論文の内容の要旨

論文題目 Black-Box Traitor Tracing Schemes for Copyright Protection
(著作権保護のためのブラックボックス不正者追跡方式に関する研究)

氏名　松下 達之

Copyright protection plays an important role in content distribution such as pay-TV, DVD-ROM distribution, etc. Both a content supplier and users can get the benefit of appropriate copyright protection in the sense that the content supplier can offer the digital contents to users without concern about the piracy and the users can enjoy up-to-date contents with higher quality.

We consider the following content distribution system in which the contents should be available only to authorized users. The content supplier broadcasts an encrypted version of the digital contents (e.g., a movie) to subscribers (users), and only users can decrypt them with their decryption devices (decoders) in which their decryption keys are embedded. In this system, there are two kinds of piracy malicious users (traitors) might commit in order to allow the non-users to have illegal access to the contents. One is the redistribution of the decryption key, e.g., the traitors construct a pirated version of a decoder (pirate decoder) using their decryption keys and sell it at the black market. The other is the redistribution of the contents themselves. In this thesis, we focus on a countermeasure against the former piracy since, from the traitors' view, the risk of being detected in the former piracy is lower than in the latter one. In the former piracy, the leaked decryption keys can also be used to illicitly obtain any contents distributed in the system once the traitors redistribute their decryption keys, while the traitors have to redistribute each of the entire contents in the latter one, although it is also a serious problem.

As a deterrent to the piracy, traitor tracing has been studied extensively. Since a traitor tracing scheme can identify at least one of the traitors from the pirate decoder, it can discourage them from committing the piracy. There are two desirable properties to be supported in a traitor tracing scheme. One is black-box tracing and the other is public-key setting. In black-box tracing, a tracer, who performs tracing, can identify the traitor(s) without breaking open the pirate decoder, i.e., in a black-box manner. Since it is assured that the traitor(s) can be identified no matter how the pirate decoder is implemented, it is desirable to support black-box tracing. In the public-key setting, there are one or more public keys corresponding to the decryption keys of the users.

Since no secret information is needed to encrypt the contents and to execute the tracing algorithm, anyone can work as a content supplier and/or a tracer. This property is desirable as well because of the following two reasons: (i) it enhances the sender-scalability in the sense that plural content suppliers can use the same system and (ii) it provides public availability of the tracing algorithm, which can be a stronger deterrent to the piracy. We propose public-key black-box tracing schemes. All of the proposed schemes are proved to be secure under the decision Diffie-Hellman assumption, which is one of the standard intractability assumptions. Each scheme is also analyzed in terms of efficiency.

First, we propose a new type of revocation scheme for efficient public-key black-box traitor tracing. Our revocation scheme is flexible and efficient in the sense that (i) any number of subscribers can be revoked in each distribution under an assumption that the number of revoked subscribers who collude in one coalition is limited to a threshold and (ii) all of the required storage at each user, the transmission overhead, and the public-key size are independent of n, while (i) the maximum number of revoked ones cannot be changed or (ii) at least one of the three depends on n in previous schemes, where n is the total number of users. The flexibility in revocation is significant since flexible revocation can be integrated with efficient black-box tracing and this integration can be achieved without a substantial increase in the transmission overhead over the previous schemes. In this chapter, we show a concrete construction of an efficient public-key black-box traceable and revocable scheme by combining flexible revocation with a known black-box tracing algorithm which works under the same attack model as assumed in the previous schemes. Our scheme achieves that (i) the required storage at each user is constant, (ii) the transmission overhead remains efficient, especially linear only in k in case of bulk revocation and (iii) the public-key size is linear only in k, while the previous ones cannot satisfy all of these properties, where k is the maximum number of traitors in a coalition.

Secondly, we suppose stronger pirates against which the first proposed scheme cannot work. Here, we propose a public-key traitor tracing scheme in which (i) the size of a ciphertext is sublinear in n, actually of the order of the square root of n and (ii) black-box tracing is efficiently achieved against the stronger pirates. When assuming that a pirate decoder can take some self-defensive reaction (e.g., erasing all of the internal keys and shutting down) to escape from tracing if it detects tracing, it has been an open question to construct a sublinear black-box tracing scheme that can detect efficiently at least one traitor with overwhelming probability, although a tracing algorithm that works successfully against self-defensive pirate decoders itself is known.

In this chapter, we answer affirmatively this question by presenting a concrete construction of a public-key black-box tracing scheme in which the known tracing algorithm can be used while keeping the size of a ciphertext sublinear.

Finally, we improve our second scheme from the viewpoint of the ciphertext size. We propose a hierarchical key-assignment method which can be used to construct a public-key black-box tracing scheme in which (i) the size of a ciphertext can be reduced to $O(k+\log(n/k))$ without a substantial increase in the size of a secret key and (ii) black-box tracing can be performed against self-defensive pirate decoders. In this chapter, we show a concrete construction of a public-key black-box tracing scheme by using our hierarchical key assignment method. Additionally, we point out that our black-box tracing scheme can also be used as an anonymous revocation scheme in which the identity of a revoked receiver cannot be revealed to the other receivers. Moreover, we present a combined scheme in which the mechanism of flexible revocation in the first proposal is integrated into our black-box tracing scheme.