様式 C-19

科学研究費補助金研究成果報告書

平成２２年　５　月　３１　日現在

研究種目：若手研究（B）
研究期間：2006～2008
課題番号：18700006
研究課題名（和文）　双線形写像を用いた暗号プロトコルの提案

研究課題名（英文）　Research on Cryptographic Protocol based on Bilinear Maps

研究代表者
國廣　昇（KUNIHIRO NOBORU）
東京大学・大学院新領域創成科学研究科・准教授
研究者番号：60345436

研究成果の概要：
本研究課題では，双線形写像を用いた暗号プロトコルの提案を行った．具体的には，Secret Handshake プロトコルの拡張を行い，Monotone Condition という条件を持つ複数グループの認証の場合に，効率的に動作する方式を提案した．また，妥当な仮定の下で，安全であることの証明を行った．ついで，墨塗り署名方式の拡張を行い，墨塗りだけでなく，文書の削除を含む，より詳細な部分文書の制御が可能である方式を提案した．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００６年度	1,200,000	0	1,200,000
２００７年度	900,000	0	900,000
２００８年度	1,300,000	390,000	1,690,000
年度			
年度			
総　計	3,400,000	390,000	3,790,000

研究分野：暗号理論
科研費の分科・細目：情報学・情報学基礎
キーワード：暗号プロトコル，双線形写像，墨塗り署名

１．　研究開始当初の背景

インターネットの普及とともに，様々な機能が電子的なものに置き換わろうとしている．電子投票はその良い例である．電子投票においては，不正の投票を検知することが必須の要請である．大規模な選挙においては，さらに，その検査が実時間で行われることが必須である．既存の電子投票においては，票の正当性を一票ごとに検査をするのが一般的である．票の正当性の検査には，おもにゼロ知識対話証明やブラインド署名などの計算処理，通信コストに負荷のかかるプロトコルをサブルーチンとして用いて構成することが一般的である．不正者の数が多い場合には，たしかに，全ての投票のチェックを行なうことが当然の要請であるが，わずかの不正者しかいない場合（実際の選挙においては妥当な仮定）には，このような「重い」処理を全ての投票に対して行うことは明らかに非効率的である．一度に多くの票の検査を行なうことができれば，処理の軽い投票システムとなる．不正票の「探索」自身が重要ではなく，不正票の「存在」確認が重要なためである．この処理に双線形写像の適用を検討する．

暗号の分野で双線形写像が積極的に使わ

れ始めたのは，2000 年頃のことである．不正者追跡方式，ID に基づく暗号方式，各種電子署名方式などが次々に提案されている．現在のところ，暗号プリミティブレベルでの研究が多く，具体的な実用的で大規模なプロトコルへの応用は始まったばかりである．この研究課題では，幅広く実用的なプロトコルへの拡張を目指す．

２．研究の目的

本研究の主たる目的は，双線形写像を用いた暗号及び暗号プロトコルの提案を行うことである．これまでに，いくつかの基本的なプロトコルが提案されているが，双線形写像の適用範囲を拡大することが副次的な目的である．暗号プロトコルの提案として，次の二つのアプローチ
1. 双線形写像を用いることにより，初めて実現されるプロトコルの提案，
2. 双線形写像を用いることにより既存プロトコルの効率化，
が考えられるが，特に，本研究課題では，後者のアプローチからの研究を主に行なう．暗号および暗号のプロトコルにおいて，効率的であることはもちろんのことながら，より高い安全性が実現されていること，さらに，その安全性に関して，数学的な証明がついていることが必須である．本研究では，効率的であり，なおかつ安全性の高いプロトコルの構築を目指す．研究期間内に，双線形写像の特徴をうまく利用し，安全かつ効率的で多機能な暗号プロトコルの提案を目指す．また，平行して総線形写像を用いない方式の提案も行った．

３．研究の方法

本研究課題では，大きく分けて以下の二つの暗号のプトロコルの提案に取り組んだ．
(1) Secret Handshake プロトコル
(2) 付加機能のついた墨塗り署名
研究の方法に関して，順に説明する．

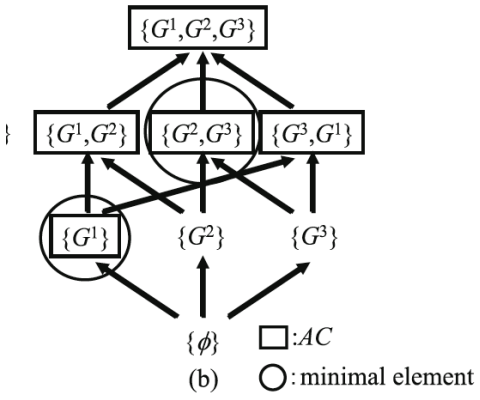
(1) Secret Handshake は，グループ認証方式の一つである．あるユーザが自分と同じグループに属するかを，自ら属するグループを明かすことなく検証することができるという特徴を有する．既存方式では，単一グループ，もしくは，所属するグループが全て等しい場合にしか，適用できなかったが，本研究課題では，緩やかな条件でも適用できる方式を提案した．ついで，提案方式の安全性の評価を行ない，妥当な仮定の下で安全であることを示した．

(2) 通常の署名方式では，文書の一部分を修正した場合，その性質上，その文書は改変されたと判断される．情報公開などの要請により，文章の一部分を墨塗りし，文章を公開する状況がある．この場合は，通常の署名方式を用いたのでは，正規の墨塗り操作による修正なのか，文書の改変なのかを検知することができない．そこで，文書の一部分を正規の手段により墨塗りをしても，署名検証時に有効と判断される方式が必要となる．また，状況によっては，墨塗りだけでなく，部分文書の削除が必要となるケースもある．しかしながら，墨塗りと削除の両者を同時に実現する方式はこれまでに提案されてこなかった．我々は既存の方式を拡張することにより．墨塗りおよび削除を同時に実現する方式を提案する．

４．研究成果

本研究課題では，
(1) Secret Handshake プロトコル
(2) 付加機能のついた墨塗り署名方式
に関して重点的に研究を行った．得られた研究成果を順に説明する．

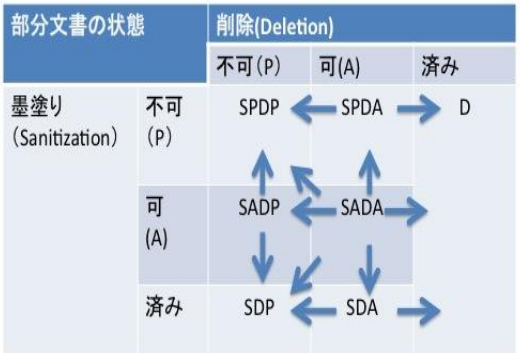
(1) Secret Handshake プロトコル
既存の Secret Handshake 方式では，認証できるグループの種類が一つだけであるか，複数のグループが関係する場合でも，全てのグループが同じであるかのどちらかであった．本研究課題では，この制限を緩め，任意の認証条件に適用できる方式を提案した．まず，素朴な方式として，全ての認証条件に対して，Secret Handshake プロトコルを行う方式を考える．しかしながら，この素朴な方式では，認証条件に比例したコストがかかるため，効率が悪い．この問題点を解決するため，本研究課題では，Monotone 性という条件を認証条件に導入し，この条件下で効率的な方式の提案を行った．Monotone 性に関して，下図を用いて説明する．



AC は，認証条件を示す．認証条件が monotone 性をみたすとは，ハッセ図において，下に位置する要素が AC に含まれている場合，その上の要素も全て含まれていることに対応する．提案方式では，まず，AC の最小要素を求めることから始める．この例では，{G1}と{G2, G3}が最小要素となる．素朴な方式では，５個の認証条件全てに対して，Handshake プロトコルを実行するが，monotone 性を有する認証条件の場合は，最小要素に対してのみ，Handshake プロトコルを実行すればよい．この例の場合では，2 回の実行で可能である．Monotone 性は，現実に即した条件であり，実質的には，適用範囲に制限を加えたことにならない．

ついで，提案方式の安全性を検証した．計算 Diffie-Hellman 問題が困難であるという仮定のもとで，提案方式は，Impersonation Resistance，Detector Resistance という安全性を持つことを証明した．

(2)付加機能のついた墨塗り署名方式
既存の墨塗り署名方式を拡張し，削除機能を付加した墨塗り署名方式の提案を行った．提案方式が保持する機能をまとめたのが下図である．



A，B をそれぞれ状態として，A→B は，遷移が可能であることを意味する．例えば，SADP →SPDP は，署名の墨塗りが許可されており，削除が禁止されている状態から，墨塗りも削除も禁止された状態へ遷移が可能であることを意味している．また，D という状態は，削除された状態を意味するが，一旦，削除された場合には，そこからどの状態にも遷移できないことを意味する．上の図は，我々の方式が意味のある全ての遷移を実現していることを示している．

次の表は，提案方式の特長を既存方式と比較を示している．ここで，n は署名を行う部分文書の個数を意味する．

	機能		効率
	墨塗り	削除	署名長
MIM+05	○	×	1
SIT06	○	×	n+1
MHI06	×	○	n
提案方式	○	○	2n

MIM+05，SIT06，MHI06 方式は既存方式を意味する．既存方式では，墨塗りか削除のどちらかの機能しか持っていないが，提案方式では，墨塗り，削除とも可能であるという特長を持っている．提案方式のデメリットとして，必要となる署名が長いという点が上げられる．署名長の削減が研究課題である．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　　3 件）

(1) Y. Kawai, S. Tanno, T. Kondo, K. Yoeneyama, K. Ohat and N. Kunihiro, “Extension of Secret Handshake Protocols with Multiple Groups in Monotone Condition,” IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E93-A, No.6 に掲載決定，2010.査読あり

(2) 伊豆哲也，國廣昇，太田和夫，武仲正彦，“双線形写像を用いた墨塗り署名方式の安全性について，” 情報処理学会論文誌，Vol. 47，No. 7，pp. 2409-2416，2006.査読あり

(3) N. Kunihiro W. Abe and K. Ohta, “Maurer-Yacobi ID based Key Distribution Revisited, ” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No.5, pp. 1421-1424, 2006.査読あり

〔学会発表〕(計　8　件)
(1) T. Izu, N. Kunihiro, K. Ohta, M. Sano, M. Takenaka, “Yet Another Sanitizable Signature from Bilinear Maps,” in Proc. of ARES 2009, pp.941-946, IEEE CS, 2009. Fukuoka, Japan.

(2) T. Izu, N. Kunihiro, K. Ohta, M. Sano and M. Takenaka, “Sanitizable and Deletable Signature,” In Proc. of WISA2008, LNCS5379, pp. 130-144, 2008. Jeju Island, Korea.

(3) 丹野翔太郎, 米山一樹, 川合豊, 國廣昇, 太田和夫, “複数グループ用 Secret Handshake の拡張方式の提案,” 暗号理論と情報セキュリティシンポジウム 2008, 3E2-3, 2008年1月, 宮崎.

(4) 牛田芽生恵, 川合豊, 國廣昇, 太田和夫,” 委託可能検証者指定署名, “ 暗号理論と情報セキュリティシンポジウム 2008, 3F3-2, 2008年1月, 宮崎.
(5) 泉雅巳, 伊豆哲也, 國廣昇, 太田和夫, “墨塗り・削除署名の拡張,” 電子情報通信学会情報セキュリティ研究会, ISEC2007-67, pp.147-154, 2007年7月, 函館.

(6) T. Izu, N. Kunihiro, K. Ohta, M. Takenaka and T. Yoshioka, “Sanitizable Signature with Aggregation,” in Proc. of ISPEC 2007, LNCS4464, pp.51-64, May 7-9, 2007, Hong Kong, China.

(7) 佐野 誠, 伊豆 哲也, 國廣 昇, 太田 和夫, 武仲 正彦, “部分情報の墨塗りと削除が可能な電子署名方式について,” 暗号理論と情報セキュリティシンポジウム 2007, 2C4-1, 2007年1月, 長崎

(8) 伊豆 哲也, 佐野 誠, 國廣 昇, 太田 和夫, 武仲 正彦, “Aggregate 署名を用いた墨塗り署名方式,” 暗号理論と情報セキュリティシンポジウム2007, 2C4-3,2007年1月, 長崎

６．研究組織
(1)研究代表者
國廣昇 (KUNIHIRO NOBORU)
東京大学・大学院新領域創成科学研究科・准教授
研究者番号：60345436