軽量な失効可能グループ署名方式の提案

A Proposal of Lightweight Revocable Group Signature Scheme

赤間 滉星 [1] 近藤 賢郎 [2] 甲斐 賢 [3] 佐藤 雅明 [4] 手塚 悟 [1]
Kosei Akama Takao Kondo Satoshi Kai Masaaki Sato Satoru Tezuka

慶應義塾大学 環境情報学部 [1]
Faculty of Information and Environment Studies, Keio University
慶應義塾 情報セキュリティインシデント対応チーム [2]
CSIRT, Keio University
慶應義塾大学 SFC 研究所 [3]
Research Institute at SFC, Keio University
慶應義塾大学 大学院政策・メディア研究科 [4]
Graduate School of Media and Governance, Keio University

1 はじめに

1.1 背景

匿名掲示板などのサービスでは，ユーザが不正を行った場合に，追跡して責任を明らかにできる必要がある．しかし安易に追跡をできることは，プライバシの懸念をもたらす．

本稿ではこの問題の解決のために，正当性，偽造不可能，否認不可に加え，以下に定義する匿名・リンク不可能，追跡可能，失効可能を同時に満たすことにより問題の解決を図る．

匿名・リンク不可能. ユーザは匿名性を守った上でサービスを利用できる
追跡可能. ユーザの不正が発覚した場合，そのユーザを特定可能である
失効可能. ユーザのサービス利用権を失効させることができる

失効可能以外の要件を実現する手段に，グループ署名方式 [1] が挙げられる．グループ署名方式とは，署名者が特定のグループに含まれることを証明するディジタル署名方式である．グループ署名方式の署名者は検証者から見て匿名であるが，署名者の不正があった際は，*GM* (*Group Manager*) が署名から署名者を追跡できる．さらに失効可能なグループ署名方式 [2] が提案されてきた．

1.2 関連研究

グループ署名方式や匿名認証について多くの研究が存在する. 匿名認証プロトコル [3] は軽量な匿名認証方式を提案しているが，メッセージの否認不可を満たさない．匿名認証プロトコルをもとにした証明書なしグループ署名方式 [4] は，*KGC* (*Key Generation Center*) を必要とし，かつ追跡機能が定義されていない．ペアリングなしグループ署名方式 [2] は軽量でかつ，ローカルで失効可能なグループ署名方式を提案しており，大規模サービスの計算負荷を下げ，計算資源が貧弱なデバイス環境で利用可能な署名・署名検証・失効検証コストを実現する．

1.3 貢献

本稿では，1.1 節で述べた要件を満たす匿名認証方式を，より多くの大規模サービスやモバイル環境上で実現することを目的に，新しいグループ署名方式を提案する．提案方式では，匿名認証プロトコルをもとに実現する．提案方式ではペアリングを用いず，ローカルで失効確認をするための計算をし ないため ，大規模サービスの計算負荷を下げ，計算資源が貧弱なデバイス環境で利用可能な署名・署名検証・失効検証コストを実現する．

2 失効可能なグループ署名方式

失効可能なグループ署名方式を，以下のエンティティ，手順，セキュリティ要件から定義する．

2.1 エンティティ

失効可能なグループ署名方式は以下に定義する GM，メンバ，検証者から成り立つ．

GM メンバを管理するエンティティ．メンバの追加，失効，追跡を実施．
メンバ 署名を行うエンティティ．署名者．
検証者 メンバによる署名を検証するエンティティ．

2.2 セキュリティ要件

失効可能グループ署名は以下のセキュリティ要件を満たす．

正当性 メンバが作成した署名は必ず検証者に受理される．
偽造不可能性 メンバ以外が作成した署名は，必ず検証者に棄却される．
匿名性 GM 以外は，署名からメンバを特定できない
リンク不可能性 GM 以外は，複数の署名が同じメンバによって署名されているかわからない．
追跡可能性 GM は署名からメンバを特定できる．
失効可能性 GM はメンバごとに署名を失効させることができる．

2.3 手続き

失効可能なグループ署名方式は以下の手続きから成り立つ．

準備 GM はグループ署名のために，必要なパラメータと公開鍵と秘密鍵を生成する．生成したパラメータと，公開鍵は公開する．
参加 メンバが GM に登録を求める．GM はメンバを登録し，メンバに対して署名に必要なクレデンシャルを送信する．
署名 メンバは署名したいメッセージに対する署名を生成し，メッセージとともに署名を検証者に送信する．
署名検証 検証者は公開パラメータ，GM の公開鍵，署名，メッセージをもとに，署名の検証を行う．
追跡 GM は署名をもとに，署名したメンバを追跡する．
失効 GM は特定のメンバを失効リストに追加する．
失効検証 検証者は署名から，署名したメンバが失効されているか確認する．

3 提案方式

提案方式の手順を示す．2.3 節に述べた手続きを満たす．提案方式は CDH 仮定 [3] に基づき安全である．

3.1 準備

GM は大きな素数 ~~q~~ p，暗号学的ハッシュ関数 $H_1 : \{0,1\}^* \to \mathbb{Z}_p$，$H_2 : \{0,1\}^* \to \mathbb{Z}_p$，乗法巡回群 $\mathbb{G}$ を決め，$\mathbb{G}$ の生成元 g とともに，それぞれ公開する．GM はランダムに $s \xleftarrow{\$} \mathbb{Z}_p$ を選択し，$PK_{GM} = g^s$ を計算し，PK_{GM} を公開する．

3.2 参加

i をメンバの番号とする．GM はランダムに $r \xleftarrow{\$} \mathbb{Z}_p$ を選択し，式 1, 2 を計算する．|| は文字列の連結である．

$$R = g^r \tag{1}$$

$$S = r + H_1(i||R) \cdot s \tag{2}$$

GM はメンバリスト ML に (i, R) を挿入し，$\delta = (i, R, S)$ をメンバに送信する．メンバは $g^S = R \cdot (PK_{GM})^{H(i,R)}$ が成り立つか確認する．

3.3 署名

msg を署名する文章とする．メンバはランダムに $a \xleftarrow{\$} \mathbb{Z}_p$ と $c \xleftarrow{\$} \mathbb{Z}_p$ をそれぞれ選択し，式 3 - 8 を計算する．

$$A = g^a \tag{3}$$

$$P = c \cdot H_1(i||R) \tag{4}$$

$$R' = R^c \tag{5}$$

$$S' = c \cdot S \tag{6}$$

$$h = H_2(msg||P||R'||A) \tag{7}$$

$$V = a + S' \cdot h \tag{8}$$

メンバは署名 $\sigma = (P, R', A, V)$ と msg を検証者に送信する．

3.4 署名検証

検証者は式 9, 10 を計算する．式 11 を確認し，成り立てば受理，成り立たなければ棄却する．

$$Q = R' \cdot (PK_{GM})^P \tag{9}$$

$$h = H_2(msg||P||R||A) \tag{10}$$

$$g^V = A \cdot Q^h \tag{11}$$

3.5 失効

失効するメンバの番号を i とする．メンバに対応する R を用いて，失効リスト RL に対し，(i, R) を挿入する．

3.6 失効検証

検証者は署名 σ を GM に送り，GM は RL の全ての要素に対して，$c' = P \cdot H_1(i, R)^{-1}$ を計算し，$R^{c'} = R'$ が成り立つか検証する．等式が成り立つ要素がある場合，GM は失効していることを検証者に伝える．

3.7 追跡

検証者は署名 σ を GM に対して送信する．GM は ML の全ての要素に対して，式 12 の計算を行い， 式 13 が成り立つか検証する．

$$c' = P \cdot H_1(i||R)^{-1} \tag{12}$$

$$R^{c'} = R' \tag{13}$$

上記が成り立つ要素の i が，署名したメンバの番号である．

4 セキュリティに関する考察

2.2 節に述べたセキュリティ要件，正当性，偽装不可能性，匿名性，リンク不可能性，追跡可能性，失効可能性について考察する．

正当性 正当な署名 σ と 式 9, 10 より計算される (Q, h) の上で，式 11 が必ず成り立ち，署名は受理される．

偽造不可能性 有効な署名には，V が必要である．式 2, 6, 8 より，V を計算するためには，GM の秘密鍵 s を用いて計算された S が必要である．よって GM に発行された証明書 S を持たないユーザは，有効な署名を生成できない．

匿名性 検証者は署名 P, R', A, V から，ユーザを特定できない．

リンク不可能性 署名 σ の要素 P, R', A, V は，それぞれ署名ごとに生成される秘密の乱数 a または c をもとに計算されるため，検証者は複数の署名が同じメンバによって，生成されたのか判断できない．

追跡可能性 3.7 節より，GM は署名から署名したメンバを追跡できる．

失効可能性 3.5 節と 3.6 節より，GM はメンバごとに，署名を失効させることができる．

表 1　演算回数と署名サイズの比較.

方式	署名サイズ	演算回数		
		署名	署名検証	失効検証
[2]	$2\|\mathbb{G}\| + 4\|\mathbb{Z}_p^*\|$	$e:5$ $m:1$	$e:3$ $m:2$	$e:2\|RL\|+5$ $m:\|RL\|+4$
提案	$2\|\mathbb{G}\| + 2\|\mathbb{Z}_p\|$	$e:2$ $m:0$	$e:3$ $m:2$	$e:\|RL\|$ $m:0$

5 効率性の評価

一回の署名，署名検証，失効検証に必要な $\mathbb{G}$ の要素に対する演算回数と，一つのグループ署名の署名サイズについて比較し表 1 にまとめた.[1][2][3][4] 署名サイズ，署名コスト，失効検証コストにおいて，提案方式はペアリングなしグループ署名方式 [2] よりそれぞれ小さい．そのため，提案方式が [2] に比べて，大規模サービスの計算負荷を下げ，計算資源が貧弱なデバイス環境に適する．

6 まとめ

本稿では，1.1 節で述べた要件を満たす匿名認証方式を，大規模サービスやモバイル環境において実現することを目的に，匿名認証方式をもとに実現されるグループ署名方式を提案した．提案方式では，ペアリングを用いず，ローカルで失効確認をする計算をしないため，大規模サービスの計算負荷を下げ，計算資源が貧弱なデバイス環境で利用可能な署名・署名検証・失効検証コストを実現する．

参考文献

[1] D. Chaum and E. Van Heyst. Group signatures. In Workshop on the Theory and Application of of Cryptographic Techniques, pp. 257–265. Springer, 1991.

[2] K. Gu and B. Yin. Efficient group signature scheme without pairings. International Journal of Network Security, Vol. 22, pp. 504–515, 2020.

[3] X. Yang, X. Yi, I. Khalil, H. Cui, X. Yang, S. Nepal, X. Huang, and Y. Zeng. A new privacy-preserving authentication protocol for anonymous web browsing. Concurrency and Computation: Practice and Experience, Vol. 31, No. 21, p. e4706, 2019.

[4] H. Zhu, C. Cui, F. Li, Zh. Liu, and Q. Zhang. Design of anonymous communication protocol based on group signature. In International Symposium on Cyberspace Safety and Security, pp. 175–181. Springer, 2019.

[1] $|\mathbb{G}|$, $|\mathbb{Z}_p|$, $|\mathbb{Z}_p^*|$ は，それぞれ $\mathbb{G}$，$\mathbb{Z}_p$，$\mathbb{Z}_p^*$ の点の大きさである．

[2] e は $\mathbb{G}$ 上での累乗，m は $\mathbb{G}$ 上での乗算の回数である．

[3] $|RL|$ は失効数である．

[4] 署名サイズ，署名コスト，検証コストそれぞれ $O(1)$ であり，失効検証コストは $O(|RL|)$ である．