Yan-wei ZHOU, Bo YANG, Hao CHENG, Qing-long WANG, 2018. A leakage-resilient certificateless public key encryption scheme with CCA2 security. *Frontiers of Information Technology & Electronic Engineering*, **19**(4): 481-493.
https://doi.org/10.1631/FITEE.1601849

A leakage-resilient certificateless public key encryption scheme with CCA2 security

Key words: Certificateless public-key encryption; Leakage-resilience; Provable security; CCA2 security; Decisional Diffie-Hellman

Corresponding author: Bo Yang
E-mail: byang@snnu.edu.cn

ORCID: http://orcid.org/0000-0002-7254-3579

Motivation

1. In recent years, much attention has been focused on designing provably secure cryptographic primitives in the presence of key leakage. Many constructions of leakage-resilient cryptographic primitives have been proposed.

2. For any polynomial time adversary, most existing leakage-resilient cryptographic primitives are unable to ensure that their outputs are random, and any polynomial time adversary can obtain a certain amount of leakage on the secret key from the corresponding output of a cryptographic primitive.

Main idea

1. In the leakage setting, the corresponding construction of CL-PKE scheme can maintain their claimed security even if the adversary obtains a certain amount of internal secret state leakage; in other words, the message is encrypted through random value created by a strong randomness extractor.

2. In a CCA2 secure CL-PKE scheme, all of elements of the ciphertext are random in the view of adversary; that is, the element used to verify the correctness of ciphertext is also produced by a strong randomness extractor.

Method

1. In the encryption algorithm, the message is hided by an average-case strong extractor. That is, the randomness extraction is performed by an average-case strong extractor.
2. In the encryption algorithm, the validity verification information of ciphertext is created through a special universal hash function. In other words, a special universal hash function is employed as an average-case strong extractor.

Major results

1. Our proposal can maintain CCA2 security in the leakage setting, and the length-of-bits leakage is up to $\lambda \leq \log q - l_m - \omega(\log k)$.

2. Our proposal is presented based on the prime-order group.

3. The striking advantage of our method is the key leakage ratio, which can achieve 1/2.

3. All of the elements of ciphertext will be random, and no any adversary can be leaked on the private key from the corresponding ciphertext.

Conclusions

1. To achieve better performance, we introduced a new method to construct a more practical LR-CL-PKE scheme without sacrificing CCA2 security.

2. We presented a concrete construction and proved its security based on the hardness of the classical DDH assumption. The results of security analysis show that our proposal not only resists leakage attacks, but also achieves better performance, because no any adversary can be leaked on the private key from the corresponding ciphertext.