福井大学
工学部　研究報告
第47巻　第1号
1999年3月

Blum-Goldwasser 確率公開鍵暗号系のディジタル署名

王　尚平*　西野 順二**　小高 知宏**　小倉 久和**

The Digital Signature of Blum-Goldwasser Probobilistic Public Key Cryptosystem

Shangping WANG, Junji NISHINO, Tomohiro ODAKA and Hisakazu OGURA

(Received Feb. 26, 1999)

The digital signature algorithm for Blum-Goldwasser probabilistic public key cryptosystem is proposed. In the proposed cryptosystem both encryption and digital signature can be done at the same time. The security of the proposed cryptosystem is not lower than both RSA public key cryptosystem and Blum-Goldwasser probabilistic public key cryptosystem.

Key Words : Public Key, Digital Signature, Blum Number, Cryptosystem

1　はじめに

電子郵便 (electronic mail) や電子送金 (electronic funds transfer) などのデータ通信では，ディジタル署名は文書の署名、捺印に相当する．従ってビジネスの上での争いを避けるためにはディジタル署名は必要不可欠である．

公開鍵系の中には暗号化 E と復号 D の順序を交換できる，すなわち，M をメッセージとして．

$$E[D(M)] = D[E(M)] = M \tag{1}$$

のような性質をもつものがある．これを用いてディジタル署名と同時に秘匿の機能も備わった認証システムを構成できる [1]．RSA 公開鍵暗号系 [2] は暗号化 E と復号 D の順序を交換できる暗号系の例である．しかし公開鍵系の中には暗号化 E と復号 D の順序を交換できない公開鍵系がある．Blum-Goldwasser 確率公開鍵暗号系 [3] はそのような公開鍵系の例である．本研究は RSA 公開鍵暗号系を参考にして，Blum-Goldwasser 確率公開鍵暗号系を修正することで，Blum-Goldwasser 確率公開鍵暗号系におけるディジタル署名システムを提案する．

*大学院情報工学専攻 (現在, 西安理工大学理学院)
**情報工学科

2 Blum-Goldwasser 確率公開鍵暗号系

確率公開鍵暗号系は Goldwasser と Micali[4] によるアイデアで，メッセージの各ビットをそれぞれ暗号化する公開鍵暗号系である．さらに効率的な確率暗号系が Blum と Goldwasser によって提案されている．この Blum-Goldwasser 確率暗号系は次の通りである．

B の公開鍵：n_b (Blum 数)
B の秘密鍵：n_bの素因数 p_b、q_b

A が B にメッセージ $m = m_1 \circ m_2 \circ \ldots\ldots \circ m_l$ を送りたいとする．ここで $m_i \in \{0, 1\}$ $(i = 1, \ldots, l)$ である．$\circ$は連接である．

A の暗号化手順：
A は乱数 $x_0 \in \mathrm{QR}(n_b)$ を発生し，これを BBS 生成器 [2] に与える．BBS 生成器は，シード x_0が与えられると n_bによる平方剰余を連続して行うことで $x_1, x_2, \ldots, x_l$を計算する．各 x_iの最下位ビットをとることで b_iを得る．

$$x_{i+1} = x_i^2 \bmod n_b \quad (i = 0, 1, \ldots, l) \tag{2}$$
$$b_i = lsb(x_i) \quad (i = 1, \ldots, l) \tag{3}$$

$lsb(x_i)$ は x_iの最下位ビットである．そこでメッセージ m の各 m_iに対して次の式 (4), (5) により，暗号文 c を作成する．

$$c_i = b_i \oplus m_i \quad (i = 1, \ldots, l) \tag{4}$$
$$c = c_1 \circ c_2 \circ \ldots\ldots \circ c_l \tag{5}$$

ここに，$\oplus$は環和である．A は暗号文 c と $x_{l+1}(x_{l+1} = x_l^2 \bmod n_b)$ を B に送る．

B の復号手順：
B は，受け取った x_{l+1}から，その平方根を n_bの素因数 p_b, q_bを用いて次々に求め，$x_l, \ldots, x_1, x_0$を得ることができる [2]．これらの下位ビット b_iから次の式 (6), (7) により，メッセージ m を復元できる．

$$m_i = b_i \oplus c_i \quad (i = 1, \ldots, l) \tag{6}$$
$$m = m_1 \circ m_2 \circ \ldots\ldots \circ m_l \tag{7}$$

明らかに Blum-Goldwasser 確率暗号系では，暗号化 E と復号 D の順序を交換できない．

3 Blum-Goldwasser 確率公開鍵暗号系のディジタル署名

従来の Blum-Goldwasser 確率公開鍵暗号系でディジタル署名を実現するためには，たとえば ElGamal 署名システム [5] のような特別の署名専用のアルゴリズムが必要である．これは他のシステムを使われなければならないことを意味し，この結果，暗号系が複雑になり，計算量が増加する．

公開鍵暗号系では暗号化とディジタル署名の両方が行える方が便利である．RSA 公開鍵暗号系にはこの性質がある．そこで，Blum-Goldwasser 確率公開鍵暗号系の中でディジタル署名ができるように，Blum-Goldwasser 確率公開鍵暗号系の拡張方法を提案する．

3.1 提案するシステムの構成と送受手順

提案するシステムは次のように構成される．
A の公開鍵：n_a (Blum 数)，e_a

A の秘密鍵：p_a, q_a, d_a
B の公開鍵：n_b (Blum 数)，e_b
B の秘密鍵： p_b, q_b, d_b
ここで，次の式 (8), (9) が成り立つものとする．

$$n_a = p_a \cdot q_a \tag{8}$$
$$p_a \bmod 4 = q_a \bmod 4 = 3 \tag{9}$$

p_a、q_aは異なる大きさの素数である．このような n_aを Blum 数という．e_aは $lcm(p_a - 1, q_a - 1)$ と互いに素な乱数 $(2 < e_a < lcm(p_a - 1, q_a - 1))$ である．このとき次の式 (10) が成り立つ．

$$gcd(e_a, lcm(p_a - 1, q_a - 1)) = 1 \tag{10}$$

d_aは $lcm(p_a - 1, q_a - 1)$ を法とするときの e_aの逆数である．すなわち

$$e_a d_a \equiv 1 \bmod lcm(p_a - 1, q_a - 1) \tag{11}$$

とする．B についても同様である．
いま，A は式 (7) で表されるメッセージを B に送りたいとする．

A の暗号化手順

A は乱数 $x_{-1} \in Z^*_{n_b}$を発生し，式 (2)(3) に示した BBS 生成器を使い $x_0, x_1, \ldots, x_{l+1}$と $b_0, b_1, \ldots, b_l$を計算する．ここで

$$Z^*_{n_b} = \{x | 1 \le x \le n_b - 1, gcd(x, n_b) = 1\} \tag{12}$$

$$x_0 = x_{-1}^2 \bmod n_b \tag{13}$$
$$\begin{aligned} x_{l+1} &= x_l^2 \bmod n_b \\ &= x_{l-1}^{2^2} \bmod n_b \\ &= \ldots\ldots \\ &= x_0^{2^{l+1}} \bmod n_b \end{aligned} \tag{14}$$

ただし，以上の計算において $x_{l+1} < min\{n_a, n_b\}$ を条件とする．もしこの条件を満たさない場合には，新しい乱数 x_{-1}を再発生する．次にメッセージ m の各 m_iに対して

$$c_i = b_i \oplus m_i \ (i = 1, \ldots, l) \tag{15}$$

からなる暗号文 $c = c_1 \circ c_2 \circ \ldots\ldots \circ c_l$ と x_{l+1}を作成する．

A がディジタル署名暗号文を作る方法

ユーザー A とユーザー B の使用する n_aおよび n_bの値が異なるために，mod n_aと mod n_bの計算順序の違いにより計算結果が異なる．このような問題に対して，n_aと n_bの大小関係により以下の二つの場合に分けてディジタル署名を作成する．

(1) $n_a < n_b$の場合
ユーザー A が自分の秘密鍵 d_aを用いた署名文 kを計算する．

$$k = x_{l+1}^{d_a} \bmod n_a \tag{16}$$

次に，ユーザー B の公開鍵 e_bを用いた署名暗号文 h を計算する．

$$h = k^{e_b} \bmod n_b \tag{17}$$

そして，gを計算する．

$$g = x_{l+1}^{e_b} \bmod n_b \tag{18}$$

暗号文 c とディジタル署名暗号文 h および g を B に送る．

(2) $n_a > n_b$の場合

ユーザー A が B の公開鍵 e_bを用いた暗号文 k'を計算する．

$$k' = x_{l+1}^{e_b} \bmod n_b \tag{19}$$

次に，自分の秘密鍵 d_aを用いた署名暗号文 h'を計算する．

$$h' = (k')^{d_a} \bmod n_a \tag{20}$$

そして，gと fを計算する．

$$g = x_{l+1}^{e_b} \bmod n_b \tag{21}$$
$$f = (n_a - n_b)^{d_a - x_0} \bmod n_a \tag{22}$$

を計算する．

暗号文 c とディジタル署名文 h'および gと fを B に送る．

B の復号手順

(1) $n_a < n_b$の場合

B は受け取った (h, g) から， p_b, q_b, e_a, n_a, d_bを用いて，次のように復号する．

step(1-1) $$\bar{k} = h^{d_b} \bmod n_b \tag{23}$$

step(1-2) $$\bar{x}_{l+1} = \bar{k}^{e_a} \bmod n_a \tag{24}$$

step(1-3) $$x'_{l+1} = g^{d_b} \bmod n_b \tag{25}$$

step(1-4) もし$\bar{x}_{l+1} = x'_{l+1}$ならば，メッセージは A が送ったことが確認できる．そして $x_{l+1} = \bar{x}_{l+1} = x'_{l+1}$である．

step(1-5) $$a_1 = [(p_b + 1)/4]^{l+1} \bmod (p_b - 1) \tag{26}$$
$$a_2 = [(q_b + 1)/4]^{l+1} \bmod (q_b - 1) \tag{27}$$
$$t_1 = x_{l+1}^{a_1} \bmod p_b \tag{28}$$
$$t_2 = x_{l+1}^{a_2} \bmod q_b \tag{29}$$

step(1-6) $$x_0 = (t_1 q_b^{p_b - 1} + t_2 p_b^{q_b - 1}) \bmod n_b \tag{30}$$

step(1-7) $$x_{i+1} = x_i^2 \bmod n_b \quad (i = 0, 1, \ldots, l)$$
$$b_i = lsb(x_i) \quad (i = 1, \ldots, l)$$

step(1-8) $1 \leq i \leq l$ に対して $m_i = c_i \oplus b_i$を求めて，平文 $m = m_1 \circ m_2 \circ \cdots\cdots \circ m_l$を得る．

(2) $n_a > n_b$の場合

B は受け取った (h', g, f) から， p_b, q_b, e_a, n_a, d_bを用いて，次のように復号する．

step(2-1) $$\bar{k}' = (h')^{e_a} \bmod n_a \tag{31}$$

step(2-2) $$\bar{x}'_{l+1} = (\bar{k}')^{d_b} \bmod n_b \tag{32}$$

step(2-3) $$x'_{l+1} = g^{d_b} \bmod n_b \tag{33}$$

step(2-4) もし $\bar{x}_{l+1} = x'_{l+1}$ならば，$x_{l+1} = \bar{x}_{l+1} = x'_{l+1}$である．

step(2-5), step(2-6) は step(1-5), step(1-6) と同様である．これより x_0を見つけることができる．x_0を用いて次の式 (34), (35) を計算する．

$$f_1 = f \cdot (n_a - n_b)^{x_0} \bmod n_a \tag{34}$$
$$f_2 = (f_1)^{e_a} \bmod n_a \tag{35}$$

もし $f_2 = n_a - n_b$が成立するならば，このときメッセージは A が送ったことを確認できる．

step(2-7)，step(2-8) は step(1-7)，step(1-8) と同様である．

こうして平文 $m = m_1 \circ m_2 \circ \ldots\ldots \circ m_l$ を得る．

3.2 B の復号の有効性

ここで $n_a < n_b$の場合の B の復号手順の有効性を証明する．$n_a > n_b$の場合も同様に証明できる．

step(1-1) の$\bar{k}$は，

$$\begin{aligned}\bar{k} &= h^{d_b} \bmod n_b \\ &= k^{e_b d_b} \bmod n_b \\ &= k^{1+r_1 lcm(p_b-1,\, q_b-1)} \bmod n_b \\ &= k \end{aligned} \tag{36}$$

であるから式 (16) の kと一致する．また，$k^{lcm(p_b-1,\, q_b-1)} \bmod n_b = 1$が成立することが $k^{p_b-1} \bmod p_b = 1$，$k^{q_b-1} \bmod q_b = 1$ より導かれる．

step(1-2) において，

$$\begin{aligned}\bar{x}_{l+1} &= \bar{k}^{e_a} \bmod n_a \\ &= k^{e_a} \bmod n_a \\ &= x_{l+1}^{e_a d_a} \bmod n_a \\ &= x_{l+1}^{1+r_2 lcm(p_a-1,\, q_a-1)} \bmod n_a \\ &= x_{l+1} \end{aligned} \tag{37}$$

step(1-3) では，

$$\begin{aligned}x'_{l+1} &= g^{d_b} \bmod n_b \\ &= x_{l+1}^{e_b d_b} \bmod n_b \\ &= x_{l+1} \end{aligned} \tag{38}$$

であるから step(1-4) が保証される．

step(1-5) において，

$$\begin{aligned}& x_{l+1}^{(\frac{p_b+1}{4})^{l+1}} \bmod p_b \\ &= (x_0^{2^{l+1}} \bmod n_b)^{(\frac{p_b+1}{4})^{l+1}} \bmod p_b \\ &= x_0^{(\frac{p_b-1}{2}+1)^{l+1}} \bmod p_b \\ &= x_0^{\sum_{i=0}^{l+1} C_{l+1}^i (\frac{p_b-1}{2})^i} \bmod p_b \\ &= \Pi_{i=0}^{l+1} x_0^{C_{l+1}^i (\frac{p_b-1}{2})^i} \bmod p_b \\ &= x_0 \Pi_{i=1}^{l+1} x_0^{C_{l+1}^i (\frac{p_b-1}{2})^i} \bmod p_b \\ &= x_0 \bmod p_b \end{aligned} \tag{39}$$

p_bを素数とすると，次の式 (40) が成り立つ．

$$x_0^{(\frac{p_b-1}{2})} \bmod p_b = (\frac{x_0}{p_b}) \tag{40}$$

ここで，$(\frac{x_0}{p_b})$ は Jacobi 符号である．$QR(p_b)$ を p_bを法とする二次剰余の集合とすると，$x_0 \in QR(p_b)$ のとき，$(\frac{x_0}{p_b}) = 1$ となる．式 (13) によって，$x_0 = x_{-1}^2 \bmod p_b$が成立する，すなわち $x_0 \in QR(p_b)$ である．したがって $(\frac{x_0}{p_b}) = 1$.

p_bが素数ならばフェルマーの定理によって，$x_0^{p_b-1} \bmod p_b = 1$ である．したがって

$$\begin{aligned}t_1 &= x_{l+1}^{a_1} \bmod p_b \\ &= x_{l+1}^{(\frac{p_b+1}{4})^{l+1} \bmod p_b - 1} \bmod p_b \\ &= x_0 \bmod p_b \end{aligned} \tag{41}$$

すなわち，$x_0 = t_1 \bmod p_b$．同様にして $x_0 = t_2 \bmod p_b$が示される．

step(1-6) では，$x_0 = t_1 \bmod p_b$ と $x_0 = t_2 \bmod p_b$ から x_0 を求めるが，孫子定理 (中国人剰余定理) [1] を利用すれば次の式 (42) で得られる．

$$\begin{aligned} x_0 &= (q_b)^{\varphi(p_b)} \cdot t_1 + (p_b)^{\varphi(q_b)} \cdot t_2 \bmod n_b \\ &= t_1 q_b^{p_b-1} + t_2 p_b^{q_b-1} \bmod n_b \end{aligned} \tag{42}$$

ここで，$\varphi(\cdot)$ はオイラー関数であり，$\varphi(p_b) = p_b - 1, \varphi(q_b) = q_b - 1$ である．

step(1-7) と step(1-8) は明らかに成立する．

4 調停者によるディジタル署名の認証

以上のような暗号通信において，ユーザー A とユーザー B の間で，なんらかの争いが生じた場合，調停者の助けを借りて，以下のような方法で，ディジタル署名の認証を行うことにより解決できる．

(1) $n_a < n_b$の場合

ユーザー B は調停者に $(g,\ x'_{l+1})$ と $(h,\ \bar{k})$ を呈示する．ここで $x'_{l+1} = g^{d_b} \bmod n_b$，$\bar{k} = h^{d_b} \bmod n_b$．調停者は始めに B の公開鍵 e_b, n_bを用いて s, t を計算する．

$$s = (x'_{l+1})^{e_b} \bmod n_b \tag{43}$$

$$t = \bar{k}^{e_b} \bmod n_b \tag{44}$$

もし g=s かつ h=t が成立するならば，B が提供した署名暗号文の有効性を確認できる．次に調停者は A の公開鍵 e_a, n_aを用いて

$$\bar{x}_{l+1} = \bar{k}^{e_a} \bmod n_a \tag{45}$$

を計算する．もし $x'_{l+1} = \bar{x}_{l+1}$が成立するならば，メッセージは A が送ったものであることを確認できる．

(2) $n_a > n_b$の場合

ユーザー B が調停者に (g, x'_{l+1}) と $(h', \bar{x}'_{l+1})$ 及び (f, x_0) を呈示する，ここで $x'_{l+1} = g^{d_b} \bmod n_b$，$\bar{k}' = (h')^{e_a} \bmod n_a$，$\bar{x}'_{l+1} = (k')^{d_b} \bmod n_b$である．調停者は A の公開鍵 e_a, n_aと B の公開鍵 e_b, n_bを用いて u, v, s, wを計算する．

$$u = (h')^{e_a} \bmod n_a \tag{46}$$

$$v = (\bar{x}'_{l+1})^{e_b} \bmod n_b \tag{47}$$

$$s = (x'_{l+1})^{e_b} \bmod n_b \tag{48}$$

$$w = x_0^{2^{l+1}} \bmod n_b \tag{49}$$

もし $u = v$かつ $g = s$ 及び $w = x'_{l+1} = \bar{x}'_{l+1}$が成立するならば，B が提供した署名暗号文の有効性を確認できる．次に調停者は A の公開鍵 e_a, n_aと x_0を用いて f_1, f_2を計算する．

$$f_1 = f \cdot (n_b - n_a)^{x_0} \bmod n_a \tag{50}$$

$$f_2 = (f_1)^{e_a} \bmod n_a \tag{51}$$

もし $f_2 = n_a - n_b$が成立するならば，メッセージは A が送ったものでことを確認できる．

ここで $n_a > n_b$の場合，A の署名の中に f を付け加えなければならないことに注意する．もしユーザー C が式 (20) の暗号署名文 h'を入手したとすると，C は A の署名 h'を次の式 (52), (53) により自己の署名 h_1と置き換えることができてしまう．

$$k' = (h')^{e_a} \bmod n_a \tag{52}$$

$$h_1 = (k')^{d_c} \bmod n_c \tag{53}$$

そして，C が h_1と gを B に送れば，C の署名が B に確認される．B はメッセージは C のもとで書かれたものであると誤って判定にしまう．故に fを付け加えることが必要である．fは乱数 x_0を用いて式 (22) により計算する．このため n_bの素因数分解がわからなければ，離散対数と平方剰余問題を効率よく解く方法はないので，C は h'から x_0を求めることができず，fの置き換えを防止できる．

5 むすび

本論文では，Blum-Goldwasser 確率公開鍵暗号系にディジタル署名のアルゴリズムを付け加えた．提案した暗号系を破るためには RSA 公開鍵暗号系と Blum-Goldwasser 確率公開鍵暗号系を同時に破らなければならない．だから暗号系の安全性は RSA 公開鍵暗号系と Blum-Goldwasser 確率公開鍵暗号系よりは低くない．またこの公開鍵暗号系は効率性がある．よってこの確率公開鍵暗号系は安全性、効率性、認証機能をすべて備えている．

参考文献

[1] 辻井 重男，笠原 正雄，“暗号と情報セキュリティ，” 昭晃堂，東京，1994.

[2] R. L. Rivest, A. Shamir, and L. Adlman, “A method for obtaining digital signatures and public key cryptosystems, ” Communication of the ACM, vol. 21, No. 2, pp. 120-126, 1978.

[3] M. Blum and S. Goldwasser, “An efficient probabilistic public-key cryptosystem that hides all partial information, ” Lecture Note in Computer Science, pp. 289-302, Advances in Cryptology-CRYPTO’84 , 1984.

[4] S. Goldwasser and S. Micali, “Probabilistic encryption , ” Journal of Computer and Systems Science, vol. 28, no. 2, pp. 270-299, 1984.

[5] T. ElGamal, “A public key sryptosystem and a signature scheme base on discrete logarithms , ” IEEE Trans. Inform. Theory, vol . IT-31, no. 4, pp. 469-472, 1985.