L-027

多者多重署名とその応用
Multisignatures with Multiple-Signability and Its Applications

矢内 直人 † 千田 栄幸 ‡ 満保 雅浩 § 花岡 悟一郎 ¶ 岡本 栄司 †
Naoto Yanai Eikoh Chida Masahiro Mambo Goichiro Hanaoka Eiji Okamoto

1. はじめに

多重署名は n 人の署名者がいる状況において, 個々の署名を n 個集めるよりも計算効率, 署名長ともに効率的に処理するプリミティブである [3]. 既存の多重署名の多くは各署名者に多重回署名することを認めていない. これらの問題は安全性証明に起因する. 実は既存の多重署名における安全性は一回限り署名する場合のみ保証され, 多重回の署名処理を施す場合, 各署名は鍵を新たに作り直すか, 直前の署名を保持して多重署名から一旦自分の署名を消去すること (Dividing-Out 法) が必要となる.

この問題点に対し, 我々は SCIS 2013 にて多重回の署名処理を各署名者に認める多者多重署名という新たなプリミティブを提案し, 具体的な構成について安全性を議論した [8]. 本稿では多者多重署名が本質的に持つべき数学的な性質を考察し, 安全性証明の要因を一般的に示す. また, 文献 [8] で考察が不足していたアプリケーションについても考察し, 多者多重署名の有用性を示す.

2. 準備

2.1. 表記

署名者の数を n とする. m を署名対象の message , σ_i を i 番目の署名者が生成した署名, pk_i と sk_i を i 番目の署名者の公開鍵と秘密鍵とする. また, 任意の要素 a, b において, a と b の連結を $a \parallel b$ で表す. ここで, この連結を容易に元の a, b に戻せるものとする. また, pk_1 から pk_i までの署名順序を $\psi_i := pk_1 \parallel \cdots \parallel pk_i$ と表す.

2.2. 双線形写像

Definition 1 (双線形写像)**.** $\mathbb{G}$ と $\mathbb{G}_T$ を素数位数 p の群, $\mathbb{G}$ の生成元を g とする. 以下の条件を満たす写像 $\boldsymbol{e}$ を双線形写像という；(双線形性) 任意の $u, v \in \mathbb{G}$ と $a, b \in \mathbb{Z}_p^*$ において, $\boldsymbol{e}(u^a, v^b) = \boldsymbol{e}(u, v)^{ab}$ が成り立つ；(非退化) 任意の生成元 $g \in \mathbb{G}$ において, $\boldsymbol{e}(g, g) \neq 1_{\mathbb{G}_T}$ が成り立つ. ここで $1_{\mathbb{G}_T}$ は $\mathbb{G}_T$ における単位元を表す；(計算可能性) 任意の $u, v \in \mathbb{G}$ において, $\boldsymbol{e}(u, v)$ を容易に計算できる.

本稿において, 上述のすべての条件が成り立つグループ $\mathbb{G}$ を双線形群と呼び, 双線形群において離散対数問題 (DLP) は困難であると仮定する. そのようなパラメータを双線形写像パラメータと呼び, $(p, \mathbb{G}, \mathbb{G}_T, \boldsymbol{e})$ と表す.

†筑波大学, システム情報工学研究科, 茨城県つくば市天王台 1-1-1, Graduate School of Systems and Information Engineering, University of Tsukuba , 1-1-1 Tennodai, Tsukuba, Ibaraki, Japan
‡一関工業高等専門学校, 電気工学科, 岩手県一関市萩荘字高梨, Department of Electrical and Coputer Engineering, Ichinoseki National College of Technology, Hagishou Aza Takanashi, Ichinoseki, Iwate, Japan
§金沢大学, 理工研究域, 石川県金沢市角間町, Graduate School of Natural Science and Technology, Kanazawa University, Kakuma, Kanazawa, Ishikawa, Japan
¶産業技術総合研究所, 茨城県つくば市梅園 1 − 1 − 1, AIST, Umezono 1-1-1, Tsukuba, Ibaraki, Japan

2.3.LOSSW06 アグリゲート署名方式

本節では Lu らによるアグリゲート署名方式 [4] を紹介する, 我々は SCIS 2013 において, この方式が多者多重署名であることを満たした. この方式において, 各ユーザはそれぞれ固有の message m_i に署名できるものとし, m_i は任意の l におけるビット列 $\{0,1\}^l$ として扱われる. なお, ここでの順序情報 ψ_i はユーザグループの構成を反映するだけであり, 署名順序の検証は考慮しない.

Setup: セキュリティパラメータ 1^k を与えられ, 双線形写像パラメータ $(p, \mathbb{G}, \mathbb{G}_T, \boldsymbol{e})$ を生成し, $(g_1, g_2) \in \mathbb{G}^2$ を公開パラメータとして生成する.

Key Generation: $(p, \mathbb{G}, \mathbb{G}_T, \boldsymbol{e}, g_1, g_2)$ を与えられ, $\alpha_i, v_i' \leftarrow \mathbb{Z}_p^*$ と l-bit vector $v_{i,1}, \cdots, v_{i,l} \leftarrow \mathbb{Z}_p^l$ を生成する. その後, $A_i = g_1^{\alpha_i}, V_i' = g_1^{v_i'}, V_{i,1} = g_1^{v_{i,1}}, \cdots, V_{i,l} = g_1^{v_{i,l}}$ を計算する. $(g_2^{\alpha_i}, v_i', v_{i,1}, \cdots, v_{i,l})$ を秘密鍵 sk_i とし, $(A_i, V_i', V_{i,1}, \cdots, V_{i,l})$ を公開鍵 pk_i として公開する.

Signing: message $\{m_j\}_{j=1}^i$, ψ_{i-1}, 署名 σ_{i-1} を与えられ, それぞれの m_j をビット列 $(m_{j,1}, \cdots, m_{j,l}) \in \{0,1\}^l$, 署名を (S_{i-1}, R_{i-1}) として出力する. ID_i が最初の署名者である場合, $(S_{i-1}, R_{i-1}) = (1, 1)$ を初期値として設定する. $r_i \leftarrow \mathbb{Z}_p^*$ を生成し, 以下を計算する;$R_i = R_{i-1} \cdot g_1^{r_i}$, $S_i = S_{i-1} \cdot g_2^{\alpha_i} (R_i)^{v_i' + \sum_{j=1}^l v_{i,j} m_{i,j}} \left(\prod_{j=1}^{i-1} \left(V_j' \prod_{e=1}^l V_{j,e}^{m_{j,e}} \right) \right)^{r_i}$.

$\psi_i = \psi_{i-1} \parallel pk_i$ をセットし, $\{m_j\}_{j=1}^i, \sigma_i = (S_i, R_i)$ を出力する.

Verification $(m, \psi_n, \sigma_n, \{pk_i\}_{i=1}^n)$ を与えられ, 以下が成り立つか計算する. 成り立つ場合は *accept* を返し, そうでないなら *reject* を返す.

$$\boldsymbol{e}(S_n, g_1) \stackrel{?}{=} \boldsymbol{e}\left(g_2, \prod_{i=1}^n A_i\right) \boldsymbol{e}\left(R_n, \prod_{i=1}^n \left(V_i' \prod_{j=1}^l V_{i,j}^{m_{i,j}} \right)\right).$$

3. 多者多重署名の構成に向けた考察

3.1. 方式構成上の問題点

証明可能安全な多者多重署名の構成は容易ではない. 署名技術の証明可能安全性の難しさは一般に, 証明における署名オラクルのシミュレーションに依存する. 多者多重署名ではこの難しさは一回しか署名できない従来の構成よりも深刻な問題となる. 具体的には, 従来の署名方式では秘密鍵は各署名クエリにおいて一回しか利用されないが, 多者多重署名では秘密鍵が複数回利用される. これは直観的に署名オラクルの構成がより難しいことを意味する. 加えて, このオラクルシミュレーションは多重署名としての効率性を維持することも必要となる. つまり, 単純には一人分の署名オラクルの処理を n 個独立して走らせるだけでは効率の面で不十分と言える.

3.2. 提案アプローチ

多者多重署名の構成に当たる本質的な問題は一回の多重署名クエリにおいて各署名者が多重回の署名処理を施すことである. この問題を解決するに当たり, 我々は

衝突困難性が与えられる要素のもとで一回の計算で複数個の署名を生成できるならば, そもそも複数回の処理を行う必要がないことに気付いた．そのような計算は programmable hash function [2] を用いることで実現可能である．つまり, programmable hash function があれば多者多重署名は構成できると考えられる．また, 多者多重署名の構成はランダムオラクルの存在が仮定されない場合であっても達成可能である．事実, 我々は SCIS 2013 にてスタンダードモデルにおいて安全性を証明した多者多重署名を構成している [8]．具体的には $u' \prod_{j=1}^{\ell} u_j^{m_j}$ からなる Waters hash function [6] から方式を構成している．ここで Waters hash function は平文 m に対する多項式 $G(m), K(m)$ において $H(m) = (g^b)^{G(m)} g^{K(m)}$ と定義される．Waters hash function を通じて, これら多項式に対して複数個のクエリを同時に与えることで, [8] において多者多重署名のシミュレーションは達成できる．

4.Applications

本節では, 多者多重署名のアプリケーションを紹介する．

4.1.Content Editing System [5]

YouTube [7] のような consumer generated media (CGM) サービスが近年では広まっている．このようなサービスではユーザは自ら生成したコンテンツを配信し, それを閲覧したユーザが編集し再配布している．このような状況ではユーザが自らが生成した署名付きコンテンツに再度署名することが考えられる．Sano らは [5] はこれら CGM サービスに対してコンテンツ編集システムを提案した．このシステムにおいて, ユーザは生成したコンテンツの正当性を保証するために署名し, また, 他のユーザはコンテンツを編集するごとに既に添付されている署名から多重署名を生成する．[5] のシステムでは既に署名済みのユーザが再度署名処理を施す場合, ユーザは 1 節で述べた Dividing-Out 法のために過去に生成した署名を保持していなければならない．これによる効率面の損失はただ署名を保持するだけではない．通常, YouTube などにアップされるコンテンツのデータサイズは数メガバイトから数百メガバイトと大きい．上述の手法ではこのすべてが必要であり, メモリ容量が大幅に必要となる．これに対し, 多者多重署名は例えば差分データだけに署名するということが可能となる．これにより, 多者多重署名により効率的なシステム運用が期待できる．

4.2.Electronic Toll Pricing

Electronic toll pricing (ETP) はドライバーの走行距離などのパラメーターに基づき, 道路料金を計算する計算システムである．これは市民や政府に利点がある．前者は自分が走行した道路料金だけ払えばよく, 後者は congestion pricing を導入することにより, 交通量を制限することが可能となる．このシステムのエンティティは on-board unit (OBU), toll service provider (TSP), Toll Charger (TC) から構成される．OBU は各車両に搭載される電子機器であり, ETP へのデータ提出はこの OBU を介して行われる．TSP は ETP サービスを提供するプロバイダであり, 各 OBU から提出されるデータの正当性を確認する．TC はユーザに実際に料金を請求する．

ETP システムの問題点は (1) OBU を起動させずに走行する車両と (2) 偽の GPS 情報を提出する OBU s である．Balash ら [1] はこれらの問題点を取り扱うために, 電子署名を用いたシステムことを提案しているが, その一方で OBU がプロバイダから受け取るコミットメントがゲート数に対して線形になるという問題がある．また, 一部のユーザは支払いをクレジットにて例えば月末などに一括して払うことがあり得るが, この場合, OBU にすべての署名を格納しておく必要がある．これらは OBU のメモリを著しく消費し, 設計者の側でどの程度のリソースを用意すればいいのか事前に見積ることも現実的ではない．我々はこれらを解決するために, 新たなアプローチとして多者多重署名 を使うことを提案する．まず, ここで署名大将データは各車両が搭載している OBU であり, この ID 情報を message, また, 高速道路における各ゲートが署名者としてその通貨履歴が署名順序となる．多者多重署名を使うには以下の理由がある．まず, 従来の多重署名の機能として, 走行時に得た署名を集約して格納することができる．また, 上述したクレジットによる一括支払いに対しても, 多者多重性により通過したことがあるゲートが発行する署名すら集約することが可能である．これらにより署名の記憶容量を走行距離に依存せず固定長で抑えることが可能となる．これは ETP 導入コストを大幅に改善することが期待できる．

謝辞

本研究の一部は JSPS A3 Foresight Program によって支援されている．また, 第一著者はテレコム先端技術研究支援センターに支援されている．彼らの多大な支援に感謝する．

参考文献

[1] Josep Balasch, Alfredo Rial, Carmela Troncoso, Bart Preneel, Ingrid Verbauwhede, and Christophe Geuens. Pretp: Privacy-preserving electronic toll pricing. In *Proc. of the 19th Unenix Security Symposium (Usenix Security 2010), Washington, USA*, Vol. 10. Usenix, August 2010.

[2] Dennis Hofheinz and Eike Kiltz. Programmable hash functions and their applications. In *Proc. of the 28th Annual Internatinal Cryptology Conference (CRYPTO 2008), Santa Barbara, USA*, Vol. 5157 of *Lecture Notes in Computer Science*, pp. 21–38. Springer-Verlag, August 2008.

[3] Kazuharu Itakura and Katsuhiro Nakamura. A public-key cryptosystem suitable for digital multi-signatures. *NEC Research and Development*, Vol. 71, pp. 1–8, 1983.

[4] Steve Lu, Rafail Ostrovsky, Amit Sahai, Hovav Shacham, and Brent Waters. Sequential aggregate signatures and multisignatures without random oracle. In *Proc. of the 25th Theory and Applications of Cryptographic Techniques (EUROCRYPT 2006), Petersburg, Russia*, Vol. 4004 of *Lecture Notes in Computer Science*, pp. 465–485. Springer-Verlag, May 2006.

[5] Tatsuhiko Sano, Yoshio Kakizaki, Masaki Inamura, and Keiichi Iwamura. Implementation and evaluation of a content editing system enabling pre-control for content circulation. In *Proc. of the 30th Symposium on Cryptography and Information Security (SCIS 2013), Kyoto, Japan*. IEICE, January 2013. Japanese.

[6] Brent Waters. Efficient identity-based encryption without random oracles. In *Proc. of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2005), Aarhus, Denmark*, Vol. 3494 of *Lecture Notes oi Computer Science*, pp. 114–127. Springer-Verlag, May 2005.

[7] Youtube. `http://www.youtube.com/`.

[8] 矢内直人, 千田栄幸, 満保雅浩, 岡本栄司. 多者多重署名の構成に関する一考察. 2013 年 暗号と情報セキュリティシンポジウム (SCIS 2013) 予稿集, January 2013. 3A4-3.