SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Secure codes with two-stage traitor tracing

Yujie Gu [*]

Keywords: secure code, traitor tracing, two-stage decoding, code rate, copyright protection

Abstract

In 1994, Chor, Fiat and Naor proposed the traitor tracing as a mathematical approach of protecting copyrighted content in broadcast encryption, which is capable of identifying the source/traitors of pirate copies in collusion attacks [2, 3].

In the literature, anti-collusion fingerprinting codes were investigated for protecting the copyright of digital data and multimedia content against collusion attacks, see [1, 6] for example. In terms of the practical applications, a fingerprinting code corresponds to a collection of fingerprints (i.e. codewords) and each fingerprint is assigned to a unique authorized user. Therefore, a fingerprinting code is expected to have as many codewords/users (accordingly, large code rate) and efficient decoding (accordingly, fast traitor tracing) algorithm as possible.

In [1], Boneh and Shaw introduced the t-frameproof codes, which could guarantee that any innocent user would not be framed by any coalition with at most t colluders in the application of digital fingerprinting. Later it was shown in [4] that, if the coalition size is no more than t, the binary t-frameproof code could also be utilized to tracing back to all t traitors in the multimedia fingerprinting applications, with the decoding complexity $O(M)$, where M is the number of users/codewords, in general.

In this paper, we propose a new class of codes, called the t-secure codes with two-stage traitor tracing. It is shown that, on the assumption that the number of traitors in the collusion does not exceed a predetermined threshold t, the binary t-secure codes with two-stage traitor tracing could identify all t traitors with the same decoding complexity $O(M)$ as the binary t-frameproof codes in the general scenario. However, by using the probabilistic method, we show that the secure codes with two-stage traitor tracing could have much larger code rate than the frameproof codes. In particular, for the case $t = 2$, it was proven in [5] that the state-of-the-art asymptotic code rate of a binary 2-frameproof code could be no less than 0.207565; while we show that the 2-secure codes with two-stage traitor tracing could have the asymptotic code rate no less than 0.45110994.

Acknowledgment

This work has been supported by Grant-in-Aid for Early-Career Scientists 21K13830 of the Japan Society for the Promotion of Science.

References

[1] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 1897-1905, 1998.

[2] B. Chor, A. Fiat, and M. Naor, "Tracing traitors," In *Advances in Crytology - CRYPTO'94* (Lecture Notes in Computer Science), vol. 839. Berlin, Germany: Springer-Verlag, 1994, pp. 480–491.

[3] B. Chor, A. Fiat, M. Naor, and B. Pinkas, "Tracing traitors," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 893–910, May 2000.

[4] M. Cheng and Y. Miao, "On anti-collusion codes and detection algorithms for multimedia fingerprinting," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4843-4851, 2011.

[5] H. Randriambololona, "$(2,1)$-Separating systems beyond the probabilistic bound," *Israel J. Math.*, vol. 195, pp. 171–186, 2013.

[6] W. Trappe, M. Wu, Z. J. Wang, and K. J. R. Liu, "Anti-collusion fingerprinting for multimedia," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 1069-1087, 2003.

[*] Department of Informatics, Kyushu University, 744 Motooka Nishi-ku, Fukuoka 819-0395, Japan (E-mail: gu@inf.kyushu-u.ac.jp)