# 秘密分散法における不正防止技術に関する研究

OBANA, Satoshi / 尾花, 賢

(雑誌名 / Journal or Publication Title)
科学研究費助成事業 研究成果報告書
(開始ページ / Start Page)
1
(終了ページ / End Page)
5
(発行年 / Year)
2014-06

様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　　９　日現在

機関番号：　３２６７５
研究種目：　研究活動スタート支援
研究期間：　2012～2013
課題番号：　２４８０００６４

研究課題名（和文）秘密分散法における不正防止技術に関する研究

研究課題名（英文）A Study on Cheating Prevention in Secret Sharing Schemes

研究代表者
尾花　賢（OBANA, Satoshi）

法政大学・情報科学部・教授

研究者番号：７０６３３６００

交付決定額（研究期間全体）：（直接経費）　　2,400,000円、（間接経費）　　720,000円

研究成果の概要（和文）：通常の秘密分散における不正防止に関する研究においては、正当なシェアを観測した後に改ざんするシェアの値を決定する不正者に対して安全な4つの方式を提案した。方式は全て、同じ不正者特定を有する従来の方式と比較して最小のシェアサイズを実現している。また、従来存在しなかった、任意の有限体で安全性を保証する不正検知可能な秘密分散法の提案も行った。
シェア同士の演算により、秘密を復元することなく秘密に関する演算を行うd-multiplicative秘密分散法に関しては、不正成功確率が0となる方式が存在する条件を明らかにするとともに、閾値型、および一般のアクセス構造に対し、高確率で不正を検知する方式を提案した。

研究成果の概要（英文）：With respect to secret sharing schemes secure against rushing adversaries who determine their forged shares after observing shares of honest users, we construct four type of schemes secure against rushing adversaries. The sizes of shares of each proposed scheme achieves smallest bit length compared to those of existing schemes with the same security level. Further, we construct a scheme which can detect the fact of cheating and which ensure security whatever an finite field the secret belongs to. We should note that no existing schemes guarantee such a security feature.
With respect to d-multiplicative secret sharing schemes which enable each user to compute a share of a polynomial with degree less than d (where d is a predetermined constant), we clarify conditions with which a secure d-multiplicative scheme (in which no user can cheat the other users) exists. Furthermore, we construct secure and efficient schemes secure against threshold adversary and general adversary, respectively.

研究分野：　暗号・情報セキュリティ

科研費の分科・細目：　情報学基礎

キーワード：　効率の良い方式提案　理論的実現可能性の証明

１．研究開始当初の背景

秘密分散法は,秘密情報をシェアと呼ばれる複数の部分情報に分散し，アクセス構造と呼ばれるシェア集合の集合族に属するシェア集合を同時に集めない限り，元の秘密に関するいかなる部分情報も得られないことを保証する技術である．秘密分散法の中でも特に実社会での利用が多く，最も盛んに研究が行われている方式は，Shamir によって提案された(k,n)閾値型と呼ばれる秘密分散方式である(Shamir, Communications of the ACM, 1979)．(k,n)閾値型秘密分散法では，秘密情報から下記の性質を保証するｎ個のシェアを生成する：

- 任意のｋ個以上のシェアから秘密は一意に復元できる．
- どの k-1 個以下のシェアからも秘密に関する１ビットの情報も得ることができない．

前述の性質は，秘密情報をパブリッククラウドのように厳密な管理が必ずしも保証されない環境で秘密情報を安全に管理する際に望まれる性質であり，実際に多くの場面で(k,n)閾値型の秘密分散法が利用されている．

しかし，Shamir が提案した(k,n)閾値型秘密分散法は，秘密の漏えいに対する安全性は保証するが，部分情報の改ざんを行うことで，復元される秘密情報を改ざんするような不正は考慮していなかった．実際，Tompa と Woll は，Shamir の(k,n)閾値型秘密分散において，たった１つのシェアの値を改ざんするだけで，復元される秘密を，改ざんを行った不正者がある程度意図した形にコントロール可能であることを示している(Tompa, Woll, Journal of Cryptology, 1989)．Tompa と Woll は Shamir の方式に対する不正可能性を指摘するとともに，シェアを有する n-1 人の不正者の協力の下，秘密の復元時に利用される k-1 個のシェアを改ざんした場合でも圧倒的な確率で改ざんされた事実を検知することのできる方式を提案した．しかし，この提案方式はシェアのサイズ（ビット長）が元の秘密の２倍以上となり効率的ではないという問題を有していた．シェア改ざんの事実を検知することができる秘密分散法は，その後非常に盛んに研究がなされ，尾形，黒澤(Eurocrypt 1998)，Cabello, Padro, Saez (Designs, Codes and Cryptography 2002)，尾花，荒木(Asiacrypt 2006)らによって，シェアのサイズが理論的限界を達成，あるいは理論的限界と高々１ビットしか差のない方式が提案されている．一方，シェアが改ざんされた際に，改ざんされた事実を検知するだけではなく，改ざんされたシェアの特定までを行うことのできる方式も盛んに研究が行われている．このような方式においては，改ざんされたシェアを除去し，改ざんされていない新たなシェアを加えることで正しい秘密の復元を行うことが可能となるため，実用上非常に便利である．改ざんされたシェアを特定できる方式に関しては,Ben-Or と Rabin が n-1 人の不正者の協力の下，k/2 個改ざんされたシェアを圧倒的な確率で特定できる方式が提案されている(Rabin, Ben-Or, STOC, 1989)．しかし，提案された方式はシェアのビット長が秘密のビット長の 3n 倍程度と非常に大きくなるという問題を有していた．この問題に関しては黒澤，尾花，尾形(Crypto 1995)，Cramer, Dangard, Fehr (Crypto 2001)らが,よりシェアサイズの小さい方式を提案している．また，尾花(Eurocrypt 2011)によって，不正者の人数が k/3 以下の場合にシェアサイズの理論的限界をほぼ達成する方式が提案されている．

秘密分散法を秘密情報の安全な管理だけでなく，秘密情報を用いた安全な情報処理に利用するための研究も盛んに行われている．その中の一つに，Secure Multiparty Computation と呼ばれる技術がある(Ben-Or, Goldwasser, Wigderson, STOC, 1988)．Secure Multiparty Computation は，秘密情報 s1,s2,…,sN に対するシェアを有する n 人のユーザが協力して，秘密情報を明かすことなく秘密情報を入力とした任意の関数の出力 F(s1,s2,…,sN)を計算するプロトコルである．この分野は暗号の主要なトピックであり，多くの研究が盛んになされている．しかし，Secure Multiparty Computation では，関数 F の中に積算(AND ゲート)が現れるたびに n 人がネットワークを介して通信を行う必要があり，効率の改善が望まれている．一方，関数Ｆに現れる積算の回数の上限を設定することにより，他のシェア保有者とのネットワークを介した通信を行わずに所望の関数値 F(s1,s2,…,sN)に対するシェアを計算できる技術の研究も進んでいる．この技術は，d-multiplicative 秘密分散法と呼ばれる技術である．d-multiplicative 秘密分散法に関しては，今までに，個々のシェアから関数値のシェアを計算可能にするためのアクセス構造（どれだけのシェアを集めると秘密が復元できるかを表す構造）の必要十分条件の研究(Barkol, Ishai, Weinreb, Journal of Cryptology, 2010)や，d-multiplicative 秘密分散法の効率的な実現方法に関する研究(Chen, et al., Eurocrypt, 2008)などが盛んに行われてきた．

２．研究の目的

(1)　不正を検知する秘密分散，あるいは不正なシェアを特定する秘密分散に関する研究では，以下に挙げる三つの主要な課題が残されている．

① シェアのサイズが非常に小さい尾花(Eurocrypt 2011)の方式は，不正者の人数が k/3 以下の場合でしか安全性が担保

できず，また同論文で示されている不正者の人数が k/2 以下の場合に安全な方式は，改ざんされたシェアの特定に指数時間の計算量を有する．

② 不正を防止する秘密分散においては，秘密として扱うことのできる構造に制限が加えられていることが多く，任意の有限体で利用可能な方式が存在していない．

③ 黒沢，尾花，尾形方式(Crypto 1995)や尾花(Eurocrypt 2011)など，今まで知られているシェアの小さな方式は，不正者が秘密復元時にシェアを出す順序を遅らせ，正当なユーザの出したシェアを観測した後に，自分の出すシェアを決定することにより，改ざんを検知されずに誤った秘密を復元する不正が成功する．

上記の三つの問題は，秘密分散の普及のために解決すべき優先的な課題であり，特に第３の問題は，インターネットのような非同期のネットワークでは現実的な脅威となる問題であるため，早急な解決が望まれる．この状況を鑑み，本研究では，上記三つの問題を解決するような秘密分散法の提案を目的とする．

(2)　シェア同士の演算により，所望の関数 F に秘密を入力した値のシェアを生成することが可能な d-multiplicative 秘密分散においては，不正者を含んだ場合の議論は十分に行われておらず，不正者を含んだ場合に不正の検出・あるいは不正なシェアの特定が可能であるような関数あるいはアクセス構造の条件や，不正の検出・不正なシェアの特定を行う d-multiplicative 秘密分散法の具体的な構成は従来明らかになっていなかった．d-multiplicative 秘密分散法においても，不正者によるシェアの改ざんがもたらす関数の出力結果の改ざんは，アプリケーションによっては甚大な被害をもたらす可能性があるため，d-multiplicative 秘密分散における不正防止法の研究は，この技術の普及のため重要な課題となる．この状況に鑑み，本研究では，d-multiplicative 秘密分散において，不正防止が可能な条件の検討，および不正を防止可能な d-multiplicative 秘密分散法の具体的な方式提案を目的とする．

## ３．研究の方法

非同期なネットワークにおいて脅威となる，正当なシェアを観測した後に改ざんするシェアを決定する不正者(以下，このような不正者のことを Rushing Adversary と記すこととする)に対しても安全な方式の検討に当たっては，通常の(Rushing Adversary ではない)不正者に対してのみ安全性を担保可能ないくつかの効率の良い方式が存在している．例えば，k-1 人の不正者による不正を検知する方式としては，Cabello, Padro, Saez (Designs, Codes and Cryptography 2002), 尾花，荒木(Asiacrypt 2006)らが理論的限界をほぼ達成する方式を提案している．また，k/3 人，および k/2 人の不正者が存在する下で効率的に改ざんされたシェアを特定する方式としては，Eurocrypt 2011 で尾花が非常に効率の良い方式を提案している．研究の方法の一つとしては，これらの効率の良い方式をベースとして，Rushing Adversary による不正に対しても耐性を有するように方式の改良を検討した．

また，秘密分散における不正検知・不正なシェアの特定を行うための技術として，従来，ユニバーサルハッシュ関数族と呼ばれる暗号技術が多く利用されてきた．Rushing Adversary に対しても安全性を保証できる秘密分散，d-multiplicative 秘密分散，任意の有限体で安全性を保証できる秘密分散，いずれの秘密分散においても，ユニバーサルハッシュ関数をベースとした構成が有効なのではないかと考えることができる．そこで，本研究では，従来知られているユニバーサルハッシュ関数だけではなく，新たなユニバーサルハッシュ関数を構成することなどにより，従来達成できなかった安全性を有する方式の構成を行った．

不正を検知する d-multiplicative 秘密分散法が構成可能な条件の導出に当たっては，Barkol 等が提案している汎用的なアクセス構造に対する d-multiplicative 秘密分散法(Barkol, Ishai, Weinreb, Journal of Cryptology, 2010)の構成法をベースにした検討を行った．具体的には，この構成法にシェアの全員一致による合意という暗号プロトコルで汎用的に用いられるテクニックを導入することにより，改ざんの事実を検知する方式の構成可能性条件を明らかにした．

## ４．研究成果

Rushing Adversary に対しても安全性を保証できる秘密分散法に関しては，4 つの効率的な方式の提案を行った．シェアの総数を n，秘密を復元するために必要なシェアの数を k，不正者数の上限を t とした時，4 つの提案方式それぞれの方式の特徴は以下の通りとなっている．

(1)　第一の方式は，t<k/3 という条件の下で，不正の検知(不正が起こった場合にその事実を検知)する方式である．方式の構成に当たっては，不正防止可能な秘密分散でよく利用されるユニバーサルハッシュ関数を利用している．ユニバーサルハッシュ関数を Rushing Adversary に対して安全にする際には，ユニバーサルハッシュ関数のハッシュ値が不正者に対して明らかになってしまい，そのために，秘密分散が本来有しているはずの「k-1 個以下のシェアから秘密に関する情報が漏えいしない」という性質が損なわれる点が課題であった．提案方式では，秘密の情報を漏えいする可能性のある秘密のハッシ

ュ値自体も秘密分散で分散するという新しいアイデアを開発することで，上述の問題の解決に成功した．提案方式における秘密のサイズを|S|，不正者の不正成功確率をεとした時，提案方式のシェアサイズ|V|は$|V|=|S|/\varepsilon^3$となっている．

(2)　第二の方式は，t<n-1という条件の下で，不正の検知を行う方式である．この方式では，シェアを保有するユーザ全員に復元されたシェアのチェックを行う独立なユニバーサルハッシュ関数を保持させ，さらに全てのユーザのハッシュ値を秘密分散で分散するというアイデアにより，n-1人という非常に多い不正者に対して安全な方式の開発に成功した．提案方式のシェアサイズ|V|は$|V|=|S|/\varepsilon^{k+1}$となっている．

(3)　第三の方式は，t<k/3という条件の下，不正な(改ざんされた)シェアを特定することが可能な方式である．この方式は，Rushing Adversaryに対して安全ではない尾花の方式(Eurocrypt2011)をベースに提案を行っている．尾花の方式をRushing Adversaryに対して直接適用すると，方式で利用している鍵情報が不正者に漏えいし，結果として不正に成功してしまうという問題点が存在していたが，提案方式においては，Rushing Adversaryに対しても鍵情報が漏えいしないための鍵の符号化法を新たに開発することにより，Rushing Adversaryに対して安全な方式の開発に成功した．提案方式のシェアサイズ|V|は$|V|=|S|/\varepsilon^k$となっている．

(4)　第四の方式は，t<k/2という条件の下，不正な(改ざんされた)シェアを特定することが可能な方式である．この方式は，従来方式であるBen-OrとRabin (STOC'89)による方式をベースに構成した. Ben-OrとRabinの方式は，簡単な変換によってRushing Adversaryに対して安全な方式を構成できることが示されるが，シェアサイズが非常に大きくなるという問題点を有していた．提案方式では，Ben-Or, Rabinの利用していたユニバーサルハッシュ関数を最適化することにより，ユニバーサルハッシュ関数が利用する鍵のサイズを大幅に削減することに成功した．提案方式のシェアサイズ|V|は$|V|=|S|/\varepsilon^{n+t-1}$となっている．

上記の4方式はいずれも，同じ性質を有する従来の方式と比較して，最小のシェアサイズを実現しており，本研究の優位性を示している．

任意の有限体で安全性を保証できる秘密分散については，不正を検知可能な二つの方式を提案した．第一の方式は，不正の検知が可能な従来方式であるCabelloらの方式をベースに構成を行った．Cabelloらの方式は，非常にシェアサイズの小さな方式であるが，秘密分散において最も利用頻度の高い秘密の要素数が2のべき乗の体($GF(2^N)$)で安全性が保証できず，不正者が確率1で不正に成功してしまうという問題点を有していた．提案方式では，Cabelloらの方式で利用している改ざん検知用の関数$a(x)=x^2$を$a(x)=x^2+x^3$に変更することで，任意の有限体で安全性が保証できることを示した．また，この変更によるシェアサイズの増加分はわずか1ビットであることも示し，変更により方式の効率も損なわれないことも示した．

第二の方式は，新たなチェック関数を開発することによって構成した．第二の方式では，従来扱われたことのない，体上の情報逆元を利用した関数$a(x)=1+x^{-1}$を導入し，この関数を秘密のチェック用関数として利用することにより，任意の有限体で安全性が保証できる方式が構成できることを証明した．方式のシェアサイズはCabelloらの方式と比較して2ビット程度長くなるが，十分な効率を有していることが示されている．

シェア同士の演算により，秘密を復元することなく秘密を入力とした演算を可能とするd-multiplicative秘密分散法に関しては，まず，不正成功確率が0となるd-multiplicative秘密分散の存在する条件を明らかにした．さらに，閾値型のアクセス構造に対しては，従来知られているShamirの(k,n)閾値秘密分散(Shamir, 1979)の復元アルゴリズムを改良することにより，シェア同士の掛け算が可能，かつ不正成功確率を0にするような方式が構成可能であることを示した．また，より複雑な一般のアクセス構造の場合にも，CNF秘密分散と呼ばれる一般的な秘密分散の構成法と，参加者が秘密復元の際に提出するシェアの全員の一致を確認する暗号で汎用的に用いられるテクニックを組み合わせることにより，不正の成功確率が0となる方式が構成可能であることを示した．

上記で構成した方式は，理論的な実現可能性を示す上では非常に重要な方式であるが，シェアの総数nに対して方式のシェアのビット長が秘密の$2^n$倍となってしまい，実用性に難があった．そこで本研究では，不正者の不正成功確率を0ではなく，例えば$2^{-128}$等の非常に小さい値を許すことでシェアのサイズの改良を試みた．その結果，秘密のわずか3倍のビット長で上記で構成した方式と同じクラスの関数のシェアを計算することが可能な方式を構成することに成功した．本方式，および上記の方式は，不正を検知可能でかつ秘密を入力とした演算を可能とする初めての秘密分散方式となっており，理論的にも実用的にも非常に意味のある成果となっている．

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１件）

① Maki Yoshida and Satoshi Obana, Detection of Cheaters in Non-interactive Polynomial Evalucation, IACR Cryptology ePrint Archive, 査読なし, 2013/032, pp. 1-15, 2013

〔学会発表〕（計３件）

① Satoshi Obana and Kazuya Tsuchida, Cheating Detectable Secret Sharing Schemes Supporting an Arbitrary Finite Field, IWSEC 2014 to Appear, 2014年8月27日～2014年8月29日, 青森県, 発表予定

② 尾花賢, シェアの後出しをする不正者に対して安全な効率のよい秘密分散法, 電子情報通信学会情報セキュリティ研究会, 2014年3月10日～2014年3月11日, 名古屋大学

③ 吉田真紀, 尾花賢, Detection of Cheaters in Non-interactive Polynomial Evaluation, 2013年Compview暗号理論ワークショップ, 2013年2月20日～2013年2月21日, 東京工業大学

６．研究組織

(1)研究代表者

尾花　賢（OBANA, Satoshi）

法政大学・情報科学部・教授

研究者番号：７０６３３６００