科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　２０　日現在

機関番号：　１２６１２
研究種目：　若手研究(B)
研究期間：　2011～2013
課題番号：　２３７６０３３０

研究課題名（和文）統計的に不正検知可能な情報理論的暗号方式とその応用

研究課題名（英文）Information Theoretic Cryptography with Statistical Cheating Detection and Its Applications

研究代表者
岩本　貢（Iwamoto, Mitsugu）

電気通信大学・先端領域教育研究センター・准教授

研究者番号：５０３７７０１６

交付決定額（研究期間全体）：（直接経費）　　3,200,000円、（間接経費）　　960,000円

研究成果の概要（和文）：本研究では，情報理論的暗号理論における攻撃手法，および，それを検知する手法について研究した．特に，(2,2)しきい値秘密分散法におけるなりすまし攻撃検知確率の減衰指数と，シェアのサイズのトレードオフ関係を解明した．その結果．シェアサイズを冗長にすると，どのくらいなりすまし攻撃を防止しやすくなるかが厳密に明らかになった．それ以外に，視覚復号型秘密分散法に対して，不正を防止する手法や，視覚復号型秘密分散法が秘密情報（画像）を視覚的に復号するという物理的な特性をもつ点に着目して，現実的な観点から不正を行う方法を提案した．その他にも情報理論的暗号に関する幾つかの基礎的成果を得た．

研究成果の概要（英文）：In this research, we investigated the way of detecting cheating in information theoretic cryptography. In particular, we clarified that the trade-off between share size and the exponent of the success probability in impersonation attack on (2,2)-threshold secret sharing schemes. This result implies how we can easily detect the impersonation by making each share redundant. In addition, we proposed a method of preventing the cheating in visual secret sharing schemes (VSSS). We also discussed how to cheat the visual secret sharing schemes in a practical setting by focusing on the situation where VSSS is decrypted without computers. Other than the above, we clarified several fundamental results on information theoretic cryptography.

研究分野：　工学

科研費の分科・細目：　電気電子工学・通信・ネットワーク工学

キーワード：　不正検知　情報理論的安全性　情報理論的暗号　秘密分散法　視覚復号型秘密分散法

１．研究開始当初の背景

現在の暗号方式の多くは，安全性を計算量的な困難性に置いている．しかし，計算速度やアルゴリズムが高度に進歩した場合，あるいは量子計算機が登場した場合などに，これらの安全性が保証できなくなる可能性がある．このような背景に基づき，攻撃者の計算能力に依存せずに安全性が保証できる，情報理論的に安全な暗号方式が研究されている．

情報理論的に安全な暗号方式は暗号化や認証など様々な方式が研究されている．本研究では特に，暗号文に不正（改ざんや成りすましなど）が行われた場合にそれを検知し，正規の暗号文は正しく復号されるような方式に注目する．このような研究は秘密分散法を中心に精力的に行われてきた．

本研究に先立って，岩本・古賀・山本は秘密分散法において成りすまし攻撃を検知する方式と，統計学における仮説検定が密接に関係することを利用して，成りすまし攻撃成功確率の指数部と分散されたシェア（暗号文）のサイズがトレードオフの関係にあることを明らかにした．

２．研究の目的

本研究では，情報理論や統計学の成果を基に，情報理論的暗号理論における不正検知に対する理論的知見を深め，その応用を模索することを目的とする．

不正検知を行う暗号プリミティブは背景に述べた秘密分散法に限らず，他の情報理論的暗号方式も視野に入れる．また，不正検知だけでなく，不正防止手法や，実際の攻撃手法の提案なども含めて幅広く研究を行う．

３．研究の方法

本研究では，基礎的な理論と最新の情報に基づいて新しい理論や方式を創出し，応用することを目指した．特に，情報理論や統計学に関連する知見を深めつつ研究を進め，必要に応じて計算機実験を行うことを想定した．

研究を進めるにあたっては，研究成果にあるように，各組織の研究者および研究室の学生と適宜連携して研究を行っている．

目的で述べたとおり，不正検知に関連する，情報理論的暗号を広く視野に入れて研究を進め，情報理論的暗号やその安全性に関する考察なども行った．

４．研究成果

(1) 秘密分散法における不正検知

秘密分散法とは，秘密情報を幾つかの「シェア」と呼ばれる暗号文に暗号化し，シェアを幾つか集めれば秘密が復号できるが，それより集めたシェアの数が少ないと秘密情報に関する情報が一切漏洩しない方式である．最も基本的な秘密分散方式ではシェアが僅かでも改竄されるとその改竄を検知できないことが証明されていた．そこで，暗号化に冗長な情報をもたせることで，改竄や成りすましを検知する方法が研究されてきた．

本研究では，シェアからの復号誤り確率と，成りすまし攻撃の成功確率が，仮説検定における第一種，第二種の誤り確率と見なせることに注目し，仮説検定の理論を用いてこの問題を解析した．本研究では，研究開始時に得ていたこの視点をもとに議論を深め，研究の位置づけの明確化や，モデルの厳密化・一般化などをより洗練させた．

最終的に，（２，２）しきい値秘密分散法では，シェア間の相互情報量が最小のシェアサイズ（ビット長）と，最良の攻撃成功確率指数（攻撃成功確率が符号長の増加と共に減少する速度を表す指数）に本質的な働きをすることを明らかにした．この相互情報量を大きくすると，シェアサイズは大きくなるが，攻撃成功確率の減衰速度（指数）を速く（大きく）することが出来る．本研究ではこれらの関係，および最適値を，厳密な数学的理論として明らかにした．

最終的に纏められた成果は，情報理論分野で最もレベルの高い論文誌である IEEE Trans. on IT に載録された（論文 1）．

(2) 視覚復号型秘密分散法における不正防止手法

画像を用いて秘密分散法を実現する方法である視覚復号型秘密分散法に対して，改竄攻撃を防止する手法を提案した．具体的には，通常の復号操作（シェア画像の物理的な重ね合わせ）以外に，シェアをずらして重ねたりすることで別の画像が得られるようにする手法を開発した．このような機能を追加することで，シェアの改竄が難しくなることと，シェアの改竄が行われたかどうかを容易にチェック出来ることが期待できる（論文２）．

(3) 視覚復号型秘密分散法の現実的な設定の下での改ざん攻撃・およびその対策

不正検知の問題と関連して，不正そのものを行う研究も行った（学会発表４）．

通常の暗号方式の安全性は秘密情報（秘密鍵など）以外の仕様を全て公開した状態でもなお安全であることを求められる（ケルクホフスの原理）．しかし，計算機を使用せずに復号が可能な視覚復号型秘密分散法に対しては，このような仮定は必ずしも現実的とはいえず，仕様を知らなくても改ざんが成功する場合を考える方が現実的である．より具体的には，計算機を用いず復号する復号者は，復号された画像が自然な画像であれば，わざわざ暗号化方式の使用を詳細に検討することなく，改竄された復号画像をオリジナルな秘密画像として受け入れてしまう可能性が

充分考え得る.

本研究では，ケルクホフスの原理の下で，改竄攻撃が無視できる確率でしか成功しないことが証明されていた視覚復号型秘密分散法が，ケルクホフスの原理を満たさない現実的な状況の下では常に（確率１で）改竄可能であることを示した.

本課題については研究期間終了後も研究を継続している．特に提案した攻撃に対する対策が今後の課題である.

(4) その他

情報理論的安全性そのものに関する研究として，秘密鍵暗号と，視覚復号型秘密分散法の安全性規準の提案と解析を行った.

まず，情報理論的安全性と計算量的安全性の関係を明らかにするために，通常の確率的独立性で定義された安全性概念と，強秘匿性や識別不可能性といった種々の安全性概念の帰着関係を調べ，情報理論的安全性概念が計算量的な概念よりどのような意味で強い安全性をもつかを明らかにした（学会発表３）.

また，雑誌論文３，学会発表１において，視覚復号型秘密分散法に新しい安全性基準を導入することで，従来の方式の効率（復号画像の画質）の限界値を突破する暗号化方式が存在することを示した.

改竄攻撃検知が必要とされる暗号方式として電子オークションの提案と解析に関しては，改竄攻撃を考慮するところまで研究が進展しなかったので，これも今後の課題としたい（国内発表５，８，１０）.

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. M. Iwamoto, H. Koga, and H. Yamamoto, “Coding theorems for a (2, 2)-threshold scheme with detectability of impersonation attacks,” IEEE Trans. on Information Theory, vol.58, no.9, pp. 6194-6206, 2012. http://dx.doi.org/10.1109/TIT.2012.2204546（査読あり）

2. A. E. Torujillo, M. N. Miyatake, M. Iwamoto, and H. P. Maena, “A cheating prevention EVC scheme using watermarking techniques,” Revista Facultad de Ingenieria, Univ. Antioquia, no.63, pp. 30-42, June, 2012. http://www.redalyc.org/pdf/430/43025100003.pdf（査読あり）

3. M. Iwamoto, “A weak security notion for visual secret sharing schemes,” IEEE Trans. on Information Forensics and Security, vol. 7, no. 2, pp. 372-382, 2012. http://dx.doi.org/10.1109/TIFS.2011.2170975（査読あり）

〔学会発表〕（計 11 件）

1. M. Iwamoto, “Security notions of visual secret sharing schemes,” International Workshop on Advanced Image Technology (IWAIT2013),pp.95-100, Jan., 2013.（招待講演, 2013 年 1 月 7 日）

2. M. Iwamoto and J. Shikata, “Information theoretic security for encryption based on conditional Rényi entropies,” Proc. of International Conference on Information Theoretic Security (ICITS), pp.103-121, 2013.（査読有, 2013 年 11 月 28 日）

3. M. Iwamoto and K. Ohta, “Security Notions for Information Theoretically Secure Encryptions,” IEEE-ISIT 2011, pp.1743-1747, 2011.（査読有, 2011 年 8 月 4 日）

4. P. Lumyong, M. Iwamoto, and K. Ohta, “Cheating on Visual Secret Sharing Schemes in Practical Setting,” 暗号と情報セキュリティシンポジウム (SCIS2014), 1E1-1, 2014.（査読無し, 2014 年 1 月 21 日）

5. 西出隆志, 岩本貢, 岩崎敦, 太田和夫, “自動タイブレークの仕組みを持つ第 M+1 価格暗号オークション方式 ,” 暗号と情報セキュリティシンポジウム (SCIS2014), 2D4-2, 2014.（査読無し, 2014 年 1 月 22 日）

6. M. Iwamoto and J. Shikata, “Revisiting Conditional Rényi Entropy and its Application to Encryption: Part I –Properties of Conditional RÅLenyi Entropy–,” 暗号と情報セキュリティシンポジウム(SCIS2013), 1F1-3, 2013（査読無し, 2013 年 1 月 22 日）.

7. J. Shikata and M. Iwamoto, “Revisiting Conditional Rényi Entropy and its Application to Encryption: Part II –Fano’s Inequality and Shannon’s Bound–,” 暗号と情報セキュリティシンポジウム (SCIS2013), 1F1-4, 2013（査読無し, 2013 年 1 月 22 日）.

8. M. Iwamoto, K. Ohara, Y. Sakai, and K. Ohta, “Information Theoretic Analysis of a t-resilient First-Price Auction Protocol,” 暗号と情報セキュリティシンポジウム (SCIS2013), 4D1-2, 2013（査

読無し，2013 年 1 月 25 日）．

9. 岩本貢，“しきい値法の一般化とその構成法，”電子情報通信学会総合大会（公募セッション：ネットワーク符号加法と秘密分散法），AS-2-2，2012（査読無し，2012 年 3 月 22 日）．

10. 大原一真，坂井祐介，岩本貢，太田和夫，“情報理論的に安全な First-Price オークションプロトコル，”暗号と情報セキュリティシンポジウム（SCIS2012），4B1-3，2012．（査読無し，2012 年 1 月 31 日）

11. 岩本貢，太田和夫，“共通鍵暗号方式における情報理論的安全性と計算量的安全性の関係，”電子情報通信学会研究会研究報告，IT2011-5，25-30，May，2011．（査読無し，2011 年 5 月 20 日）

〔その他〕
研究成果等は
http://ohta-lab.jp/member/mitsugu/，
http://ohta-lab.jp/users/mitsugu/index.html
http://www.ghrdp.uec.ac.jp
にて随時公開している．

６．研究組織

(1)研究代表者
岩本　貢（IWAMOTO，Mitsugu）
電気通信大学・先端領域教育研究センター
特任准教授
研究者番号：５０３７７０１６

(2)分担研究者　なし

(3)連携研究者　なし