様式 C-19

科学研究費補助金研究成果報告書

平成２３年６月３日現在

機関番号：１２６１２
研究種目：若手研究（B）
研究期間：２００８～２０１０年度
課題番号：２０７６０２３６
研究課題名（和文）　情報理論的に安全な暗号システム実現のための理論的研究

研究課題名（英文）　Theoretical Study for Practical Applications of Information Theoretically Secure Cryptosystems

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・特任助教
研究者番号：５０３７７０１６

研究成果の概要（和文）：本研究では，情報理論的暗号をより実用化しやすくするために必要と思われる基礎的な理論研究を行い，幾つかの結果を得た．主要成果は大きく３つあり，(1) 不正検出可能な(2,2)しきい値秘密分散法に対する符号化定理,(2) 視覚復号型秘密分散法の効率的な実現方式の提案,および (3) 共通鍵暗号における情報理論的暗号方式の安全性概念に関する新しい知見，である．その他，情報理論的な手法を通常の暗号理論や暗号実装の諸問題に応用し，新たな成果を得た．

研究成果の概要（英文）：We studied information theoretically secure cryptosystems in order to make them more practical. As a result, we obtained three results along with this research direction. Three main results are: (1) coding theorems for (2,2)-threshold secret sharing schemes secure against cheaters, (2) a proposal of efficient visual secret sharing schemes by relaxing information theoretical security notion, and (3) a new look at relations among information theoretically secure and computationally secure symmetric key encryptions. Furthermore, we obtained several results in cryptography and information security in which information theoretic methods are effectively utilized.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,100,000	330,000	1,430,000
2009 年度	1,000,000	300,000	1,300,000
2010 年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,100,000	930,000	4,030,000

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：暗号・情報セキュリティ，情報理論的暗号，秘密分散法，不正検出

１．研究開始当初の背景

情報理論的暗号システムは，強い安全性を保証することから，長期的に安全性を保証したい場面等での実用が強く求められている．しかし，情報理論的暗号方式を実用化するためには様々な問題が存在する．例えば，符号化効率の悪さや，真の乱数を使用している（実際には疑似乱数を使う）などの問題である．

このような問題を解決するためには，安全性を緩和したり，問題設定を変更することで対処することが考えられるが，そのような理論的研究はあまり行われていない．このよう

な背景から，情報理論的暗号方式を実用化するための基礎的な知見をより深める必要がある．

２．研究の目的

上記の背景に基づき，情報理論的に安全な暗号システムを実現するために必要となる技術を理論的側面から模索する．
特に，情報理論的暗号技術を実用化するにあたって障害となりそうな部分を適宜修正し，高い安全性は出来るだけ保ちつつ，より効率的な手法を確立することを目指す．

３．研究の方法

情報理論的暗号理論で通常用いられる安全性条件や設定に囚われることなく，柔軟に問題を設定して解決の方法を模索する．
情報理論的暗号理論は暗号理論の一分野であるが，情報理論とも非常に関係の深い分野であるため，研究においては，情報理論や計算量理論，確率論などの理論を積極的に取り入れる．必要に応じて計算機実験も行う．
情報理論的暗号の研究は種々の対象があるが，研究者がこれまで行ってきた秘密分散方や視覚復号型秘密分散法を題材に，研究を進める．

４．研究成果

計画当初の目的に対して，得られた成果は以下の３点である

1）秘密分散法における不正検出

情報理論的暗号の代表的方式である秘密分散法において，不正検出の問題は以前から研究されてきた．しかし，これらの方式には不正検出の成功確率を１に近づけると，暗号文のレートが発散するということが知られている．本研究では，この問題を解決するために，任意に小さい攻撃成功確率を許すことで，成りすまし攻撃に対する不正検出が，有限のレートで１に漸近させられることを示した（文献②，③，⑮，⑯，⑱）．
成りすまし攻撃については符号化定理の形で一定の成果が出ており，論文を投稿中である．しかし，この攻撃を強化した改ざん攻撃については何も分かっておらず，今後の研究課題といえる．

2）弱い視覚復号型秘密分散法の提案

秘密分散法の視覚的実現手法である視覚復号型秘密分散法は，情報理論的安全性を保証するために，非常に復号画質が悪い方式であることが知られている．本研究では，視覚復号型秘密分散法における情報理論的安全性を現実的な範囲内で緩和することで，復号画像の画質を向上させる方式を提案した（文献④）．この成果は現在論文投稿中である．

3）情報理論的安全性の再考察

情報理論的安全性概念を計算量的暗号の観点から再考察し，安全性の強弱関係を明らかにした．その結果，安全性の強弱関係を明らかにするだけでなく，情報理論的安全性と乱数生成問題などの関係も判明しつつある（文献⑥，⑪）．本成果は 2011 年 8 月に開催予定の国際会議，IEEE International Symposium on Information Theory に採録が決定している．
本研究は，暗号の安全性概念全体という広い視点で情報理論的安全性を見直す作業となっており，このような基礎的な考察を通して，今後，より効率的な情報理論的暗号方式が提案できることを目指している．

その他，視覚復号型秘密分散法の新たな実現手法の提案（①，⑭），情報理論的・確率論的手法を用いて，暗号技術の構築・解析を行う研究を行っている（⑦，⑧，⑩，⑬）．

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 0 件）

〔学会発表〕（計 16 件）

[査読付き国際会議]

① A. Espejel-Trujillo, M. Nakano-Miyatake, and M. Iwamoto, “Visual Secret Sharing Schemes for Multiple Secret Images Including Shifting Operation of Shares,” 6th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE 2009), pp.433-438, November 20, 2009.

② H. Koga, M. Iwamoto, and H. Yamamoto, “Coding Theorems for a (2, 2) Threshold Scheme Secure against

Impersonation by an Opponent," IEEE-ITW 2009, pp.188-192, October 13, 2009.

③ M. Iwamoto, H. Yamamoto, and H. Koga, "A coding theorem for cheating-detectable (2,2)-threshold blockwise secret sharing schemes," IEEE-ISIT 2009, pp.1308-1312, June 30, 2009.

④ M.Iwamoto, "Weakly secure visual secret sharing schemes," ISITA2008, pp.42-47, December 8, 2008.

[国内シンポジウム等（査読なし）]

⑤ 李奇，五味澤重友，岩本貢，太田和夫，崎山一男，"Trivium のセットアップタイム違反に基づく新しい故障差分解析," **電子情報通信学会研究会研究報告**, IEICE-ISEC2010-122, pp.333-339, 2011 年 3 月 4 日.

⑥ 岩本貢，太田和夫，" 情報理論的に安全な暗号化のための安全性概念," **CompView 暗号理論ワークショップ**，東京工業大学，東京，2011 年 2 月 21 日.

⑦ 坂井 祐介，岩本 貢，駒野 雄一，太田和夫，"FDH 署名の安全性証明の再考," **暗号と情報セキュリティシンポジウム** (SCIS2011), 4A2-1, 2011 年 2 月 21 日.

⑧ 名渕大樹，岩本貢，崎山一男，太田 和夫，"Joux-Lucks の 3-collisions 探索アルゴリズムに関する計算量の詳細な検討," **暗号と情報セキュリティシンポジウム** (SCIS2011), 4B1-4, 2011 年 1 月 28 日.

⑨ 落合隆夫，山本大，伊藤 孝一，武仲正彦，鳥居直哉，内田大輔，永井利明，若菜伸一，岩本貢，太田和夫，崎山 一男，"電磁波解析における局所性と放射磁界方向について," **暗号と情報セキュリティシンポジウム** (SCIS2011), 2D3-3, 2011 年 1 月 26 日.

⑩ 山本大，崎山一男，岩本貢，太田和夫，落合 隆夫，武仲 正彦，伊藤 孝一，" ラッチの乱数出力位置を利用した PUF による ID 生成/認証システムの信頼性向上手法," **暗号と情報セキュリティシンポジウム** (SCIS2011), 2D1-1, 2011 年 1 月 26 日.

⑪ 岩本貢，太田和夫，" 情報理論的に安全な暗号化のための安全性概念," **情報理論とその応用シンポジウム** (SITA2010), pp.202-207, December 1, 2010.

⑫ M. Iwamoto, Y. Li, K. Sakiyama, and K. Ohta, "A general construction method of visual secret sharing schemes with share rotations," Technical Report of IEICE, ISEC2010-49, pp.67-74, September 10, 2010.

⑬ 長井大地，塙知剛，岩本貢，崎山一男，太田和夫，"PUF-HB 認証プロトコルに対する能動的な攻撃," **暗号と情報セキュリティシンポジウム**, 2C2-5, January 21, 2010.

⑭ 李 陽，岩本 貢，太田和夫，崎山一男，"画像の回転に対する新しい視覚復号型秘密分散法," **電子情報通信学会研究会研究報告**, ISEC2009-5, pp.29-36, May 22, 2009.

⑮ 古賀弘樹，岩本貢，山本博資，"なりすまし攻撃を検出できる (2, 2) しきい値法に関する符号化定理," **電子情報通信学会研究会研究報告**, IT2008-66, ISEC2008-124, WBS2008-79, pp.143-150, March 9, 2009.

⑯ 岩本貢，山本博資，"漸近的にほぼ確実に不正検出可能な秘密分散法," **暗号と情報セキュリティシンポジウム**, 1F1-2, January 20, 2009.

⑰ M. Iwamoto, "Weakly secure visual secret sharing schemes," **暗号と情報セキュリティシンポジウム**, 1F1-4, January 20, 2009.

⑱ 岩本貢，山本博資，"漸近的にほぼ確実に不正検出可能な秘密分散法," **情報理論とその応用シンポジウム**, pp.532-537, October 9, 2008.

〔図書〕（計１件）

⑲ 電子情報通信学会 知識ベース「知識の森」
http://www.ieice-hbkb.org/portal/
1群1編「情報理論」13.4章「秘密分散」

〔その他〕
ホームページ等
http://www.quest.is.uec.ac.jp/mitsugu/
http://www.ghrdp.uec.ac.jp/

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・特任助教
研究者番号：５０３７７０１６

(2)研究分担者　なし

(3)連携研究者　なし