Traitor Traceable Signature Scheme

Yuji Watanabe[1]
Institute of Industrial Science
University of Tokyo
7-22-1 Roppongi, Minatoku, Tokyo
106-8558, Japan

Yuliang Zheng
Monash University
McMahons Road, Frankston,
Melbourne, Victoria 3199,
AUSTRALIA

Hideki Imai[1]
Institute of Industrial Science
University of Tokyo
7-22-1 Roppongi, Minatoku, Tokyo
106-8558, Japan

mue@imailab.iis.u-tokyo.ac.jp Yuliang.Zheng@infotech.monash.edu.auimai@iis.u-tokyo.ac.jp

Abstract — **The new signature scheme, *traitor traceable signature scheme* is presented, which allows the signer to convince any arbiter of the recipient's infringement, if the recipient distributes illegally the signature which he got. We use the techniques of a proof of knowledge of discrete logarithm[1][2], identification of double spender in an off-line electronic cash[3][4], and a signcryption scheme[5]. Our scheme consists of 3-move and it is more compact and efficient compared with the previous scheme[6], due to eliminate the cumbersome cut-and-choose like techniques. Moreover, our accusation protocol does not require the private-key of the recipient of signature, i.e., signer can convince any arbiter of the recipient's infringement without help of original recipient.**

I. Introduction

In a conventional digital signature scheme, after issueing the digital document with his signature, the signer cannot convince anyone who has leaked his signed document, since he can reproduce it arbitrarily. Recently, [6] proposed that the technique of tracing traitor[7][8] could be applied to the message with signature in order to prevent illegal proliferation of it. This approach is effective in case that both the message and signature are valuable for anyone.

However, this method[6] is not efficient in communication and computation, due to involve the cumbersome cut-and-choose like technique. Moreover, [6] has the following two problems, 1) an accusation protocol requires the private-key of the recipient of signature. Therefore, if the recipient is not available, the arbiter cannot make decision of accusation, 2) after accusation protocol, the signer can know the complete signature which is known only by recipient before accusation. This means that [6] is not robust against signer making wrong accusations.

II. Traitor traceable signature

In this paper, we propose the new signature scheme, *traitor traceable signature*, which solves several problems of [6] : 1) if the recipient distributes illegally the signature which he got, our scheme allows the signer to convince any arbiter of the recipient's infringement, 2) We use the technique of a proof of knowledge of discrete logarithm, identification of double spender in an off-line electronic cash, and a signcryption scheme, which are well estimated to be (provably) secure, 3) our scheme consists of 3-move and it is more compact and efficient compared with the previous scheme[6], due to eliminate the cumbersome cut-and-choose like techniques, 4)our accusation protocol does not require the private-key of the recipient of signature (the signer can convince any arbiter of the recipient's infringement without help of original recipient), 5)the signature can be generated to the recipient only once per each execution of this protocol in order to prevent the signer from making wrong accusations.

Table 1: Traitor Traceable Signature Scheme

Alice		*Bob*
$x \in_R \mathbf{Z}_q$ $X \leftarrow g^x$ $init_A(x) \leftarrow (X, sig_A(X))$	$\xrightarrow{init_A(x)}$	
		verify $init_A(x)$ $i, j, r_1, r_2, u_1 \in_R \mathbf{Z}_q$ $I \leftarrow g^i$ $J \leftarrow g^j$ $R_1 \leftarrow g^{r_1}$ $R_2 \leftarrow g^{r_2}$ $\sigma_1 \leftarrow r_1 - iH(R_1) \bmod q$ $\sigma_2 \leftarrow r_2 - jH(R_2) \bmod q$ $v_1 \leftarrow i - ju_1 \bmod q$ $u_2 \leftarrow H(I, J, R_1, R_2, \sigma_1, \sigma_2, u_1, v_1)$ $v_2 \leftarrow i - ju_2 \bmod q$ $V \leftarrow g^{v_2}$ $W(i, x) = (I, J, R_1, R_2, \sigma_1, \sigma_2, u_1, v_1, u_2, V)$
	$\xleftarrow{req_B(i, x)}$	$req_B(i, x) \leftarrow (W(i, x), sig_B(W(i, x)))$
verify $req_B(i, x)$ by $R_1 \overset{?}{=} g^{\sigma_1} I^{H(R_1)}$ $R_2 \overset{?}{=} g^{\sigma_2} J^{H(R_2)}$ $I \overset{?}{=} g^{v_1} J^{u_1}$ $I \overset{?}{=} V J^{u_2}$ generate (c, r, s) by $V^x \rightarrow k_1, k_2$ $r = KH_{k_2}(m)$ $s = x/(r + x_a) \bmod q$ $c = E_{k_1}(m)$	$\xrightarrow{(c, r, s)}$	
		obtain (c, r, s, v_2)

References

[1] A. Fiat and A. Shamir. How to prove yourself: practical solutions to identification and signature problems. In *Proc. of Crypto'86*, pages 186–194, 1986.

[2] C. P. Schnorr. Efficient identification and signatures for smart cards. In *Proc. of Eurocrypt'89*, pages 688–689, 1989.

[3] W. Mao. Blind certification of public keys and efficiently revocable electronic cash: Secure against capable attackers. In *HPL-96-134*, 1996.

[4] S. Brands. Untraceable off-line cash in wallets with observers. In *Proc. of Crypto'93*, pages 302–318, 1993.

[5] Y. Zheng. Digital signcryption or how to achieve cost (signature & encryption << cost (signature) + cost (encryption). In *Proc. of Crypto'97*, pages 165–179, 1997.

[6] K. Baba, K. Iwamura, Y. Zheng, and Hideki Imai. A protocol tc detect who has leaked a signed document. In *Proc. of SCIS'9: (in Japanese)*, pages 257–262, 1999.

[7] B. Chor, A. Fiat, and M. Naor. Tracing traitors. In *Proc. o Crypto '94*, pages 257–270, 1994.

[8] K.Kurosawa and Y.Desmedt. Optimum traitor tracing and nev direction for asymmetricity. In *Proc. of Eurocrypt '98*, page 145–157, 1998.

[1] This work was performed in part of Research for the Future Program (RFTF) supported by Japan Society for the Promotion of Science (JSPS) under contract no. JSPS-RFTF 96P00604.

0-7803-5857-0/00/$10.00 ©2000 IEEE.