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　元 年　 ６ 月 ２０ 日現在

機関番号：３２６９２
研究種目：基盤研究(C)（一般）
研究期間：2015～2018
課題番号：１５Ｋ００１８３

研究課題名（和文）理論的な安全性評価が可能な耐タンパーソフトウェア技術の研究

研究課題名（英文）Study on tamper-resistant software technology with theoretic security evaluation

研究代表者
布田　裕一（FUTA, Yuichi）

東京工科大学・コンピュータサイエンス学部・准教授

研究者番号：５０７０６２２３

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：White-Box Cryptography(WBC)技術は、プログラムや実行中のデータのすべてにアクセス可能な攻撃者に最も有利な状況においてもセキュリティを維持する技術であるため重要である。
本研究では、WBC技術の演算テーブルの識別不可能性を満たすために、テーブルの入出力関係が全単射である性質をなくす必要性を見出し、その方式モデルを提案した。WBC技術の安全性や計算量評価で必要となる、計算機を用いた形式検証技術を開発した。

研究成果の学術的意義や社会的意義
プログラムや実行中のデータに攻撃者がアクセス可能という条件下において、安全な本研究のWBC技術を用いることで、ハードウェアによるセキュリティの補助がなくても、ソフトウェアのみで高いセキュリティレベルを維持できる。そのため、携帯端末におけるアプリケーションを安全に実行することが可能になり、携帯端末を用いたインターネットバンキングやスマート家電の操作が安全に実現できる。
また、WBC技術の形式検証技術により、システムに組み込む際の安全性や計算量評価の補助が可能となる。

研究成果の概要（英文）：White-Box Cryptography(WBC) techniques, that achieve security under harsh security conditions, are important.
In this research, we have found the necessity to remove bijective characteristic of input-output relation of tables, and have proposed a scheme model. For security evaluation and estimation of computation amount of WBC techniques, we have developed formalized verification techniques using computers.

研究分野：情報セキュリティ

キーワード：White-Box Cryptography　耐タンパー技術　形式検証

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

Android 端末や iPhone 携帯電話をはじめとする携帯端末において、インターネットバンキングや企業の業務を実施するなどの高いセキュリティレベルが求められる場面が多くなってきている。最近では、家電をスマートフォンで家庭外から操作しており、攻撃者による不正操作による事故などのセキュリティリスクは、ますます高くなってきている。

携帯端末では、アプリケーションをダウンロードして処理を実行するため、ソフトウェアの安全性が、上記ケースにおけるセキュリティリスクを回避する上で重要である。

プログラムコードや実行中のデータの一部を用いて解析するソフトウェアのタンパー攻撃に対抗する耐タンパー技術が注目されており、種々の技術が研究開発されているが、理論的な安全性を持つ技術は少なく、実用化されているものはほとんどない。理論的な安全性を持つ技術として、準同型写像を応用したものがあるが、安全なハードウェアを前提としたものであり、上記の携帯端末のようなソフトウェアのみで守るケースでは適用しにくい。

2002 年にソフトウェアのみで理論的に守る技術として、White-Box Cryptography（以下で、WBC と略記）技術が提唱されている。WBC 技術は、最も攻撃者に有利であるプログラムコードやプログラムの実行中の中間データのすべてにアクセス可能な環境（理想的な攻撃モデル）において、ソフトウェアに含まれる秘密情報を取得する攻撃や、ソフトウェアの改ざん攻撃を防ぐ技術である。Chow らにより、ソフトウェアで実行する処理を変換して処理と等価なテーブルを作成し隠蔽することで、処理の内容や中間データを攻撃者が直接アクセスできない形にする方式が提案されている。しかし、テーブルの値を解析することで、その変換を取り去る攻撃が発見され、安全でなくなっている。

また、WBC 技術は、対象とする暗号が AES 暗号のような共通鍵暗号であり、公開鍵暗号を対象とした WBC 技術はほとんど存在しない。公開鍵暗号は処理内容が共通鍵暗号より複雑であり、処理をテーブル化しにくく、テーブルのサイズも非常に大きくなる課題があるためである。

２．研究の目的

本研究では理想的な攻撃モデルから攻撃者の能力を緩和させても問題がほとんどない攻撃モデルを構築し、その攻撃モデルにおいて安全な共通鍵暗号に対する WBC 方式を考案する。考案した方式を公開鍵暗号に適用するときのテーブル化の困難さやテーブルサイズの大きさの課題を解決し、公開鍵暗号に対する WBC 方式を考案する。

また、それぞれの WBC 方式の安全性や計算量の評価を計算機により実施する目的で、形式検証ツールにおける形式検証方法や、形式化ライブラリを開発する。

３．研究の方法

本研究では、AES 暗号に対する WBC 方式、RSA 暗号等の公開鍵暗号に対する WBC 方式と、WBC 技術の形式検証について研究開発を実施する。

(1)AES 暗号に対する WBC 方式の検討

実装する携帯端末等の環境において、攻撃者がソフトウェアに対して攻撃をかける場合で必須となる安全性の要件を抽出し、それを WBC の攻撃モデル（セキュリティモデル）に反映していく。反映した攻撃モデルの安全性検証を実施する。その攻撃モデルにおいて WBC 技術と、その技術に基づいた AES 暗号の WBC 方式を提案する。

(2)RSA 暗号等の公開鍵暗号に対する WBC 方式の検討

RSA 暗号において、攻撃者から隠蔽すべき対象の演算は秘密鍵を用いたべき乗演算であるが、その演算結果は秘密鍵のビット列に応じて乗算及び 2 乗算を実行するバイナリ法により得られる。攻撃者はプログラムコードや中間データの値を用いて、プログラム実行中のデータの動きを把握し、秘密鍵のビット列に応じた乗算や 2 乗算の実行箇所を特定することで秘密鍵を推測する。その攻撃に対抗するため、プログラムや中間データを用いた乗算と 2 乗算の識別を実現する WBC 方式を提案する。

(3)WBC 技術の形式検証技術の検討

WBC 技術の安全性や計算量の評価を、計算機を用いた形式検証で実施する形式検証技術を検討する。

４．研究成果

(1)AES 暗号に対する WBC 方式の検討

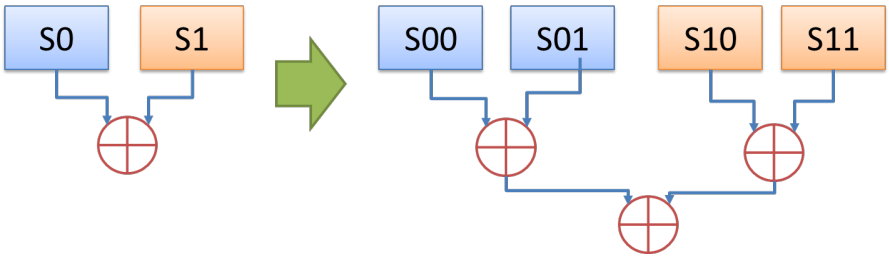
代数的な変換を利用する Billet らの攻撃方法及びその改良版である Mulder らの攻撃方法について分析した。WBC 技術においては、対象とする処理を変換してテーブルを作成しているが、これらの攻撃ではその変換を線形変換と非線形変換に分離することで攻撃している。攻撃の前提として、テーブルの入出力を線形移動させるために、そのテーブルの入出力の関係が全単射であるという性質が必要となることが判明した。

WBC 技術に対する新たな攻撃として、Differential Computation Analysis(DCA)が提案されたため、これに対する安全性を検証するために、DCA の攻撃方法について検討した。その結果、秘密情報を含むテーブルと含まないテーブルの識別不可能性を満たす必要があることが判明した。

WBC 技術の応用として、Symbolic Execution 技術による攻撃を防止するため、WBC 技術と

Linear Obfuscation 技術を組み合わせた方式を考案した。また、WBC 技術の対象となる共通鍵暗号の暗号解析を実施した。

(2)RSA 暗号等の公開鍵暗号に対する WBC 方式の検討
テーブルの入出力の関係が全単射である性質をなくすような対策を検討した。その結果、テーブルの入力をいくつかの範囲に分割し、それぞれの範囲に対応したテーブルを作成し、各テーブルが範囲外の入力に対しダミーの値を出力する方式を提案した(図 1)。



テーブルS0

S0(0)	S0(1)	S0(2)	S0(3)
S0(4)	S0(5)	S0(6)	S0(7)
S0(8)	S0(9)	S0(10)	S0(11)
S0(12)	S0(13)	S0(14)	S0(15)

テーブルS00

S0(0)	ダミー	S0(2)	S0(3)
S0(4)	ダミー	S0(6)	ダミー
ダミー	S0(9)	ダミー	S0(11)
ダミー	S0(13)	ダミー	ダミー

テーブルS01

ダミー	S0(1)	ダミー	ダミー
ダミー	S0(5)	ダミー	S0(7)
S0(8)	ダミー	S0(10)	ダミー
S0(12)	ダミー	S0(14)	S0(15)

図 1：入力ドメインの分割とダミーを追加したテーブル

これにより、各テーブルは一部の範囲のみ出力が対応するため、全単射性をなくすことが可能になる。
図 1 では、テーブル S0 と S1 の XOR を計算する処理に対し、テーブル S0，S1 の入力ドメインをそれぞれ 2 つに分けて、テーブル S00 と S01、S10 と S11 を作成している。S0 の入力は 0～15 までの 4 ビットの数としており、その{0，2，3，4，6，9，11，13}の入力ドメインを S00、{1，5，7，8，10，12，14，15}の入力ドメインを S01 に分割させている。入力ドメイン以外の入力に対しては、ダミーを出力させるようにさせる。このようにすることで、テーブルの変換を線形部と非線形部に分ける Billet らの攻撃を防止する。WBC 方式に対しては、先で述べた DCA が提案されており、DCA に対する安全性評価については今後の課題としたい。
プログラムの中間値が漏えいするが、漏えいさせる情報を攻撃者がコントロールできないという Gray-box に近い攻撃モデルを検討した。公開鍵暗号の理論における仮定（最上位ビットが 1）などが、現実のシステムでは NIST のテストデータにおいても前提とできない矛盾が生じている。任意の入力においても、攻撃者が情報を入手できないアルゴリズムを検討した。
WBC 技術の対象となる公開鍵暗号では耐量子公開鍵暗号の性質が必須である。そこで、有力な耐量子暗号の候補である符号ベースの暗号の解析も実施した。

(3) WBC 技術の形式検証技術の検討
暗号プロトコルの攻撃を形式的に導出する ProVerif において、観測透過性を利用した WBC の攻撃モデルの記述方法について検討した。プロセス内で公開通信路に中間値のデータを出力させて、攻撃者が取得できるような記述方法を検討した。さらに、処理フローをチェーンとみなした木構造を含めたモデルを、自動検証ツール ProVerif において検討した。
形式検証ツール Mizar において、WBC 技術の形式検証で必要な計算量の見積もりや、プログラムの状態遷移の追跡を実施するための形式検証ライブラリの検討を実施した。WBC 技術の計算量の評価を形式検証ツール Mizar で検証するために、計算量の形式化を検討した。バイナリ法とユークリッドアルゴリズムの計算量評価を実施する形式化ライブラリを作成した。さらに、アルゴリズム中の分岐やサブルーチンコールの形式化方法を検討した。計算量評価のために、分岐及びサブルーチンを表現した木構造を用いる方法を検討した。WBC 技術の安全性の形式検証のために、Mizar において確率分布の識別不可能性の形式化を検討した。
上記で検討・開発した形式検証技術は、WBC 方式のみならず、暗号プロトコルやブロックチェーンなどの方式にも適用可能であり、それらの安全性検証やアルゴリズムの検証、計算量評価を実現する上で有効である。今後は、暗号プロトコルやブロックチェーンへの具体的な適用方法を検討していく。

５．主な発表論文等
〔雑誌論文〕（計 12 件）
①Hiroyuki Okazaki, Koh-ichi Nagao and Yuichi Futa, “Maximum Number of Steps Taken by

Modular Exponentiation and Euclidean Algorithm”, Formalized Mathematics, 査読有, Vol. 27, Issue 1, 2019, 87–91.
DOI: 10.2478/forma-2019-0009
② Mohammad Saiful Islam Mamun, Chunhua Su, Anjia Yang, Atsuko Miyaji and Ali Ghorbani, “OTP-IoT: An ownership transfer protocol for the internet of Things”, Journal of Information Security and Applications, 査読有, Vol. 43, 2018, 73–82.
DOI: 10.1016/j.jisa.2018.10.009
③ Yuichi Futa and Yasunari Shidama, “Dual Lattice of Z-module Lattice”, Formalized Mathematics, 査読有, Vol. 25, Issue 2, 2018, 157–169.
DOI: 10.1515/forma-2017-0015
④ Ryoma Ito and Atsuko Miyaji, “Refined Construction of RC4 Key Setting in WPA”, IEICE Trans., Fundamentals. 査読有, Vol. E100-A, No.1, 2017, 138-148.
⑤ Ryoma Ito and Atsuko Miyaji, “Refined RC4 key correlations of internal states in WPA”, IEICE Trans., Fundamentals. 査読有, Vol. E99-A, No.6, 2016, 1132-1144.
⑥Jiageng Chen, Shoichi Hirose, Hidenori Kuwakado, and Atsuko Miyaji, “A Collision Attack on a Double-Block-Length Compression Function Instantiated with 8-/9-Round AES-256”, IEICE Trans., Fundamentals. 査読有, Vol. E99-A, No.1, 2016, 14-21.

〔学会発表〕(計 15 件)
①荒井 研一, 岡崎 裕之, 布田 裕一, “ProVerif を用いた CT 及びブロックチェーンの形式化”, 暗号と情報セキュリティシンポジウム(SCIS) 2019, 2019.
② Ryoma Ito and Atsuko Miyaji, “New Iterated RC4 Key Correlations”, The 23rd Australasian Conference on Information Security and Privacy(ACISP 2018), Lecture Notes in Computer Science, Vol.10946, Springer-Verlag, 2018, 154–171.
③Yohei Maezawa, T Chou and Atsuko Miyaji, “A Closer Look at the Guo-Johansson-Stankovski Attack Against QC-MDPC Codes”, Information Security and Cryptology – ICISC 2018, Lecture Notes in Computer Science, Vol. 11396, Springer-Verlag, 2018, 341-353.
④荒井 研一, 岡崎 裕之, 布田 裕一, “ProVerif を用いた CT の形式化”, 暗号と情報セキュリティシンポジウム(SCIS) 2018, 2018.
⑤ステュワート ギャヴィンレン, 布田 裕一, 宮地 充子, “共通鍵暗号方式における Linear Obfuscation を用いた効果的な難読化手法”, 信学技報, Vol. 116, No. 505, ISEC2016-90, 2017, 7–14.
⑥ステュワート ギャヴィンレン, 宮地 充子, 布田 裕一, “Symbolic Execution に対する難読化の評価”, コンピュータセキュリティシンポジウム(CSS) 2015, 2015, 297-303.
⑦Jiageng Chen, Atsuko Miyaji, Chunhua Su and Je Sen The, “Improved Differential Characteristic Searching Methods”, The 2nd IEEE International Conference on Cyber Security and Cloud Computing (CSCloud 2015), IEEE, 2015, 500-508.
⑧Jiageng Chen, Atsuko Miyaji, Chunhua Su and Liang Zhao, “A New Statistical Approach for Integral Attack”, The 9th International Conference on Network and System Security (NSS 2015), Lecture Notes in Computer Science, Vol. 9408, Springer-Verlag, 2015, 345-356.

６．研究組織
(1)研究分担者
研究分担者氏名：宮地 充子
ローマ字氏名：(MIYAJI, Atsuko)
所属研究機関名：大阪大学
部局名：工学系研究科
職名：教授
研究者番号（8 桁）：10313701

研究分担者氏名：CHEN Jiageng　(2015 年 8 月 24 日に削除)
ローマ字氏名：(CHEN, Jiageng)
所属研究機関名：北陸先端科学技術大学院大学
部局名：情報科学研究科 (2015 年当時)
職名：助教
研究者番号（8 桁）：90640748

(2)研究協力者
研究協力者氏名：岡崎 裕之
ローマ字氏名：(OKAZAKI, Hiroyuki)