Hui-fang Yu, Bo Yang. Low-computation certificateless hybrid signcryption scheme. *Frontiers of Information Technology & Electronic Engineering*, **18**(7):928-940. http://dx.doi.org/10.1631/FITEE.1601054

Low-computation certificateless hybrid signcryption scheme

Key words: Hybrid signcryption; Scalar multiplication; Certificateless cryptosystem; Provable security

Corresponding author: Huifang Yu
E-mail: yuhuifang@qhnu.edu.cn
ORCID: http://orcid.org/0000-0003-4711-3128

Motivation

- Hybrid signcryption is an important technique signcrypting bulk data using symmetric encryption.
- The computational cost of one pairing operation is higher than that of ECC scalar multiplication.
- Apply the technique of certificateless hybrid signcryption to an elliptic curve cryptosystem, and devise a cryptographic algorithm suitable for the resources-limited environment .

Main idea

- Low-computation certificateless hybrid signcryption (LC-CLHS) scheme has high computation efficiency because it does not rely on pairing operation.
- In the random oracle model, the IND-CCA2 security of the LC-CLHS scheme is based on intractability of the elliptic curve computation Diffie-Hellman problem.
- Moreover, the sUF-CMA security of the LC-CLHS scheme is based on the hardness of the elliptic curve discrete logarithm problem.

Method

1. Using elliptic curve computation Diffie-Hellman (ECCDH) and elliptic curve discrete logarithm (ECDL) assumption.
2. Using random oracle model as the security model
3. Combine the techniques of elliptic curve cryptosystem with certificateless hybrid signcryption.
4. Using the method of reduction to prove the IND-CCA2 and sUF-CMA security.

Major Results

- **Efficiency and security comparison**

The computational cost of one pairing operation is considerably higher than that of an ECC scalar multiplication operation. In the light of the comparison in Table 1, it is easy to see that the new scheme (LC-CLHS) with no pairing operations is more efficient than the existing schemes; moreover, it satisfies both IND-CCA2 and sUF-CMA security. In brief, the LC-CLHS scheme is superior to the existing schemes in efficiency and security.

Table 1 Comparison of efficiency and security in different schemes

Scheme	Efficiency		Security	
	Mul	Pair	Con	Unf
Li *et al*. (2013)	5	1(+6)	Yes	Yes
Yu and Yang (2015b)	3	1(+7)	Yes	Yes
Sun and Li (2011)	2	2(+0)	Yes	No
New scheme	9	0(+0)	Yes	Yes

Mul: number of scalar multiplication operations in additive groups; Pair: number of bilinear pairing operations in multiplication groups; Con: confidentiality (IND-CCA2 security); Unf: unforgeability (sUF-CMA security). $x(+y)$ indicates x times pairing computations and y times pairing pre-computations

Conclusions

- The LC-CLHS scheme is proven to has the IND-CCA2 and sUF-CMA security.
- The computational efficiency of the LC-CLHS scheme is superior to the existing schemes.
- The LC-CLHS scheme can realize secure, authentic and efficient communication of arbitrary messages in resources-limited environment.