Huifang YU, Zhewei QI, 2022. Certificateless broadcast multi-signature for network coding. *Frontiers of Information Technology & Electronic Engineering*, 23(9):1369-1377. https://doi.org/10.1631/FITEE.2200271

Certificateless broadcast multi-signature for network coding

Key words: Network coding; Certificateless multi-signature; Linear combination; Homomorphic hash function

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

Motivation

1. Network coding exists many security problems, such as pollution attacks and forgery attacks. Devising secure network coding scheme is still an open problem.
2. Aim of devising the certificateless broadcast multi-signature for network coding (NC-CLBMS) is to improve the computing efficiency and solve the security problem in wireless sensor networks, mobile wireless networks, fifth-generation wireless networks, unmanned aerial vehicle (UAV) communication networks, and Internet of Things.
3. Evaluate the scheme performance by the simulation experiments.

Main idea

1. Technology study of homomorphic hash function, broadcast multi-signature, and certificateless public key is based on the transmission model of multi-source network.
2. Algorithm model and security model are adopted to describe the formal definition of devised scheme.
3. Anti-forgery and anti-pollution of broadcast multi-signature for network coding are based on the hard assumptions. Reduction technology to hard assumptions is based on the random oracle model.

Method

1. A novel integrating method of the multi-source network coding and broadcast multi-signature is proposed.

2. Elliptic cure discrete logarithm and computational Diffie-Hellman problems are used to ensure the security of anti-pollution and anti-forgery.

Major results

1. Table 2 describes the time complexity of cryptographic operations

Table 2 Operation time of cryptographic algorithms

Notation	Meaning
C_{me}	Time of running an exponential operation: 6.85 ms
C_{mul}	Time of running a scalar multiplication: 0.75 ms
C_{mtp}	Time of running a hash operation: 19.60 ms
C_{par}	Time of running a bilinear operation: 22.73 ms
C_{ex}	Time of running a modular exponentiation operation: 34.20 ms

Major results (Cont'd)

2. Table 3 describes the signature time and verification time of several schemes.

Table 3 Comparison of computational efficiency of several schemes

Scheme	Signature time (ms)	Verification time (ms)
ZX	$C_{mtp}+(m+n)C_{mul}+3nC_{me}+6C_{ex}$	$C_{mtp}+3nC_{me}+3C_{ex}$
YG	$2C_{par}+(2n+m)C_{mul}+2nC_{me}$	$2C_{mtp}+(2n+m)C_{mul}+nC_{me}+3C_{par}$
WZZ	$C_{par}+(m+n)C_{mul}+2nC_{me}+5C_{ex}$	$C_{mtp}+3nC_{me}+C_{ex}$
YL	$3C_{par}+(3n+m)C_{mul}+nC_{me}$	$3C_{mtp}+(4n+m)C_{mul}+nC_{me}$
YW	$2C_{par}+(m+n)C_{mul}+nC_{me}$	$3C_{mtp}+3(m+n)C_{mul}+nC_{me}+2C_{par}$
NC-CLBMS	$2C_{par}+(2(n+m)+1)C_{mul}$	$2C_{mtp}+(2(n+m)+1)C_{mul}+3C_{par}$

Major results (Cont'd)

3. Simulation curves of signature time are in Fig. 2. Simulation curves of verification time are in Fig. 3. With the increase of the message vector dimension, the growth rate of NC-CLBMS is lower than those of other schemes. So, NC-CLBMS is an efficient multi-source scheme.

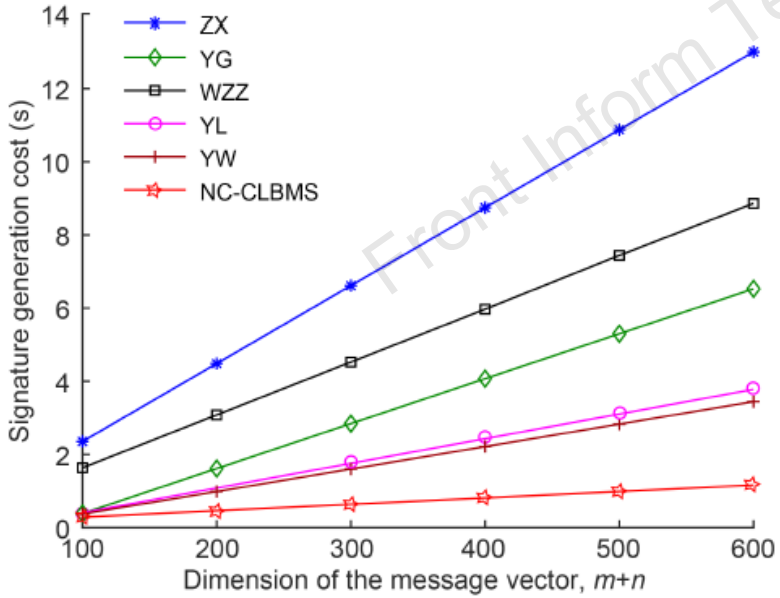

Fig. 2 Signature time of NC-CLBMS and other schemes

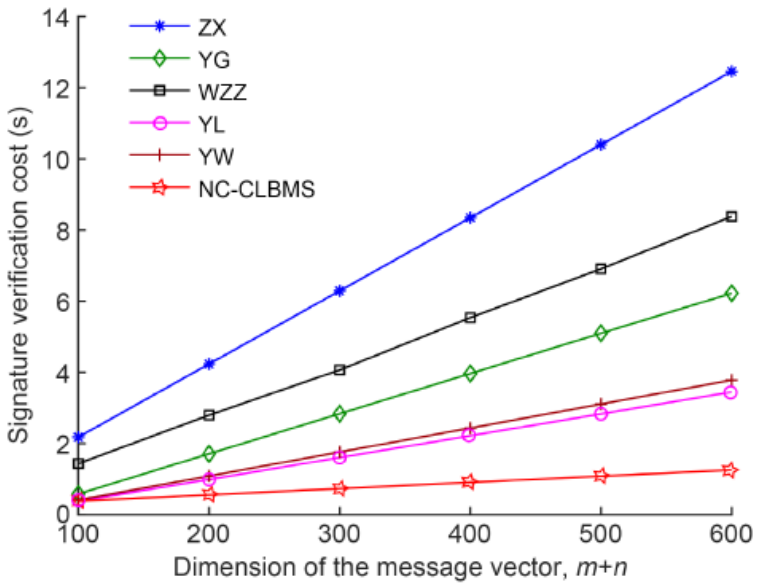

Fig. 3 Verification time of NC-CLBMS and other schemes

Conclusions

1. NC-CLBMS has the advantages of anti-pollution and anti-forgery, and its security relies on the hardness of the elliptic curve discrete logarithm and computational

Diffie-Hellman problems. The homomorphic hash function enables the node to ensure that signature and verification processes are correct.

2. NC-CLBMS avoids the certificate use and key escrow, and its signature length is fixed, and has strong robustness and low computation complexity.

3. NC-CLBMS can be applied in fifth-generation wireless networks, unmanned aerial vehicle (UAV) communication networks, wireless sensor networks, Internet of Things, and wireless mesh networks.

Huifang YU received the PhD degree in cryptography from Shaanxi Normal University. She is a professor of Xi'an University of Posts & Telecommunications. Her research interests include cryptographic theory, data security, anti-quantum cryptography, and network coding schemes. She has completed more than twenty research projects including the 973 Basic Research Project of China and National Natural Science Foundation of China. She has published three books, sixteen national invention patent, and more than eighty papers.

Zhewei QI received master degree in cyberspace security in 2022 from Xi'an University of Posts & Telecommunications. His research interests include public key cryptography and secure network coding.