様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　　元 年　　６ 月 １８ 日現在

機関番号：３２６５７
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１９２

研究課題名（和文）次世代型コンテンツセキュリティを実現するための多機能電子署名技術の研究

研究課題名（英文）Study of Multifunctional Digital Signature for Realizing Next-Generation Content Security

研究代表者

稲村　勝樹（INAMURA, Masaki）

東京電機大学・理工学部・助教

研究者番号：７０５７７３９５

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：既存のグループ署名のアグリゲート化、さらには順序付きアグリゲート署名への拡張に関する提案について、その実現性や安全性を評価し、実用性があることを示した。また、この電子署名の応用システムとして、企業・組織間連携における電子コンテンツの保証・管理をその署名順を含めて行えるシステムの提案を行った。この結果に、2019年2月にチェコ・プラハで開催された国際会議ICISSP2019に採録され、発表を行った。また、この発表について、Springerで発行予定のCCISに推薦され、現在投稿準備中である。

研究成果の学術的意義や社会的意義
既存の電子署名ベースにアグリゲート化、さらには順序付きアグリゲート化の拡張を行うことで、コンテンツの編集管理や流通過程の制御など、新たなコンテンツへの要求を解決する技術の創出が可能となった。
また、その提案署名方式をベースにコンテンツの共有過程を制御するシステムの提案を行うことで、企業・組織間でのコンテンツ共有を制御できることを示し、実際のサービスとして有用であることも示した。
さらに、この署名方式について実際にプログラミングによって実装評価を行い、提案した方式が実際の使用に耐えうるものであることを示し、今後の様々なコンテンツ保護方式に活用できる電子署名方式を実現できた。

研究成果の概要（英文）：Regarding proposal that existing group-signature is extended to aggregate-signature and order-specified aggregate-signature, we show that our proposed scheme has practicality with evaluation of possibility and security. Furthermore, we propose a new system with application of new signature scheme, which can guarantee and manage e-content files under collaboration of companies/organizations including protecting of order of signing. As a result, our proposal is accepted in ICISSP2019, and we present this scheme. Furthermore, this proposal is recommended to CCIS in Springer as a result of the presentation, and We are getting ready for submitting paper.

研究分野：セキュリティ

キーワード：電子署名　コンテンツ保護

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

これまでの技術革新により、著作物としてのコンテンツの「著作権」を保護する DRM はほぼ完成されている。その一方で、著作物には「著作権」と並んで「著作者人格権」がベルヌ条約や日本の著作権法でも規定されている。これは著作物において表現されている主義・主張が著作者のものであることを保証する権利で、他人への譲渡ができない重要な権利であり、(今後必須となるものであるが、) この保護技術は確立されていない。また、著作物とは異なるコンテンツとして、企業間で連携する仕様書などの業務書類について、インターネットなどによりオンラインでコンテンツ共有を行うようになった。このようなコンテンツについて、企業「内」におけるコンテンツ管理はこれまでも提案されているが、企業「間」にまたがってコンテンツを管理する技術は確立されていない。

２．研究の目的

近年著作物や業務書類などデジタルコンテンツの利用形態が拡大した状況を鑑み、コンテンツの流通や活用を前提においた異なる新たなコンテンツセキュリティ技術の確立を目的とする。既存の電子署名ベースにアグリゲート化、さらには順序付きアグリゲート化の拡張を行うことで、コンテンツの編集管理や流通過程の制御など、新たなコンテンツへの要求を解決する技術の創出が本研究の目的となる。

３．研究の方法

(1) 目的となる署名方式の機能はペアリング暗号技術のものと一部重複することから、ペアリング暗号技術の基本的な方法論を把握し、既存方式の理解に努めた後、それを電子署名に拡張することでプロトタイプを設計し、安全性も含めて理論評価を行う。

(2) 上記(1)で提案した電子署名をベースにし、著作者人格権の保護や企業間共有コンテンツの保護を実現するプロトコルを設計し、その実用性の理論評価を行う。

(3) 上記(1)で提案した電子署名を実際にプログラミングによって実装評価を行い、そのパフォーマンスについて検討を行う。

４．研究成果

(1) 既存のグループ署名をベースに、新しいアグリゲート権限委譲署名とその順序付きアグリゲート化拡張の設計を行った。
アグリゲート権限委譲署名の設計は以下の通りである。

[記号の説明]

G_1, G_2, G_3:位数qの巡回群

ペアリング$\mathrm{e}: G_1 \times G_2 \to G_3$

一方向性ハッシュ関数 $H_1:\{0,1\}^* \times G_2 \to G_1$,　$H_2:\{0,1\}^* \times G_2 \to Z_q^*$

$P \in G_1, Q \in G_2$

[準備]

グループ開設

グループ管理者 GM はランダムに$g \in Z_q^*$を選ぶ。そして、$Gpk = gQ \in G_2$を計算する。

グループ管理者 GM の秘密鍵と公開鍵のペアは(g, Gpk)

メンバになる予定の方々U_iはランダムに$s_i \in Z_q^*$を選ぶ。$U_i pk = s_i P \in G_1$を計算する。

メンバになる予定の方々U_iの秘密鍵と公開鍵のペアは$(s_i, U_i pk)$

[メンバ登録]

①　メンバになる予定になる人U_iは自身の公開鍵$U_i pk$をグループ管理者 GM に送る。

②　グループ管理者 GM は公開鍵$U_i pk$の本人確認をする。

③　グループ管理者 GM はメンバに同一の公開鍵$U_i pk$がいないか確認してから、メンバU_iにメンバ識別子ID_iを発行する。

④　メンバリスト ML に公開鍵$U_i pk$、メンバ識別子ID_iとの組$(ID_i, U_i pk)$を登録する。

[鍵発行]

メンバ

ランダムに$x_n \in Z_q^*$を選ぶ。

$K_{i,n} = x_n s_i Q$を計算する。

$\{ID_i, K_{i,n}, x_n Q\}$をグループ管理者 GM に送る。

グループ管理者 GM

受取った$\{ID_i, K_{i,n}, x_n Q\}$からメンバリスト ML を参照し、ID_iが登録されているか確認してから、対応する公開鍵$U_i pk$を見つけて、

$e(P, K_{i,n}) = e(U_i pk, x_n Q)$が成立するか検証する。

（$K_{i,n}$が本当にメンバU_iによって作られているか確認）

$K_{i,n}$が既に登録されていないか確認する。

$K_{i,n}$は署名者特定に使用するので、$(ID_i, K_{i,n})$を署名リスト SL に登録する。

メンバの権限情報をTとする。

$A = g \times H_1\{T||K_{i,n}\}$を計算して、メンバ$U_i$に送る。

[署名作成]

メンバU_iはメッセージ M に署名を行う。

ランダムに$r_n \in Z_q^*$を選ぶ。

グループ管理者 GM から受け取ったAを使用し、

$B = r_n Q$

$C = A + H_2(M||B) x_n s_i P + r_n P$

$K = K_{i,n} = x_n s_i Q$

T:権限情報

を計算する。

署名$\sigma = \{B, C, K, T\}$

[署名検証]

検証者はグループ公開鍵$Gpk = gQ$を入手する。

権限情報Tを確認する。

メッセージ M から$H_1\{K_{i,n}||T\}, H_2(M||B)$を計算する。

$e(C, Q) = e(H_1\{K_{i,n}||T\}, Gpk) \cdot e(P, H_2(M||B)K + B)$

が成立するか検証する。

以上の提案方式において、ペアリングにおける co-CDH 仮定により、正しく署名を作成・検証することができた。

さらに、上記提案の署名作成と署名検証を以下の通り拡張することで、順序付きアグリゲート化できることを示した。
[署名作成]

i番目の署名者Uはグラフψ_iになるようにメッセージM_iに署名を行う。署名者Uは自分の署名を行う前にグラフを参照し, 自分より前のすべての署名者の署名を検証する。署名者Uは$\left(para, \{P_{A_j}, M_j\}_{j\subset\psi_{T(i)}}, \psi_{T(i)}, \{\sigma_{Agg_j}\}_{j\in T(i)}\right)$が与えられてそれを用いて検証を行う。検証が失敗したならば終了する。検証が成功した場合は, ランダムに$r \in Z_q^*$を選ぶ。そして以下を計算する。

$$B_i = rQ$$
$$K_{u_i} = xs_uQ$$
$$h_i = H_2(M_i||B_i)$$
$$\{h_j = H_2(M_j||B_j)\}_{j\subset\psi_{T(i)}}$$

最後に, $C_i = \sum_{j\in T(i)} C_j + S_{u_i} + xs_u\left(\sum_{j\subset\psi_{T(i)}} h_j + h_i\right)P + rP$を計算する。$S_{u_i} = s_{A_i}H_1(T_{u_i}||K_{u_i})$は管理者から受け取った権限移譲署名鍵である。そして, 順序付きアグリゲート権限移譲署名$\sigma_{Agg_i} = (\{B_j, K_{u_j}, T_{u_j}\}_{j\subset\psi_i}, C_i)$を出力する。

検証者には, $\left(para, \{P_{A_j}, M_j\}_{j\subset\psi_{I(i)}}, \psi_{I(i)}, \{\sigma_{Agg_j}\}_{j\in I(i)}\right)$が与えられる。初めに, $i \le 3\frac{\log P}{\log a}$を満たしているか確認する[9]。満たしてなかったら検証失敗。次に, 権限情報$\{T_{u_j}\}_{j\subset\psi_{I(i)}}$がすべて適切であるか確認する。検証者は$\left|\{\sigma_{Agg_j}\}_{j\in I(i)}\right| > 1$の場合, $C = \sum_{j\in I(i)} C_j$とし, それ以外の$\left|\{\sigma_{Agg_j}\}_{j\in I(i)}\right| = 1$の場合は$C = C_j$とする。すべての$j$に対して, 以下の式が成立するか計算する。

$$e(C, Q) = \prod_{j\subset\psi_{I(i)}} \left\{e\left(\omega_j(\psi_{I(i)})H_1\left(K_{u_j}||T_{u_j}\right), P_{A_j}\right)\right\}$$
$$* e\left(P, \sum_{j\subset\psi_{I(i)}} \left\{\left\{\sum_{l\subset\psi_{T(j)}} \{H_2(M_l||B_l)\}\right.\right.\right.$$
$$\left.\left.\left. + H_2(M_j||B_j)\right\}\omega_j(\psi_{I(i)})K_{u_j}\right\} + \sum_{j\subset\psi_{I(i)}} \omega_j(\psi_{I(i)})B_j\right).$$

(2) 上記(1)で提案した署名方式をベースとし、各企業間で共有するコンテンツの流通過程を保証するプロトコルの提案を行った。

このプロトコルにおけるエンティティの役割について図 1 に示す。
この役割の元に構成されるプロトコルは以下の通りとなる。
[準備、メンバ登録、鍵発行、署名作成]
1 の順序付きアグリゲート化拡張方式と同じ。

[署名検証]

検証者には$\left(para, \{P_{A_j}, M_j\}_{j\subset\psi_{I(i)}}, \psi_{I(i)}, \{\sigma_{Agg_j}\}_{j\in I(i)}\right)$が与えられる。初めに,$i \le 3\frac{\log P}{\log 3}$を満たしているか確認する。満たしてなかったら検証失敗。権限情報$\{T_{u_j}\}_{j\subset\psi_{I(i)}}$がすべて適切であるか確認する。権限情報$\{T_{u_j}\}_{j\subset\psi_{I(i)}}$からシリアル番号を取り出し,取り出したすべてのシリアル番号を OCSP レスポンダに送信する。OCSP レスポンダは失効情報リストを参照し,検証者から受け取ったシリアル番号を確認する。受け取ったすべてのシリアル番号が失効情報リストになかったら,有効の情報を検証者に返し,それ以外なら,失効の情報を返す。検証者は OCSP レスポンダから失効の情報を受け取った場合は,検証失敗である。次に,検証者は$\left|\{\sigma_{Agg_j}\}_{j\in I(i)}\right| > 1$の場合,$C = \sum_{j\in I(i)} C_j$とし,それ以外の$\left|\{\sigma_{Agg_j}\}_{j\in I(i)}\right| = 1$の場合は$C = C_j$とする。すべての$j$に対して,以下の式が成立するか計算する。

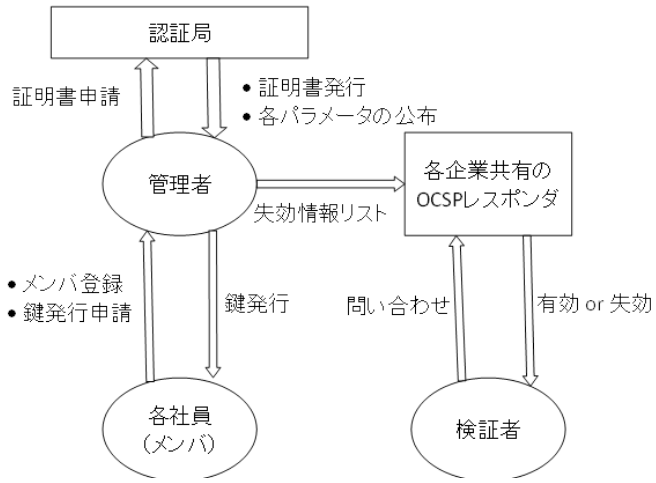

図 1：エンティティの役割

$$e(C,Q) = \prod_{j\subset\psi_{I(i)}} \left\{ e\left(\omega_j(\psi_{I(i)}) H_1\left(K_{u_j} || T_{u_j}\right), P_{A_j}\right)\right\}$$
$$* e\left(P, \sum_{j\subset\psi_{I(i)}} \left\{\left\{\sum_{l\subset\psi_{T(j)}} \{H_2(M_l||B_l)\}\right.\right.\right.$$
$$\left.\left.\left. + H_2(M_j||B_j)\right\}\omega_j(\psi_{I(i)}) K_{u_j}\right\} + \sum_{j\subset\psi_{I(i)}} \omega_j(\psi_{I(i)}) B_j\right).$$

(3) 提案方式についてプログラミングにより実装し、検証時におけるパフォーマンスを測定した。計測方法は、Intel 製の CPU である Core i3-3120M で動作する Windows10 上に Cygwin をインストールし、その上で動作する C コンパイラ GCC を用いて、メンバを 1000 人と想定し、1000 人分の署名を作成した後、その署名の検証時間を測定した。
なお、既存のアグリゲート署名である BLS 方式①、BGLS 方式②、YAO 方式③も実装し、比較した。
その比較結果を表 1 に示す。
この結果から、BLS や YAO の方式と比較しても充分に速く、一番速い BGLS と比較しても 1000

人あたりで0.5秒程度の差で収まっていることが確認でき、充分実用的であることを示した。

表1 検証時のペアリングの回数と検証時間（署名数1000個）

方式	ペアリングの回数（署名数N）	検証時間（秒）
BLS	2000(2N)	22.92
BGLS	1001(N+1)	14.27
YAO	2001(2N+1)	21.88
提案方式	1002(N+2)	14.72

＜引用文献＞
① Boneh D, Lynn B, Shacham H, Short signatures from the weil pairing, Proc. ASIACRYPT 2001, Vol.2248 of LNCS, pp.514-532, 2001.
② Boneh D, Gentry C, Lynn B, Shacham H, “Aggregate and verifiably encrypted signatures from bilinear maps”, Proc. EUROCRYPT 2003, Vol.2656 of LNCS, pp.416-432, 2003.
③ Yao D, Tamassia R, “Compact and Anonymous Role-Based Authorization Chain”, ACM Transactions on Information and System Security, Vol.12(15), 2009.

５．主な発表論文等

〔雑誌論文〕（計　0件）

〔学会発表〕（計　2件）
① Takuya Ezure, Masaki Inamura, An Order-Specified Aggregate Authority-Transfer Signature, 5th International Conference on Information Systems Security and Privacy (ICISSP2019), 2019.
② 江連拓也，稲村勝樹，順序付きアグリゲートグループ署名，2018年暗号と情報セキュリティシンポジウム（SCIS2018），2018.

〔図書〕（計　0件）

〔産業財産権〕
○出願状況（計　0件）

○取得状況（計　0件）

〔その他〕
特になし。

６．研究組織

(1)研究分担者
なし

(2)研究協力者
研究協力者氏名：江連拓也
ローマ字氏名：EZURE, Takuya