On Perfect Traitor Tracing

Yvo Desmedt[1], Mike Burmester
Florida State University
Tallahassee, FL 32306-4530
email: {desmedt,burmester}@cs.fsu.edu

Kaoru Kurosawa
Ibaraki University
Nakanarusawa, Hitachi, Ibaraki, Japan
e-mail: kurosawa@cis.ibaraki.ac.jp

Abstract — **We analyze the perfect security aspects of traitor tracing and show that perfect fairness (an innocent party is *never* accused) is impossible, except if the pirate key allows full decryptability or if nobody is ever accused. Similarly, perfect accusability (at least one traitor is *always* correctly accused) is impossible, except if the pirate key allows full decryptability or some innocent people will always be among the accused. We also show possibility results.**

I. Introduction

In many broadcast systems which distribute messages to authorized users a data supplier T gives each authorized user i a personal decryption key e_i. However, some malicious authorized users (traitors) might create a pirate key e_p and give it to a pirate. Then the pirate can obtain messages for free.

A (k, n)-traceability scheme is a scheme for which at least one traitor is detected from a pirate key e_p, if there are at most k traitors among n authorized users. Several (k, n) traceability schemes have been proposed so far [2, 4, 3, 1]. These schemes, however, guarantee traceability with negligible error probability *only* when the pirate can decrypt ciphertexts *perfectly* (no errors).

II. Broadcast Encryption Schemes

Definition II.1 A *Broadcast Encryption Scheme* (BES) consists of three algorithms: a *Key Generation algorithm* G, an *Encryption algorithm* E and a *Decryption algorithm* D such that:

1. G on input 1^l outputs: $(h, s_1, s_2, \ldots, s_n)$, where s_i is the key of user i and h the key of the data supplier,
2. $D_{(i,s_i)}(E_h(m)) = m$ for any message m,
3. $\Pr[M = m \mid C = c] = \Pr[M = m]$ for any ciphertext c and any message m.

III. Traceability schemes

A *Traceability scheme* is a Broadcast Encryption Scheme (G, E, D) with three additional algorithms: a *Traitor algorithm* T, a *Pirate decoder* P and a *Tracing algorithm* F, such that:

- T selects a set **Traitors** of at most k traitors from the set of receivers $\{1, 2, \ldots, n\}$. When **Traitors** $= \{i_1, i_2, \ldots, i_{k'}\}$, where $i_j < i_{j+1}$, T obtains from the set **Traitors** the keys $s_T = (s_{i_1}, s_{i_2}, \ldots, s_{i_{k'}})$. After some computation, T outputs a pirate key s_P.
- P takes as input the pirate key s_P and a ciphertext c. P outputs a message $\widetilde{m}$.
- F takes as input the keys $(h, s_1, s_2, \ldots, s_n)$ output by G and the pirate key s_P output by T. F outputs a set of receivers **Accused** $\subseteq \{1, 2, \ldots, n\}$ who are accused as traitors.

Definition III.1 A BES is a $(k, n; \delta, \Delta_1, \Delta_2)$ *Traceable Broadcast Encryption Scheme* (TBES) if, for every traitor algorithm T and every pirate decoder P there is a Tracing algorithm F such that, either

- *Non-decryptability*: $\Pr[M = \widetilde{M}] < \delta$, or
- *Traceability*: $\Pr[\textbf{Accused} \cap \textbf{Traitors} = \emptyset] \leq \Delta_1$, and $\Pr[\textbf{Accused} \setminus \textbf{Traitors} \neq \emptyset] \leq \Delta_2$.

IV. Our Results

Theorem IV.1 For any $\delta < 1$ and $n > 2$, if either

1. $\Delta_1 = 0$ with $0 \leq \Delta_2 < 1$, or
2. $\Delta_2 = 0$ with $0 \leq \Delta_1 < 1$,

there do not exist any $(k, n; \delta, \Delta_1, \Delta_2)$-TBESs.

Theorem IV.2 If there exists a BES which is both, a $(k, n; \delta, \Delta_{11}, \Delta_{21})$-TBES and a $(k, n; \delta, \Delta_{12}, \Delta_{22})$-TBES, then there exists a $(k, n; \delta, \beta\Delta_{11} + (1 - \beta)\Delta_{12}, \beta\Delta_{21} + (1 - \beta)\Delta_{22})$-TBES for every $0 \leq \beta \leq 1$.

V. Open problem

Further work is required to decide whether there exists a $(k, n; \delta, 1/2 - \epsilon, 1/2 - \epsilon)$-TBES for some constant $0 < \epsilon < 1/2$. Or, whether there does not exist a $(k, n; \delta, 2^{-l}, 2^{-l})$-TBES ($l$ is the security parameter).

[1]Part of this work was supported by NSF CCR-0096247.

References

[1] D. Boneh and M. Franklin. An efficient public key traitor tracing scheme. In M. Wiener, editor, *Crypto '99*, LNCS 1666, pp. 338–353. Springer-Verlag, 1999.

[2] B. Chor, A. Fiat, and M. Naor. Tracing traitors. *Crypto '94*, LNCS 839, pp. 257–270. Springer-Verlag, 1994.

[3] K. Kurosawa and Y. Desmedt. Optimum traitor tracing and asymmetric schemes. *Eurocrypt '98*, LNCS 1403, pp. 145–157. Springer-Verlag, 1998.

[4] D. R. Stinson and R. Wei. Combinatorial properties and constructions of traceability schemes and frameproof codes. *SIAM Journal on Discrete Mathematics*, 11(1), pp. 41–53, 1998.