様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ７ 月　 ６ 日現在

機関番号：３１３０２
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００１９０

研究課題名（和文）耐タンパー軽量ブロック暗号の論理実装評価

研究課題名（英文）Logic design and security evaluation for tamper-resistant light weight block cipher

研究代表者

神永　正博（Kaminaga, Masahiro）

東北学院大学・工学部・教授

研究者番号：６０２６６８７２

交付決定額（研究期間全体）：（直接経費）　　3,800,000円

研究成果の概要（和文）：本研究は、ICカード、RFIDタグ、スマート家電等のセキュアデバイスに対して安全な暗号アルゴリズムを実装することを目的として、電力解析攻撃，差分故障攻撃のようなサイドチャネル攻撃に耐性を持つ方法を開発した。
大きく分けて、ラビン暗号に関する攻撃（モジュラス破壊攻撃）と安全な実装（安全なランダムパディングサイズの決定）、命令を強制的にスキップさせるDFAによるFeistelブロック暗号における鍵導出法、IoT端末でマスキング等のサイドチャネル攻撃対策を実現する無線通信に伴う雑音を利用した乱数発生技術の開発を行った。

研究成果の学術的意義や社会的意義
無線通信でネットワーク化された小型の暗号装置が大量に普及している現在では、1つの端末の暗号が破られると他の暗号装置の安全性も脅かされる。例えば、スマートランプを乗っ取られてしまうと、攻撃者が故意に火災を発生させるなど物理的な意味でも危険が生ずる。本研究の意義は、現在急速に拡大しているICカード、携帯電話SIM、RFIDタグ、その他のIoT端末で使われる軽量な暗号をサイドチャネル攻撃から防衛するための基礎技術を提供し、安全で安心な社会を提供する一助となっていることにある。

研究成果の概要（英文）：This work aims to implement secure cryptographic algorithms for secure devices such as smartcards, RFID tags, and smart home appliances by developing methods that are resistant to side channel attacks such as power analysis attacks and differential fault attacks. Broadly speaking, we have developed attacks(crashing modulus attack for Rabin cryptosystem) and secure implementations of Rabin cryptosystem(determination of the size of secure random padding using lattice reduction technique), a key reconstruction method in Feistel block cipher using instruction-skipping DFA, and a random number generation technique using the noise associated with wireless communications to realize countermeasures against side channel attacks such as masking at IoT terminals.

研究分野：暗号理論

キーワード：暗号理論　耐タンパー技術

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

ICカード、携帯電話SIM、RFIDタグ、スマート家電等のIoT端末の普及は目覚ましいものがある。これらの端末は、暗号の秘密鍵を格納しているため、ハードウェアの特性を利用したサイドチャネル攻撃として知られる処理時間解析(TA)、電力解析(SPA/DPA/CPA)、故障解析(DFA)、物理解析(PA)によって秘密が漏洩する危険性があり、対策が必要である。しかしながら、これらの端末の安全性には大きなばらつきがある。例えば、ICカード、携帯電話SIMに関しては、Anderson-Kuhnが、96年のUSENIX Workshopで発表したTamper Resistance - a Cautionary Note[1]や、[2]において、既にハードウェア経由の攻撃（物理解析、DFA）の危険性について警告を発していたこともあり、製品化初期からサイドチャネル攻撃に対する対策技術（耐タンパー技術）が組み込まれていた。一方、新たに出現したRFIDタグなどではハードウェアの制約もあり、そのセキュリティは限定的なものにとどまっている。しかし、端末同士がネットワークで接続されている現在では、弱い端末を破ることができれば、ネットワーク化された端末全てが影響を受ける可能性がある。弱い端末を破ることで強いはずの端末も破れてしまうのである。これは危険な状態である。Shamirは、Financial Cryptography 2016のキーノートスピーチ”Financial Cryptography: Past, Present, and Future”において、”The Internet of Things will be a security disaster.”と述べているが、それは、ネットワーク化されたIoT端末の危険性を指摘したものである。このような背景から、IoT端末のようなハードウェア規模の小さい端末に向けて軽量な暗号技術が数多く考案されてきているが、限定された回路規模の中でいかにして暗号処理を実現するかが大きな問題であり、そのサイドチャネル攻撃への対策は不十分であった。対策を十分なものにするため、耐タンパー性を下げずにできるだけ規模の小さい対策技術を確立する必要があるが、それにともなって、軽量暗号向けの攻撃方法を考案し、耐タンパー技術を組み込むために必要な周辺技術を開発する必要があった。

２．研究の目的

本研究の第一の目的は、ICカード、携帯電話SIM、RFIDタグの他、スマート家電等のIoT端末における暗号処理のサイドチャネル攻撃に対する耐性（耐タンパー性）を高めるため、(1)新しい攻撃方法の探索すること、(2)サイドチャネル攻撃対策の効果をシミュレーション、実験によって確認すること、(3)サイドチャネル耐性を高めるのに必要な周辺技術の開発を行うことである。

３．研究の方法

我々の研究グループが得意とする命令スキップ現象を利用したDFA（ラウンド加算DFA）について、Feistel構造を持つブロック暗号一般について攻撃の枠組みを整理し、DFA実験との照らし合わせて評価を行う。DFA実験には、Atmel社のマイコンと我々が開発したDFAステーションを用いる。DFAステーションは、ファンクションジェネレータ、デジタルオシロスコープなどから構成される自動評価システムである。この他、SIMON, PRESENT, LBlockという軽量ブロック暗号について、相関電力解析の実証実験を行い、PRESENTについては、マスキングの効果についても詳細な実験を行う。SIMONについては、様々な状況で攻撃実験を行うことにより、従来研究で相関電力解析について不十分な結果しか得られていない原因を調べる。相関電力解析については、実験環境、必要なソフトウェアの開発なども同時進行で進めていく。実験の結果は、攻撃シナリオにフィードバックする。IoT端末における暗号処理、耐タンパー技術実装のために必要となる乱数発生装置については、その基本原理の確立のため、電波無響室において無線通信端末を用いた実験を行い、結果を代表的な乱数性テストであるNIST test, DIEHARD testに基づいて評価する。

４．研究成果

最初の研究成果は、研究分担者の吉川英機による Feistel 型ブロック暗号一般に対するラウンド加算DFAによる鍵導出法を明らかにしたものである。電源電圧の瞬時降下によって、カウンタのインクリメントまたはデクリメント命令をスキップさせ、余計なラウンド処理を実行させることで正常な処理結果と比較し１ラウンド分の解析に帰着させる方法がラウンド加算 DFA である。我々はATmegaマイコンに対してこの攻撃を行い、高確率で命令スキップが生ずることを確認している。この結果は、これまで散発的に行われてきたこの攻撃をFeistel型ブロック暗号一般に拡張するものであり、今後の Feistel 型の軽量ブロック暗号に対する防衛技術に統合的な視点を与えるものである。Feistel型のブロック暗号は、DES以来様々な形で提案され、実システムに実装されており、比較的最近では、SIMONなどの軽量暗号が有名である。Feistel型暗号一般に関する考察は現在でも有益と思われる。この結果は、論文[3]にまとめた。なお、この研究の過程で、ラウンド鍵から鍵全体を計算する際の鍵スケジュール部の構造についてより一層の解析の必要性が認識された。

第2の研究成果は、IoT端末向けの軽量公開鍵暗号として有力なRabin暗号のモジュラス破壊攻撃に関する研究である。Rabin暗号は素因数分解の困難性と同等の安全性を持つことがRabin自身によって証明されており、素因数分解の困難性を前提にすれば、理論的に安全な暗号である。素因数分解の困難性に基づく暗号としては、RSA暗号の方が有名であるが、RSA暗号では計算量的な安全性が同等であることは証明されていない。Rabin暗号は、このような理論的な利点を持

っているだけでなく、うまく実装することによって高速な処理が可能である。代表的なものとして、WIPR 方式[9]と RAMON がある。前者は Shamir が考案した方法で、長いレジスタを必要とする代わりに剰余演算を行わない方法、RAMON[10]は、ドイツの Giesecke & Devrient 社が開発したもので、モンゴメリ法を利用して高速な処理と回路構成の縮小を実現する方法である。いずれの実装においても Rabin 暗号に対する DFA のターゲットは、公開鍵 N である。フォールト印加によってレジスタ値が変わったり、命令スキップが生じたりすると、デバイスは誤った結果を出力するが、この違いを利用して公開鍵を素因数分解することができることを論文[5]に示した。

第 3 の研究成果は、Rabin 暗号に対するランダムパディングサイズの最適値を決定したことである。IoT 端末で Rabin 暗号を使う場合、同一の暗号文が出力されるとリプレイ攻撃が可能になるため、ランダムパディングが欠かせない。しかし、ランダムパディングのサイズに関しては、Wu-Stinson の結果等で散発的に触れられているのみであり、また、そのセキュリティ上十分なサイズについては十分明らかになっていなかった。我々は、格子理論とバースデーパラドックスを応用し、攻撃にかかる時間に関する高精度の予測式をつくることによって、Figure 1 のように従来の格子と我々が改良した格子に対し、最も効率的な攻撃パラメータを決定した。これにより、セキュリティ上十分なランダムパディングサイズを明らかにすることに成功し、論文[6]にまとめた。

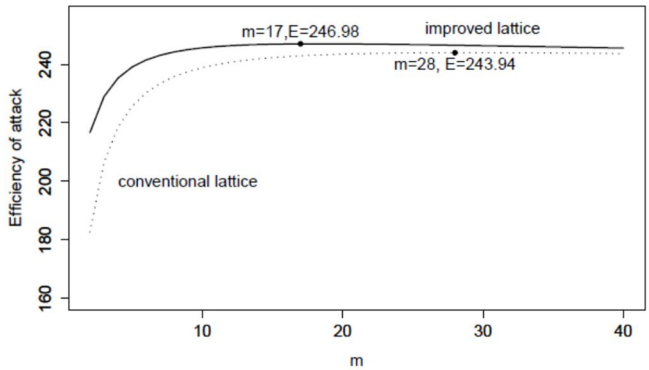

Figure 1　最も効率のよい攻撃パラメータ

第 4 の研究成果は、無線通信ノイズを利用して統計的性質がよく、かつ予測不能な乱数発生方式を提案したことである。一般に、電力解析やタイミングアタックなどに対する耐タンパー技術の実装には、マスキングと呼ばれる暗号処理の暗号化が必要となる。また、前述の Rabin 暗号などでもランダムパディングが必須である（WIPR では、パディングだけでなく、暗号文に乱数を加えて出力する）。そのために、例えば、Arbit et al.[8]では、Rabin 暗号の WIPR 実装のために、Feistel 暗号と類似の回路によって疑似乱数を生成している。しかし、純粋な疑似乱数では十分なセキュリティを維持することはできず、少なくともそのシードとしてなんらかの予測不能な乱数発生源が必要になる。我々は、IoT 端末が、その性質上、無線通信を必須としていることから、無線通信で生ずるノイズを用いて高速な（単位時間あたりに生成できる乱数ストリームのビットサイズが大きい）乱数発生方式を提案した。Figure 2 は、提案する真正乱数発生装置の無線システムにおける機能的な位置付けを示しており、DUP/SW は送信と受信の両方に単一のアンテナを用いたデュプレクサまたはスイッチであり、RX は受信回路、TX は送信回路、proc. は情報処理装置を表している。一般的な無線システムでは、無線端末はネットワーク側からシステム情報や送信許可を取得する必要があるため、送信前に基地局からの信号を受信する必要があるが、無線端末での受信処理中に真正乱数発生装置が動作すれば十分である。この方式は、無線ノイズを利用しているので予測困難であり、その統計的性質（NIST test, DIEHARD test）も Table 1 のように大変良好なものであることが実験的に確認できた。この方法は、一般の IoT 端末に備わっている無線通信の回路があれば、新たな回路はほとんど必要のない軽量な方法であり、IoT 端末の暗号セキュリティに有効であると考えられる。この結果を、論文[7]にまとめた。

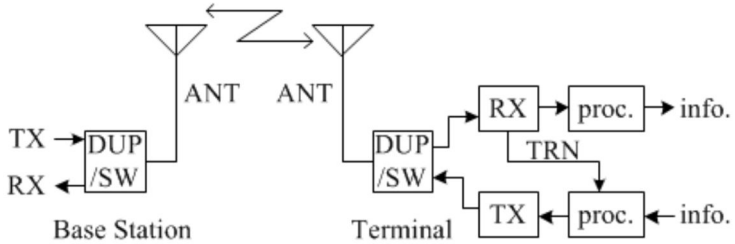

Figure 2 乱数発生装置の概念図

Table 1　乱数の統計的性質

P_{out} dBm	$-\infty$	−60	−50	−40	−30	−20	−10	0
Most Common Value	0.998798	0.998768	0.998575	0.998845	0.999083	0.998671	0.999132	0.998974
Collision	0.966577	0.966577	0.966577	0.977632	0.955606	0.955606	0.955606	0.977632
Markov	0.999036	0.999109	0.998852	0.998803	0.999193	0.998847	0.999475	0.999327
Compression	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000
t-Tuple	0.936758	0.936758	0.940114	0.938417	0.936758	0.933552	0.936758	0.940114
LRS	0.999989	0.995650	0.999112	0.997434	0.999961	0.999848	0.987004	0.995447
Multi MCW	0.999621	0.999470	0.999005	0.999895	0.999466	0.998892	0.999143	0.999275
Lag	0.999121	0.999302	0.999151	0.998891	0.999277	0.998659	0.999282	0.998915
Multi MMC	0.999043	0.999382	0.999266	0.999249	0.998962	0.999110	0.999394	0.999665
LZ78Y	0.998979	0.998940	0.998752	0.998704	0.998861	0.998876	0.999734	0.999259
Min-entropy	0.936758	0.936758	0.940114	0.938417	0.936758	0.933552	0.936758	0.940114

第 5 の研究成果として、BPSK-OFDM 信号のブラインド系列推定法がある。乱数発生装置について考察している際に、小型 IoT 端末における省電力通信の問題点が浮かび上がった。もともと小さなデバイスであり、電力を故意に下げたり、ノイズを発生させて DFA を行うことが容易だという問題である。そこで、暗号理論からは若干離れるが、通信品質（誤り率や到達距離）を落とさずに，送信電力を下げるための技術を開発した。通常，無線機からの送信信号にはパイロット信号が挿入される。これは，伝送路の状態を受信側で補正して，送信信号を正しく復元するために使用されるものである。このパイロット信号を排除することで送信電力を抑え，送信機の消費電力を削減するため、受信側では、パイロット信号なしに伝送路を推定しなければならない。論文ではその推定法を提案し，性能を評価し、論文[4]にまとめた。送信側の消費電力を抑える代わりに受信側の計算量は増えるのですが，受信側(基地局)の負荷が増大しても，バッテリーで長時間動作する必要がある小型 IoT 端末にとってセキュリティ上も有用な技術と考えられる。

相関電力解析とその対策に関する実験結果については、今回の研究ではトランザクション論文の形には反映できなかったが、所属研究室の学生によって 9 回にわたり口頭発表されており、国際会議も含まれている(口頭発表[1]-[9])。そのうち、PRESENT という軽量ブロック暗号についての相関電力解析に関して第 18 回情報科学技術フォーラム(FIT2019)で発表した「軽量ブロック暗号における S-BOX マスキング保護の検討・評価」(口頭発表[7])では、研究奨励賞をいただいた。

＜参考論文＞

[1] Ross J. Anderson, Markus G. Kuhn, Tamper Resistance - a Cautionary Note, 2nd USENIX Workshop on Electronic Commerce Proceedings, pp. 1-11(1996)

[2] Ross J. Anderson, Markus G. Kuhn, Low Cost Attacks on Tamper Resistant Devices, Security Protocols, 5th International Workshop, Paris, France, April 7-9, 1997, Proceedings, Springer LNCS 1361, pp. 125-136(1997)

[3] 吉川英機，ラウンド加算 DFA による Feistel ブロック暗号における鍵導出法，電子情報通信学会論文誌，vol. J101-D(7)，pp.1027-1036，2018 年

[4] 鈴木利則，佐藤拓也，BPSK-OFDM 信号のブラインド系列推定法，電子情報通信学会論文誌 B　Vol.J101-B　No.3　pp.254-263

[5] M. Kaminaga, H. Yoshikawa, A. Shikoda, T. Suzuki, Crashing Modulus Attack on Modular Squaring for Rabin Cryptosystem, IEEE Transaction on Dependable and Secure Computing 15(4), pp. 723 – 728(2019)

[6] M. Kaminaga, T. Suzuki, M. Fukase, Determining the Optimal Random-padding Size for Rabin Cryptosystems, IEEE Transactions on Information Forensics and Security 14(8), pp. 2232 – 2242(2019)

[7] T. Suzuki and M. Kaminaga, A True Random Number Generator Method Embedded in Wireless Communication Systems, IEICE Transactions on Fundamentals E103-A(4), pp. 686 – 694(2020)

[8] Alex Arbit, Yoel Livne, Yossef Oren, Avishai Wool, Implementing public-key cryptography on passive RFID tags is practical, International Journal of Information Security Vol. 14, pages85-99(2015)

[9] A. Shamir, Memory Efficient Variants of Public-Key Schemes for Smart Card Applications, Proc. Advances in Cryptology (EUROCRYPT ' 94), LNCS 950, pp. 445-449(1995).

[10] W. Hinz, K. Finkenzeller, M. Seysen, "Secure UHF Tags with Strong Cryptography - Development of ISO/IEC 18000-63 Compatible Secure RFID Tags and Presentation of First Results," SENSORNETS, pp. 5-13(2013)

＜口頭発表＞

口頭発表　2018 年度

[1]加納広太（登壇者）,志子田有光,神永正博,"Development and evaluation of CPA system for 8bit microcontroller utilizing a parallel plain text transfer,"
平成 30 年度電気関係学会東北支部連合大会講演論文集，2F05，Sep．2018．

[2]安達司（登壇者）,志子田有光,神永正博「軽量暗号 SIMON に対する差分電力解析の検討」,平成 30 年度電気関係学会東北支部連合大会講演論文集，2H04，Sep．2018．

[3] 佐藤純（登壇者）,吉川英機,志子田有光,神永正博「軽量ブロック暗号 LBlock に対する差分電力解析の検討」，平成 30 年度電気関係学会東北支部連合大会講演論文集，2H05，Sep．2018.http://www.ieice.org/ess/sita/SITA2018/schedule.html

[4] 安達司（登壇者）,加納広太,志子田有光,神永正博「軽量暗号 SIMON に対する相関電力解析の検討」,第 41 回情報理論とその応用シンポジウムポスターセッション，Dec．2018．

[5] 佐藤純（登壇者）,加納広太,志子田有光,神永正博「軽量ブロック暗号 LBlock に対する差分電力解析への対策の検討」，第 41 回情報理論とその応用シンポジウムポスターセッション，Dec．2018．

[6] A．Shikoda，H．Yoshikawa，M．Kaminaga，T．Suzuki，K．Kanou（登壇者），T．Adachi，J．Sato，and M．Fukase，"Detailed experimentation know-how about CPA against lightweight cipher implemented 8-bit microcontroller for tamper resistance test bench," Proceedings of 2018 International Symposium on Information Theory and its Applications (ISITA2018)，Recent Results Poster Session，p.518，Oct．2018．

口頭発表　2019 年度

[7] 加納広太（登壇者），志子田有光，神永正博，吉川英機「軽量ブロック暗号における S-BOX マスキング保護の検討・評価」,第 18 回情報科学技術フォーラム(FIT2019)，L-009，Sep．2019．
https://www.ipsj.or.jp/event/fit/fit2019/FIT2019program_web/data/html/program/l.html#s3p

[8] 加納広太（登壇者），吉川英機，神永正博，志子田有光「FPGA 実装の軽量ブロック暗号 LBlock における S-BOX マスキング保護の検討・評価」，第 42 回情報理論とその応用シンポジウム(SITA2019)，ポスターセッション，Nov．2019．
https://www.ieice.org/ess/sita/SITA2019/poster.html

[9] 加納広太（登壇者），吉川英機，神永正博，志子田有光「軽量ブロック暗号 LBlock に対する相関電力解析への対策の検討」電気関係学会東北支部連合大会２０１９（秋田大学）1A05
http://www.ecei.tohoku.ac.jp/tsjc/index.html

５．主な発表論文等

〔雑誌論文〕　計8件（うち査読付論文　7件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Toshinori Suzuki , Masahiro Kaminaga	４．巻 Volume E103.A Issue 4
２．論文標題 A True Random Number Generator Method Embedded in Wireless Communication Systems	５．発行年 2020年
３．雑誌名 IEICE Transactions on Fundamentals	６．最初と最後の頁 686-694
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2019EAP1130	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 SUZUKI Toshinori、KAMINAGA Masahiro	４．巻 E103.A
２．論文標題 A True Random Number Generator Method Embedded in Wireless Communication Systems	５．発行年 2020年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 686～694
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1587/transfun.2019EAP1130	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Kaminaga Masahiro、Suzuki Toshinori、Fukase Masaharu	４．巻 Volume 14(Issue:8)
２．論文標題 Determining the Optimal Random-padding Size for Rabin Cryptosystems	５．発行年 2019年
３．雑誌名 IEEE Transactions on Information Forensics and Security	６．最初と最後の頁 2232-2242
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIFS.2019.2895545	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 吉川英機	４．巻 vol. J101-D no.7
２．論文標題 ラウンド加算DFAによるFeistelブロック暗号における鍵導出法	５．発行年 2018年
３．雑誌名 電子情報通信学会和文論文誌	６．最初と最後の頁 1027-1036
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transinfj.2017JDP7087	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Masahiro Kaminaga, Hideki Yoshikawa, Arimitsu Shikoda, Toshinori Suzuki	４．巻 15(4)
２．論文標題 Crashing Modulus Attack on Modular Squaring for Rabin Cryptosystem	５．発行年 2018年
３．雑誌名 IEEE Transaction on Dependable and Secure Computing	６．最初と最後の頁 723-728
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TDSC.2016.2602352	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 神永正博・深瀬道晴	４．巻 52
２．論文標題 RSA秘密鍵計算と素因数分解の決定的多項式時間同値性	５．発行年 2018年
３．雑誌名 東北学院大学工学部研究報告	６．最初と最後の頁 29-38
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 鈴木利則・佐藤拓也	４．巻 Vol.J 101-B,No.3
２．論文標題 BPSK-OFDM信号のブラインド系列推定法	５．発行年 2018年
３．雑誌名 電子情報通信学会　論文誌　B	６．最初と最後の頁 254-263
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transcomj.2017JBP3029	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 吉川英機	４．巻 Vol.J101-D,No.7
２．論文標題 ラウンド加算DFAによるFeistel型ブロック暗号における鍵導出法	５．発行年 2018年
３．雑誌名 電子情報通信学会論文誌 D	６．最初と最後の頁 1027-1036
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transinfj.2017JDP7087	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計9件（うち招待講演　0件／うち国際学会　1件）

１．発表者名
加納広太,志子田有光,神永正博

２．発表標題
Development and evaluation of CPA system for 8bit microcontroller utilizing a parallel plain text transfer

３．学会等名
平成30年度電気関係学会東北支部連合大会

４．発表年
2018年

１．発表者名
安達司,志子田有光,神永正博

２．発表標題
軽量暗号SIMONに対する差分電力解析の検討

３．学会等名
平成30年度電気関係学会東北支部連合大会

４．発表年
2018年

１．発表者名
佐藤純,吉川英機,志子田有光,神永正博

２．発表標題
軽量ブロック暗号LBlockに対する差分電力解析の検討

３．学会等名
平成30年度電気関係学会東北支部連合大会

４．発表年
2018年

１．発表者名
安達司,加納広太,志子田有光,神永正博

２．発表標題
軽量暗号SIMONに対する相関電力解析の検討

３．学会等名
第41回情報理論とその応用シンポジウム

４．発表年
2018年

１．発表者名
佐藤純,加納広太,志子田有光,神永正博

２．発表標題
軽量ブロック暗号LBlockに対する差分電力解析への対策の検討

３．学会等名
第41回情報理論とその応用シンポジウム

４．発表年
2018年

１．発表者名
A. Shikoda, H. Yoshikawa, M. Kaminaga, T. Suzuki, K. Kanou, T. Adachi, J. Sato, and M. Fukase

２．発表標題
Detailed experimentation know-how about CPA against lightweight cipher implemented 8-bit microcontroller for tamper resistance test bench

３．学会等名
2018 International Symposium on Information Theory and its Applications (ISITA2018)（国際学会）

４．発表年
2018年

１．発表者名
加納広太，志子田有光，神永正博，吉川英機

２．発表標題
軽量ブロック暗号におけるS-BOXマスキング保護の検討・評価

３．学会等名
第18回情報科学技術フォーラム(FIT2019)

４．発表年
2019年

１．発表者名
加納広太，吉川英機，神永正博，志子田有光

２．発表標題
FPGA実装の軽量ブロック暗号LBlockにおけるS-BOXマスキング保護の検討・評価

３．学会等名
第42回情報理論とその応用シンポジウム(SITA2019)，ポスターセッション

４．発表年
2019年

１．発表者名 加納広太，吉川英機，神永正博，志子田有光
２．発表標題 軽量ブロック暗号LBlockに対する相関電力解析への対策の検討
３．学会等名 電気関係学会東北支部連合大会2019
４．発表年 2019年

〔図書〕　計1件

１．著者名 神永正博	４．発行年 2017年
２．出版社 講談社ブルーバックス	５．総ページ数 240
３．書名 現代暗号入門	

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	志子田　有光 (Shikoda Arimitsu) (00215972)	東北学院大学・工学部・教授 (31302)	
研究分担者	鈴木　利則 (Suzuki Toshinori) (20500432)	東北学院大学・工学部・教授 (31302)	
研究分担者	吉川　英機 (Yoshikawa Hideki) (60259885)	東北学院大学・工学部・教授 (31302)	