Efficient Lattice-Based Blind Signatures via Gaussian One-Time Signatures

Vadim Lyubashevsky[1], Ngoc Khanh Nguyen[12], Maxime Plançon[12]

[1]IBM Research Europe, Switzerland, [2]ETH Zurich

February 28, 2022

Notations

- q a prime modulus for the blind signature ($\simeq$ 64 bits)
- q' a prime modulus for the encryption scheme ($\simeq$ 128 bits)
- d is a power of two ($= 128$)
- $\mathbb{Z}_q$ is the field of integers modulo q
- $\mathcal{R}_q$ is the cyclotomic ring $\mathbb{Z}_q[X]/(X^d + 1)$
- S_γ is the set of ring elements of infinity norm less than γ
- n, m, k, l are dimensions over $\mathcal{R}_q$

Summary

Our blind signature scheme is built upon 3 major components :

→ An encryption scheme which tolerates some computations on the ciphertext

Summary

Our blind signature scheme is built upon 3 major components :

- An encryption scheme which tolerates some computations on the ciphertext
- A one-time signature scheme

Summary

Our blind signature scheme is built upon 3 major components :

- An encryption scheme which tolerates some computations on the ciphertext
- A one-time signature scheme
- A set membership zero-knowledge proof black-box.

Summary

Our blind signature scheme is built upon 3 major components :

- An encryption scheme which tolerates some computations on the ciphertext
- A one-time signature scheme
- A set membership zero-knowledge proof black-box.

The scheme is round-optimal (2 rounds of communication) and the signature size is $\simeq$ 150 KB.

Part 1

Lattice-Based One-Time Signatures (OTS).

Lattice-Based Construction from [LM18]

Setup

- Uniformly random matrix $\mathbf{A} \leftarrow \mathcal{R}_q^{n\times m}$
- Secret key : $(\mathbf{s},\mathbf{y}) \leftarrow \{(\mathbf{s},\mathbf{y}) \in \mathcal{R}_q^m \times \mathcal{R}_q^m \;/\; \|(\mathbf{s},\mathbf{y})\|_\infty \leq b\}$
- Public key : $(\mathbf{v},\mathbf{w}) := (\mathbf{As},\mathbf{Ay})$

Lattice-Based Construction from [LM18]

Setup

- Uniformly random matrix $\mathbf{A} \leftarrow \mathcal{R}_q^{n \times m}$
- Secret key : $(\mathbf{s}, \mathbf{y}) \leftarrow \{(\mathbf{s}, \mathbf{y}) \in \mathcal{R}_q^m \times \mathcal{R}_q^m \ / \ \|(\mathbf{s}, \mathbf{y})\|_\infty \leq b\}$
- Public key : $(\mathbf{v}, \mathbf{w}) := (\mathbf{As}, \mathbf{Ay})$

Sign

Signature of a message $\mu \in \{0,1\}^d$: $\mathbf{z}(\mu) := \mu\mathbf{s} + \mathbf{y}$

Lattice-Based Construction from [LM18]

Setup

- Uniformly random matrix $\mathbf{A} \leftarrow \mathcal{R}_q^{n\times m}$
- Secret key : $(\mathbf{s}, \mathbf{y}) \leftarrow \{(\mathbf{s}, \mathbf{y}) \in \mathcal{R}_q^m \times \mathcal{R}_q^m \ / \ \|(\mathbf{s}, \mathbf{y})\|_\infty \leq b\}$
- Public key : $(\mathbf{v}, \mathbf{w}) := (\mathbf{As}, \mathbf{Ay})$

Sign

Signature of a message $\mu \in \{0,1\}^d$: $\mathbf{z}(\mu) := \mu\mathbf{s} + \mathbf{y}$

Verify

To verify a signature $\mathbf{z}$: check that $\mathbf{Az} \stackrel{?}{=} \mu\mathbf{v} + \mathbf{w}$, and $\|\mathbf{z}\| \leq \kappa b$.

Overview of the Security

Consider an adversary $\mathcal{A}$ against the unforgeability game of the OTS that sees a signature $\sigma(= \mathbf{y} + \mu\mathbf{s})$ of some message μ of his choice.

Overview of the Security

Consider an adversary $\mathcal{A}$ against the unforgeability game of the OTS that sees a signature $\sigma(= \mathbf{y} + \mu\mathbf{s})$ of some message μ of his choice. We have

- A forgery $(\mu', \mathbf{z}')$ produced by $\mathcal{A}$

Overview of the Security

Consider an adversary $\mathcal{A}$ against the unforgeability game of the OTS that sees a signature $\sigma(= \mathbf{y} + \mu\mathbf{s})$ of some message μ of his choice. We have

- A forgery $(\mu', \mathbf{z}')$ produced by $\mathcal{A}$
- A honestly generated signature $\mathbf{z} := \mu'\mathbf{s} + \mathbf{y}$ of μ'

Overview of the Security

Consider an adversary $\mathcal{A}$ against the unforgeability game of the OTS that sees a signature $\sigma(= \mathbf{y} + \mu\mathbf{s})$ of some message μ of his choice. We have

- A forgery $(\mu', \mathbf{z}')$ produced by $\mathcal{A}$
- A honestly generated signature $\mathbf{z} := \mu'\mathbf{s} + \mathbf{y}$ of μ'

Both $\mathbf{z}, \mathbf{z}'$ pass verification, hence $\mathbf{Az} = \mathbf{Az}' = \mu'\mathbf{v} + \mathbf{w}$. To conclude that $\mathbf{z} - \mathbf{z}'$ is a solution to MSIS for $\mathbf{A}$, only remains to prove that $\mathbf{z} \neq \mathbf{z}'$.

Overview of the Security

Consider an adversary $\mathcal{A}$ against the unforgeability game of the OTS that sees a signature $\sigma(= \mathbf{y} + \mu\mathbf{s})$ of some message μ of his choice. We have

- A forgery $(\mu', \mathbf{z}')$ produced by $\mathcal{A}$
- A honestly generated signature $\mathbf{z} := \mu'\mathbf{s} + \mathbf{y}$ of μ'

Both $\mathbf{z}, \mathbf{z}'$ pass verification, hence $\mathbf{Az} = \mathbf{Az}' = \mu'\mathbf{v} + \mathbf{w}$. To conclude that $\mathbf{z} - \mathbf{z}'$ is a solution to MSIS for $\mathbf{A}$, only remains to prove that $\mathbf{z} \neq \mathbf{z}'$.

The parameters of the scheme are chosen so there exists at least another pair $(\mathbf{s}^*, \mathbf{y}^*)$ such that

$$\mathbf{As}^* = \mathbf{v},\ \mathbf{Ay}^* = \mathbf{w},\ \sigma = \mathbf{y}^* + \mu\mathbf{s}^*,\ \text{and } \|(\mathbf{s}^*, \mathbf{y}^*)\|_\infty \leq b.$$

Overview of the Security

Consider an adversary $\mathcal{A}$ against the unforgeability game of the OTS that sees a signature $\sigma(= \mathbf{y} + \mu\mathbf{s})$ of some message μ of his choice. We have

- A forgery $(\mu', \mathbf{z}')$ produced by $\mathcal{A}$
- A honestly generated signature $\mathbf{z} := \mu'\mathbf{s} + \mathbf{y}$ of μ'

Both $\mathbf{z}, \mathbf{z}'$ pass verification, hence $\mathbf{Az} = \mathbf{Az}' = \mu'\mathbf{v} + \mathbf{w}$. To conclude that $\mathbf{z} - \mathbf{z}'$ is a solution to MSIS for $\mathbf{A}$, only remains to prove that $\mathbf{z} \neq \mathbf{z}'$.

The parameters of the scheme are chosen so there exists at least another pair $(\mathbf{s}^*, \mathbf{y}^*)$ such that

$$\mathbf{As}^* = \mathbf{v}, \ \mathbf{Ay}^* = \mathbf{w}, \ \sigma = \mathbf{y}^* + \mu\mathbf{s}^*, \ \text{and } \|(\mathbf{s}^*, \mathbf{y}^*)\|_\infty \leq b.$$

- From the adversary's perspective, both worlds are information-theoretically indistinguishable, therefore with probability at least $1/2$, $\mathbf{z} \neq \mathbf{z}'$.

Gaussian version of [LM18]

Setup

- Uniformly random matrix $\mathbf{A} \leftarrow \mathcal{R}_q^{n\times m}$
- Secret key : $(\mathbf{s}, \mathbf{y}) \leftarrow D_{\sigma_s}^m \times D_{\sigma_y}^m$
- Public key : $(\mathbf{v}, \mathbf{w}) := (\mathbf{As}, \mathbf{Ay})$

Sign

Signature of a message $\mu \in \{0,1\}^d$: $\mathbf{z}(\mu) := \mu\mathbf{s} + \mathbf{y}$

Verify

To verify a signature $\mathbf{z}$: check that $\mathbf{Az} \stackrel{?}{=} \mu\mathbf{v} + \mathbf{w}$,

Security of the Gaussian version

→ For the original uniform distribution, one takes n, m, b such that there exists at least two solutions to

$$\mathbf{As}^* = \mathbf{v},\ \mathbf{Ay}^* = \mathbf{w},\ \sigma = \mathbf{y}^* + \mu\mathbf{s}^*,\ \text{ and } \|(\mathbf{s}^*, \mathbf{y}^*)\|_\infty \leq b.$$

Security of the Gaussian version

- For the original uniform distribution, one takes n, m, b such that there exists at least two solutions to

$$\mathbf{A}\mathbf{s}^* = \mathbf{v},\ \mathbf{A}\mathbf{y}^* = \mathbf{w},\ \sigma = \mathbf{y}^* + \mu\mathbf{s}^*,\ \text{and } \|(\mathbf{s}^*, \mathbf{y}^*)\|_\infty \leq b.$$

- For the Gaussian version, we take n, m, σ_s, σ_y such that

$$\max_{(\mathbf{s}^*,\mathbf{y}^*)} D_{\Lambda,\sigma}(\mathbf{s}^*, \mathbf{y}^*) \leq 1/2,$$

where $\Lambda = \{(\mathbf{s}^*, \mathbf{y}^*) \in \mathcal{R}_q^m \times \mathcal{R}_q^m \ /\ \mathbf{A}\mathbf{s}^* = \mathbf{v},\ \mathbf{A}\mathbf{y}^* = \mathbf{w},\ \mathbf{z} = \mathbf{y}^* + \mu\mathbf{s}^*\}$ is a coset of a lattice and $\sigma = (\sigma_s, \ldots, \sigma_s, \sigma_y, \ldots, \sigma_y)$.

Part 2

Blind signatures.

Blind Signature Definition

Two parties : the user and the signer

Blind Signature Definition

Two parties : the user and the signer

After their interaction, the user shall obtain a signature of his message μ under the public key of the signer.

Blind Signature Definition

Two parties : the user and the signer

After their interaction, the user shall obtain a signature of his message μ under the public key of the signer.

Security notions

→ *Blindness.* The signer cannot learn anything about μ, nor during which interaction the signature σ was produced.

Blind Signature Definition

Two parties : the user and the signer

After their interaction, the user shall obtain a signature of his message μ under the public key of the signer.

Security notions

- *Blindness.* The signer cannot learn anything about μ, nor during which interaction the signature σ was produced.
- *One-More Unforgeability.* After some number ℓ of interactions with the signer, the user cannot produce $\ell + 1$ valid signatures for the public key of the signer.

Intuition of our construction

A naive not blind approach :

→ The public key is a collection of N OTS public keys

Intuition of our construction

A naive not blind approach :

- The public key is a collection of N OTS public keys
- The user sends his message to the signer

Intuition of our construction

A naive not blind approach :

- → The public key is a collection of N OTS public keys
- → The user sends his message to the signer
- → The signer sends the OTS of the message for the i-th public key

Intuition of our construction

A naive not blind approach :

- → The public key is a collection of N OTS public keys
- → The user sends his message to the signer
- → The signer sends the OTS of the message for the i-th public key
- → The blind signature is a zero-knowledge proof of knowledge of some $\mathbf{z}$ such that

$$\mathbf{A}\mathbf{z} \in \{\mu \mathbf{v}_i + \mathbf{w}_i,\ i \in [N]\}.$$

Intuition of our construction

- The public key is a collection of N OTS public keys
- The user encrypts his message, and sends the ciphertext together with a well-formedness zero-knowledge proof to the signer
- The signer homomorphically computes an encryption of the OTS of the ciphertext for the i-th public key
- The user decrypts the signer's response. The blind signature is a zero-knowledge proof of knowledge of some $\mathbf{z}$ such that

$$\mathbf{A}\mathbf{z} \in \{\mu \mathbf{v}_i + \mathbf{w}_i,\ i \in [N]\}.$$

Blind signature scheme : setup

Server setup

1. Sample a trapdoor : $\mathbf{R} \leftarrow (S_1^{n\times n})^{2\times 3}$
2. $\mathbf{A}' \leftarrow \mathcal{R}_q^{n\times 2n}$, $\mathbf{A} = [\mathbf{A}'|\mathbf{A}'\mathbf{R} - \mathbf{G}] \in \mathcal{R}_q^{n\times m}$
3. For $i \in [N]$, $(\mathbf{v}_i, \mathbf{w}_i) \leftarrow \mathcal{R}_q^m \times \mathcal{R}_q^m$

Public key : $(\mathbf{A}, (\mathbf{v}_i, \mathbf{w}_i)_{i\in[N]})$, Secret key : $\mathbf{R}$

Blind signature scheme : setup

Server setup

1. Sample a trapdoor : $\mathbf{R} \leftarrow (S_1^{n \times n})^{2 \times 3}$
2. $\mathbf{A}' \leftarrow \mathcal{R}_q^{n \times 2n}$, $\mathbf{A} = [\mathbf{A}' | \mathbf{A}'\mathbf{R} - \mathbf{G}] \in \mathcal{R}_q^{n \times m}$
3. For $i \in [N]$, $(\mathbf{v}_i, \mathbf{w}_i) \leftarrow \mathcal{R}_q^m \times \mathcal{R}_q^m$

Public key : $(\mathbf{A}, (\mathbf{v}_i, \mathbf{w}_i)_{i \in [N]})$, Secret key : $\mathbf{R}$

For each signature, the server will sample a secret key $(\mathbf{s}_i, \mathbf{y}_i)$ for the OTS public key $(\mathbf{v}_i, \mathbf{w}_i)$ using the trapdoor $\mathbf{R}$

For each signature, the user generates a key pair (pk, sk) for an encryption enc and runs the setup of a set membership proof.

Blind signature scheme : sign

Blind signature scheme : sign

1. User with message μ :
   - $(\mathbf{t}, t') = \mathrm{enc}(\mathrm{pk}, \mu)$

Blind signature scheme : sign

1. User with message μ :
   - $(\mathbf{t}, t') = \mathrm{enc}(\mathrm{pk}, \mu)$
   - Compute a proof π_{enc} of well-formedness of the ciphertext
   - Send $(\mathbf{t}, t', \pi_{\mathrm{enc}})$

Blind signature scheme : sign

1. User with message μ :
   - $(\mathbf{t}, t') = \mathrm{enc}(\mathrm{pk}, \mu)$
   - Compute a proof π_{enc} of well-formedness of the ciphertext
   - Send $(\mathbf{t}, t', \pi_{\mathrm{enc}})$
2. Signer with state $i \in [N]$:
   - Verify π_{enc}
   - $(\mathbf{s}_i, \mathbf{y}_i) \leftarrow D^m_{\sigma_s} \times D^m_{\sigma_y}$ conditionned on $(\mathbf{A}\mathbf{s}_i, \mathbf{A}\mathbf{y}_i) = (\mathbf{v}_i, \mathbf{w}_i)$

Blind signature scheme : sign

1. User with message μ :
   - $(\mathbf{t}, t') = \text{enc}(\text{pk}, \mu)$
   - Compute a proof π_{enc} of well-formedness of the ciphertext
   - Send $(\mathbf{t}, t', \pi_{\text{enc}})$
2. Signer with state $i \in [N]$:
   - Verify π_{enc}
   - $(\mathbf{s}_i, \mathbf{y}_i) \leftarrow D_{\sigma_s}^m \times D_{\sigma_y}^m$ conditionned on $(\mathbf{A}\mathbf{s}_i, \mathbf{A}\mathbf{y}_i) = (\mathbf{v}_i, \mathbf{w}_i)$
   - Compute an encryption $(\mathbf{F}, \mathbf{f}')$ of $\mathbf{z} := \mu \mathbf{s}_i + \mathbf{y}_i$
   - Update $i = i + 1$ and send $(\mathbf{F}, \mathbf{f}')$

Blind signature scheme : sign

1. User with message μ :
   - $(\mathbf{t}, t') = \mathrm{enc}(\mathrm{pk}, \mu)$
   - Compute a proof π_{enc} of well-formedness of the ciphertext
   - Send $(\mathbf{t}, t', \pi_{\mathrm{enc}})$
2. Signer with state $i \in [N]$:
   - Verify π_{enc}
   - $(\mathbf{s}_i, \mathbf{y}_i) \leftarrow D_{\sigma_s}^m \times D_{\sigma_y}^m$ conditionned on $(\mathbf{A}\mathbf{s}_i, \mathbf{A}\mathbf{y}_i) = (\mathbf{v}_i, \mathbf{w}_i)$
   - Compute an encryption $(\mathbf{F}, \mathbf{f}')$ of $\mathbf{z} := \mu \mathbf{s}_i + \mathbf{y}_i$
   - Update $i = i + 1$ and send $(\mathbf{F}, \mathbf{f}')$
3. User :
   - $\mathbf{z} = \mathrm{dec}(\mathrm{sk}, \mathbf{F}, \mathbf{f}')$

Blind signature scheme : sign

1. User with message μ :
   - $(\mathbf{t}, t') = \mathrm{enc}(\mathrm{pk}, \mu)$
   - Compute a proof π_{enc} of well-formedness of the ciphertext
   - Send $(\mathbf{t}, t', \pi_{\mathrm{enc}})$
2. Signer with state $i \in [N]$:
   - Verify π_{enc}
   - $(\mathbf{s}_i, \mathbf{y}_i) \leftarrow D^m_{\sigma_s} \times D^m_{\sigma_y}$ conditionned on $(\mathbf{A}\mathbf{s}_i, \mathbf{A}\mathbf{y}_i) = (\mathbf{v}_i, \mathbf{w}_i)$
   - Compute an encryption $(\mathbf{F}, \mathbf{f}')$ of $\mathbf{z} := \mu \mathbf{s}_i + \mathbf{y}_i$
   - Update $i = i + 1$ and send $(\mathbf{F}, \mathbf{f}')$
3. User :
   - $\mathbf{z} = \mathrm{dec}(\mathrm{sk}, \mathbf{F}, \mathbf{f}')$
   - Verify that $\exists j \in [N]$ such that $\mathbf{A}\mathbf{z} = \mu \mathbf{v}_j + \mathbf{w}_j$
   - Return the signature $\pi_{\in}(\mathbf{A}, (\mathbf{w}_j + \mu \mathbf{v}_j)_{j \in [N]}, \mathbf{z})$

Encryption scheme I

Key generation

- $\mathbf{B} \leftarrow \mathcal{R}_{q'}^{k \times l}$
- $\mathbf{x} \leftarrow S_{\gamma}^{k}$
- $\mathbf{b}^{T} = \mathbf{x}^{T}\mathbf{B} \mod q'$
- $\mathrm{pk} = (\mathbf{B}, \mathbf{b})$, $\mathrm{sk} = \mathbf{x}$

Encryption scheme II

enc(pk, μ):

- $(\mathbf{r}, \mathbf{e}, e') \leftarrow S_\gamma^l \times S_\gamma^k \times S_{gamma}$
- $\mathbf{t} = p\mathbf{B}\mathbf{r} + p\mathbf{e} \mod q'$
- $t' = p\mathbf{b}^T\mathbf{r} + pe' + \mu \mod q'$
- Return $(\mathbf{t}, t')$

dec(sk, $\mathbf{t}$, t')

- $z = t' - \mathbf{x}^T\mathbf{t} \mod q'$
- Return $z \mod p$

Blind computation on the ciphertext

The encryption scheme is a Regev-type encryption. The signer can homomorphically compute an encryption of $\mathbf{z} := \mathbf{y} + \mu\mathbf{s}$ as $\mathbf{F} = \mathbf{t}\mathbf{s}_i^T$, $\mathbf{f}' = \mathbf{y}_i + t'\mathbf{s}_i$.

Blind computation on the ciphertext

The encryption scheme is a Regev-type encryption. The signer can homomorphically compute an encryption of $\mathbf{z} := \mathbf{y} + \mu\mathbf{s}$ as $\mathbf{F} = \mathbf{t}\mathbf{s}_i^T$, $\mathbf{f}' = \mathbf{y}_i + t'\mathbf{s}_i$.

Problem : This leaks $\mathbf{s}_i$ and $\mathbf{y}_i$!

Blind computation on the ciphertext

The encryption scheme is a Regev-type encryption. The signer can homomorphically compute an encryption of $\mathbf{z} := \mathbf{y} + \mu \mathbf{s}$ as $\mathbf{F} = \mathbf{t}\mathbf{s}_i^T$, $\mathbf{f}' = \mathbf{y}_i + t'\mathbf{s}_i$.

Problem : This leaks $\mathbf{s}_i$ and $\mathbf{y}_i$!

Fix : Drowning : generate an encryption of 0 with wide enough Gaussian noises :

→ Sample $(\mathbf{Y}, \mathbf{Y}', \mathbf{y}')$ with independent Gaussian coefficients

Blind computation on the ciphertext

The encryption scheme is a Regev-type encryption. The signer can homomorphically compute an encryption of $\mathbf{z} := \mathbf{y} + \mu\mathbf{s}$ as $\mathbf{F} = \mathbf{t}\mathbf{s}_i^T$, $\mathbf{f}' = \mathbf{y}_i + t'\mathbf{s}_i$.

Problem : This leaks $\mathbf{s}_i$ and $\mathbf{y}_i$!

Fix : Drowning : generate an encryption of 0 with wide enough Gaussian noises :

- Sample $(\mathbf{Y}, \mathbf{Y}', \mathbf{y}')$ with independent Gaussian coefficients
- Compute the masks $\mathbf{M} = p\mathbf{B}\mathbf{Y} + p\mathbf{Y}' \mod q'$ for $\mathbf{t}$
- $\mathbf{m}' = p\mathbf{b}^T\mathbf{Y} + p\mathbf{y}' + \mu \mod q'$ for t'

Blind computation on the ciphertext

The encryption scheme is a Regev-type encryption. The signer can homomorphically compute an encryption of $\mathbf{z} := \mathbf{y} + \mu\mathbf{s}$ as $\mathbf{F} = \mathbf{t}\mathbf{s}_i^T$, $\mathbf{f}' = \mathbf{y}_i + t'\mathbf{s}_i$.

Problem : This leaks $\mathbf{s}_i$ and $\mathbf{y}_i$!

Fix : Drowning : generate an encryption of 0 with wide enough Gaussian noises :

- Sample $(\mathbf{Y}, \mathbf{Y}', \mathbf{y}')$ with independent Gaussian coefficients
- Compute the masks $\mathbf{M} = p\mathbf{B}\mathbf{Y} + p\mathbf{Y}' \mod q'$ for $\mathbf{t}$
- $\mathbf{m}' = p\mathbf{b}^T\mathbf{Y} + p\mathbf{y}' + \mu \mod q'$ for t'
- Set $\mathbf{F} = \mathbf{t}\mathbf{s}_i^T + \mathbf{M}$, $\mathbf{f}' = \mathbf{y}_i + t'\mathbf{s}_i + \mathbf{m}'$

Parameters

Parameter	Definition	Instantiation
N	maximum number of signing queries	2^{18}
d	dimension of the ring $\mathcal{R}$	128
q	modulus for the blind signature	$\approx 2^{64}$
q'	modulus for the encryption	$\approx 2^{128}$
α	height of the matrix $\mathbf{A} = [\mathbf{A}'\mid\mathbf{A}'\mathbf{R} - \mathbf{G}]$	21
σ_y	standard deviation for sampling $\mathbf{y}$	$\approx 2^{30}$
σ_s	standard deviation for sampling $\mathbf{s}$	$\approx 2^{30}$
n	height of the encryption public key matrix $\mathbf{B}$	80
m	width of the encryption public key matrix $\mathbf{B}$	40
γ	maximum coefficient of the $\mathbf{x}, \mathbf{r}$ and errors $\mathbf{e}, e'$	4
p	additional prime number, less than q', used for encryption	$\approx 2^{43}$
σ'	standard deviation used to sample maskings $\mathbf{Y}, \mathbf{Y}'$ and $\mathbf{y}''$	$\approx 2^{26}$

Fig. 3. Definition and concrete numbers for parameters used in the blind signature construction.

Sizes :

Public key : 1.3 MB, Secret key : 75 KB, Signature 150 KB, Communication 16 MB

Bibliography I

Vadim Lyubashevsky and Daniele Micciancio.
Asymptotically efficient lattice-based digital signatures.
Journal of Cryptology, 31(3):774–797, 2018.