Jiang-shan CHEN, Yu-pu HU, Hong-mei LIANG, Wen GAO, 2021. Novel efficient identity-based signature on lattices. *Frontiers of Information Technology & Electronic Engineering*, 22(2):244-250. https://doi.org/10.1631/FITEE.1900318

Novel efficient identity-based signature on lattices

Key words: Identity-based signature; Lattice; Strong unforgeability; Random oracle model

Corresponding author: Jiang-shan CHEN
E-mail: JSChen@mnnu.edu.cn
ORCID: https://orcid.org/0000-0002-2469-1307

Motivation

- Lattice-based cryptography is one of the popular post-quantum cryptographies, and has attracted a lot of attention.
- Because public keys do not require authentication, the use of identity-based cryptosystems is becoming widespread. Identity-based signature (IBS) is one of the important applications.
- There is no IBS scheme on lattices without trapdoors.

Main idea

- Lyubashevsky (2009) constructed a signature scheme based on the hardness of finding the approximate shortest vector within a factor of $O(n^2)$ in the random oracle model.
- Lyubashevsky's scheme does not use Gaussian sampling or trapdoor technologies, which would take up much computing resource.
- By employing Lyubashevsky's scheme twice, we can construct an IBS scheme based on the hardness of finding the approximate shortest vector problem.

Method

1. Extract algorithm

Given params, msk, and identity $\mathrm{ID} \in \{0,1\}^*$, the calculation is as follows:

(1) Choose $\hat{\boldsymbol{r}}_{\mathrm{ID}} \xleftarrow{\$} D^m$ and compute $\tilde{Q}_{\mathrm{ID}} = h(\hat{\boldsymbol{r}}_{\mathrm{ID}})$;

(2) Calculate $\tilde{e} = H(\mathrm{ID}, \tilde{Q}_{\mathrm{ID}})$ and $\hat{\boldsymbol{s}}_{\mathrm{ID}} = \hat{\boldsymbol{s}}_0\tilde{e} + \hat{\boldsymbol{r}}_{\mathrm{ID}}$;

(3) If $\hat{\boldsymbol{s}}_{\mathrm{ID}} \notin D_z^m$, then go to step (1);

(4) Return $(\hat{\boldsymbol{s}}_{\mathrm{ID}}, \tilde{Q}_{\mathrm{ID}})$ to the user with identity ID, where $\hat{\boldsymbol{s}}_{\mathrm{ID}}$ is secret and $\tilde{Q}_{\mathrm{ID}}$ is public.

Users can verify the correctness of the secret key $\mathrm{sk}_{\mathrm{ID}} = \hat{\boldsymbol{s}}_{\mathrm{ID}}$ by checking if $\hat{\boldsymbol{s}}_{\mathrm{ID}} \in D_z^m$ and $h(\hat{\boldsymbol{s}}_{\mathrm{ID}}) = \tilde{S}\tilde{e} + \tilde{Q}_{\mathrm{ID}}$, where $\tilde{e} = H(\mathrm{ID}, \tilde{Q}_{\mathrm{ID}})$.

2. Sign algorithm

Given params, message $\mu \in \{0,1\}^*$, and signing key $\mathrm{sk}_{\mathrm{ID}}$, the calculation is as follows:

(1) Choose $\hat{\boldsymbol{y}} \xleftarrow{\$} D_s^m$ and compute $\tilde{Y} = h(\hat{\boldsymbol{y}})$;

(2) Calculate $\tilde{c} = H(\mu, \tilde{Y}, \tilde{Q}_{\mathrm{ID}})$ and $\hat{\boldsymbol{z}} = \hat{\boldsymbol{y}}\tilde{c} + \hat{\boldsymbol{s}}_{\mathrm{ID}}$;

(3) If $\hat{\boldsymbol{z}} \notin D_z^m$, then go to step (1);

(4) Output the signature $\mathrm{sig} = (\hat{\boldsymbol{z}}, \tilde{Y})$.

Major results

Table 2 Comparison of the scheme size

Scheme	Signing key size (bit)	Signature size (bit)
Xie et al. (2016)'s	$2n\log(\hat{s}\sqrt{n})$	$2n\log(12\hat{\sigma}) + n(\log\lambda + 1)$
Tian and Huang (2014)'s	$m'k\log(s\sqrt{m'})$	$m'\log(12\sigma) + \lambda(\log k + 1)$
Ours	$mn\log(2d) + n\log p$	$mn\log(2d) + n\log p$

Table 4 Comparison of the computation complexity and security

Scheme	Gaussian sampling	Trapdoor generation	Security
Xie et al. (2016)'s	Yes	Yes	EU-CMA
Tian and Huang (2014)'s	Yes	Yes	EU-CMA
Ours	No	No	SU-CMA

Our scheme is not optimal in size, but has lower computational complexity and higher security.

Conclusions

- By studying Lyubashevsky’s scheme, we can know how the IBS scheme avoids using the sampling or trapdoor technique. Thus, we have constructed a new IBS scheme based on lattices.
- Our scheme does not use the sampling or trapdoor technique. This makes our scheme more computationally efficient than prior schemes.
- We have proved that our scheme is strongly unforgeable against adaptive chosen message and identity attacks in the random oracle model.