Zero-Knowledge Protocols for Code-Based Public-Key Encryption and Their Applications

胡, 荣

https://doi.org/10.15017/1543929

出版情報：九州大学, 2015, 博士（数理学）, 課程博士
バージョン：

（様式３）

氏　　名　：　　胡荣

論 文 名　：　　Zero-Knowledge Protocols for Code-Based Public-Key Encryption and Their Applications
(符号ベース公開鍵暗号に対するゼロ知識証明とその応用)

区　　分　：　　甲

論　文　内　容　の　要　旨

Cryptography relies on Mathematics in all its aspects, beginning from the constructions relying on various mathematical theories, continuing with security evaluation of cryptographic systems, and proving their security, and finally ending in implementation.

Recently, new security threats are posed by the emerging quantum computing technology. Specifically, quantum algorithms can break some public-key encryption schemes such as RSA and Elgamal, which are widely used for protection of computer systems and networks. This issue demands us to develop a new generation of cryptographic systems, which will serve as secure alternatives to the currently used ones. Such the new systems are referred to as the post-quantum cryptography.

One promising direction in post-quantum cryptography is the systems whose security is based on hardness of mathematical problems arising in the context of coding theory. In particular, the problem of decoding random linear codes has been studied for over 30 years, and still no polynomial-time solution has been proposed, even when using quantum algorithms. In this thesis, we focus on this area, which is called the code-based cryptography.

The first code-based public-key encryption (PKE) scheme was introduced by R.J. McEliece in 1978. Since then, various code-based public-key encryption, digital signature and identification schemes were introduced, but currently, one of the main challenges is to introduce more advanced cryptographic functionalities based on coding.

In this thesis, first, we give a brief introduction about post-quantum cryptography and code-based cryptography, and then we provide the background information about the cryptographic primitives, which we will study, as well as the relevant notions and results from coding theory and cryptography.

Next, we introduce our contributions as follows. Firstly, we study zero-knowledge (ZK) identification schemes based q-ary linear codes. We show that when $q<5$, a straightforward generalization of Stern's ZK identification scheme (1993) is more efficient in terms of both communication and computation, as

compared to the ZK identification scheme by Cayrel, Véron and El Yousfi Alaoui (2010), which is specifically designed for q-ary codes.

Secondly, we introduce the first proof of plaintext knowledge (PPK) for the McEliece PKE and the Niederreiter PKE. These protocols allow the encryptor to prove the knowledge of the plaintext contained in a given ciphertext to any party, who does not hold the secret key for decryption. We also provide a performance evaluation for the proposed schemes.

As an application of the above PPK for the McEliece PKE, we present the first verifiable public-key encryption, which allows the encryptor to prove to any party that a given plaintext is contained in a given ciphertext, again without decrypting it. We also discuss why this idea cannot be applied to the case of Niederreiter PKE. We also provide a performance evaluation for our proposal.

Lastly, the first designated confirmer signatures based on coding is constructed following the framework of El Aimani (2010). This type of signature can only be verified via the interaction with the signer or the designated party called a ``confirmer''. The above proposal for verifiable PKE is applied to construct the signature verification protocol.

Finally, we provide our concluding remarks and discuss the future work.

Keywords: Code-based Cryptography; Zero-Knowledge Protocol, Identification Protocol, Proof of Plaintext Knowledge, Verifiable Encryption, Niederreiter PKE, McEliece PKE, Designated Confirmer Signature