近隣サービスで同時検証するためのマルチグループ署名

野村 健太[†1]　毛利 公美[†2]　白石 善明[†1]　森井 昌克[†1]

概要：多種多様な機器がインターネットに接続される IoT(Internet of Things)の環境ではリソースが限られた機器からの情報発信がある．そういった機器が地理的に近接したノードへ同報通信するときの電子署名の構成を本論文では与える．複数の公開鍵ペアの異なる秘密鍵の和を用いることで複数の検証者に対応できるマルチグループ認証方式が提案されている．本論文ではマルチグループ認証方式からマルチグループ署名方式を構成するための変換方法を示す．マルチグループ署名方式では複数の秘密鍵を用いて一つのメッセージに署名し，複数の検証者が一つの署名で検証できる．そして，もとにしたマルチグループ認証方式が IMP-PA（impersonation against passive attacks）安全ならば，変換後のマルチグループ署名方式がランダムオラクルモデルにおいて EUF-CMA（existentially unforgeable against chosen-message attacks）安全であることを証明する．具体的な構成例としてある誤り訂正符号に基づくマルチグループ認証方式を変換し，マルチグループ署名方式を構成した例を示す．

キーワード：Internet of Things，同報通信，電子署名，Fiat-Shamir 変換，省電力

Multi-Group Signature Scheme for Simultaneous Verification by Neighbor Services

Kenta Nomura[†1]　Masami Mohri[†2]　Yoshiaki Shiraishi[†1]　Masakatu Morii[†1]

Abstract: We focus on the construction of the digital signature scheme for local broadcast, which allows the devices with limited resources to securely transmit broadcast message. A multi-group authentication scheme that enables a node to authenticate its membership in multi verifiers by the sum of the secret keys has been proposed for limited resources. This paper presents a transform which convert a multi-group authentication into a multi-group signature scheme. We show that the multi-group signature scheme converted by our transform is existentially unforgeable against chosen message attacks (EUF-CMA secure) in the random oracle model if the multi-group authentication scheme is secure against impersonation under passive attacks (IMP-PA secure). In the multi-group signature scheme, a sender can sign a message by the secret keys which multiple certification authorities issue and the signature can validate the authenticity and integrity of the message to multiple verifiers. As a specific configuration example, we show the example in which the multi-group signature scheme by converting an error correcting code-based multi-group authentication scheme.

Keywords: Internet of Things, Local broadcast, Digital signature, Fiat-Shamir Transform, Low energy

1. はじめに

Internet of Things (IoT) では様々なデバイスやセンサがインターネットに繋がり，取得した情報をデータとしてクラウドへ送信したり周囲のデバイスへ発信したりする．また，そのようにして収集されたデータを取得しデバイスの動作や制御に利用することもある．そのような IoT 社会では各デバイス間が正しく認証されることが不可欠である．このとき，独立したアプリケーションやサービスでは異なる秘密情報によって認証を行うのが望ましい．公開鍵を用いた認証で，認証される側（認証者）が秘密鍵と公開鍵のペアを，認証を行う側（検証者）は公開鍵を持ち，そして認証者と検証者のやり取りで認証者が公開鍵に対応する秘密鍵を確かに持っていることを検証者が確認する場合，検証者であるアプリケーションのシステムはそれぞれ独自の公開鍵基盤（Public Key Infrastructure, PKI）を持ち，認証者はアプリケーション毎に異なる秘密鍵と公開鍵のペアを用の安全性については，Pointc

そのような環境ではアプリケーションやサービスの種類の増加に伴い，認証に用いる送信データ量も比例的に増加する．また，あるアプリケーションに対して単一の秘密情報によって認証者の正当性を保証しているため，秘密鍵が漏洩するとそのアプリケーションに対してなりすましが可能となる．そこで認証者が持つ異なる公開鍵ペアの秘密鍵の総和を用いて認証を行うマルチグループ認証が提案されている[1]．この方式では一般的なサービス毎の認証を行う方式と比べ送信データ量の増加が抑えられることが示されている．また，複数の秘密鍵の和によって認証を行うため，認証者が持つ秘密鍵が全て漏洩しない限りなりすましが不可能である．

一方で，送受信したデータによって制御を行う IoT 機器の中には偽のデータに含まれる誤った情報により深刻なトラブルが引き起こされるものがある．データが改ざんされていないことを保証する電子署名は，認証と同様にアプリケーションやサービス毎に異なる鍵のペアを用意するのが一般的である．その場合，同一のデータであっても送信先が異なればその相手の数だけ繰り返し電子署名を作成することになる．そこでマルチグループ認証方式のように複数の鍵を用いて署名を作成し，複数の検証者に一つの署名文を検証可能とするマルチグループ署名方式を考える．

本稿では対話型認証方式から署名方式を構成する

†1 神戸大学
Kobe University
†2 岐阜大学
Gifu University

Fiat-Shamir 変換[2]を元に，マルチグループ認証方式からマルチグループ署名方式を構成する変換法を示し，安全性証明を与える．その変換法を用いて，複数の秘密鍵を用いて署名を行い，複数の検証者が同時に検証できる一つの署名を作成できる具体的なマルチグループ署名方式を示す．単一の秘密鍵を用いる方式を繰り返し適用した場合と送信データ量を比較することで，マルチグループ署名方式が効率的な署名方式であることを示す．

2. 認証方式

2.1 認証方式の分類

証明者の正当性を確認する認証方式を分類すると主に，ID とパスワードを用いる（[3]-[6]など），公開鍵ベース（[7]-[9]など），さらに証明者と検証者のやり取りによる対話型プロトコルによる方式がある．ゼロ知識対話証明による認証方式の中では，例えば文献[10]はエネルギー効率の点からリソース制約のあるワイヤレスセンサーネットワーク向けに設計している．それに関連して，符号ベースの認証方式が Stern[11]より提案され，それを元により効率的な方式が提案されている[12]-[15].

利用モデルとして 1 人の証明者が 1 人の検証者に認証される最も単純なモデルから，ユースケースの拡大やアプリケーションの多様化に伴い，複数の証明者・検証者向けの方式が提案されるようになった．証明者が複数存在する例として，インターネット利用者の増加に対応するため複数の証明者が認証サーバに情報を送り，システムが同時に認証する方式[16]や，複数の証明者が同一グループに属しているかを認証する方式[17],[18]が提案されている．また検証者が複数存在する例として，異なる秘密鍵の和を用いることで複数の検証者に対応できるマルチグループ認証方式[1]が提案されている．

2.2 エンティティ

認証方式は認証を受ける側の証明者，認証を行う側の検証者によって構成される．本稿では証明者と検証者の 3 回のやり取りによって認証を行う方式に着目する．

[証明者]認証要求としてコミットメントを送信し，秘密鍵と検証者から受け取ったチャレンジをもとにレスポンスを生成し，検証者に送信する．

[検証者]コミットメントを送信した証明者に対し，乱数であるチャレンジを返信する．証明者から受け取ったレスポンスと公開鍵，コミットメント，チャレンジから得られるレスポンスが矛盾していないかを確認し，正しければ証明者を認証する．

2.3 単一の公開鍵ペアを用いる認証方式

2.3.1 アルゴリズム

証明者と検証者の 3 回のやり取りで証明者の正当性を証明する認証方式IDは 5 つのアルゴリズム(K, Co, Ch, R, V_A)から構成される．Kはセキュリティパラメータ1^kを入力とし，公開鍵・秘密鍵の鍵ペア(pk, sk)を出力する．コミットメントアルゴリズムCoはskを入力とし，検証者に送信するコミットメントCmtを出力する．チャレンジアルゴリズムChはチャレンジの長さcを入力とし，cビットのランダムな文字列Chを出力する．レスポンスアルゴリズムRは(sk, Ch)を入力とし，レスポンスRspを出力する．検証アルゴリズムV_Aは検証者が証明者を検証するためのアルゴリズムである．(pk, Cmt, Ch, Rsp)を入力とし，Rspを(pk, Cmt, Ch)によるレスポンスの計算結果と比較する．一致したとき，またそのときに限り 1 を出力する．Co，Rは証明者によって実行され，Ch，Vは検証者によって実行される．

2.3.2 安全性定義

認証方式においては鍵を持たない不正者による正しい証明者へのなりすましを防ぐことになる．認証方式の IMP-PA（impersonation against passive attacks）安全性[19]は次のように定義されている．

定義 1 認証方式の IMP-PA 安全性

$ID = (K, Co, Ch, R, V_A)$を認証方式，Iをなりすましを行う攻撃者，stを状態，kをセキュリティパラメータとする．このときIの優位性は

$$\mathbf{Adv}^{\mathrm{ima-pa}}_{ID,I}(k) = \Pr\left[\mathbf{Exp}^{\mathrm{ima-pa}}_{ID,I}(k)\right]$$

と定義できる．ここで，実験$\mathbf{Exp}^{\mathrm{ima-pa}}_{ID,I}(k)$は以下で定義される．

実験 $\mathbf{Exp}^{\mathrm{ima-pa}}_{ID,I}(k)$

$(pk, sk) \xleftarrow{\$} K(k);\ st \| Cmt \xleftarrow{\$} I^{\mathrm{Tr}^{ID}_{pk,sk,k}(pk)}$

$Ch \xleftarrow{\$} \{0,1\}^{c(k)};\ Rsp \xleftarrow{\$} I(st, Ch)$

Dec $\leftarrow V_A(pk, Cmt \| Ch \| Rsp)$; return Dec

また，ここで$\mathrm{Tr}^{ID}_{pk,sk,k}$は”honest”な出力を返答する transcript オラクルとし，以下のような動作を行う．

オラクル $\mathrm{Tr}^{ID}_{pk,sk,k}$

$R_p \xleftarrow{\$} \mathrm{Coins}_P(k)$

$Cmt \leftarrow Co(sk; R_p);\ Ch \xleftarrow{\$} \{0,1\}^{c(k)}$

$Rsp \leftarrow R(sk, Cmt \| Ch; R_P)$

return $Cmt \| Ch \| Rsp$

$\mathbf{Adv}^{\mathrm{ima-pa}}_{ID,I}(k)$が任意の確率的多項式時間の攻撃者に対して無視できるとき，IDは受動攻撃に対してなりすましが不可（IMP-PA 安全）であるという．

2.4 マルチグループ認証

異なる認証サービスのそれぞれで異なる公開鍵ペアを使用，すなわち複数の公開鍵ペアを所有している場合，同時に複数の認証サービスを受けるならば 2.3 節の認証では鍵ペアの個数だけプロトコルを実行しなければならない．そこで複数の鍵を同時に認証することが可能なマルチグループ認証方式[1]が提案された．マルチグループ認証では複数の秘密鍵の保持を証明することで複数の検証者に対して同時に認証が可能となる．

2.4.1 アルゴリズム

マルチグループ認証方式$mg-ID$は 5 つのアルゴリズム$(mgK, mgCo, Ch, mgR, mgV)$から構成される．チャレンジアルゴリズム$Ch$は 2.3.1 項におけるものと同様とする．鍵生成アルゴリズムmgKはセキュリティパラメータ1^k及び検証者の数Mを入力とし，KをM回分実行することでM個の公開鍵・秘密鍵の鍵ペア(pk, sk)を出力する．コミットメントアルゴリズム$mgCo$は認証に用いるN個のskを入力とし，検証者に送信するコミットメントCmtを出力する．レスポンスアルゴリズムmgRは$mgCo$で用いたN個のsk及びChを入力とし，レスポンスRspを出力する．検証アルゴリズムmgVは認証に用いるN個のskに対応したpk及び(Cmt, Ch, Rsp)を入力とし，Rspを(pk, Cmt, Ch)によるレスポンスの計算結果と比較する．すなわち，一致したとき，またそのときに限り 1 を出力する．$mgCo$，mgRは証明者によって実行され，Ch，mgVは検証者によって実行される．

2.4.2 安全性定義

マルチグループ認証方式の IMP-PA 安全性を定義する．定義 1 では一つの鍵ペアに対してなりすましを試みていたが，次の定義 2 ではN組の鍵のペアを持つ証明者のなりすましを行う．そのため，transcript オラクルからはN個の秘

密鍵を持つ証明者の”honest”な出力を得られるものとする．

定義 2 マルチグループ認証方式の IMP-PA 安全性

$mg-ID=(mgK,mgCo,Ch,mgR,mgV)$をマルチグループ認証方式，$I$をなりすましを行う攻撃者，$st$を状態，$k$をセキュリティパラメータとする．また，$I$は$N$個の秘密鍵を持つ正当な証明者$P$をなりすましの対象とする．このとき$I$の優位性は

$$\mathbf{Adv}^{\mathrm{ima-pa}}_{mg-ID,I}(k)=\Pr\left[\mathbf{Exp}^{\mathrm{ima-pa}}_{mg-ID,I}(k)\right]$$

と定義できる．ここで，実験$\mathbf{Exp}^{\mathrm{ima-pa}}_{mg-ID,I}(k)$は以下で定義される．

実験 $\mathbf{Exp}^{\mathrm{ima-pa}}_{mg-ID,I}(k)$

$\{(pk,sk)\}^M \xleftarrow{\$} mgK(k,M)$

$st \parallel Cmt \xleftarrow{\$} I^{\mathrm{Tr}^{mg-ID}_{N,pk,sk,k}}(\{pk\}^N)$

$Ch \xleftarrow{\$} \{0,1\}^{c(k)};\ Rsp \xleftarrow{\$} I(st,Ch)$

Dec $\leftarrow mgV(\{pk\}^N, Cmt \parallel Ch \parallel Rsp)$; return Dec

また，ここで$\mathrm{Tr}^{mg-ID}_{N,pk,sk,k}$は”honest”な出力を返答する transcript オラクルとし，以下のような動作を行う．

オラクル $\mathrm{Tr}^{mg-ID}_{N,pk,sk,k}$

$R_p \xleftarrow{\$} \mathrm{Coins}_P(k)$

$Cmt \leftarrow mgCo(\{sk\}^N; R_p); Ch \xleftarrow{\$} \{0,1\}^{c(k)}$

$Rsp \leftarrow mgR(\{sk\}^N, Cmt \parallel Ch; R_P)$

return $Cmt \parallel Ch \parallel Rsp$

$\mathbf{Adv}^{\mathrm{ima-pa}}_{mg-ID,I}(k)$が任意の確率的多項式時間の攻撃者に対して無視できるとき，$mg-ID$は受動攻撃に対してなりすましが不可である（IMP-PA 安全）といえる．

3. 署名方式

3.1 エンティティ

署名方式は署名を行う署名者とその署名が正当なものかを検証する検証者によって構成される．

[署名者]秘密鍵を用いて文書に署名する．

[検証者]公開鍵を用いて署名が特定の文書の署名として正しいものであるかを検証する．

3.2 単一の公開鍵ペアを用いる署名方式

3.2.1 アルゴリズム

署名方式DSは 3 つのアルゴリズム(K,S,V_s)から構成される．鍵生成アルゴリズムKはセキュリティパラメータ1^kを入力とし，公開鍵・秘密鍵の鍵ペア(pk,sk)を出力する．署名アルゴリズムSはsk及びメッセージmを入力とし，署名σを出力する．検証アルゴリズムV_sは(pk,m,σ)を入力とし，σがpkにおけるmの署名であるとき，またそのときに限って 1 を出力する．

3.2.2 安全性定義

署名方式の安全性は偽造の困難性及び攻撃方法によって定義される．定義 3 でランダムオラクルモデル[20]上での署名方式の EUF-CMA（existentially unforgeable under adaptive chosen-message attacks）安全性[21]の定義を示す．攻撃者Fは署名オラクル及びランダムオラクルを利用可能であるとし，新しいメッセージに対して正当な署名を出力できるならばFは勝利となる．$[\{0,1\}^* \to [0,1]^c]$を$\{0,1\}^*$から$[0,1]^c$への全ての写像の集合と定義する．全ての写像の集合からランダムにハッシュ関数hを選ぶことを$h \xleftarrow{\$} [\{0,1\}^* \to [0,1]^c]$と表記する．

定義 3 署名方式の EUF-CMA 安全性

$DS=(K,S,V_s)$を署名方式，Fを偽造文を作成する攻撃者，kをセキュリティパラメータとする．実験$\mathbf{Exp}^{\mathrm{euf-cma}}_{DS,I}(k)$は以下で定義される．

実験 $\mathbf{Exp}^{\mathrm{euf-cma}}_{DS,I}(k)$

$h \xleftarrow{S} [\{0,1\}^* \to [0,1]^c]$

$(pk,sk) \xleftarrow{\$} K(k);\ (m,\sigma) \xleftarrow{\$} F^{S^h_{sk}(\cdot),h(\cdot)}(pk)$

Dec $\leftarrow V^h_s(pk,m,\sigma)$

mがすでに$S^h_{sk}(\cdot)$へクエリとして要求されているならば0を出力する．そうでなければDecを出力する．

Fの優位性は

$$\mathbf{Adv}^{\mathrm{euf-cma}}_{DS,F}(k)=\Pr\left[\mathbf{Exp}^{\mathrm{euf-cma}}_{DS,F}(k)=1\right]$$

と定義でき，$\mathbf{Adv}^{\mathrm{euf-cma}}_{DS,F}(k)$が任意の多項式時間攻撃者$F$に対しても無視できるとき，$DS$は選択文書攻撃に対して存在的偽造不可（EUF-CMA 安全）であるという．

3.3 マルチグループ署名方式

3.3.1 アルゴリズム

マルチグループ署名方式$mg-DS$は 3 つのアルゴリズム(mgK,mgS,mgV_s)から構成される．鍵生成アルゴリズムmgKはセキュリティパラメータ1^k及び検証者の数Mを入力とし，M個の公開鍵・秘密鍵の鍵ペア(pk,sk)を出力する．mgSは署名するN個のsk及びメッセージmを入力とし，署名σを出力する．mgV_sは証明するN個のskに対応したpk及び(m,σ)を入力とし，σがpkにおけるmの署名であるとき，またそのときに限って 1 を出力する．また，mgSとmgV_sは関数$h:\{0,1\}^* \to \{0,1\}^{c(k)}$へアクセスするオラクルを持つ．

3.3.2 安全性定義

定義 4 で，ランダムオラクルモデル上でのマルチグループ署名方式の EUF-CMA（existentially unforgeable under adaptive chosen-message attacks）安全性を定義する．定義 3 では 1 つの秘密鍵によって得られる署名を偽造対象としていたが，定義 4 ではN個の秘密鍵による署名を偽造対象とする．そのためN個の秘密鍵によって署名された正当な署名が得られる署名クエリが利用できると仮定する．

定義 4 マルチグループ署名方式の EUF-CMA 安全性

$mg-DS=(mgK,mgS,mgV_s)$をマルチグループ署名方式，Fを偽造文を作成する攻撃者，kをセキュリティパラメータとする．実験$\mathbf{Exp}^{\mathrm{euf-cma}}_{mg-DS,I}(k)$は以下で定義される．

実験 $\mathbf{Exp}^{\mathrm{euf-cma}}_{mg-DS,I}(k)$

$h \xleftarrow{S} [\{0,1\}^* \to [0,1]^c]$

$\{(pk,sk)\}^N \xleftarrow{\$} mgK(k,N);\ (m,\sigma) \xleftarrow{\$} F^{S^h_{N,sk}(\cdot),h(\cdot)}(\{pk\}^N)$

Dec $\leftarrow mgV^h_s(\{pk\}^N,m,\sigma)$

mがすでに$S^h_{N,sk}(\cdot)$へクエリとして要求されているならば0を出力する．そうでなければDecを出力する．

Fの優位性は

$$\mathbf{Adv}^{\mathrm{euf-cma}}_{mg-DS,F}(k)=\Pr\left[\mathbf{Exp}^{\mathrm{euf-cma}}_{mg-DS,F}(k)=1\right]$$

と定義でき，$\mathbf{Adv}^{\mathrm{euf-cma}}_{mg-DS,F}(k)$が任意の多項式時間攻撃者$F$に対しても無視できるとき，$mg-DS$は選択文書攻撃に対して存在的偽造不可（EUF-CMA 安全）であるという．

4. マルチグループ署名方式を構成する変換法

Fiat-Shamir 変換（以下，FS 変換）[2]は認証方式から署名方式を構成する手法である．FS 変換によって構成された署名の安全性については，Pointcheval ら[22]によって，認証方式が正当な検証者に対してゼロ知識証明であるとき，ランダムオラクルモデルにおいて選択文書攻撃に対して存在的偽造不可（EUF-CMA 安全）であることが示されている．また，Abdalla ら[23]は上記の条件を緩和し，「FS 変換

ゲーム G_0
Initialize
000 $(pk, sk) \xleftarrow{\$} mgK(k); hc \leftarrow 0; sc \leftarrow 0$
001 $fp \xleftarrow{\$} \{1, \dots, 1 + q_h(k)\}$
002 $Ch^* \xleftarrow{\$} \{0,1\}^{c(k)}$
003 For $i = 1, \dots, q_s(k)$ do
004 $R_P^i \xleftarrow{\$} \mathrm{Coins}_P(k)$
005 $TCmt_i \xleftarrow{\$} mgCo(\{sk\}^N; R_P^i)$
006 $TCh_i \xleftarrow{\$} \{0,1\}^{c(k)}$
007 $TRsp_i \leftarrow mgR(\{sk\}^N, TCmt_i \parallel TCh_i; R_P^i)$
008 return pk

On H-query x
010 If $\mathrm{HT}[x] = \perp$ Then
011 $hc \leftarrow hc + 1; \mathrm{QT}[hc] \leftarrow x$
012 If $hc \neq fp$ Then
013 $y \xleftarrow{\$} \{0,1\}^{c(k)}; \mathrm{HT}[x] \leftarrow y$
014 Else $\mathrm{HT}[x] \leftarrow Ch^*$
015 return $\mathrm{HT}[x]$

On Sign-query M
020 $sc \leftarrow sc + 1; R \xleftarrow{\$} \{0,1\}^s$
021 $x \leftarrow R \parallel TCmt_{sc} \parallel m$
022 $\mathrm{HT}[x] \leftarrow TCh_{sc}$
023 return $R \parallel TCmt_{sc} \parallel TRsp_{sc}$

Finalize (M, σ)
030 Parse σ as $R \parallel Cmt \parallel Rsp$
031 Let i such that $\mathrm{QT}[i] = R \parallel Cmt \parallel m$
032 If $i \neq fp$ Then **bad** $\leftarrow$ true
033 return $V(\{pk\}^N, Cmt \parallel Ch^* \parallel Rsp)$

ゲーム G_1/G_2
Initialize
100 $(pk, sk) \xleftarrow{\$} mgK(k); hc \leftarrow 0; sc \leftarrow 0$
101 For $i = 1, \dots, q_s(k)$ do
102 $R_P^i \xleftarrow{\$} \mathrm{Coins}_P(k)$
103 $TCmt_i \xleftarrow{\$} mgCo(\{sk\}^N; R_P^i)$
104 $TCh_i \xleftarrow{\$} \{0,1\}^{c(k)}$
105 $TRsp_i \leftarrow mgR(\{sk\}^N, TCmt_i \parallel TCh_i; R_P^i)$
106 return pk

On H-query x
110 If $\mathrm{HT}[x] = \perp$ Then
111 $hc \leftarrow hc + 1; \mathrm{QT}[hc] \leftarrow x$
112 $\mathrm{HT}[x] \xleftarrow{\$} \{0,1\}^{c(k)}$
113 return $\mathrm{HT}[x]$

On Sign-query M
120 $sc \leftarrow sc + 1; R \xleftarrow{\$} \{0,1\}^s$
121 $x \leftarrow R \parallel TCmt_{sc} \parallel m$
122 $\mathrm{HT}[x] \leftarrow TCh_{sc}$
123 return $R \parallel TCmt_{sc} \parallel TRsp_{sc}$

Finalize (M, σ)
130 Parse σ as $R \parallel Cmt \parallel Rsp$
131 Let i such that $\mathrm{QT}[i] = R \parallel Cmt \parallel m$
132 $Ch^* \xleftarrow{\$} \mathrm{HT}[\mathrm{QT}[i]]$
133 $fp \xleftarrow{\$} \{1, \dots, 1 + q_h(k)\}$
134 If $i \neq fp$ Then
135 **bad** $\leftarrow$ true ; $Ch^* \xleftarrow{\$} \mathrm{HT}[\mathrm{QT}[fp]]$
136 return $V(\{pk\}^N, Cmt \parallel Ch^* \parallel Rsp)$

図1 ゲームG_0, G_1及びG_2

による署名がランダムオラクルモデルにおいて EUF-CMA 安全であることと，元の認証方式が受動攻撃に対してなりすましが不可（IMP-PA 安全）であることが等価であること」(*) を示した．本稿では命題 (*) がマルチグループにおいても成り立つことを示す．

4.1 マルチグループ認証方式から署名方式への変換法

FS 変換によってマルチグループ認証方式から 3.3 節の定義に沿ったマルチグループ署名方式を構成する手法を示す．

$mg - ID = (mgK, mgCo, Ch, mgR, mgV_A)$をマルチグループ認証方式，$s$をシード長と呼ばれる関数とする．署名方式は認証方式と同じ鍵生成アルゴリズムを持ち，ハッシュ関数hの出力長は認証方式におけるチャレンジの出力長と同じ長さである．署名・検証アルゴリズムは以下で定義される．

署名アルゴリズム$mgS^h(\{sk\}^N, m)$
$R \xleftarrow{\$} \{0,1\}^{s(k)}; R_p \xleftarrow{\$} \mathrm{Coins}_P(k)$
$Cmt \leftarrow mgCo(\{sk\}^N; R_p)$
$Ch \leftarrow h(R \parallel Cmt \parallel m)$
$Rsp \leftarrow mgR(\{sk\}^N, Cmt \parallel Ch; R_p)$
return $R \parallel Cmt \parallel Rsp$

検証アルゴリズム$mgV_s^h(\{pk\}^N, m, \sigma)$
parse σ as $R \parallel Cmt \parallel Rsp$
$Ch \leftarrow h(R \parallel Cmt \parallel m)$
Dec $\leftarrow mgV_A(\{pk_i\}_{i=1}^N, Cmt \parallel Ch \parallel Rsp)$
return Dec

署名アルゴリズムを無作為化するためにハッシュ関数の入力に$s(k)$ビットの乱数を追加する．またその乱数を署名の一部に含むことで検証を可能としている．上記の変換によってマルチグループ認証方式からマルチグループ署名方式$mg - DS = (mgK, mgS^h, mgV_s^h)$が構成される．

4.2 安全性

文献[23]で引用されているように，本稿でもコミットメントが固定値とどの程度衝突するかを測るために最小エントロピーの概念[24]を用いる．

定義 5 マルチグループ認証方式のコミットメントの最小エントロピー

$mg - ID = (mgK, mgCo, Ch, mgR, mgV)$をマルチグループ認証方式，$\{(pk, sk)\}^M$を入力$k$とした$mgK$によって生成された$M$個の鍵ペアとする．$\mathcal{C}(\{sk\}^N) = \{mgCo(\{sk\}^N; R_P) : R_p \in \mathrm{Coins}_P(k)\}$を$N$個の秘密鍵に関連するコミットメントの集合とする．コミットメントが特定の値を取る最大確率は

$$\alpha(\{sk\}^N) = \max_{Cmt \in \mathcal{C}(\{sk\}^N)} \left\{ \Pr\left[\left(mgCo(\{sk\}^N; R_P) = Cmt : R_P \xleftarrow{\$} \mathrm{Coins}_P(k) \right) \right] \right\}$$

と定義され，このとき，最小エントロピー関数は以下で定義される．

$$\beta(k) = \min_{\{sk\}^N} \left\{ \log_2 \frac{1}{\alpha(\{sk\}^N)} \right\}$$

マルチグループ署名の安全性について，以下の定理が成り立つ．

定理 1 $mg - ID = (mgK, mgCo, Ch, mgR, mgV)$をマルチグループ認証方式とし，$s(\cdot)$をシード長，$mg - DS = (mgK, mgS^h, mgVf^h)$を 4.1 節に基いて構成されたマルチグループ署名方式とする．また，$\beta(\cdot)$を$mg - ID$に関連する最小エントロピー関数とする．$mg - DS$を攻撃する多項式時間$t(\cdot)$の攻撃者をFとする．Fは$q_s(\cdot)$，$q_h(\cdot)$回，署名オラクル，ハッシュオラクルを利用可能であるとする．このとき，以下の式(1)を満たす，$mg - ID$に対してなりすましを行う多項式時間$t(\cdot)$の攻撃者Iが存在する．

ゲーム $\boxed{G_3}/G_4$
Initialize
300 $(pk, sk) \xleftarrow{\$} mgK(k); hc \leftarrow 0; sc \leftarrow 0$
301 return pk

On H-query x
310 If HT$[x] = \perp$ Then
311 $hc \leftarrow hc + 1$; QT$[hc] \leftarrow x$
312 HT$[x] \xleftarrow{\$} \{0,1\}^{c(k)}$
313 return HT$[x]$

On Sign-query M
320 $sc \leftarrow sc + 1; R \xleftarrow{\$} \{0,1\}^{s}$
321 $R_P^i \xleftarrow{\$} \mathrm{Coins}_P(k)$
322 $TCmt_{sc} \leftarrow mgCo(\{sk\}^N; R_P^i); TCh_{sc} \xleftarrow{\$} \{0,1\}^{c(k)}$
323 $x \leftarrow R \parallel TCmt_{sc} \parallel m$
324 If HT$[x] \neq \perp$ Then
325 **bad** $\leftarrow$ true ; $\boxed{TCh_{sc} \leftarrow \mathrm{HT}[x]}$
326 $TRsp_{sc} \leftarrow mgR(\{sk\}^N, TCmt_{sc} \parallel TCh_{sc}; R_P^i)$
327 HT$[x] \leftarrow TCh_{sc}$
328 return $R \parallel TCmt_{sc} \parallel TRsp_{sc}$

Finalize (M, σ)
330 Parse σ as $R \parallel Cmt \parallel Rsp$
331 Let i such that QT$[i] = R \parallel Cmt \parallel m$
332 $Ch^* \xleftarrow{\$} \mathrm{HT}[\mathrm{QT}[i]]$
333 return $V(\{pk\}^N, Cmt \parallel Ch^* \parallel Rsp)$

ゲーム G_5
Initialize
500 $(pk, sk) \xleftarrow{\$} mgK(k); hc \leftarrow 0; sc \leftarrow 0$
501 return pk

On H-query x
310 If HT$[x] = \perp$ Then
311 $hc \leftarrow hc + 1$; QT$[hc] \leftarrow x$
312 HT$[x] \xleftarrow{\$} \{0,1\}^{c(k)}$
313 return HT$[x]$

On Sign-query M
520 $sc \leftarrow sc + 1; R \xleftarrow{\$} \{0,1\}^{s}$
521 $R_P^i \xleftarrow{\$} \mathrm{Coins}_P(k)$
522 $TCmt_{sc} \leftarrow mgCo(\{sk\}^N; R_P^i)$
523 $x \leftarrow R \parallel TCmt_{sc} \parallel m$
524 If HT$[x] \neq \perp$ Then HT$[x] \xleftarrow{\$} \{0,1\}^{c(k)}$
525 $TCh_{sc} \xleftarrow{\$} \{0,1\}^{c(k)}$
526 $TRsp_{sc} \leftarrow mgR(\{sk\}^N, TCmt_{sc} \parallel TCh_{sc}; R_P^i)$
527 return $R \parallel TCmt_{sc} \parallel TRsp_{sc}$

Finalize (M, σ)
530 Parse σ as $R \parallel Cmt \parallel Rsp$
531 Let i such that QT$[i] = R \parallel Cmt \parallel m$
532 $Ch^* \xleftarrow{\$} \mathrm{HT}[\mathrm{QT}[i]]$
533 return $V(\{pk\}^N, Cmt \parallel Ch^* \parallel Rsp)$

図 2 ゲームG_3, G_4及びG_5

$$\begin{aligned}&\mathbf{Adv}^{\mathrm{euf-cma}}_{mg-DS,F}\\ &\leq \big(1 + q_h(k)\big) \cdot \mathbf{Adv}^{\mathrm{ima-pa}}_{mg-ID,I}(k)\\ &+ \frac{[1 + q_h(k) + q_s(k)] \cdot q_s(k)}{2^{s(k)+\beta(k)}}.\end{aligned} \tag{1}$$

また，Iはたかだか$q_s(\cdot)$回 transcript オラクルを実行可能であるとする．

定理 1 の証明は文献[23]及び[23]で引用されている[25]におけるコードベースゲーム列によって行う．攻撃者AによるゲームG_iにおいて値yが出力されることを$G_i^A \Rightarrow y$と定義する．この手法では確率変化の上限を求めるために文献[25]における基本補題を利用する．基本補題が適用できるのはG_iとG_{i+1}が *identical until* **bad** と呼ばれる「変数 **bad** に 1 が代入される時点までは全く同じ」というゲーム上の同値関係を満たす場合にのみである．また，G_iにおいて **bad** に 1 が代入されないイベントをGood_iと定義すると，以下の補題が成り立つ．

補題 1 G_i, G_jが *identical until* **bad** であり，攻撃者をAとすると以下が成立する．

$$\Pr[G_i^A \Rightarrow 1] - \Pr[G_j^A \Rightarrow 1] \leq \Pr[G_i \; sets \; \mathbf{bad}]$$

補題 2 G_i, G_jが *identical until* **bad** であり，攻撃者をAとすると以下が成立する．

$$\Pr[G_i^A \Rightarrow 1 \wedge \mathrm{Good}_i] = \Pr[G_j^A \Rightarrow 1 \wedge \mathrm{Good}_j]$$

証明: まず, Fを以下の特性を持つ多項式時間$t(\cdot) + O(q_s)$の攻撃者Aに変換する．Aはたかだか$q_s(\cdot)$，$1 + q_h(\cdot)$回，署名オラクル, ハッシュオラクルを利用可能であるとする．Aのもつ特性は以下である．

(1) 任意の$R \in \{0,1\}^{s(k)}, Cmt, m \in \{0,1\}^*$に対して，全てのハッシュクエリの形式は$R \parallel Cmt \parallel m$とする．
(2) 偽造署名$(m, R \parallel Cmt \parallel Rsp)$を出力する前に$A$はハッシュクエリ$R \parallel Cmt \parallel m$を実行する．
(3) もしAが$(m, R \parallel Cmt \parallel Rsp)$を出力した場合，$m$はサインクエリの入力ではないとする．

次に$mg - ID$を攻撃する攻撃者Iを定義する．入力pkを持ち，transcript オラクルへのアクセスを行い，初期化と共に実行する．

IはAを入力pkで実行する．

Aがハッシュクエリxを実行したとき，Iは値がすでに定義されているならばHT$[x]$を返答し，そうでなければhcを 1 増やす．$hc \neq fp$でなければHT$[x]$の値を乱数としてAに返答する．$hc = fp$であるならxを$R \parallel Cmt^* \parallel m$とみなし，$Cmt^*$を検証者とのプロトコルにおける$mgCo$の出力として送信する．返ってきた$Ch^*$をHT$[fp]$の値とし，$A$に返答する

Aが署名クエリmを実行したとき，Iはscの値を 1 増やし，乱数Rを選択する．TCh_{sc}をHT$[R \parallel TCmt_{sc} \parallel m]$の値とし，$A$に署名$R \parallel TCmt_{sc} \parallel TRsp_{sc}$を返答する．$R \parallel TCmt_{sc} \parallel m$のハッシュ値として$TCh_{sc}$が定義されているが，$TRsp_{sc}$は transcript オラクルによって定義されているので正しい署名として利用できる．

最終的にAは偽造署名$(m, R \parallel Cmt \parallel Rsp)$を出力する．$I$は検証者とのプロトコルにおける$mgR$の出力として$Rsp$を返答する．

以上のAとIのやり取りを通して以下が成立する．

$$\begin{aligned}\mathbf{Adv}^{\mathrm{ima-pa}}_{mg-ID,I}(k) &\geq \frac{1}{1 + q_h(k)}\\ &\cdot \left(\mathbf{Adv}^{\mathrm{euf-cma}}_{mg-DS,F} - \frac{[1 + q_h(k) + q_s(k)] \cdot q_s(k)}{2^{s(k)+\beta(k)}}\right).\end{aligned} \tag{2}$$

これは式(1)と等価であり，式(2)をゲームの書き換えによって求める．証明には図 1，2 で表されるゲーム$G_0 - G_5$の 5 つのゲームを用いる．Iの優位性はゲーム列によって以下のように定義される．

$$\mathbf{Adv}^{\mathrm{ima-pa}}_{mg-ID,I}(k) \geq \Pr[G_0^A \Rightarrow 1 \wedge \mathrm{Good}_0] \tag{3}$$
$$= \Pr[G_1^A \Rightarrow 1 \wedge \mathrm{Good}_1] \tag{4}$$
$$= \Pr[G_2^A \Rightarrow 1 \wedge \mathrm{Good}_2] \tag{5}$$
$$= \Pr[G_2^A \Rightarrow 1] \cdot \Pr[\mathrm{Good}_0] \tag{6}$$

G_0はIの実行環境をシミュレートしている．検証者とのやり取りは明示的ではない代わりに検証者から送られてくるチャレンジCh^*は **Initialize** フェーズの 002 行で選択される．004-007 行で生成する値がIが transcript オラクルから得られる transcript の役割を果たす．しかし，G_0では 000 行で選択

された秘密鍵を用いてそれらの値を生成する．QT[fp]を$R \| Cmt^* \| m$とみなすと，値Cmt^*はIから検証者に送られるコミットメントの役割を果たす．031 行で生成されるiがfpと等しいならば，検証者とIの対話は$Cmt \| Ch^* \| Rsp$となる．このとき$Cmt = Cmt^*$である．よって$mgV(pk, Cmt \| Ch^* \| Rsp) = 1$のとき，$I$は成功となり，式(3)が成立する．

G_0における乱数Ch^*はG_1では **Initialize** フェーズでは選ばれないが，代わりに **Finalize** フェーズでそれをHT[fp]に割り当てる．G_1では囲い文字が含まれているので 132，134，135 行でこれを実行する．fpはハッシュクエリの返答には使われないので，G_1ではその選択を 133 行まで遅らせることができる．以上より式(4)を満たす．

G_1, G_2は *identical until* **bad** であるため，補題 2 より式(5)が成立する．しかしG_2では 135 行の囲みが無くなっている．fpはゲームの出力を決定するためには使われないので，Good_2のイベントと$G_2^A \Rightarrow 1$は独立している．よって式(6)が成り立つ．

G_2における 133-135 行より

$$\Pr[\mathrm{Good}_2] = 1/\{1 + q_h(k)\}$$

は明らかに成り立つ．

G_3における **Finalize** フェーズの出力はG_2のものと同じであるが，133-135 行が無くなっている．他の相違点は 101-105 行の選択がサインクエリの返答に必要となるまで遅らされている点である．しかしサインクエリの返答はG_2と同じであり，**bad** の値はゲームの出力に影響を与えないため，

$$\Pr[G_2^A \Rightarrow 1] = \Pr[G_3^A \Rightarrow 1] \geq \Pr[G_4^A \Rightarrow 1] - \Pr[G_4^A \text{ sets } \mathbf{bad}] \quad (7)$$

が成立し，G_3, G_4が *identical until* **bad** であるため，補題 2 より式(7)が導ける．

G_4におけるi回目のサインクエリにおいて **bad** に 1 が代入される確率はたかだか$\{1 + q_h(k) + (i+1)\}/\{2^{s(k)+\beta(k)}\}$であり，したがって，

$$\begin{aligned}&\Pr[G_4^A \text{ sets } \mathbf{bad}]\\ &\leq \sum_{i=1}^{q_s(k)} \frac{1 + q_h(k) + (i+1)}{2^{s(k)+\beta(k)}}\\ &= \frac{q_h(k)q_s(k) + \frac{q_s(k)(q_s(k)+1)}{2}}{2^{s(k)+\beta(k)}}\\ &\leq \frac{[1 + q_h(k) + q_s(k)]q_s(k)}{2^{s(k)+\beta(k)}} \quad (8)\end{aligned}$$

が得られる．

G_4における囲み文字が無いと仮定すると，サインクエリに返答する記述は **bad** への代入が無いことを除けば同等である．**bad** への代入はゲームの出力に影響を与えないので，

$$\Pr[G_4^A \Rightarrow 1] = \Pr[G_5^A \Rightarrow 1]$$

となる．しかし，G_5はAの優位性を定義する実験とみなせるため，

$$\Pr[G_5^A \Rightarrow 1] = \mathbf{Adv}^{\mathrm{euf-cma}}_{mg-DS,A}(k) \quad (9)$$

$$\geq \mathbf{Adv}^{\mathrm{euf-cma}}_{mg-DS,F}(k) \quad (10)$$

が成り立つ．式(3)から式(10)より式(2)が得られる．

5. 具体的な構成

5.1 アルゴリズム

2.3 節の定義に沿った IMP-PA 安全な誤り訂正符号を用いたマルチグループ認証方式[1]から 4.1 節の変換法に従って得られる EUF-CMA 安全なマルチグループ署名方式の具体的な構成を示す．署名方式は**KeyGen**, **Sign**, **Verify**の 3 つのアルゴリズムから構成される．

KeyGen$(1^k, M)$: ハミング重み$\omega_i = \mathrm{wt}(s_i)$の$n$次元ベクトル$s_i \in_R \mathbb{F}_2^n$を秘密鍵$sk_i$とし，パリティ検査行列$H$，シンドローム$p_i = Hs_i^T$，ハミング重み$\omega_i$の 3 要素を$pk_i$に対応する公開鍵$pk_i = (H, p_i, \omega_i)$とする．これにより公開鍵・秘密鍵のペア$(pk_i, sk_i)$を出力する．これを$M$回繰り返し，$M$組の公開鍵・秘密鍵ペアを出力する．

Sign$(\{sk_i\}_{i=1}^M, m)$: メッセージ$m \in \{0,1\}^*$を署名するために以下のステップを実行する．

1. nビットの整数$y_j \in_R \mathbb{F}_2^n$及び整数の置換$\sigma_j \in_R S_n$を選択する．
2. Step1 のy_j, σ_jを用いて
$$\begin{cases} c_1^{(j)} = h(\sigma_j, Hy_j^T) \\ c_2^{(j)} = h\left(\sigma_j(y_j)\right) \\ c_3^{(j)} = h\left(\sigma_j\left(y_j + \sum_{i=1}^M s_i\right)\right) \end{cases}$$
と計算し，$Cmt^j = (c_1^{(j)}, c_2^{(j)}, c_3^{(j)})$とする．
3. Setp1,2 を r 回繰り返し，$Cmt = \{Cmt^j\}^r = (Cmt^1, \dots, Cmt^r)$とする．
4. メッセージmとCMTのハッシュ値を
$$Ch^j = h'(m; Cmt^j) \in_R \{0,1,2\}$$
と計算し，$Ch = \{Ch^j\}^r = (Ch^1, \dots, Ch^r)$を求める．
5. Ch^jに対応するRsp^jを以下のように選択する．
$Ch^j = 0$のとき$Rsp^j := (y_j, \sigma_j)$.
$Ch^j = 1$のとき$Rsp^j := \left(y_j + \sum_{i=1}^M s_i, \sigma_j\right)$.
$Ch^j = 2$のとき$Rsp^j := (\sigma_j(y_j), \{\sigma_j(s_i)\}_{i=1}^M)$
6. Step1-5 により以下のように署名 Σ を出力する．
$$\Sigma = (Cmt^1, \dots, Cmt^r; (Ch^1, \dots, Ch^r); Rsp^1, \dots, Rsp^r)$$

Verify$(\{pk_i\}_{i=1}^M, m, \Sigma)$: mに対する Σ の正当性を以下の Step で検証する．

1. $(Ch^1, \dots, Ch^r) \neq h'(m; Cmt^1, \dots, Cmt^r)$であるとき，不受理 (Reject) とし，Reject を出力．そうでなければ，Step へ進む．
2. $j = 1$からrに対して，Ch^j, Cmt^jに対応するRSP^{j}を検証する．
$Ch^j, = 0$のときc_1, c_2を検証する．
$$\begin{cases} c_1 = h(\sigma_j, Hy_j^T) \\ c_2 = h\left(\sigma_j(y_j)\right) \end{cases}$$
$Ch^j, = 1$のときc_1, c_3を検証する．
$$\begin{cases} c_1 = h\left(\sigma_j, H\left(y_j + \sum_{i=1}^M s_i\right)^T + \sum_{i=1}^M p_i\right) \\ c_3 = h\left(\sigma_j\left(y_j + \sum_{i=1}^M s_i\right)\right) \end{cases}$$
$Ch^j, = 2$のときc_2, c_3及びハミング重み$\mathrm{wt}(\sigma(s_i))$を検証する．
$$\begin{cases} c_2 = h\left(\sigma_j(y_j)\right) \\ c_3 = h\left(\sigma_j(y_j) + \sum_{i=1}^M \sigma_j(s_i)\right) \\ \left\{\mathrm{wt}\left(\sigma_j(s_i)\right) = \omega_i\right\}_{i=1}^M \end{cases}$$
1 つでも検証結果が異なれば Reject とする．
3. Step1,2 で不受理されなかった場合，正当な署名として受理 (acceptt) する．

5.2 比較

5 章で示したマルチグループ署名方式の構成例と単一の鍵を用いる署名方式を比較する．2.3.1 項の定義に沿う認証方式である Stern96 方式[11]を FS 変換により構成した署名方式が 3.2.1 項の定義に沿う通常の署名方式と仮定し，比

較対象とする．4 章の変換法を用いて 2.4.1 項で定義されるマルチグループ認証方式から構成されるマルチグループ署名方式の署名のデータ量は認証方式のエンティティ間の送信データ量と等しい．同様に，FS 変換を用いて 2.3.1 項で定義される認証方式から構成される比較対象方式の署名のデータ量は，認証方式におけるエンティティ間の送信データ量と等しい．したがって文献[1]より，M 個の署名鍵を用いるとすると 5.1 節で示したマルチグループ署名方式の署名のデータ量は 7784+700{(M+1)/3}[bits]となる．Stern96 を変換した比較対象の署名方式の署名のデータ量は 8251[bits]となり，M 個の署名鍵を用いる場合，データ量は比例的に増加するので 8251M[bits]となる．横軸に同時に検証する検証者数 M，縦軸に署名のデータ量をとったグラフを図 3 に示す．マルチグループ署名方式は単一の鍵による方式を繰り返すよりも M=3 程度で 2 倍以上の効率となる．

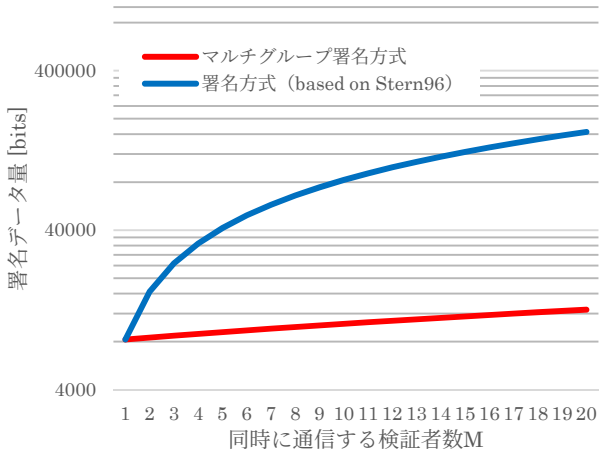

図 3：送信データ量の比較

6. 一部の秘密鍵を持つ攻撃者に対する安全性

証明者が複数の鍵を持つマルチグループ署名方式では，偽造対象となる署名の作成に必要な秘密鍵のうち，一つも保持していないモデル（攻撃モデル 1），一部を保持しているモデル（攻撃モデル 2）の 2 つの攻撃者のモデルが考えられる．4.2 節では攻撃モデル 1 の証明のみを与えた．5 章で用いた Halford らの方式によって構成された署名方式ではモデル 2 においても安全であることが以下のように示される．

5.1 節で構成された署名方式を攻撃する攻撃者が秘密鍵の部分集合S_Qを持ち，Ch^j,に対して以下のRsp^jを用いて署名を作成するとする．

$$Ch^j = 0 : Rsp^j = (y_0, \sigma_0)$$
$$Ch^j = 1 : Rsp^j = (w_1, \sigma_1)$$
$$Ch^j = 2 : Rsp^j = (z_2, t_{2,1}, \dots, t_{2,\mathrm{M}})$$

ここで，$w_1, z_2, t_{2,i}$はそれぞれ$y + \sum_{i=1}^{M} s_i$，$\sigma(y), \sigma(s_i)$を表す．**Verify**アルゴリズムにおいて$Ch^j = 0$もしくは$Ch^j = 1$であるならばc_1, c_2またはc_1, c_3の検証を行うため，c_1が等しくなることが求められる．正しい証明者は

$$\begin{aligned} c_1[\mathrm{Ch}^j = 1] &= h\left(\sigma_j, H\left(y_j + \sum_{i=1}^{M} s_i\right)^T + \sum_{i=1}^{M} p_i\right) \\ &= h\left(\sigma_j, Hy_j^T + H\left(\sum_{i=1}^{M} s_i\right)^T + \sum_{i=1}^{M} p_i\right) \\ &= h\left(\sigma_j, Hy_j^T + \sum_{i=1}^{M} Hs_i^T + \sum_{i=1}^{M} p_i\right) \\ &= h\left(\sigma_j, Hy_j^T\right) = c_1[\mathrm{Ch}^j = 0] \end{aligned}$$

と計算できるが，攻撃者は

$$c_1 = h(\sigma_0, Hy_0^T) = h\left(\sigma_1, Hw_1^T + \sum_{i=1}^{M} p_i\right)$$

を満たすことが求められる．これは，ハッシュ関数$h()$が不完全ハッシュ関数である，または，$\sigma_0 = \sigma_1 = \sigma$かつ$Hy_0^T = Hw_1^T + \sum_{i=1}^{M} p_i$であることを示している．同様にして，$c_2, c_3$も等しくなることが求められ，

$$c_2 = h(\sigma_o(y_0)) = h(z_2)$$
$$c_3 = h(\sigma_1(w_1)) = h\left(z_2 + \sum_{i=1}^{M} t_{2,i}\right)$$

となる必要がある．ハッシュ衝突が起こらない限り，$\sigma_0(y_0) = z_2, \sigma_1(w_1) = z_2 + \sum_{i=1}^{M} t_{2,i}$であることが示せる．また，$t_{2,i}$=$\sigma(s_i)$を表すため，$\sum_{i=1}^{M} t_{2,i} = \sigma(y_0 + w_1)$であることが示せる．すべての$i$に対して，$\mathrm{wt}(t_{2,\mathrm{i}}) = \omega_i$であるため$y_0 + w_1$は$M$個の正当な秘密鍵の総和である．このような和を求めるためには攻撃者は

$$\sum_{i\in\mathcal{T}} Ht_{2,i}^T = \sum_{i\in\mathcal{T}} p_i \ \text{かつ} \ \mathrm{wt}(t_{2,\mathrm{i}}) = \omega_i \ \forall i \in \mathcal{T}$$

を満たす$M - S_Q$個のn次ベクトル集合を求める必要がある．ここで$\mathcal{T} = [1, M] \setminus S_Q$とする．攻撃者が持っている秘密鍵集合は$S_Q$であるため，保持していない秘密鍵をすべて求める必要がある．すなわち，攻撃者はM個の秘密鍵のうち少なくとも 1 つでも持ってないとすると，署名を偽造するためには以下で定義された NP 完全問題を解く必要がある．

定義 6 q元語の和の復号問題

入力: ランダム$r \times n$ q元行列H，$z \in_R \mathbb{F}_q^r$，$\omega_1 > 0$，および$i \in [2, M]$について$\omega_{\mathrm{i}} \geq 0$を満たす$M$個の整数$\{\omega_i\}_{i=1}^{M}$

出力: すべての$i \in [1, M]$について$\mathrm{wt}(\mathrm{s_i}) \leq \omega_i$を満たし，かつ$\sum_{i=1}^{M} Hs_i^T = z$を満たす，$M$個の$n$次$q$元ベクトル$\{s_i\}_{i=1}^{M}$

Barg の q 元シンドローム復号問題により NP 完全であることが導ける[26].

攻撃モデル 2 においてもフォーマルな証明を与え，必要な秘密鍵を全て持たない限り正当な署名が作成できないことを示すことが今後の課題として挙げられる．

7. まとめ

本稿では，異なる認証者に対して同時に複数の認証を行うマルチグループ認証方式からマルチグループ署名方式を構成する変換手法を示し，安全性証明を与えた．その変換手法を用いて IMP-PA 安全な誤り訂正符号を用いるマルチグループ認証方式から EUF-CMA 安全なマルチグループ署名方式を構成し，単一な鍵を用いる署名方式を繰り返したときに比べて送信データ量が少ないことを確認した．

謝辞 本研究は JSPS 科研費 16K00184, 22700067 の助成を受けたものである．

参考文献

[1] T.R. Halford, “How to Prove Yourself to Multiple Parties: Energy-Efficient Multi-group Authentication,” in Proc. IEEE MILCOM 2013, pp. 237-242, Nov. 2013.

[2] A. Fiat, and A. Shamir, “How to prove yourself: Practical solutions to identification and signature problems,” in Advances in Cryptology-CRYPTO’86, pp.186-194, Dec. 1986..

[3] K. H. Wong, Y. Zheng, J. Cao, and S. Wang, “A dynamic user authentication scheme for wireless sensor networks,” IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC’06), Vol.1, pp.244-251, Jun. 2006.

[4] M. L. Das, “Two-factor user authentication in wireless sensor

networks," IEEE Transactions on Wireless Communications, Vol.8, no.3, pp.1086-1090, May 2009.
[5] M. K. Khan, and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'". Sensors, Vol.10, no.3, pp.2450-2459. Mar. 2010.
[6] B. Vaidya, D. Makrakis, and H. T. Moeuftah, "Improved two-factor user authentication in wireless sensor networks," in Proc. IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp.600-606, Oct. 2010.
[7] B. Vaidya, D. Makrakis, and H. T. Moeuftah, "Improved two-factor user authentication in wireless sensor networks," in Proc. IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp.600-606, Oct. 2010.
[8] N. Bruce, and H. J. Lee, "Cryptographic computation of private shared key based mutual authentication protocol: Simulation and modeling over wireless networks," in Proc. The International Conference on Information Networking 2014 (ICOIN2014), pp.578-582, Feb. 2014
[9] M. K. Sharma, R.S. Bali, and A. Kaur, "Dyanimc key based authentication scheme for Vehicular Cloud Computing," in Proc. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), pp.1059-1064, Oct. 2015.
[10] S. K. Udgata, A. Mubeen, and S. L. Sabat, "Wirelss sensor network security model using zero knowledge protocol," in Proc. International Conference on Communications (ICC), pp.1-5, Jun. 2011.
[11] J. Stern, "A new paradigm for public key identification," IEEE Transaction on Information Theory, Vol.42, no.6, pp.1757–1768, Nov. 1996.
[12] P. Véron, "Improved identification schemes based on error-correcting codes," Applicable Algebra in Engineering, Communication and Computing, Vol.8, no.1, pp.57-69, Jan. 1997.
[13] R. Ghanbarimaman, and A. N. Pour, "A new definition of group authentication increasing performance of server calculation," in Proc. 2012 International Conference on Information Science and Applications (ICISA), p.1-6, May 2012.
[14] L. Harn, "Group authentication," IEEE Transactions on Computers Vol.62, no.9, pp.1893-1898, Sept. 2013.
[15] C. Guo, R. Zhuang, L. Yuan, and B. Feng, "A Group Authentication Scheme Supporting Cheating Detection and Identification," in Proc. 2015 Ninth International Conference on Frontier of Computer Science and Technology (FCST), pp.110-114. Aug. 2015.
[16] P. Gaborit, and M. Girault, "Lightweight code-based identification and signature," in Proc. IEEE International Symposium on Information Theory, pp.191-195, Jun. 2007.
[17] C. Aguilar, P. Gaborit, and J. Schrek, "A new zero-knowledge code based identification scheme with reduced communication," CoRR, abs/1111.1644, 2011.
[18] A. Dambra, P. Gaborit, M. Roussellet, J. Schrek, and N. Tafforeau, "Improved Secure Implementation of Code-Based Signature Schemes on Embedded Devices," IACR Cryptology ePrint Archive: Report 2014/163, Mar. 2014.
[19] U. Feige, F. Amo, and S. Adi, "Zero-knowledge proofs of identity," Journal of cryptology, Vol.1, no.2 pp.77-94, Jun 1988.
[20] M. Bellare, and R. Phillip, "Random oracles are practical: A paradigm for designing efficient protocols." in Proc. 1st ACM conference on Computer and communications security (CCS'06), pp.62-73, Dec 1993.
[21] S. Goldwasser, M. Silvio, and R. L. Ronald, "A digital signature scheme secure against adaptive chosen-message attacks," SIAM Journal on Computing Vol.17, no.2, pp.281-308, 1988.
[22] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," Journal of Cryptology, Vol.13, no.3, pp.361–396, 2000.
[23] M. Abdalla, J.H. An, M. Bellare, and C. Namprempre, "From Identification to Signatures Via the Fiat-Shamir Transform: Necessary and Seufficient Conditions for Security and Forward-Security," Information Theory, IEEE Transactions on, Vol.54, no.8, pp.3631–3646, 2008. (Conference Ver.: Proc. EUROCRYPT 2002, LNCS, vol. 2332, pp. 418–433, 2002).
[24] B. Chor, and O. Goldreich, "Unbiased bits from sources of weak randomness and probabilistic communication complexity," SIAM Journal on Computing, Vol.17, no.2, pp.230-261, 1988.
[25] M. Bellare, and P. Rogaway, "The security of triple encryption and a framework for code-based game-playing proofs," in Advances in Cryptology-EUROCRYPT 2006, pp.409-426, May. 2006.
[26] M. R. Garey, and D. S. Johnson, "Computers and Intractability: A Guide to the Theory of NP-Completeness," New York: W.H. Freeman and Company, 1979.