論文の内容の要旨

論文題目： Unified Frameworks for Practical Broadcast Encryption and Public Key Encryption with High Functionalities

（和訳： 放送型暗号と高機能公開鍵暗号方式のための統合的枠組みに関する研究）

氏名 アッタラパドゥン ナッタポン

（本文） In this thesis, we study encryption schemes with various “high functionalities” including one specific focus on broadcast encryption. As for the main contributions, we propose a framework for constructing practical broadcast encryption schemes and a unified framework for public-key encryption with various functionalities.

The first focus of the thesis is on a special but important kind of encryption schemes, namely broadcast encryption. Such a scheme has many useful applications; the most important one to be mentioned is the digital right management. More precisely, broadcast encryption enables the protection of digital contents such as copyrighted DVD. Such a technology is “inevitable” nowadays as modern advancements in communication infrastructure and digital storage technologies have, on one hand, enabled pervasive digital media distribution, but on the other hand, also allowed the spread of “pirate” contents to be done easier than ever before.

There are some broadcast encryption schemes available in the literature; however, as the number of all users in the system tends to be increased, these existing solutions tend to be quite inefficient, and eventually cannot be used in the real-world application. Our focus is then to construct practical broadcast encryption schemes, which can be “scalable”, in the sense that the efficiency of scheme will not be affected by the increasing number of users. As a result of the research, we achieve this goal by constructing the first schemes whose the main two parameters, namely the ciphertext size and the private key size, are independent of the number of all users, while the computational cost is semi-scalable (namely, the cost is increasing but slowly as logarithmically). Behind this scheme, we proposed a theoretical framework that can be used to construct efficient schemes in a systematical way.

The second topic shifts the research focus from the practical point of views to more theoretical ones and looked beyond to more general encryption schemes with “high functionalities”. The motivation came from the fact that in recent years, there have been many cryptographic primitives which extend the normal public-key encryption to achieve useful functionalities such as ID-based encryption, Key-insulated

encryption, Forward-secure encryption, Certificate-less encryption, and many more. Each functionality is proved to be useful in different scenarios and applications thereof. Although being seemingly related primitives, there was no unified framework for defining or constructing them.

In this work, we proposed a unified framework called Directed Acyclic Graph Encryption (DAGE) that unifies these highly-functional encryption primitives into a unified syntax, a unified security notion, and unified generic/specific constructions. More precisely, we reduce a specification of such a primitive to its necessary and sufficient information, which is turned out to be its underlying graph: by specifying a graph, the definition and constructions will be automatically induced by the framework. We also give a primitive implication theorem which gives a simple criterion whether a primitive implies another.

In the theoretical point of view, the merits of the proposed framework are direct. It helps understanding the theoretical essences of the encryption schemes with high-functionalities from our unified characterization. This result simplifies the previous complicated researches into one piece. The result on the primitive implication theorem gives an automated verification of relations among primitives. This reduces the proof of relations which has to be performed based on complexity-theoretic approaches in the previous individual researches, which is quite complicated and can be verified only by human, to the logical-based approach, which is much simpler and can be verified automatedly by computer.

The proposed generic construction implies the possibility result for arbitrary graphs. This has merits not only in the theoretical point of view but also in the practical point of view where the protocol designer can just specify a “tailor-made” graph for the on-purposed application and the implementation of the scheme will be prompted to use. Furthermore, any esoteric scheme featured with many combined functionalities can be directly implemented; for example, a forward-secure certificate-less public-key encryption with keyword-searchability. This is also something that previous works cannot achieve, particularly since there was no unified framework to cope with.

For the third main topic, we focus on the combination of the above-mentioned two previous results: public-key broadcast encryption schemes that are simultaneously practical and feature high functionalities. To be able to attain such practical broadcast schemes, it is unavoidable to focus on more specific functionalities (not generic as in the second topic above). We focused on some most useful functionalities, namely forward-security and keyword-searchability. Forward-security enables the private-key updating and guarantees the security of the previously-encrypted ciphertexts even when the present-time private key is exposed. We presents the most practical and scalable forward-secure broadcast encryption so far in the literature. Keyword-searchability enables the search over encrypted data. It has a killer application of encrypted file sharing systems over public database. We presented the first such scheme in the literature.