1J－4

離散対数問題に基づく複数仲介者による ディジタル署名交換方式

小林和男　廣瀬勝一　池田克夫
京都大学大学院工学研究科

1　はじめに

ネットワーク上で商取引等を行う場合, 当事者双方がある文書に同意することを示すために, その文書にディジタル署名を施して交換することが行われるようになると考えられる. このような場合にいかにして公平にディジタル署名を交換するかということが課題となる. 当事者のみの場合には効率良く公平に交換することが困難である [1] と考えられるため, 本研究では仲介者の存在を仮定して効率の良い交換方式を構築することを試みる. 仲介者を用いる場合では仲介者と一方の当事者の結託が問題となる. 本研究では仲介者を複数人とし, 検証可能な秘密分散方式 [3] を利用して結託の問題に対処する.

2　複数仲介者による ElGamal 署名交換方式

本節では U_i $(i = 0,1)$ の二者が N 人の仲介者 C_j $(1 \le j \le N)$ を通じてメッセージ m に対する各々の ElGamal 署名 [2] (r_i, s_i) (i = 0,1) を交換する方式について述べる. 本方式では U_0 と U_1 の間及び, 各 U_i と各 C_j $(1 \le j \le N)$ の間の個別の通信路と U_0 から全 C_j , U_1 から全 C_j への放送通信路の存在を仮定する. これらの通信路では, 発信者及びメッセージの内容が改竄されないことが保証されるものとする. さらに, 個別の通信路では必要に応じてメッセージを秘密にした通信が可能であると仮定する. また, 本方式では N 人の仲介者のうち少くとも $K(> N/2)$ 人が方式に従うものと仮定する. なお秘密通信や放送通信路を用いた通信を行う場合はその旨明記する.

以下に交換方式を示す. 準備 p, q を十分大きな素数とし, q を $p-1$ の約数とする. $N << q$ である. α を GF(p) の位数 q の元とする. e_i, d_i をそれぞれ U_i の ElGamal 署名の公開鍵, 秘密鍵とする

交換の手順

1. U_i は K 個の乱数 $a_{ik} \in \{1, 2, \cdots, q-1\}$ $(0 \le k \le K-1)$ を選び, $v_{ik} = r_i^{a_{ik}} \bmod p$ $(0 \le k \le K-1)$ 及び $w_i = a_{i0} - s_i \bmod q$ を計算し, U_{1-i} に r_i, v_{ik}, w_i を送る.
2. U_i は
$$v_{(1-i)0} \equiv \alpha^m e_{1-i}^{-r_{1-i}} r_{1-i}^{w_{1-i}} \pmod p$$
を検証する. 検証に失敗すれば U_i は以降の処理を打ち切る.
3. U_i は
$$f_i(x) \stackrel{def}{=} a_{iK-1}x^{K-1} + \cdots + a_{i1}x + a_{i,0} \bmod q$$
について, $c_{ij} = f_i(j)$ $(1 \le j \le N)$ を計算し, 仲介者 C_j に c_{ij}, r_i を秘密に送る.
4. 仲介者 C_j は $u_{ij} = r_i^{c_{ij}} \bmod p$ を計算し, u_{ij}, r_i を U_i に送る.
5. U_i はすべての j $(1 \le j \le N)$ について
$$v_{(1-i)(K-1)}{}^{j^{K-1}} \cdots v_{(1-i)1}{}^{j} \cdot v_{(1-i)0} \equiv u_{(1-i)j} \bmod p$$
を検証する. また 1 で U_{1-i} から得た r_{1-i} と 4 で各 C_j から得た r_{1-i} が等しいことも検証する. K 個以上の j について検証が成功しなければ以降の処理を打ち切る. 検証に成功すればその旨を全 C_j に放送する.
6. U_0, U_1 からの検証成功のメッセージを受け取ると仲介者 C_j は $f_{1-i}(j)$ を U_i に, $f_i(j)$ を U_{1-i} にそれぞれ秘密に送る.

A Protocol for Exchange of Digital Signatures with Arbiters based on Discrete Logarithm Problem
Kazuo Kobayashi, Shouichi Hirose, Katsuo Ikeda
Kyoto University

7. U_i は N 個の $f_{1-i}(j)$ についてそれぞれ $u_{(1-i)j} \equiv r_{1-i}^{f_{1-i}(j)} \pmod p$ を検証し，検証に成功した値のうち任意の K 個を用いて $a_{(1-i)0}$ を求める．これより，$s_{1-i} = a_{(1-i)0} - w_{1-i} \bmod q$ から s_{1-i} を得ることができる．

3 考察

3.1 安全性

ここでは前節で提案した方式の安全性について考察する．以下の三条件を満たすとき，ディジタル署名交換方式は安全であると定義する．

(1) 当事者の両方が方式に従えば，当事者はそれぞれ相手の署名を得ることができる．
(2) 一方の当事者が方式に従えば，他方が $T(< K)$ 人の仲介者と結託しても一方的に相手の署名を得ることはできない．
(3) 当事者の双方が方式に従えば，仲介者はどちらの当事者の署名も得ることはできない．

上の三条件について，提案方式に関しては以下のことが言える．

条件 (1) 当事者及び仲介者の K 人以上が正しく方式に従うので，前節の手順により U_i は公平に相手の署名を得ることができる．

条件 (2) U_1 が不正を行って U_0 の署名 (r_0, s_0) を一方的に得ようと試みるものとする．r_0 は 2 節の方式の 1 で得ることができる．s_0 を一方的に得るためには T 人の仲介者と結託しても，離散対数問題を解くか，秘密分散方式を破る以外に方法がない．従って離散対数問題及び秘密分散方式が安全である限り，一方的に相手の署名を得ることはできない．

条件 (3) 仲介者 C_j に送られる情報は r_i と $f_i(j)$ $(i = 0, 1)$ だけである．これらからでは仲介者の全員の情報を集めたとしても，得られるものは $a_{i0}, a_{i1}, \cdots, a_{iK-1}$ だけである．よって仲介者だけでは s_i に関する情報は得られないので U_i の署名を得ることはできない．

3.2 効率

署名が付けられるメッセージの長さを n ビットとするときの，通信回数，通信量，べき乗剰余計算の回数，記憶量を以下の表 1,2 に示す．通信回数はメッセージを送信する回数であり，複数のメッセージを同時に送る場合は 1 回とする．通信量は送信されるメッセージ長の合計，保持する情報のサイズは方式の実行中に保持する必要のあるメッセージの長さの合計である．

表 1: 通信回数と通信されるデータ量

	通信回数	通信量
当事者 → 当事者	1	$(K+2)n$
当事者 → 仲介者	4	$6Nn$
仲介者 → 当事者	2	$2Nn$

表 2: 計算量と記憶量

	べき乗剰余計算回数	保持する情報のサイズ
当事者	$3N + K + 1$	$(2N + 3K + 5)n$
仲介者	2	$4n$

4 おわりに

本稿では複数の仲介者を通じてディジタル署名を交換する方式を提案し，その安全性と効率について考察した．本方式は Schnorr の署名方式 [4] にも適用することができる．今後の課題としてはより厳密な安全性の定義，効率化等が挙げられる．

参考文献

[1] Even, S., Goldreich, O. and Lempel, A.: A randomized protocol for signing contracts, *Commun. ACM*, vol. 28, no. 6, pp. 637–647 (1985).
[2] ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472 (1985).
[3] Feldman, P.: A practical scheme for non-interactive verifiable secret sharing, *Proc. IEEE FOCS87*, pp. 427–438 (1985).
[4] Schnorr, C. P.: Efficient identification and signatures for smart cards, *Proc. CRYPTO '89*, no. 435, pp. 239–252 (1990).