変形ElGamal署名の設計

新保 淳
shimbo@isl.rdc.toshiba.co.jp

(株) 東芝 研究開発センター
〒 210 川崎市幸区小向東芝町一番地

あらまし　離散対数ベースの典型的なディジタル署名法として ElGamal 法や Schnorr 法が挙げられる。近年、これらの署名法に対する機能拡張の提案や安全性の解析が盛んに行われいる。本文は、筆者が数年前に提案した変形 ElGamal 署名法の概要と共に、最近の安全性解析を参考に、若干の修正を行った結果を示すものである。変形 ElGamal 署名法の特徴は 2 巡型や 1 巡型など様々な形態の多重署名への適用が容易に実現できることにある。
和文キーワード　ディジタル署名, 多重署名, 離散対数, ElGamal 署名

Design of a modified ElGamal Signature Scheme

Atsushi Shimbo
shimbo@isl.rdc.toshiba.co.jp

TOSHIBA Corp., Research and Development Center
1, Komukai Toshiba-cho, Saiwai-ku, Kawasaki, 210 Japan

Abstract　In this paper we present a modification of our earlier proposal on digital signature shceme which is a variant of the ElGamal scheme. Several multisignature schemes can be construced based on the scheme. One of those multisignature schemes is two round type, where signers circulate the partial signed messages twice in order to generate a multisignature. Another is non-circulating type, where each signer has only to transmit his signed message to the next signer.
key words　Digital Signature, Multisignature, Discrete Logarithm, ElGamal Signature Scheme

1 はじめに

複数のエンティティが同一の文書に対する承認を行う場合、ディジタル署名生成者を多者に拡張した方法が有効となる。ディジタル署名方式を単純に拡張すれば、個々のエンティティが生成した署名文を連結する方法が得られるが、署名サイズや検査処理量が署名者数に比例して増加する欠点がある。この点を改良した “多重署名方式 (multisignature)” がいくつかのディジタル署名方式に対して提案されている。

特に、離散対数ベースの方式では、システムで共通のモジュラスを利用できるため、多重署名やグループ署名といった拡張が素因数分解ベースの方式と比べて容易に構成できる可能性がある。また、楕円曲線上の離散対数問題をベースにすることにより、署名サイズや処理速度の面で近い将来有利になる可能性もある。こうした背景もあって、近年、ElGamal 署名に代表される離散対数ベースの方式の拡張や安全性解析に関する検討が増えている。

筆者も数年前に ElGamal 署名に対して多重署名の構成を試みて、同署名方式を若干変形し、様々な多重署名を構成可能なことを特徴とした方式を提案している [1][2]。

本文は、この変形 ElGamal 署名法の概要と共に、最近の ElGamal 署名系に対する安全性解析結果 [6][9][7] を参考にして、従来の提案方式に対する若干の改良をまとめたものである。

2 変形 ElGamal 署名

鍵、パラメータ

- 素数 p,q, 但し $q|(p-1)$, q の典型的なサイズは 160 ビット。
- 整数 g, Z_pの位数 q の元。但し、$g \neq 0 \bmod q$。
- 秘密鍵 $x(\in Z_q)$
- 公開鍵 $y = g^x \bmod p$
- 一方向ハッシュ関数 $h(\cdot)$。但し、$h(x) \neq 0$ とする。

署名手順

以下の手順により求めた (r,s) が文書 M に対する署名文である。

1. 乱数 $k(\in Z_q^*)$ を生成。r を次式により定める。

$$r = g^k \bmod p$$

2. s を次式により定める。

$$s = x \cdot h(M) + k \cdot h(r) \bmod q$$

検証手順

1. $m = h(M), r' = h(r)$ を求める。
2. $g^s = y^m r^{r'} \bmod p$ が成立することを確認する。

変形法では ElGamal 法の検査式における $(h(M), s, r')$ の位置を入れ換えている。特に、g^sなる項を設けたことにより以降で述べる多重署名が構成可能となっている。

以前の方式 [1] からの修正は g を Z_p^*の位数 q の部分群の生成元としたこと、検証式における r の指数部の項を r から $h(r)$ に変更したことである。

本方式の安全性に関して以下のことが分かっている。

- ElGamal 法と同様に、乱数 r が使い捨てである限り複数署名文を連立させても秘密 x を求めることは

できない。また、$m = h(M)$ とおいた場合、検査式を満たす (m, r, s) の生成は可能であるが、ハッシュ関数の存在により与えられた文書 M に対する署名の偽造は困難。

- ElGamal 法に対して指摘されている偽造法 [6] は $g^k = cw = \beta \bmod p$(但し、c は p の smooth な因数) となる (k, β) を, システムパラメータの生成過程において構成できることに基づく。この偽造法は ElGamal 法が Z_p^*の原始元を g としていることに起因しており、g を位数 q(素数) の元とすることで困難となる。さらに、この偽造法を g の位数を q とした署名法に適用することもできる [8]。本署名法に適用した場合、$s = xm + kr' \bmod q$ において、$r' \equiv 0 \bmod q$ ならば $s = xm \bmod q$ となるため、秘密鍵 x が漏洩する。しかしながら本署名法ではハッシュ関数を導入しているため、k を変えた時に、$r' = h(g^k) \equiv 0 \bmod q$ となる確率の高い (g, q) を求めることは困難である。

3 変形 ElGamal 署名に基づく多重署名

本文での多重署名は、同一の文書に対する複数利用者のディジタル署名を単純に連結する方法と比べて、署名データサイズの縮小、署名検査処理量の削減を達成するものとして定義する。さらに理想的には、多重署名のデータサイズが署名者数に比例せずに定数オーダとなる方式が望まれる。

3.1 2 巡型多重署名

署名者を $U_i (1 \leq i \leq n)$ とし、その公開情報を y_i，秘密情報を x_iとする。多重署名作成手順を以下に示す。

(1) 第 1 round： r_nの生成

以下の手順を $i = 1, 2, \cdots, n$ まで繰り返す。

＜署名者 U_iの処理＞

署名者 U_iは乱数 $k_i (\in Z_q^*)$ を生成する。次に、署名者 U_{i-1}からの送信情報 r_{i-1}と乱数 k_iを用いて以下の r_i を生成し、(r_i, M) を U_{i+1}に送る。

$$r_i = r_{i-1} \cdot g^{k_i} \bmod p$$

以上を U_nまで実行し、r_nが得られる。U_{n+1}は r_nを U_1に送る。

(2) 第 2 round： s_nの生成

以下の手順を $i = 1, 2, \cdots, n$ まで繰り返す。

＜署名者 U_iの処理＞

署名者 U_{i-1}から送信された部分署名 (s_{i-1}, r_n) と (M, r_{i-1}) (第 1round での送信情報) に対して以下の検査を行う。

$$r' = h(r_n, M)$$

$$g^{s_{i-1}} =? (y_1 y_2 \cdots y_{i-1})^{h(M)} r_{i-1}^{r'} \bmod p$$

検査に通った場合、以下の s_iを作成し、(s_i, r_n) を U_{i+1}に送る。

$$s_i = s_{i-1} + x_i \cdot h(M) + k_i r' \bmod q$$

以上により多重署名文 (s_n, r_n, M) が得られる。

検査時には以下の式を満たすことを確認する。

$$g^{s_n} = \left(\prod_{i=1}^{n} y_i \right)^{h(M)} r_n^{h(r_n, M)} \bmod p$$

この多重署名方式による署名サイズは単一の署名者による場合と同じであり、検査処理量も剰余乗算が $n-1$ 回増えるだけでほとんど増加しない。

以前の方式との相違点は、検査式の r_n の指数の項を r_n から $h(r_n, M)$ に修正したことにある[1] 。これは以前の方式に対して適用可能な insider attack による偽造法 [7] を困難にするためである。以下では、$h(r_n, M)$ の部分を $h(r_n)$ とした場合を例として, 攻撃法を説明する。ここでは、U_2 を不正者とし、U_2 は U_1 とメッセージ m に対して多重署名を行うふりをして、実際には別の $\tilde{m}$ に対する多重署名を生成する手順を示す。

1. 第 1round での U_1 の処理：乱数 k_1 を定め、$r_1 = g^{k_1} \bmod p$ を計算して、U_2 に送る。
2. 第 1round での U_2 の処理：乱数 k_2 を定め、$r_2 = g^{k_2} \bmod p$ を計算する。また、$d \cdot m = \tilde{m} \bmod q$ を満たす d を求める。さらに、$\tilde{r} = (r_1 r_2)^d \bmod p, \tilde{r}' = h(\tilde{r})$ を求め、$\tilde{r}$ を U_1 に送る。
3. 第 2round での U_1 の処理：$s_1 = x_1 m + k_1 \cdot h(\tilde{r}) \bmod q$ を計算し、U_2 に送る。
4. 第 2round での U_2 の処理：$s_2 = d(x_2 m + k_2 \cdot h(\tilde{r}) + s_1) \bmod q$ を計算。$s_2 = (x_1 + x_2)(dm) + d(k_1 + k_2)\tilde{r}' \bmod q$ であることから、$g^{s_2} = (y_1 y_2)^{\tilde{m}} \tilde{r}^{\tilde{r}'} \bmod p$ が成立し、偽造された多重署名 $(\tilde{r}, s_2)$ が生成できる。

この攻撃法が成立するのは、正当な多重署名の s の両辺を d 倍することで、検査式の指数部のメッセージ項 m と乱数部 k を変更可能であることに原因がある。文献 [7] に指摘されているように、メッセージと乱数の両方に依存し一方向関数によって決定される値 $h(r, M)$ を指数部に作用させることで、この攻撃は防止できる。

以上のように修正した場合に、以前の提案に比べてハッシングの処理量が増加すること以外、通信量や検証処理量への影響はない。

3.2 1 巡型多重署名

以下の手順を $i = 1,2,\cdots,n$ まで実行する。

＜署名者 U_i の処理＞

署名者 U_{i-1} から送信された部分署名 $(s_{i-1}, r_1, r_2, \cdots, r_{i-1}, M)$ に対して以下の検査を行う。

$$g^{s_{i-1}} =? (y_1 y_2 \cdots y_{i-1})^{h(M)} r_1^{h(r_1)} r_2^{h(r_2)} \cdots r_{i-1}^{h(r_{i-1})} \bmod p$$

検査に通った場合、乱数 k_i を生成し、以下の (r_i, s_i) を求める。

$$\begin{aligned} r_i &= g^{k_i} \bmod p \\ s_i &= s_{i-1} + x_i \cdot h(M) + k_i \cdot h(r_i) \bmod q \end{aligned}$$

$(s_i, r_1, r_2, \cdots, r_i, M)$ を U_{i+1} に送る。

U_n により多重署名文 $(s_n, r_1, r_2, \cdots, r_n, M)$ が得られる。この手順によれば r_i の部分は署名者数に比例してサイズが増えるが、s_n の部分はサイズが不変である。

検査時には $(s_n, r_1, r_2, \cdots, r_n, M)$ が以下の式を満たすことを確認する。

$$g^{s_n} = \left(\prod_{i=1}^{n} y_i\right)^{h(M)} \left(\prod_{i=1}^{n} r_i^{h(r_i)}\right) \bmod p$$

ベースとなる変形 ElGamal 法と比べると $r_i^{h(r_i)}$ の項の積が右辺に加わっているが、安全性が低下する例は認められていない。

[1] 文献 [1] では拡張方式として検査式における y の指数の項を $h(M, r_n)$ に置き換えたものを提案しており、その修正でも insider attack に対処できる。

この方式はベースとなる署名方式の若干の修正以外は以前の提案方式と同じであるが、2 巡型多重署名の場合と同様に、各 r_iの指数部を $h(r_i, M)$ としても良い。仮にこのように変更しても、ハッシュ関数の処理量が増える以外は、処理量、データ量ともに影響はない。

4 補足

4.1 ElGamal 法の変形とその安全性

ElGamal 署名の検証式における変数の位置を入れ換えることにより提案法以外にも幾つかの署名法が得られる。このことは筆者とは独立に、ほぼ同時期に様々な研究者により報告されている [10][11][12]。さらに様々な変形版が現在までに提案されている。指数部 (m, r, s) の 3 つの位置により以下の 6 通りが得られる。

方式 1： $g^m = y^r r^s \bmod p$ ：ElGamal 法 [3]
方式 2： $g^m = y^s r^r \bmod p$ ：Agnew らの方式 [4]
方式 3： $g^s = y^m r^r \bmod p$ ：提案方式 [1][2]
方式 4： $g^s = y^r r^m \bmod p$
方式 5： $g^r = y^m r^s \bmod p$
方式 6： $g^r = y^s r^m \bmod p$

これらのうち、2 巡型多重署名を構成可能なものは方式 3 と方式 4 であり、1 巡型多重署名を構成可能であるものは方式 3 のみである。方式 4 に対して単純な拡張により 1 巡型の多重署名を構成した場合には、偽造法が存在することが分かっている [1]。

4.2 DSA と類似の変形

署名サイズの縮小のため、DSA(Digital Signature Algorithm)[15] と類似の変形を加えることができる。

鍵、パラメータ 2 章と同じ。

署名手順

以下の手順により求めた (r, s) が文書 M に対する署名文である。

1. 乱数 $k(\in Z_q^*)$ を生成。r を次式により定めるが、$rbmodq$ が 0 となる場合には別の k の生成に戻る。

$$r' = g^k \bmod p$$

$$r = h(r')$$

2. s を次式により定める。

$$s = x \cdot h(M) + kr \bmod q$$

検証手順

1. $r \neq 0 \bmod q$ かつ $0 < s < q$ であることを確認する。
2. $w = r^{-1} \bmod q$ を求める。
3. 次式が成立することを確認する。

$$r' = g^{ws} / y^{wh(M)} \bmod p$$

$$r = h(r')$$

このように提案法を変形した場合、2 巡型の多重署名は 3 章と類似の手順で構成できる。注意すべき点は、1 巡目の処理では各署名者の間で r'_i(ハッシングする前の値) を巡回し、2 巡目の最後の署名者 U_nのところで r'をハッシングして r を作成することである。なお、1 巡型に r のサイズ縮小の技法を用いるのは困難である。

4.3 楕円曲線への適用

本署名方式は、他の離散対数ベースの方式と同様に楕円曲線上の加法群を利用した署名方式に変形することができる。

鍵、パラメータ

- 楕円曲線 E/F_q。但し、$q = p^t$(p は素数).
- 楕円曲線 E/F_q上の点 G。G の位数を z とする。z の典型的なサイズは 160 ビット。
- 秘密鍵 $x(\in Z_z)$,
- 公開鍵 $Y = xG$ over E/F_q

署名手順

以下の手順により求めた (R, s) が文書 M に対する署名文である。

1. 乱数 $k(\in Z_z)$ を生成。R を次式により定める。

$$R = kG \text{ over } E/Fq$$

2. s を次式により定める。

$$s = x \cdot h(M) + k \cdot h(R) \bmod z$$

検証手順

1. $r = h(R)$, $m = h(M)$ を求める。
2. 次式が成立することを確認する。

$$sG = mY + rR \text{ over } E/F_q$$

楕円曲線での変形 ElGamal 署名に対する多重署名は 3 章と類似の手順で構成できる。

5 比較

ここでは、ElGamal 署名法、Schnorr 署名法、提案法の 3 者に対して多重署名の構成可能性／多重署名検証の演算量／多重署名サイズ／通信量のそれぞれの比較結果を表 1 と表 2 にまとめる。

表 1 では各署名方式に対する多重署名の構成例があるものは○, ないものは×として表記した。

表 1: DLP ベース署名法の多重署名構成可能性

	連結型	2 巡型	1 巡型
ElGamal	○	×	×
DSA	○	×	×
Schnorr	○	○	×
提案法	○	○	○

表 2 では、検証演算量は最終検証時に必要なベキ乗の回数を基準としている。パラメータは,$|p| = 512, |q| = 160$, ハッシュ関数の出力は 160bit として算出した (但し、$|p|$ で p のビットサイズを表すことにする)。また、総通信量は、多重署名が完成するまでの中間署名データの通信量の総和を $|p|$ を基準に数えたものである。

表 2: DLP ベース多重署名法の処理量の比較

	検証演算量 (べき乗回数)	多重署名サイズ ($\times$ 512bit)	総通信量 ($\times$ 512bit)
ElGamal(連結型)	$3 \times n$ (n 式の検証)	$2n$	$n^2 - n$
DSA(連結型)	$2 \times n$ (n 式の検証)	$0.63n$	$0.31n^2 - 0.31n$
Schnorr(連結型)	$2 \times n$ (n 式の検証)	$0.63n$	$0.31n^2 - 0.31n$
Schnorr(2 巡型)	2	0.63	$2.31n - 1.31$
提案法 (連結型)	$3 \times n$ (n 式の検証)	$1.31n$	$0.66n^2 - 0.66n$
提案法 (2 巡型)	3	1.31	$2.31n - 1.31$
提案法 (1 巡型)	$n + 2$	$n + 0.31$	$0.5n^2 - 0.19n - 0.31$

2 巡型の多重署名は比較した項目の中では有利であるが、署名者の間を 2 巡回させるのが面倒な場合もある。特に、1 巡目の署名順通りに 2 巡目での部分署名を回覧しなければ、作成中の不正者の検出が困難となるため、実質的には署名順序に制約が生じる問題もある。

一方、1 巡型と連結型は共に署名者の間でデータを一度流すだけで済む利便性がある。この 1 巡型と連結型を比較すると、特に署名検査において違いが現われる。すなわち、連結型では署名検査をそれぞれの署名に対して独立に行わなければならないのに対し、1 巡型では多重署名の検証式は 1 つである。従って、例えばバイナリ演算を拡張した効率的なベキ積計算法 [16] を利用することにより 1 巡型は連結型よりも約 n 倍高速に署名検証できる。さらに、署名サイズや通信量の点でも, 同じ方式で比較する限り 1 巡型が有利である。

表 1 から明らかなように本稿で示した変形 ElGamal 署名法の特徴は、様々な多重署名法を構成可能なことにある。なお、4.2 章に示した DSA と類似の効率化を行うことにより、連結型や 2 巡型において DSA や Schnorr 署名と同様の署名サイズを実現することもできる。

6 むすび

ElGamal 署名を変形した署名方式を提案しているが、効率化の観点と最近, 発見されたアタックへの対策という観点から修正点を幾つか示した。近年、離散対数ベースの方式に対する解析が盛んなことから、今後も安全性の検討に注力する必要がある。

参考文献

[1] 新保 淳, “多重署名に適した ElGamal 署名の一変形方式”, 1994 年暗号と情報セキュリティシンポジウム,SCIS94-2C (1994).

[2] 新保 淳, “多重署名可能な変形 ElGamal 方式”, 1994 年電子情報通信学会春季大会 (1994).

[3] T.ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Trans. on IT, Vol.IT-31, No.4, July 1985, pp.469-472 (1985).

[4] G.Agnew, R.Mullin and S.Vanstone, “Improved Digital Signature Scheme Based on Discrete Logarithms”, Electronics Letters, Vol.26, No.14, pp.1024-1025 (1990).

[5] C.P.Schnorr, “Efficient Signature Generation by Smart Cards”, Journal of Cryptology, Vol.4, No.3, pp.161-174 (1991).

[6] D.Bleichenbacher, “Generating ElGamal Signatures Without Knowing the Secret Key”, Advances in Cryptology, Proc. of EUROCRYPT’96, Springer-Verlag, pp.10-18 (1996).

[7] M.Michels and P.Horster, “On the Risk of Disruption in Several Multiparty Signature Scheme”, Advances in Cryptology, Proc. of ASIACRYPT’96, Springer-Verlag, pp.334-345 (1996).

[8] A.Miyaji, “A Message Recovery Signature Scheme Equivalent to DSA over Elliptic Curves”, Advances in Cryptology, Proc. of ASIACRYPT’96, Springer-Verlag, pp.1-14 (1996).

[9] R.Anderson and S.Vaudenay, “Minding your p’s and q’s”, Advances in Cryptology, Proc. of ASIACRYPT’96, Springer-Verlag, pp.26-35 (1996).

[10] K.Nyberg and R.Rueppel, “Message recovery for signature schemes based on the discrete logarithm problem”, Advances in Cryptology, Proc. of Eurocrypt’94, pp.175-190 (1994).

[11] L.Harn and Y.Xu, “Design of generalised ElGamal type digital signature schemes based on discrete logarithm”, Electronics Letters, Vol.30, No.24, pp.2025-2026 (1994).

[12] P.Horster, M.Michels and H.Peterson, “Meta-Message Recovery and Meta-Blind Signature Schemes Based on the Discrete Logarithm Problem and Their Applications”, Advances in Cryptology, Proc. of ASIACRYPT’94, Springer-Verlag, pp.224-237(1995).

[13] K.Ohta and T.Okamoto, “A digital multisignature scheme based on the Fiat-Shamir scheme”, Advances in Cryptology, Proc. of ASIACRYPT’91, Springer-Verlag, pp.139-148 (1992).

[14] E.Brickell, P.Lee and Y.Yacobi, “Secure Audio Teleconference”, Advances in Cryptology, Proc. of Crypto’87, Springer-Verlag, pp.429-433 (1988).

[15] “Debating Encryption Standards”, Communications of ACM, Vol.35, No.7, pp.32-54 (1992).

[16] 新保 淳, 川村信一, “n 変数べき乗剰余演算とその応用に関する考察”, 信学技報 ISEC91-59 (1992).