社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2005－ＣＳＥＣ－30 (28)
2005／7／21

メタリング署名

岡崎　裕之† 　境　　隆一†† 　笠原　正雄†††

† 京都コンピュータ学院
†† 大阪電気通信大学工学部
〒572-8530 大阪府寝屋川市初町 18-8
††† 大阪学院大学情報学部
〒564-8511 大阪府吹田市岸部南 2-36-1
E-mail: †h_okazaki@m.ieice.org, ††sakai@isc.osakac.ac.jp, †††kasahara@utc.osaka-gu.ac.jp

あらまし　一般的に，ディジタル署名方式では秘密鍵を用いて公開鍵を計算する．メッセージに署名を行うには，メッセージと秘密鍵を用いて署名文を計算する．公開鍵，署名文はともに秘密鍵をもとにして計算されたものである．そこで我々はある署名方式の署名文を，公開鍵として用いることができるような署名方式，メタ署名について検討を行った．メタ署名とは，ある署名方式 (基本署名方式) の署名文を公開鍵として用いて，その署名文の署名者のみが新たなメッセージに署名を行えるような署名方式である．本論文ではまず基本署名，メタ署名ともにリング署名であるようなメタリング署名の概念の提案を行う．さらにメタリング署名の実現例として基本署名方式とメタ署名方式の双方をリンカブルリング署名の一種である LSAG 署名を用いて実現したメタ LSAG 署名を提案する．

キーワード　ディジタル署名，署名文を公開鍵として使う，匿名性，リング署名

Meta Ring Signature

Hiroyuki OKAZAKI†, Ryuich SAKAI††, and Masao KASAHARA†††

† KCG.edu
†† Department of Lightwave Sciences, Osaka Electro-Communication University
Hatu-tyo,Neyagawa-shi, 572-8530 JAPAN
††† Faculty of Informatics, Osaka Gakuin University
Kishibeminami 2-36-1, Suita-shi, 564-8511 Japan
E-mail: †h_okazaki@m.ieice.org, ††sakai@isc.osakac.ac.jp, †††kasahara@utc.osaka-gu.ac.jp

Abstract　In this paper, we propose a new concept "Meta Ring Signature". Suppose that a signature text work as a public key, we may achive a new digital signature "Meta Signature" such that, the signer of a signature text, in this paper we call basic signature, can sign on to another message by using the basic signature text as the public key of Meta signature scheme. First, we present a concept of Meta Ring Signature such that both basic signature and meta signature are Ring Signature. We then show the example of the way how to construct Meta Ring Signature from LSAG signature and it's application.

Key words　Digital Signature, Signature Text As Public Key, Anonymity, Ring Signature.

1. はじめに

本論文ではメタリング署名の概念を提案し，さらにその具体例を提案する．一般的に，ディジタル署名方式ではまず秘密鍵を決定する．次に秘密鍵を用いて公開鍵を計算する．メッセージに署名を行うには，メッセージと秘密鍵を用いて署名文を計算する．公開鍵，署名文はともに秘密鍵をもとにして計算されたものである．そこで我々はある署名方式の署名文を，公開鍵として用いることができるような署名方式，メタ署名について検討を行った．メタ署名とは，ある署名方式 (基本署名方式) の署名文を公開鍵として用いて，その署名文の署名者のみが新たなメッセージに署名を行えるような署名方式である．このとき，基本署名方式が通常のディジタル署名方式であれば，メタ署名方式は実用上の価値がない．なぜならば基本署名方式の署名文 (メタ署名方式の公開鍵) の基本署名方式での検証を行うために，基本署名方式の公開鍵が必要であるので，メタ署名方式の署名

検証にも基本署名方式の公開鍵が必要であるからである．

基本署名方式がリング署名[2]，グループ署名[1]等の匿名性を有する1 out of n 署名であればメタ署名は有用であろう．この場合，基本署名の署名者は匿名性を失うことなく，他のメッセージに対してメタ署名方式の署名文を生成でき，このとき基本署名文とメタ署名文が同一の署名者によって生成されたことを検証できる．同様の目的を達成できるディジタル署名方式として，リンカブルリング署名[3]，リンカブルグループ署名[4],[5]等がある．

ではさらにメタ署名方式がリング署名であればどうであろうか．基本署名文を複数集めてこれらをメタ署名の公開鍵として扱う．メタ署名の署名者は基本署名文のいずれかの署名者と同一であるが，どの基本署名を生成したのかを特定されることは困難である．このような署名方式を本論文ではメタリング署名と呼ぶ．メタリング署名は基本署名のえらびかたによってさまざまな応用が期待できる．

本論文ではメタリング署名の概念の提案を行う．さらにメタリング署名の実現例として基本署名方式とメタ署名方式の双方をリンカブルリング署名の一種であるLSAG署名を用いて実現したメタLSAG署名を提案し，さらにその応用例を簡単に示唆する．

2. メタリング署名

メタ署名は2つのディジタル署名層，基本署名層およびメタ署名層によって構成される．基本署名層，メタ署名層で使用するディジタル署名方式をそれぞれ，基本署名方式，メタ署名方式と呼ぶ．基本署名方式，メタ署名方式には既存のディジタル署名方式を使用することも可能であるが，場合によっては新たにそれぞれの署名層に用いるための方式を提案する必要があるかもしれない．本論文では基本署名方式，メタ署名方式がともにリング署名であるようなメタ署名をメタリング署名と呼ぶ．

メタ署名層では，基本署名方式の署名文，必要であるならば対応するメッセージとの対で，をメタ署名方式の公開鍵とする．メタ署名層では，複数の基本署名文からなるメタ公開鍵リストが与えられたときに，メタ公開鍵リストに含まれる基本署名文の署名者のみが，メタ署名文を生成できる．基本署名方式がリング署名であれば，検証者は基本署名文，すなわちメタ署名層の公開鍵，の署名者を特定することは困難である．また，メタ署名層がリング署名であれば，メタ署名文の署名者がメタ公開鍵リストに含まれるどの基本署名文の署名者であるかを特定することは困難である．

2.1 基本署名層

メタリング署名の基本署名層は一般的な1 out of n 署名である．本論文では基本署名方式としてリング署名を使用することにする．本節では，まずリング署名の概要と，本論文で用いる記号を示す．

リング署名は，鍵生成アルゴリズム $Gen_B()$，署名文生成アルゴリズム $Sig_B()$，署名文検証アルゴリズム $Ver_B()$ の3つのアルゴリズムから成る．$i = 1, \ldots, n$，を正整数とし，U_i をあるユーザとする．各々のユーザ U_i は鍵生成アルゴリズム $Gen_B()$ を用いて，秘密鍵，公開鍵の対 (x_i, y_i) を計算する．n 人のユーザの公開鍵のリストを $L_B = \{y_1, \ldots, y_n\}$ とする．

あるユーザ U_π，ただし $^\exists\pi \in \{1, \ldots, n\}$ である，はメッセージ m に対して，署名文生成アルゴリズムを用いて署名文 $\sigma(m, L_B) = Sig_B(m, x_\pi, L_B)$ を生成する．

検証者は入手した署名文 $\sigma_B(m, L_B)$ を署名検証アルゴリズム $Ver_B(\sigma(m, L_B), m, L_B)$ を用いて検証する．Ver_B は署名文 $\sigma(m, L_B)$ は，公開鍵リスト L_B に含まれるいずれかの公開鍵の y_i と対になる秘密鍵 x_i を用いて署名文生成が行われたか否かを検証できる．ただし，実際に署名文生成に使用された秘密鍵，あるいは署名者を特定することは困難である．しかし，グループ署名のように特定の管理者によって署名者を特定することができるような方式も存在することに注意されたい．

2.2 メタ署名層

2.2.1 メタ署名層の鍵対

メタ署名方式では，基本署名方式の署名文を公開鍵として使用する．また，メタ署名方式の秘密鍵は基本署名方式の秘密鍵である．メタ署名方式の鍵生成アルゴリズムは基本署名方式の署名文生成アルゴリズムであるとも言える．

$$L_S = \{\sigma^1(m_1, L_B), \ldots, \sigma^j(m_j, L_B), \ldots, \sigma^k(m_k, L_B)\} \tag{1}$$

を k 個の基本署名方式の署名文のリストとする．L_S に含まれる全ての基本署名文は同じ基本署名方式の公開鍵リスト L_B を用いて生成されていることに注意されたい．メタ署名層ではこの基本署名文のリスト L_S をメタ署名方式の公開鍵リストとして使用する．

2.2.2 メタ署名文生成

$Sig_M()$ をメタ署名方式の署名文生成アルゴリズムとする．U_Σ を基本署名文 $\sigma^\Sigma(m_\Sigma, L_B)$ の署名者とする．$\sigma^\Sigma(m_\Sigma, L_B)$ が L_S に含まれている場合に限り U_Σ はメッセージ m' に対する署名文

$$\sigma_M(m', L_S) = Sig_M(m', x_\Sigma, L_S) \tag{2}$$

を生成できる．このとき，U_Σ は基本署名文 $\sigma^\Sigma(m_\Sigma, L_B)$ を生成するのに用いた秘密鍵 x_Σ を用いてメタ署名文 $\sigma_M(m', L_S)$ を生成している．

2.2.3 メタ署名文検証

$Ver_M()$ をメタ署名方式の署名文検証アルゴリズムとする．検証者はメタ署名文 $\sigma_M(m', L_S)$ を

$$Ver_M(\sigma_M(m', L_S), m', L_S) \tag{3}$$

のように検証する．L_S に含まれる基本署名文のうちのいずれかひとつを生成するのに用いた秘密鍵 x_j を用いてメタ署名文 $\sigma_M(m', L_S)$ が生成されているのならば，署名文検証アルゴリズム $Ver_M()$ は $\sigma_M(m', L_S)$ を受理し，さもなくば $\sigma_M(m', L_S)$ を棄却する．

2.3 安全性要件

基本署名層の安全性要件は使用した基本署名方式に依存する．メタ署名層の安全性要件は基本署名層，または応用方式によってさまざまな場合が考えられるので，メタ署名方式として最低

限必要と思われる安全性要件に関してのみ述べる.

メタ非可鍛性　与えられた基本署名文リストを用いてメタ署名文を生成できるのは，基本署名文リストに含まれる署名文のいずれかの署名者のみである.

基本署名文特定不能性　与えられたメタ署名文の署名者が基本署名文リストに含まれるどの基本署名文を生成したのか特定することは困難である.

3. メタリング署名実現例

本章では Liu, Wei, Wong が提案した最初のリンカブルリング署名方式である LSAG 署名 [3] をもとにしたメタリング署名方式の構成方法の例を示す.

3.1 LSAG 署名

本節では LSAG 署名の概要を紹介する．詳細は [3] を参照されたい．LSAG 署名は以下の安全性要件を満たす.

非可鍛性 (Existentional Unforgeability)　公開鍵リストを与えられたときに，対応する秘密鍵を知らない攻撃者はいかなるメッセージに対しても署名文を生成できない.

署名者匿名性 (Signer Ambiguity)　何人も与えられた署名文の署名者を特定できない.

同一署名者判別可能 (Linkability)　同一の公開鍵リストを用いて生成された 2 つの異なる署名文が，同じ署名者によって生成されたか否かを判定できる.

$G = \langle g \rangle$ を素数位数 q の群，g をその生成元とする．$H_1 : \{0,1\}^* \to \mathbb{Z}_q$，$H_2 : \{0,1\}^* \to G$ をハッシュ関数とする．$i = 1, \ldots, n$ のとき，各ユーザ U_i はそれぞれの秘密鍵 x_i を選び，公開鍵 $y_i = g^{x_i}$ を計算する．$L = \{y_1, \ldots, y_n\}$ を n 人のユーザ全員の公開鍵のリストとする.

3.1.1 署名文生成

あるユーザ U_π はメッセージ $m \in \{0,1\}^*$ に対する署名文 $\sigma(m, L) = LsagSig(m, x_\pi, L)$ を以下のようにして生成する.

Step 1 : $h = H_2(L)$ と $\tilde{y} = h^{x_\pi}$ を計算する.

Step 2 : 乱数 $u \in \mathbb{Z}_q$ を選び，

$$c_{\pi+1} = H_1\left(L, \tilde{y}, m, g^u, h^u\right) \tag{4}$$

を計算する.

Step 3 : $i = \pi+1, \ldots, n, 1, \ldots, \pi-1$ それぞれについて乱数 $s_i \in \mathbb{Z}_q$ を選び，

$$c_{i+1} = H_1\left(L, \tilde{y}, m, g^{s_i} y_i^{c_i}, h^{s_i} \tilde{y}^{c_i}\right) \tag{5}$$

を計算する.

Step 4 : $s_\pi = u - x_\pi c_\pi \mod q$, を計算して，署名文

$$\sigma(m, L) = \{c_1, s_1, \ldots, s_n, \tilde{y}\} \tag{6}$$

を出力する.

3.1.2 署名文検証

署名文 $\sigma(m, L)$ を入手した検証者は署名文検証アルゴリズム $LsagVer(\sigma(m, L), m, L)$ を用いて以下のように署名文の検証を行う.

Step 1 : $h = H_2(L)$ を計算する.

Step 2 : $i = 1, \ldots, n$ それぞれについて，$z_i' = g^{s_i} y_i^{c_i}$，$z_i'' = h^{s_i} \tilde{y}^{c_i}$，および

$$c_{i+1} = H_1\left(L, \tilde{y}, m, z_i', z_i''\right) \tag{7}$$

を計算する.

Step 3 : $c_1 = H_1\left(L, \tilde{y}, m, z_n', z_n''\right)$ が成り立つならば $\sigma(m, L)$ を受理し，さもなくば棄却する.

3.1.3 リンク

2 つの署名文 $\sigma'(m', L) = \{c_1', s_1', \ldots, s_n', \tilde{y}'\}$ と $\sigma''(m'', L) = \{c_1', s_1'', \ldots, s_n'', \tilde{y}''\}$ を前節の署名文検証アルゴリズムを用いて受理された，同一の公開鍵リスト L を用いて生成された 2 つの異なる署名文とする．$\tilde{y}' = \tilde{y}''$ ならば $\sigma_L'(m')$ と $\sigma_L''(m'')$ の署名者は同一のユーザである．さもなくば，$\sigma_L''(m'')$ の署名者は互いに異なるユーザである.

3.2 メタ LSAG 署名

本節では LSAG 署名をもとにして，メタ LSAG 署名を実現する方法を提案する．提案メタ署名の基本署名方式，メタ署名方式はともに LSAG 署名である.

$$L_S = \{\sigma^1(m_1, L), \ldots, \sigma^j(m_j, L), \ldots, \sigma^k(m_k, L)\} \tag{8}$$

を k 個の基本 LSAG 署名文リストとする．ただし，それぞれの基本署名文はメッセージ m_j に対して

$$\sigma^j(m_j, L) = \{c_{(j,1)}, s_{(j,1)}, \ldots, s_{(j,n)}, \tilde{y}_j\} \tag{9}$$

のように生成されている．L_S に含まれる全ての基本署名文は同一の公開鍵リスト L を用いて生成されている．$L_S' = \{\tilde{y}_1, \ldots, \tilde{y}_j, \ldots, \tilde{y}_k\}$ を L_S に含まれる基本署名文 $\sigma^j(m_j, L)$ の最後の要素 $\tilde{y}_j$ のみを取り出したもののリストとする．メタ署名方式では，L_S' を公開鍵リストとして使用する.

3.2.1 メタ署名文生成

あるユーザ U_Σ は SAG 署名の署名文生成アルゴリズムを用いてメッセージ $m_M \in \{0,1\}^*$ に対するメタ署名文 $\sigma_M(m_M, L_S') = LsagSig(m_M, x_\Sigma, L_S')$ を計算する.

3.2.2 メタ署名文検証

メタ署名文 $\sigma_M(m_M, L_S')$ を入手した検証者は，LSAG 署名の署名文検証アルゴリズム $LsagVer(\sigma_M(m_M, L_S'), m_M, L_S')$ を用いて $\sigma_M(m_M, L_S')$ の検証を行う.

3.3 安全性

メタ非可鍛性　メタ LSAG 署名の基本署名方式，メタ署名方式はともに LSAG 署名である．もしメタ非可鍛性を破る攻撃者，すなわちメタ署名文を偽造することが可能である攻撃者がが存在するならば，その攻撃者は LSAG 署名の署名文を偽造することが可能である．しかしながら LSAG 署名は非可鍛性を有するのでメタ LSAG 署名はメタ非可鍛性を満たす.

基本署名文特定不能性　もし基本署名文特定不能性を破る攻撃者，すなわち与えられたメタ署名文の署名者が生成した基本署名文を，基本署名文リストの中から特定することが可能である攻撃者がが存在するならば，その攻撃者はLSAG署名の署名者を特定することが可能である．しかしながらLSAG署名は署名者匿名性を満たすのでメタLSAG署名は基本署名文特定不能性を満たす．

3.4 メタLSAG署名応用

本節ではメタLSAG署名の応用例として，リンカブルグループ署名方式の概要を示す．詳細については稿を改めて報告する予定である．メタLSAG署名方式にメタ署名文の署名者が自ら名乗り出ることのできるような署名者公表手順を併用することによって，リンカブルグループ署名を実現する．一般的にグループ署名では，管理者のみが署名者を特定することが可能であるが，LSAG署名はそのような機能を有してはいない．そこで，リンカブルグループ署名の鍵生成，署名文生成，署名文検証および，リンクを基本署名層のLSAG署名方式で実現し，署名者特定機能をメタ署名層と，その署名者公表手順を用いて実現する．

$\sigma(m,L)$ と $\sigma'(m',L)$ をLSAG署名方式の署名文とする．ユーザ U_i は $\sigma(m,L)$ の署名者であるとする．ユーザ U_i がなんらかの方法で自らが $\sigma(m,L)$ の署名者であることを証明することができれば，ユーザ U_i が $\sigma'(m',L)$ の署名者であることを否認できる．このことはLSAG署名が同一署名者判別可能であることから明らかであろう．$\sigma'(m',L)$ の署名者以外の全てのユーザが上記のように署名者であることの否認を行えば，$\sigma'(m',L)$ の署名者が特定される．しかしながらこのような方法では署名者匿名性を失うことになる．そこで，以下のようにメタLSAG署名を用いれば，署名者匿名性を失うことなくユーザ U_i が $\sigma'(m',L)$ の署名者であることを否認することができる．

まず，U_i は $\sigma'(m',L)$ の署名者以外のユーザが生成した署名文を集めて，基本署名文リスト L'_S をつくる．次に，ユーザ U_i はメタ署名文 $\sigma^i_M(m_i,L'_S)$ を生成する．最後にユーザ U_i がメタ署名文 $\sigma^i_M(m_i,L'_S)$ を自分自身が生成したことをなんらかの方法，例えば零知識対話型証明など，を用いて検証者に証明する．検証者は メタ署名文 $\sigma^i_M(m_i,L'_S)$ の署名者がユーザ U_i であることを検証した後に，署名文リスト L_S に含まれる全ての基本署名文と $\sigma'(m',L)$ のリンクを行い，L_S に含まれるいずれの基本署名文も $\sigma'(m',L)$ の署名者以外が生成したことを確認する．このようにしてユーザ U_i は $\sigma'(m',L)$ の署名者であることを否認する．

以上のようにして実現されたリンカブルグループ署名方式には，署名者を特定する特別な管理者が必要でない．

4. まとめ

本論文ではメタリング署名の概念の提案を行った．さらにメタリング署名の実現例として基本署名方式とメタ署名方式の双方をリンカブルリング署名の一種であるLSAG署名を用いて実現したメタLSAG署名を提案し，さらにその応用例をとして，管理者不要リンカブルリング署名方式の概要を示唆した．管理者不要リンカブルリング署名に関する詳細な検討と，他の署名方式をもとにしたメタ署名方式の考察を今後の課題とする．

文　献

[1] D. Chaum, E. van Heijst, "Group Signature", Advances in Cryptology - EUROCRYPTO '91, pp.257–265,Springer-Verlag ,1991.

[2] R. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret", ASIACRYPTO 2001, pp.552–565, Springer-Verlag, 2001. LNCS Vol. 2248.

[3] J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups", ACISP 2004, pp.325–335, Springer-Verlag Berlin, 2004. LNCS Vol. 3108.

[4] T. Nakanishi,T. Fujiwara,H. Watanabe, "A Linkable Group Signature and Its Application to Secret Voting", Trans. IPSJ, Vol.40,No.7, pp.3085-3096, 1999.

[5] H. Okazaki, R. Sakai, K.Shibayama, M. Kasahara, "A Linkable Group Signature Scheme Based on Weil Pairing", IEICE Trans. Vol.J87-A No.4, pp.563–568, 2004. (in Japanese)