科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１９　日現在

機関番号：　３２６４１
研究種目：　基盤研究(A)
研究期間：　2010～2013
課題番号：　２２２４６０５３

研究課題名（和文）ＬＳＩ物理解析攻撃に対する次世代の安全性評価基準策定のための理論体系構築と実証

研究課題名（英文）A research on constructing a security evaluation framework for physical attacks on cryptographic LSIs

研究代表者
今井　秀樹（Imai, Hideki）

中央大学・理工学部・教授

研究者番号：７００１７９８７

交付決定額（研究期間全体）：（直接経費）　　36,400,000円、（間接経費）　　10,920,000円

研究成果の概要（和文）：本研究では，LSIやスマートカード等の物理デバイス上に実装された暗号方式の安全性評価手法を確立するために，理論的・実験的に攻撃手法の解析を行い，攻撃が成功する仕組みの本質を明らかにする．その上で，物理解析攻撃に対する強力な対策手法を提案することを目指す．これにより，物理解析攻撃に対する強力な対策法が得られることになり，今後益々利用が高まると考えられる暗号LSIの安全利用に貢献する．

研究成果の概要（英文）：The results of this research provide strong countermeasures against physical attack on cryptographic devices. We first analyze existing attack algorithms and countermeasures, and evaluate the potentials of the attack algorithms by theoretical and experimental analysis. Then, we propose strong countermeasures against side-channel attacks on the basis of the results of the analysis, and evaluate the security of the countermeasures.

研究分野：　情報学

科研費の分科・細目：　計算基盤・情報セキュリティ

キーワード：　暗号理論　耐タンパデバイス　物理解析攻撃

１．研究開始当初の背景

情報機器および情報ネットワークの普及に伴い，暗号技術が一般に広く利用されるようになってきた．身近なところでは，インターネットによる通信や携帯電話，デジタル放送,あるいは Suica や Edy といった電子マネーなどに暗号技術が利用されている．これらの製品やサービスは，社会に広く普及し，社会基盤の一部ともなっているため，その安全性の確保は社会的な要請となっている．これに応えるため，暗号アルゴリズムや暗号プロトコルの安全性に関して様々な理論的研究が行われてきた．

しかし，暗号アルゴリズムや暗号プロトコルそのものが安全であっても，それらが実装された場合の安全性が保証されるとは限らない．実際，物理デバイス上に実装された暗号に対しては，様々な攻撃が提案されている．なかでも，サイドチャネル攻撃と呼ばれる攻撃は，暗号化処理を行っているデバイスの消費電力や漏洩電磁波等の物理情報を測定し，それらを統計的に解析することでデバイス内の秘密鍵を特定する攻撃である．サイドチャネル攻撃を実施するには，基本的にはオシロスコープと PC があればよく，コスト的には個人などで実施することも可能である．また，統計解析手法もそれほど高度なものではなく，ある程度の専門知識があれば解析用ソフトウェアを作成することが可能である．このような理由から，サイドチャネル攻撃は現在大きな脅威となっており，その対策手法の確立は社会的な要請となっている．

２．研究の目的

本研究では，物理デバイス上に実装された暗号方式の安全性評価指標の確立を最終的な目標として，サイドチャネル攻撃に対して有効な対策手法技術の構築を行うことを目的とする．

３．研究の方法

本研究では，まず現在知られている最先端のサイドチャネル攻撃手法やサイドチャネル攻撃対策手法に関連する技術調査を行い，それらの攻撃性能や防御性能の限界を理論的評価や実証実験により明らかにする．その上でさらに強力な攻撃手法の提案を行い，サイドチャネル攻撃法の最大攻撃能力に関して理論的・実験的の両面から評価を行う．こうして得られた知見を用いて，サイドチャネル攻撃に対する極めて有効な対策手法を確立する．

４．研究成果

本研究の主な研究成果は以下のとおりである．

(1)サイドチャネル攻撃手法に関する研究

既存研究として，差分解析，相関解析，相互情報量解析などいくつかのサイドチャネル攻撃手法が提案されている．しかしこれらの攻撃手法の優劣及び，どのような状況においてどの攻撃手法が有効かという評価はあまりなされていない．本研究ではサイドチャネル攻撃用標準評価ボード SASEBO を利用して,ASIC や FPGA などの回路の種類の違いや，様々なサイドチャネル対策手法が組み込まれた回路に対して，どの攻撃手法を用いるのが最も効率的かを網羅的に調査した．調査では,米国標準暗号である AES を攻撃対象暗号アルゴリズムとして利用した．

さらに，通常のサイドチャネル攻撃とは異なり，予め回路特性を取得しておくテンプレート攻撃と呼ばれるサイドチャネル攻撃のクラスに対して，機械学習のアプローチを用いた新しい攻撃手法を提案した．

これらの研究テーマに関して以下の①～⑥の成果を得た．

①既存のサイドチャネル攻撃対策手法の性能評価を行った．既存のサイドチャネル攻撃対策手法として回路に流れる情報を別の情報でマスクする手法が提案されている．本研究では代表的なマスク手法である WDDL(Wave Dynamic Dual-rail Logic)と MAO (Masked-And-Operation) に対して相関電力解析(Correlation Power Analysis，CPA)及び相互情報量解析(Mutual Information Analysis，MIA)という 2 種類のサイドチャネル攻撃手法による安全性評価を行った．

WDDL は LSI 内部に実装された論理回路に対し，それと相補的な論理回路も実装することで，両方の論理回路における消費電力の総和を常に一定に保ち，回路の内部状態と消費電力との相関を断ち切る手法である．また，MAO は回路内で処理される情報に対し，乱数を付加した状態で演算を行う方式である．

実験では SASEBO-R 上の ASIC チップに実装された対策済み AES に対し，CPA と MIA を用いて攻撃を行った．実験の結果，WDDL，MAO の両者共に CPA よりも MIA の方が，攻撃成功確率が高くなることが示された．

②①の研究結果から，MIA の方がサイドチャネル対策済み暗号回路に対しては攻撃能力が高いことが示された．MIA を実施する際には，回路の消費電力量を確率変数と考え，その確率密度関数を推定する必要があるが，その推定方法の違いが MIA の攻撃成功確率に大きな影響を与える可能性がある．既存の MIA に関する研究では，確率密度関数推定法が攻撃成功確率に与える影響について詳細に調査されたものはなく，どの確率密度推定法が MIA に最も適しているかを調べることは MIA の性能を評価するために重要である．

本研究では,確率密度関数の推定方法として(1)確率変数が正規分布であることを仮定したパラメトリック法，(2)ヒストグラム法，(3)カーネル密度推定法を取り上げ，どれが MIA に最も適しているかを実験により調査し

た.

実験では SASEBO-GII 上の FPGA に実装した AES に対して，確率分布推定法の異なる MIA を用いて攻撃し，鍵を完全に復元するのに必要となる消費電力波形数により攻撃の強度を推定した．実験の結果，攻撃成功のために必要とした波形数は，パラメトリック法では 12,400 波形，カーネル密度推定法では,5,900 波形であった．また，ヒストグラム法では 20,000 波形を用いても鍵の完全復元は成功しなかった.

本実験結果より，利用する確率密度推定法が MIA の攻撃能力に与える影響が大きいことが明らかとなった．また，カーネル密度推定法が MIA 最も適した推定法であるという実験結果が得られた.

③①の研究結果からサイドチャネル攻撃対策が施された回路に対しては,MIA の方が CPA よりも攻撃成功確率が高くなることが示された．本研究では，この事実をより詳細に調査するために，さらに 2 種類の対策手法（Masked Dual-rail Pre-charge Logic (MDPL)法，Threshold Implementation (TI)法）を加え，CPA と MIA それぞれに対する攻撃耐性評価を実施した.

評価実験の結果，攻撃者が LSI 内部回路の実装を知っており，実装法に特化した攻撃を実施できる環境にある場合（対策が施されていない場合や，利用されている対策手法を攻撃者が知っている場合など）には CPA の方が MIA よりも攻撃成功確率が高いことが示された．しかし，攻撃者が回路の内部実装方法を知らない状況においては，MIA の方が攻撃成功確率の高くなることが示された．これは CPA においては，回路内部のレジスタの状態遷移ビット数が消費電力と線形相関を持つことを利用しているのに対し，MIA では，相互情報量を用いることにより線形でない相関も考慮されているため，漏洩情報と内部状態が乖離している場合でも，ある程度正しく相関関係を捉えることができるためと考えられる.

④共通鍵暗号 AES の安全性はアルゴリズム内の S-BOX と呼ばれる非線形演算に強く依存している．AES においては S-BOX として拡大体 GF(256)の逆元演算とアフィン変換が組み合わされたものが利用されており，さまざまな S-BOX の実装法が提案されている．S-BOX 演算は，AES の中で最も計算コストが高い演算の一つであることから，S-BOX の計算内容と LSI の消費電力には高い相関が現れることが知られており，S-BOX 演算はサイドチャネル攻撃における攻撃対象として利用されることが多い．このような理由から，S-BOX の実装方法の違いはサイドチャネル攻撃に対し大きな影響を与える可能性があると考えられる．本研究では，S-BOX の実装方式がサイドチャネル攻撃の成功確率に与える影響を評価するために，代表的な S-BOX の実装方法であるテーブル参照方式，Positive Polarity Reed-Muller(PPRM)方式，合成体方式の三つの場合について CPA，MIA を利用した安全性評価を実施した.

実験の結果，各実装方式に対し CPA の方が MIA と比較して概ね高い攻撃成功確率を得られた．しかし，MIA に関しても PPRM 方式以外の実装方式では，攻撃に成功した．さらに，本実験において CPA と MIA を別々に利用するだけではなく，CPA で得られた相互情報量に基づいて MIA での攻撃タイミング等を設定するという攻撃の有効性が示唆された.

⑤④の結果から代表的なサイドチャネル攻撃手法である CPA と MIA をそれぞれ単体で実施するのではなく，両者を適切に組み合わせることで，それぞれ単独で利用するよりも強力な攻撃が実現できる可能性が示された．この手法の効率を検証するために，CPA と MIA の合成手法に関して検討を行い，特に CPA の攻撃成功率が低くなる状況において，それを補うように MIA を利用する組合せ手法を提案した.

一般にサイドチャネル攻撃において鍵を推定する際には，各仮定鍵に対しスコアを与え，最もスコアの高い仮定鍵を真の鍵と推定する．本提案方式では，MIA を行った際の鍵のスコアを x, CPA での鍵のスコアを y とし，これらに様々な重み付けをした組合せスコア f(x,y)を用いて鍵の推定を行った.

提案手法の性能を評価するためにサイドチャネル攻撃用標準評価ボード SASEBO-R(ASIC)と SASEBO-GII(FPGA)を利用した評価実験を行った．実験の結果，FPGA 上に実装された AES に対しては CPA を単独で利用するより，MIA と組み合わせることで攻撃成功確率が向上することが示された．これは FPGA では回路内の配線領域が暗号ロジック領域よりも大きい面積を占めるために，暗号演算以外の部分の消費電力が相対的に大きくなり，暗号ロジック回路内の状態遷移と回路全体の消費電力との線形相関が小さくなったことが原因となり CPA 単体では攻撃が困難であった部分が，MIA と組み合わせることにより補完されたのではないかと考えられる．一方，ASIC ボードにおいては，これらの攻撃を組み合わせることの効果は小さかった．これは ASIC では回路内部の状態と消費電力に高い線形相関があるため，CPA のみでも十分強力な攻撃となり得たためと考えられる.

⑥①～⑤で示した攻撃手法は，攻撃者が鍵の埋め込まれた LSI から消費電力等を測定し，直接攻撃を行う手法であった．一方で攻撃者

が攻撃対象の LSI とは別に同種の LSI を入手し，その LSI を用いて LSI 特性を評価した上で攻撃を行う方法が提案されており，テンプレート攻撃と呼ばれている．従来提案されているテンプレート攻撃では，LSI の電力消費波形が鍵の値に依存した多次元正規分布で近似できるという仮定に基づいた手法であった．

本研究では新しいテンプレート攻撃手法として機械学習理論を応用した攻撃法を提案した．提案方式ではランダムフォレスト法と呼ばれる機械学習法を利用し，AES に対して攻撃実験を行った．実験の結果，AES の最終ラウンドでのラウンド鍵について，完全ではないものの部分情報を得られることを示した．

以上の研究成果からサイドチャネル攻撃による攻撃性能の評価および既存の対策手法の有効性に関する評価を行うことができた．

(2)サイドチャネル攻撃対策手法に関する研究

前項の評価結果に基づき，サイドチャネル攻撃に対する強力な対策手法の設計，および実証実験を行った．

サイドチャネル攻撃とは，回路の実装に関する何らかの情報を持った攻撃者が鍵の一部分を仮定することで回路の内部状態を仮定鍵毎に推定し，実際の取得波形と最も整合性の高い内部状態を達成しうる鍵を真の鍵と推定する方法である．このことから，サイドチャネル攻撃に対する対策手法は，攻撃者による内部状態の推定を，いかにして困難にするかという問題に帰着される．本研究では，サイドチャネル攻撃対策として，回路の内部を攻撃者が推定し難くするための二つの手法を提案した．

①ランプ型秘密分散共有法を利用し，AES 回路を分散した状態のまま実装ができる方式を提案した．

ランプ型秘密分散共有法は秘密分散共有法の一種であり，シャミア(A. Shamir)の秘密分散共有法と比較すると安全性がやや低下する代わりに分散情報のサイズが元の秘密情報よりも小さくなるという特徴がある．シャミアの秘密分散共有法用いても本研究と同様の対策は可能であると考えられる．しかし，暗号アルゴリズムを LSI 上に実装する場合，回路全体の消費電力量の問題から回路規模が制限されることが多い．シャミアの秘密分散共有法を用いたサイドチャネル攻撃対策手法を実装する場合，回路規模が元の回路の 2 倍以上必要になると考えられることから，回路規模の観点からは，ランプ型秘密分散共有法の方がサイドチャネル攻撃対策としては適切であると考えられる．

本研究では，ランプ型秘密分散共有法を利用した AES 実装法を提案し，その性能を評価するために提案方式を SASEBO-GⅡ上の AES に実装し，攻撃実験を行った．実験では未対策の AES と提案手法による対策を施した AES に対し CPA により攻撃を行い，鍵の復元に必要となる消費電力波形数を比較することで提案手法の性能を評価した．実験の結果，未対策の AES では鍵の完全復元におよそ 4,500 波形必要であったのに対し，提案手法を組み込んだ AES では 10,000 波形を利用しても秘密鍵の 14 バイト分しか特定できなかった．

②耐漏洩ストレージ法を応用した対策手法を提案した．

耐漏洩ストレージとは，サイドチャネル攻撃よりもさらに強力な物理解析攻撃から暗号方式を保護するために開発された情報分散法である．耐漏洩ストレージは強力な攻撃に対する対策手法であることから，サイドチャネル攻撃に対しても当然高い対策効果を持つと考えられるが，データに対し高い冗長性を持たせる手法であるため，そのままでは LSI 上に実装することが困難である．本研究では，耐漏洩ストレージの情報分散機能を利用し，LSI 上にも実装可能な情報分散技術を提案した．さらに，提案手法を SASEBO-GⅡ上の AES に組み込み評価実験を行った．評価実験では，提案方式の安全性を評価するために CPA による攻撃実験を行った．実験の結果，50,000 個の消費電力波形を利用しても秘密鍵 16 バイトのうち 2 バイトまでしか復元できないことが明らかとなった．本実験結果より，耐漏洩ストレージを用いた提案手法は，サイドチャネル攻撃に対し高い耐性を持つ対策手法であると言える．

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 17 件）

[1] 吉田雅一，宮寺隆之，今井秀樹, “Qn the Security of Quantum Key Distribution Ping-Pong Protocol,” Journal of Quantum Information, vol. 3, pp. 16-19, 2013.（査読有）

[2] 吉田雅一，今井秀樹, “Re-formulation of Mean King’s Problem using Shannons’ Entropy,” Journal of Quantum Information Science, vol. 3, pp. 6-9, 2013 (査読有)

[3] 笠松宏平，松田隆宏，花岡悟一郎，今井秀樹，“Ciphertext Policy Multi-Dimentional Range Encryption,” International Conference on Information Security and Cryptology, pp. 247-261, 2012.

（査読有）

[4] **宋雪迪，古原和邦，今福健太郎，今井秀樹，** “HBb Protocol for Lightweight Authentication; its Information Theoretic Indistinguishability against MITM Attack Watching Reader’s Response,” 2012 International Conference on Information Theory and its Applications, 2012.**(査読有)**

[5] **吉田雅一，宮寺隆之，今井秀樹，** “Quantum Key Distribution using Mean King Problem with Modified Measurement Schemes,” 2012 International Conference on Information Theory and its Applications, 2012.**（査読有）**

[6] ミハイエビッチ･ミオドラッグ, 今井秀樹, 他 2 名, “Internal State Recovery of Grain-v1 Employing Normality Order of the Filter Function,” IET Information Security, vol. 6, no. 2, pp. 55-64, 2012.（査読有）

[7] **笠松宏平，松田隆宏，江村恵太，ナッタポン・アッタラパドゥン，今井秀樹，** “Time-Specific Encryption from Forward-secure Encryption,” 8th Conference on Security and Cryptography for Networks, pp. 184-204, 2012.**（査読有）**

[8] 吉田雅一, 萩原学, 宮寺隆之, 今井秀樹, “A Numerical Evaluation of Entanglement Sharing Protocols using Quantum LDPC Codes,” IEICE Trans. on Fundamentals of Electronics, Communications and Computer Science, vol. E950A, pp. 1561-1569, 2012.（査読有）

[9] 鈴木智也, 田沼均, 今井秀樹, “情報セキュリティ対策間の相互依存性を用いた内部犯行防止策のための有効性評価手法,” 情報処理学会論文誌, vol. 52, no. 9, 2011.（査読有）

[10] 今福健太郎, 今井秀樹, “Fundamental Physical Information Leakage through Computations on Physically Implemented Turing Machine,” 2011 年暗号と情報セキュリティシンポジウム予稿集, 2011.

[11] 伊左次優太, 堀洋平, 今井秀樹, “MIA の攻撃精度向上のための確率密度関数の推定法に関する考察,” 2011 年暗号と情報セキュリティシンポジウム予稿集, 2011.

[12] 佐藤弘季, 北川隆, 米澤祥子, 今井秀樹, “PUF を用いた数学的複製不可能性を必要としない模造品検出技術,” 2011 年暗号と情報セキュリティシンポジウム予稿集, 2011.

[13] 野口正俊, 北川隆, 今井秀樹, “サイドチャネル攻撃の安全性評価指標確立に向けた攻撃モデルの提案,” 2011 年暗号と情報セキュリティシンポジウム予稿集.

[14] 吉田雅一, 宮寺隆之, 今井秀樹, “On the Security of the Quantum Key Distribution using the Mean King Problem,” 2010 International Symposium on Information Theory and its Applications, 2010.（査読有）

[15] 恩田泰則, 辛星漢, 古原和邦, 今井秀樹, “How to Distinguish On-line Dictionary Attacks and Password Mis-typing in Two Factor Authentication,” 2010 International Symposium on Information Theory and its Applications, 2010.（査読有）

[16] ミハイエビッチ･ミオドラッグ, 今井秀樹, “A Security Evaluation of Certain Stream Ciphers which Involve Randomness and Coding,” 2010 International Conference on Information Theory and its Applications, 2010.（査読有）

[17] ミハイエビッチ･ミオドラッグ, 今井秀樹, 他 2 名, “A Generic Weakness of the k-normal Boolean Functions Exposed to Dedicated Algebraic Attack,” 2010 International Conference on Information Theory and its Applications, 2010.（査読有）

〔**学会発表**〕**（計 45 件）**

[1] 小島 裕貴, 北川 隆, ナッタポン アッタラパドゥン, 今井 秀樹, “フォワード安全暗号文ポリシー属性ベース暗号, ” 2013 年暗号と情報セキュリティシンポジウム, 2013 年 1 月 24 日, 京都府京都市.

[2] 近藤 大記, 北川 隆, 今井 秀樹, “データ集合に対する電子透かし法及び結託耐性符号の提案, ” 2013 年暗号と情報セキュリティシンポジウム, 2013 年 1 月 24 日, 京都府京都市.

[3] 宋 雪迪, 古原 和邦, 今福 健太郎, 北川 隆, 今井 秀樹, “軽量型認証プロトコル HBb の推奨パラメータ, ” 2013 年暗号と情報セキュリティシンポジウム, 2013 年 1 月 23 日, 京都府京都市.

[4] 吉田雅一, 今井秀樹, “情報エントロピーを用いた Mean King 問題の再定式化, ” 2013 年暗号と情報セキュリティシンポジウム, 2013 年 1 月 22 日, 京都府京都市.

[5] 早崎拓馬, 伊左次優太, 猪狩幸大, 堀洋平, 今井秀樹, “対策済み AES に対するサイドチャネル攻撃手法の有効性評価,” 2012 年暗号と情報セキュリティシンポジウム, 2012 年 1 月 31 日, 石川県金沢市.

[6] 佐野祐太郎, 北川隆, 今井秀樹, “機械学習を用いたAESに対するテンプレート攻撃,” 2012年暗号と情報セキュリティシンポジウム, 2012年1月31日, 石川県金沢市.
[7] 猪狩幸大, 伊左次優太, 早崎拓馬, 堀洋平, 今井秀樹, “S-Boxの実装方式の異なるAESに対するMIAの有効性検証,” 2012年暗号と情報セキュリティシンポジウム, 2012年1月31日, 石川県金沢市.
[8] **細谷玲奈，古原和邦，北川隆，今井秀樹,“オフラインパスワードクラックの現状とその対策,”** 2012年暗号と情報セキュリティシンポジウム, 2012年1月31日, 石川県金沢市.
[9] 吉田雅一, 宮寺隆之, 今井秀樹, “Mean King問題を応用した量子鍵配送における測定の修正および安全性に関する考察, ” 2012年暗号と情報セキュリティシンポジウム, 2012年1月31日, 石川県金沢市.
[10] 伊左次優太, 堀洋平, 今井秀樹, “Combined Side-Channel Analysisの性能向上のためのCPAとMIAの合成に関する研究,” 2012年暗号と情報セキュリティシンポジウム, 2012年1月31日, 石川県金沢市.
[11] 宋雪迪, 古原和邦, 今福健太郎, 今井秀樹, “RFID向けHB#相互認証プロトコルに対して安全性の改良, ” 2012年暗号と情報セキュリティシンポジウム, 2012年1月31日, 石川県金沢市.
[12] 久野真太郎, ナッタポン・アッタラパドゥン, 北川隆, 今井秀樹, “位置情報ベース暗号, ” 2012年暗号と情報セキュリティシンポジウム, 2012年1月30日, 石川県金沢市.
[13] 今井秀樹, 他4名, “Forward-Seucre暗号を用いたTime-Specific暗号の一般構成, ” 2012年暗号と情報セキュリティシンポジウム, 2012年1月30日, 石川県金沢市.
[14] 小島裕貴, ナッタポン・アッタラパドゥン, 北川隆, 今井秀樹, “フォワード安全属性ベース暗号,” 2012年暗号と情報セキュリティシンポジウム, 2012年1月30日, 石川県金沢市.
[15] B. Jenjarrussakul, 飛鋪亮太, 田中秀幸, 松浦幹太, 今井秀樹, “Interdependency of Information Security and its Dependence on IS Multiplier of Sub-Industries,” International workshop on security, 2011年11月9日. 東京都目黒区(査読有)
[16] 恩田 泰則, 辛 星漢, 古原 和邦, 今井秀樹, “クラウド環境に適したオンラインデータ分散管理方式, ” 2011年暗号と情報セキュリティシンポジウム, 2011年1月27日, 福岡県北九州市.
[17] 笠松宏平, 田沼均, 木村元, 今井秀樹, “クラウドコンピューティングセキュリティの経済分析による一考察, ” 2011年暗号と情報セキュリティシンポジウム, 2011年1月27日, 福岡県北九州市.
[18] 関野智啓, 崔洋, 古原和邦, 今井秀樹, “Flexible Quasi-Dyadicの実装･評価に関する考察, ” 2011年暗号と情報セキュリティシンポジウム, 2011年1月27日, 福岡県北九州市.
[19] 張瑩, ナッタポンアッタラパドゥン, 北川隆, 今井秀樹, “一定サイズの暗号文を持つ追跡と無効化が可能な放送型暗号, ” 2011年暗号と情報セキュリティシンポジウム, 2011年1月27日, 福岡県北九州市.
[20] 安藤 元紀, 木村 元, 宮寺 隆之, 今井秀樹, “HBBプロトコルのInformation-Disturbance定理による安全性評価”, 2011年暗号と情報セキュリティシンポジウム, 2011年1月27日, 福岡県北九州市.
[21] 吉田雅一, 宮寺隆之, 木村元, 今井秀樹, “Mean King Problemと量子誤り訂正符号, ” 2011年暗号と情報セキュリティシンポジウム, 2011年1月27日, 福岡県北九州市.
[22] 前田芳秀, 木村元, 田沼均, 今井秀樹, “複雑ネットワークの手法を用いた結託攻撃者数の拡大と抑制のモデル, ” 2011年暗号と情報セキュリティシンポジウム, 2011年1月27日, 福岡県北九州市.
[23] 鈴木智也, 田沼均, 今井秀樹, “対策間の相互依存関係を用いた情報セキュリティ対策のための有効性評価手法, ” 2011年暗号と情報セキュリティシンポジウム, 2011年1月26日, 福岡県北九州市.
[24] 小柳裕嵩, 萩原学, 今井秀樹, “2準位量子QC-LDPC符号をGF(2)の拡大体の同伴行列で拡張するための十分条件, ” 第33回情報理論とその応用シンポジウム(SITA2010), 2010年12月2日, 長野県長野市.
[25] 木村元, 縫田光司, 今井秀樹, “物理原理に基づく量子ビット系の導出, ” 第33回情報理論とその応用シンポジウム(SITA2010), 2010年12月1日, 長野県長野市.

6．研究組織

(1)研究代表者

今井　秀樹（IMAI, Hideki）
中央大学・理工学部・教授
研究者番号：70017987