A proven secure tracing algorithm for the optimal KD traitor tracing scheme (7 minutes for the Rump session)

Kaoru Kurosawa, Tokyo Institute of Tech., Japan. kurosawa@ss.titech.ac.jp
(Kaoru Kurosawa is the presenter)
Mike Burmester, University of London, UK. mikeb@dcs.rhbnc.ac.uk
Yvo Desmedt, Florida State University, USA. desmedt@cs.fsu.edu

April 26, 2000

Keywords: Traitor tracing, optimum scheme, proven secure.

A (k, n)-traceability scheme is a scheme in which at least one traitor is detected from a pirate key if there are at most k traitors among n authorized users. It has four components: key generation, an encryption algorithm, a decryption algorithm and a tracing algorithm.

Kurosawa and Desmedt found lower bounds on the size of keys and the size of ciphertexts of traceability schemes [1]. They also proposed two schemes, a one-time use (k, n)-traceability scheme (the KD one-time traceability scheme) which meets these bounds and a public key variant for multiple use (the KD public key traceability scheme) [1]. However, Stinson and Wei showed that the tracing algorithm of the KD schemes is subject to a linear attack. Boneh and Franklin pointed out the same attack independently.

In this paper, we present a proven secure tracing algorithm for the KD one-time traceability scheme. It will trace not only the traitors who use the Stinson-Wei/Boneh-Franklin attack but also any other traitors. Since the KD one-time traceability scheme achieves the lower bounds of Kurosawa and Desmedt [1], our result implies that the bounds are tight and the scheme is optimum.

The tracing algorithm consist of a TEST procedure and a TRACE procedure. TEST takes as input a set A of at most k users and will check if $A \cap C \neq \emptyset$, where C is the set of (at most k) traitors. TRACE takes as input a set A with $A \cap C \neq \emptyset$ and traces at least one traitor from A.

Recently, the authors have proved that our new tracing algorithm also works for the KD public traceability scheme under the decision Diffie-Hellman assumption.

Acknowledgement The authors strongly disagree with the comments from the referees of Eurocrypt 2000, who clearly misunderstood the new tracing algorithm.

References

[1] K. Kurosawa and Y. Desmedt. Optimum traitor tracing and asymmetric schemes with arbiter. Eurocrypt'98.