk,(i,j,k),\sigma_{i,j},\sigma_{j,k})$ is indistinguishable from $\sigma'_{i,k}$ on the edge $(i,k)$ generated with the $\mathrm{TS}_2.\mathrm{Sign}(sk,(i,k))$.

$\sigma_{i,j}=(v_{i,j},r_i,r_j)$ can be easily made from $\sigma_{j,i}=(v_{j,i},r_j,r_i)$ as follows:

$$v_{i,j}=-v_{j,i}=-(v_j-v_i)=v_i-v_j. \tag{12}$$

Therefore, our scheme $\mathrm{TS}_2$ is transitive for undirected graphs. □

### 4.3 Transitive Unforgeability

We show that our scheme $\mathrm{TS}_2$ is transitively unforgeable under chosen-edge attacks in the standard model.

**Theorem 4.3**. Our scheme $\mathrm{TS}_2$ is transitively unforgeable under chosen-edge attacks in the standard model if the $\mathrm{k}\text{-}\mathrm{SIS}_{q,m,\beta,s}$ problem for $\beta=1.1\cdot s\cdot\sqrt{m/\pi}$ is hard.

*Proof of Theorem 4.3*. We can construct an algorithm $\mathcal{A}$ attacking the $\mathrm{k}\text{-}\mathrm{SIS}_{q,m,\beta,s}$ problem for $\beta=1.1\cdot s\cdot\sqrt{m/\pi}$ if there exists a forger $\mathcal{F}$ mounting transitive forgery attacks on $\mathrm{TS}_2$ as follows:

- **Setup**: On input an instance $(B,v_1,\cdots,v_{\mathrm{k}})$ of the $\mathrm{k}\text{-}\mathrm{SIS}_{q,m,\beta,s}$ problem, where $B\in\mathbb{Z}_q^{n\times m}$ and $v_1,\cdots,v_{\mathrm{k}}\leftarrow\mathcal{D}_{\Lambda_q^{\perp}(B),s}$:

1. $\mathcal{A}$ chooses a chameleon hash function $\mathrm{H}(\cdot,\cdot):\{0,1\}^* \times \{0,1\}^m \to \{0,1\}^n$.
2. $\mathcal{A}$ chooses $h_1,\cdots,h_\mathrm{k} \leftarrow \{0,1\}^n$.
3. $\mathcal{A}$ lets $V = [v_1 | \cdots | v_\mathrm{k}] \in \mathbb{Z}^{m\times \mathrm{k}}$.
4. $\mathcal{A}$ lets $H = [h_1 | \cdots | h_\mathrm{k}] \in \{0,1\}^{n\times \mathrm{k}}$.
5. $\mathcal{A}$ chooses $A_2 \leftarrow \{0,1\}^{n\times m}$ such that $A_2 \cdot V = H \pmod 2$.
   i. Note that $V \pmod 2$ is uniformly random by **Lemma 2.13**.
   ii. Note that the rank of $V \in \mathbb{Z}_2^{m\times \mathrm{k}}$ is k with all but negligible probability by **Lemma 2.14**.
6. $\mathcal{A}$ computes $A \in \mathbb{Z}_{2q}^{n\times m}$ such that $A = A_2 \pmod 2$ and $A = B \pmod q$ using the Chinese remainder theorem.
   i. Note that $A \pmod{2q}$ is uniformly random by **Lemma 2.13**.
7. $\mathcal{A}$ sends $pk = (A, \mathrm{H}(\cdot,\cdot))$ to $\mathcal{F}$.

- **Signing queries**: On input the edge $(i, j)$:
1. $\mathcal{A}$ samples $r_i, r_j \leftarrow \{0,1\}^m$ such that $h_i = \mathrm{H}(i, r_i)$ and $h_j = \mathrm{H}(j, r_j)$.
2. $\mathcal{A}$ computes $v_{i,j} = v_i - v_j$.
3. $\mathcal{A}$ sends $\sigma_{i,j} = (v_{i,j}, r_i, r_j)$ to $\mathcal{F}$.
   i. Note that the number of signing queries is $\mathrm{poly}(n)$.

- **Output**: Assume that $\mathcal{F}$ output a forged signature $\sigma_{i^*,j^*} = (v_{i^*,j^*}, r_{i^*}, r_{j^*})$ on the edge $(i^*, j^*)$. $\mathcal{A}$ proceeds as follows:
1. $\mathcal{A}$ outputs $v_{i^*,j^*}$ as a solution to the $\mathrm{k}\text{-}\mathrm{SIS}_{q,m,\beta,s}$ problem.
   i. Note that the following equation is correct:

$$A \cdot v_{i^*,j^*} = q \cdot \mathrm{H}(i^*, r_{i^*}) - q \cdot \mathrm{H}(j^*, r_{j^*}) \pmod{2q} = B \cdot v_{i^*,j^*} \pmod q = 0 \pmod q. \quad (13)$$

   ii. By **Lemma 2.15**, $v_{i^*,j^*}$ is not in $\mathbb{Q}$-span$(\{v_1,\cdots,v_\mathrm{k}\})$ and the Euclidean norm of $v_{i^*,j^*}$ is as follows:

$$\| v_{i^*,j^*} \| \le 1.1 \cdot s \cdot \sqrt{m/\pi} = \beta. \quad (14)$$

The advantage $\mathrm{Adv}^{\mathrm{TU}}_{\mathrm{TS}_2,\mathcal{F}}(n)$ of $\mathcal{F}$ in the game $\mathrm{Game}^{\mathrm{TU}}_{\mathrm{TS}_2,\mathcal{F}}(n)$ is computed as follows:

$$\mathrm{Adv}^{\mathrm{k-SIS}}_{\mathcal{A}} \ge \mathrm{Adv}^{\mathrm{TU}}_{\mathrm{TS}_2,\mathcal{F}}. \quad (15)$$

## 5. Conclusion

We have proposed the first transitive signature schemes for undirected graphs from lattices. The first scheme is provably secure in the random oracle model and the second scheme is provably secure in the standard model. The question of constructing a transitive signature scheme for *directed graphs* still remains open.

## References


[1] Silvio Micali and Ronald L. Rivest, "Transitive signature schemes," in *Proc. of The Cryptographers' Track, RSA Conference - CT-RSA 2002*, LNCS 2271, pp. 236-243, February 18-22, 2002. Article (CrossRef Link)

[2] Susan Rae Hohenberger, "The cryptographic impact of groups with infeasible inversion," Master's Thesis, Massachusetts Institute of Technology, *Department of Electrical Engineering and Computer Science*, 2003.

[3] Hidenori Kuwakado and Hatsukazu Tanaka, "Transitive signature scheme for directed trees," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E86-A, no. 5, pp. 1120-1126, May 1, 2003.

[4] Xun Yi, Chik-How Tan, and Eiji Okamoto, "Security of Kuwakado-Tanaka transitive signature scheme for directed trees," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E87-A, no. 4, pp. 955-957, April 1, 2004.

[5] Xun Yi, "Directed transitive signature scheme," in *Proc. of The Cryptographers' Track, RSA Conference - CT-RSA 2007*, LNCS 4377, pp. 129-144, February 5-9, 2007. Article (CrossRef Link)

[6] Gregory Neven, "A simple transitive signature scheme for directed trees," *Theoretical Computer Science*, vol. 396, no. 1-3, pp. 277-282, May 10, 2008. Article (CrossRef Link)

[7] Philippe Camacho and Alejandro Hevia, "Short transitive signatures for directed trees," in *Proc. of The Cryptographers' Track, RSA Conference - CT-RSA 2012*, LNCS 7178, pp. 35-50, February 27-March 2, 2012. Article (CrossRef Link)

[8] Siamak Fayyaz Shahandashti, Mahmoud Salmasizadeh, and Javad Mohajeri, "A Provably Secure Short Transitive Signature Scheme from Bilinear Group Pairs," in *Proc. of 4th International Conference on Security in Communication Networks - SCN 2004*, LNCS 3352, pp. 60-76, September 8-10, 2004. Article (CrossRef Link)

[9] Mihir Bellare and Gregory Neven, "Transitive signatures based on factoring and RSA," *Advances in Cryptology - Asiacrypt 2002*, LNCS 2501, pp. 397-414, December 1-5, 2002. Article (CrossRef Link)

[10] Mihir Bellare and Gregory Neven, "Transitive signatures: new schemes and proofs," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 2133-2151, May 31, 2005. Article (CrossRef Link)

[11] Peter W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484-1509, October, 1997. Article (CrossRef Link)

[12] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. of 40th Annual ACM Symposium on Theory of Computing - STOC 2008*, pp. 197-206, May 17-20, 2008. Article (CrossRef Link)

[13] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert, "Bonsai trees, or how to delegate a lattice basis," *Advances in Cryptology - Eurocrypt 2010*, LNCS 6110, pp. 523-552, May 30-June 3, 2010. Article (CrossRef Link)

[14] Xavier Boyen, "Lattice mixing and vanishing trapdoors: a framework for fully secure short signatures and more," in *Proc. of 13th International Conference on Practice and Theory in Public Key Cryptography - PKC 2010*, LNCS 6056, pp. 499-517, May 26-28, 2010. Article (CrossRef Link)

[15] Markus Ruckert, "Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles," in *Proc. of Third International Workshop on Post-quantum Cryptography - PQCrypto 2010*, LNCS 6061, pp. 182-200, May 25-28, 2010. Article (CrossRef Link)

[16] Daniele Micciancio and Chris Peikert, "Trapdoors for lattices: simpler, tighter, faster, smaller," *Advances in Cryptology - Eurocrypt 2012*, LNCS 7237, pp. 700-718, April 15-19, 2012. Article (CrossRef Link)

[17] Geontae Noh and Ik Rae Jeong, "Scalable Hierarchical Identity-based Signature Scheme from Lattices," *KSII Transactions on Internet and Information Systems*, vol. 7, no. 12, pp. 3261-3273, December 27, 2013. Article (CrossRef Link)
[18] S. Dov Gordon, Jonathan Katz, and Vinod Vaikuntanathan, "A group signature scheme from lattice assumptions," in *Advances in Cryptology - Asiacrypt 2010*, LNCS 6477, pp. 395-412, December 5-9, 2010. Article (CrossRef Link)
[19] Jin Wang and Bo Sun, "Ring signature schemes from lattice basis delegation," in *Proc. of 13th International Conference on Information and Communications Security - ICICS 2011*, LNCS 7043, pp. 15-28, Nobember 23-26, 2011. Article (CrossRef Link)
[20] Geontae Noh, Ji Young Chun, and Ik Rae Jeong, "Strongly Unforgeable Ring Signature Scheme from Lattices in the Standard Model," *Journal of Applied Mathematics*, vol. 2014, pp. 1-12, May 5, 2014. Article (CrossRef Link)
[21] Geontae Noh and Ik Rae Jeong, "Strong designated verifier signature scheme from lattices in the standard model," *Security and Communication Networks*, vol. 9, no. 18, pp. 6202-6214, March 30, 2017. Article (CrossRef Link)
[22] Dan Boneh and David Mandell Freeman, "Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures," in *Proc. of 14th International Conference on Practice and Theory in Public Key Cryptography - PKC 2011*, LNCS 6571, pp. 1-16, March 6-9, 2011. Article (CrossRef Link)
[23] Dan Boneh and David Mandell Freeman, "Homomorphic signatures for polynomial functions," in *Advances in Cryptology - Eurocrypt 2011*, LNCS 6632, pp. 149-168, May 15-19, 2011. Article (CrossRef Link)
[24] Shweta Agrawal, Dan Boneh, and Xavier Boyen, "Efficient lattice (H)IBE in the standard model," in *Advances in Cryptology - Eurocrypt 2010*, LNCS 6110, pp. 553-572, May 30-June 3, 2010. Article (CrossRef Link)
[25] Shweta Agrawal, Dan Boneh, and Xavier Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE," in *Advances in Cryptology - Crypto 2010*, LNCS 6223, pp. 98-115, August 15-19, 2010. Article (CrossRef Link)
[26] Shota Yamada, "Adaptively Secure Identity-Based Encryption from Lattices with Asymptotically Shorter Public Parameters," *Advances in Cryptology - Eurocrypt 2016*, LNCS 9666, pp. 32-62, May 8-12, 2016. Article (CrossRef Link)
[27] Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan, "A simple BGN-type cryptosystem from LWE," *Advances in Cryptology - Eurocrypt 2010*, LNCS 6110, pp. 506-522, May 30-June 3, 2010. Article (CrossRef Link)
[28] Robert Johnson, David Molnar, Dawn Song, and David Wagner, "Homomorphic signature schemes," in *Proc. of The Cryptographers' Track, RSA Conference - CT-RSA 2002*, LNCS 2271, pp. 244-262, February 18-22, 2002. Article (CrossRef Link)
[29] Abhishek. Banerjee, Chris Peikert, and Alon Rosen, "Pseudorandom functions and lattices," in *Advances in Cryptology - Eurocrypt 2012*, LNCS 7237, pp. 719-737, April 15-19, 2012. Article (CrossRef Link)
[30] Daniele Micciancio and Oded Regev, "Worst-case to average-case reductions based on Gaussian measures," *SIAM Journal on Computing*, vol. 37, no. 1, pp. 267-302, April 2007. Article (CrossRef Link)
[31] San Ling, Duong Hieu Phan, Damien Stehlé, and Ron Steinfeld, "Hardness of $k$-LWE and Applications in Traitor Tracing," *Advances in Cryptology - Crypto 2014*, LNCS 8616, pp. 315-334, August 17-21, 2014. Article (CrossRef Link)

**Geontae Noh** received the B.S. degree in Industrial Systems and Information Engineering from Korea University, Seoul, Korea, in 2008. He received the M.S. degree in Information Management and Security from Korea University, Seoul, Korea, in 2010. He received the Ph.D. degree in Information Security from Korea University, Seoul, Korea, in 2014. Currently, he is a member of the faculty in the Department of Information Security, Seoul Cyber University, Seoul, Korea. His research interests include cryptographic protocols, lattice-based cryptosystem, and privacy-preserving technologies.

**Ik Rae Jeong** received the B.S. and M.S. degrees in Computer Science from Korea University, Korea, in 1998 and 2000, respectively. He received the Ph.D. degree in Information Security from Korea University in 2004. From June 2006 to Feb. 2008, he was a senior engineer at ETRI (Electronics and Telecommunications Research Institute) in Korea. Currently, he is a member of the faculty in the Graduate School of Information Security, Korea University, Seoul, Korea. His current research areas include cryptography and theoretical computer science.