Huifang YU, Lu BAI, 2021. Post-quantum blind signcryption scheme from lattice. *Frontiers of Information Technology & Electronic Engineering*, 22(6):891-901. https://doi.org/10.1631/FITEE.2000099

Post-quantum blind signcryption scheme from lattice

Key words: Lattice-based cryptosystem; Blind signcryption; Post-quantum computing; Learning with error assumption; Small integer solution assumption

Corresponding author: Huifang YU
E-mail: yuhuifang@xupt.edu.cn
ORCID: https://orcid.org/0000-0003-4711-3128

Motivation

1. With the development of quantum computing technology, it is imperative to study cryptographic schemes that are resistant to quantum computing.

2. As a promising candidate post-quantum cryptosystem, the lattice-based cryptosystem has attracted increasing attention in academic fields.

3. Signcryption can simultaneously complete encryption and signature operations in a logical step, and the calculation and communication cost is lower than that of the traditional signature-then-encryption method.

Main idea

1. Design a new blind signcryption function which can not only complete the blind signature and encryption functions in a polynomial step but also resist quantum computing attack.

2. Prove the security of the scheme in the standard model.

3. Verify the efficiency of the proposed scheme through efficiency analysis and parameter size analysis.

Contribution

1. A post-quantum blind signcryption scheme from lattice (PQ-LBSCS) is proposed which can simultaneously guarantee blind signature and encryption.

2. The new scheme greatly improves the computational efficiency by reducing the length of the ciphertext and public key.

Method

Blind signcryption algorithm

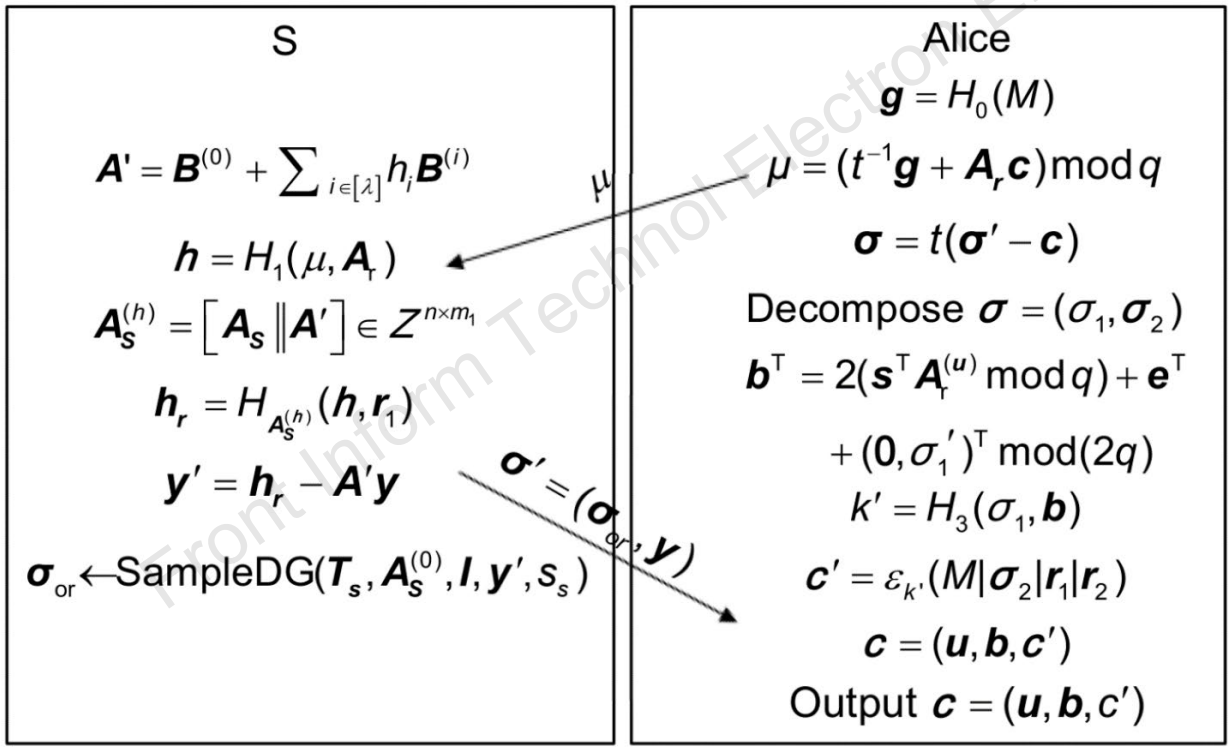

Fig. 1 Blind signcryption scenarios

Major results

1. Sizes of some parameters of the new scheme and relevant schemes

Table 2 Size of some parameters

Scheme	Length of ciphertext	Size of params	Number of hash functions	Size of the public key
SZ	$2mk^2n(\log q)^2$	$(d+3)(\log q)^2$	2	$(mk+1)\log q$
YLM	$mkn^2(\log q)^2$	$mnk\log q$	6	$k(k+1)^2m^2\lambda(\log q)^2$
YWM	$lmn^2(\log q)^2$	$m^2nl\log q$	3	$2m^2\log q$
YHW	$2m^2n(\log q)^2$	$km^3\log q$	3	$nm^2\log q$
PQ-LBSCS	$mn^2(\log q)^2$	$2ln^2\log q$	5	$2n^2\log q$

q: a large prime number; m and k: real numbers; n: a security parameter; l: number of columns of matrix $\boldsymbol{F}$; d: number of vectors $\boldsymbol{B}_i$ in Sun and Zheng (2018)

Major results (Cont'd)

2. Efficiency comparison between the new scheme and relevant schemes

Table 3 Computational efficiency of schemes

Scheme	Computational efficiency	
	Signcryption	Unsigncryption
SZ	PIS+5D_s+3C_s	4D_s+6C_s
YLM	PIS+5D_s+3C_s	7D_s+7C_s
YWM	PIS+5D_s+9C_s	6D_s+4C_s
YHW	PIS+4D_s+7C_s	3D_s+6C_s
PQ-LBSCS	PIS+4D_s+2C_s	2D_s+4C_s

C_s denotes the multiplication operation, D_s denotes the addition operation, and PIS represents the preimage sampling

Major results (Cont'd)

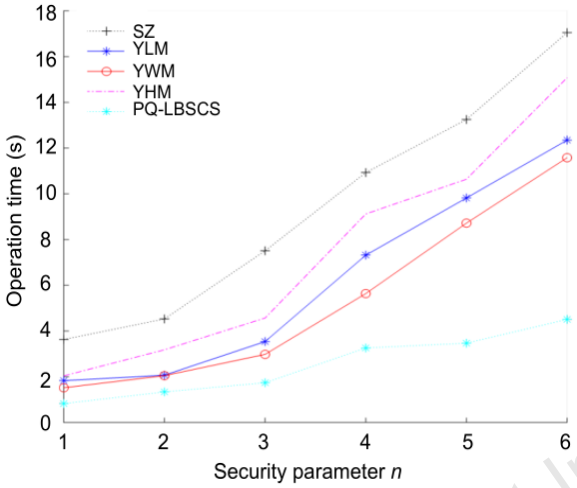

Fig. 2 Signcryption time comparison

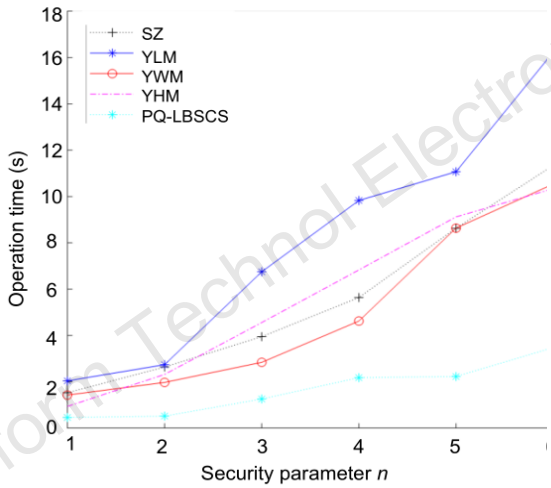

Fig. 3 Unsigncryption time comparison

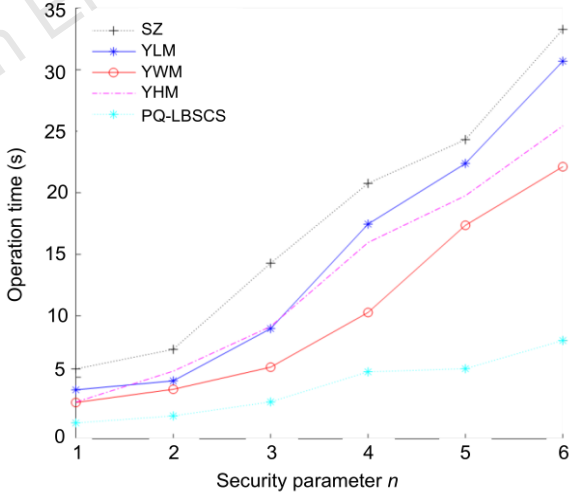

Fig. 4 Time comparison for the whole scheme

Conclusions

1. The post-quantum blind signcryption scheme from lattice (PQ-LBSCS) can ensure indistinguishability and unforgeability.

2. PQ-LBSCS can blind the message efficiently, achieve anonymous signcryption, and resist quantum computing attackers.

3. Simulation results show that the calculation complexity of PQ-LBSCS is relatively low.

Huifang YU was born in Qinghai, China. She received her Ph.D. degree from Shaanxi Normal University. Currently, she is a professor and master supervisor with Xi'an University of Posts & Telecommunications. She has completed more than 10 research projects including a 973 Basic Research Project. She is the PI of more research projects including the National Natural Science Foundation of China. She has published two books and more than 60 papers. She has been authorized five national invention patents. Her main research interests include cryptography and information security.

Lu BAI was born in Shaanxi, China. She is a master candidate at Xi'an University of Posts & Telecommunication since 2018. From 2018 to 2019, she won the provincial silver award in the "Internet+" innovation and entrepreneurship competition and the provincial first prize in the Innovation Achievement Exhibition Competition. Her main research interests include information security and cryptography.