公開

研 究 終 了 報 告 書

「IoT 機器の長期的な安全性確保のためのビヨンド軽量暗号の開拓」

研究期間:2020 年 11 月～2024 年 3 月
研 究 者:五十部　孝典

1. 研究のねらい

自動運転, 知能ロボット, スマート工場などに代表される超スマート社会では, エッジデバイスから情報を取得し, クラウドで分析を行い, システム全体としての適切な情報処理技術を行う. 大量のエッジデバイスでは, プライバシー情報や生体情報などのセンシティブな情報の処理するため, エッジデバイスでのセキュリティ技術が極めて重要になる. 実際, ヨーロッパ一般データ保護法や個人情報保護法の施行により, エッジデバイスで集めたセンシティブ情報は暗号化することが法的に義務付けられ, エッジデバイスでのセキュリティの担保することは今後ますます社会的に重要になる.

一般的にデータ収集に用いられるセンシング用のエッジデバイスは必ずしも十分なセキュリティ用のハードウェアリソースを持っていない. また, サーバとは異なり, 攻撃者が物理的にデバイスにアクセス可能であり, 攻撃者のターゲットになる可能性が非常に高い. 悪意のある攻撃者によりエッジデバイスから秘密鍵を盗まれた場合には, メッセージの改ざん, 平文情報の取得により, 大きな金銭的被害やプライバシーの侵害のみならず, 自動運転や知能ロボットの利用を考えた際には, 人命にも影響がある. リソースに制限のあるエッジデバイスにおいてセキュリティを如何に高めるかが, Society 5.0 においては重要な課題である.

本研究では, IoT におけるエッジデバイスの安全性の問題を解決するため, 新しい性質をもつビヨンド軽量共通鍵暗号の分野の開拓を目的とする. これまでの共通鍵暗号では, 秘密鍵の秘匿性の仮定に基づき, 平文の秘匿性や改ざん検知, 認証の安全性が定義されていた. しかしながら, 前述の通り, IoT におけるエッジデバイスでは攻撃者が非常に有利であるため, 秘密鍵の秘匿性を長期にわたり確保することは困難である. 本研究では, この問題を解決するため, デバイスはコンプロマイズ（物理的にアクセスされる）される前提に立ち, その場合でも秘密鍵をソフトウェアのみで保護する技術や, 仮に秘密鍵の秘匿性が破られた場合においても, 安全性を確保する技術の開発を行う. 具体的には、メモリに物理的アクセス可能であったとしてもプログラムから秘密鍵を盗むのが困難なホワイトボックスセキュリティや、仮に鍵を盗まれたとしても, 別デバイスでのプログラムの複製が計算量的に困難もしくは, 非常に重い非効率な演算になる複製困難性を持つ暗号技術の開発を目指す。

2. 研究成果

(1)概要

本研究では、テーマ A「ホワイトボックス暗号」、テーマ B「軽量暗号設計」、テーマ C「軽量暗号安全性評価」の3つのテーマを推進した。テーマ A に関しては、IoT デバイスでメモリからの鍵の流出を防ぐ技術である暗号アルゴリズム Cubicle, さらに複製困難性も付与した更新可能ホワイトボックス暗号 Yoroi, またこれらを任意長の暗号化や改ざん検知技術に拡張した暗号化モードの開発を行った。テーマ B では、「低遅延暗号 Orthros」、「低回路規模暗号 Atom」、「低消費電力暗号 Triad-LE」の技術開発を実施した。これらは、それぞれの観点で世界一の性能を達成しており、厳しいハードウェア条件での暗号化を可能とする。テーマ C に関しては、数理ソルバーを用いた解析技術により、さまざまな IoT 向け暗号の未知の脆弱性や性質の発見に成功した。また、IoT 環境において、攻撃者がメモリアクセスと通常のブラックボックスアクセスができることを想定した新しい攻撃モデル Hybrid code lifting 攻撃のフレームワークを提案した。

(2)詳細

ホワイトボックス暗号は、攻撃者が IoT デバイスのメモリに物理的アクセス可能であったとしても、プログラムから秘密鍵を盗むのが困難な技術である。具体的には、暗号演算をテーブルアクセスのみから実現し、各テーブルに鍵を隠すことで、メモリ上には鍵は出現せず、たとえデバイスにフルアクセス可能な攻撃者でも秘密鍵を取得することができない。

ハードウェアにおいては、電力や電磁波などのサイドチャネル情報を用いたメモリのリークによる攻撃が脅威となるため、本研究では、メモリがリークした場合でも安全性を保証する暗号アルゴリズム Cubicle の設計を行った。Cubicle では、IoT 向けに特化した暗号として、Cortex-M をターゲットとし、Cortex-M 向けの命令セットや RAM サイズに特化した構造を採用することで、既存技術の 4 倍以上の高速化に成功した(図 1)。安全性に関しては、150KB 以下のメモリリークの場合、安全性を保証可能である。一方通常の暗号であれば、たった 128 bit のリークで安全性が方向するため、メモリリークに対する安全性は大幅に向上させることができた。本成果は国際論文誌に採録されている。

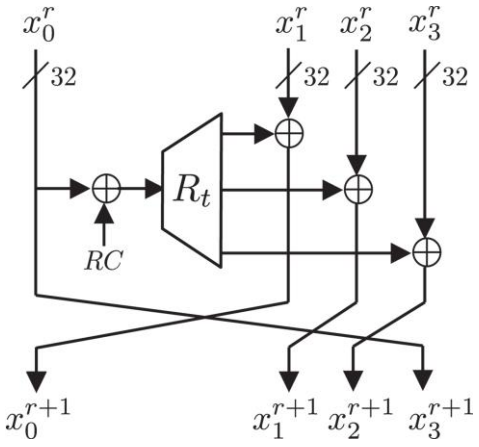

図 1: Cubicle の構成

テーブル自体の取得を防ぎ、複製困難性を付加する技術として、暗号化関数としての機能を維持したまま、セキュアにテーブルを更新可能な”Updatable Whitebox Cryptography”の理論を構築した(図 2)。この技術では、テーブルの前後に非線形関数を加えることでテーブル自体を更新するが、前後のテーブルにその逆関数を加えることで、暗号関数全体の機能は維持する構成をとっている。この理論をもとに、実際のホワイトボックス暗号アルゴリズム Yoroi を設計し、暗号実装分野のトップジャーナル TCHES に投稿し、採択された[代表的論文1]。

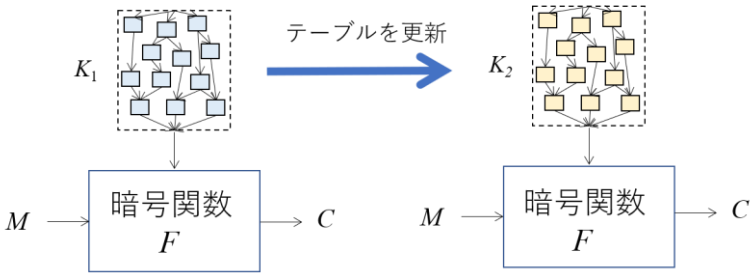

図 2:Updatable Whitebox Cryptography

Yoroi や Cubicle は特定のブロックの平文を暗号文へと変換するブロック暗号である。このブロック暗号を任意長のメッセージの暗号化や改ざん検知、認証の機能に拡張するため、暗号化モードの設計を行った。本研究では、リークがあった場合でも暗号の安全性を数学的に証明可能な暗号化モードの開発を進めた。具体的には、モードに用いる暗号プリミティブに特定の性質（1/4 のリークがあった場合でも安全である）を仮定することで、暗号化モード全体としても安全性を数学的に補償可能な初期理論の構築とプロトタイプとして WHI-SIV と呼ぶモードを設計した。このモードでは、プリミティブの安全性をモード全体に拡張可能であり、サイドチャネル攻撃や物理攻撃で多くの秘密データを攻撃者に取得された場合でも秘匿性や認証などの安全性を数学的に証明可能である(図 3)。さらにこのモードに特化した新しいプリミティブ SPACE256 を設計した。SPACE256 は、256 ビットのブロックサイズを持ち、この暗号をモードに組み込んだ場合は、数メガバイトの情報がリークした場合でも安全性を保証可能である。本成果は暗号のトップカンファレンス ASIACRYPT 2022 に採録された。

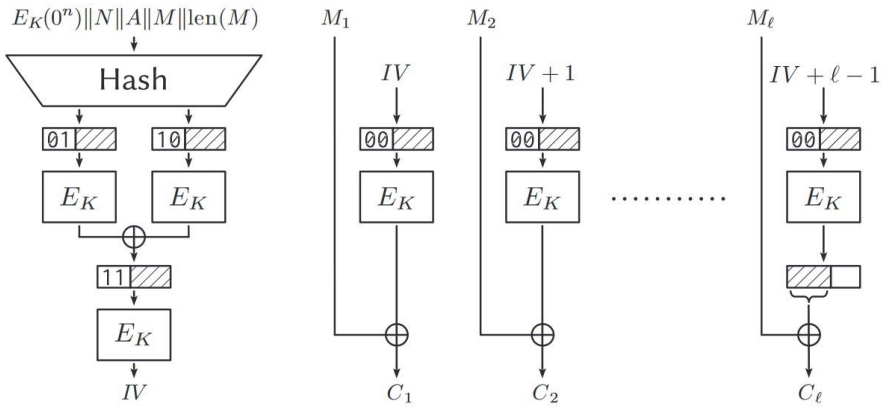

図 3: WHI-SIV mode

■　研究テーマ B「軽量暗号設計」

「低遅延暗号」と「低回路規模暗号」「低消費電力」の技術開発を実施した。

低遅延暗号技術としては、低遅延非線形関数の設計と、全体の繰り返し数を抑えるため、ブロック暗号を2つ並列に並べた 2-branch Dual Construction 技術を開発した（図4）。これらの技術を用いた低遅延暗号 Orthros を設計し、デファクトスタンダード暗号の AES と比較し、1/10 の遅延での暗号化が可能となった。この成果は、共通鍵暗号技術のトップジャーナルである ToSC 2021 に採録された[代表的論文2]。

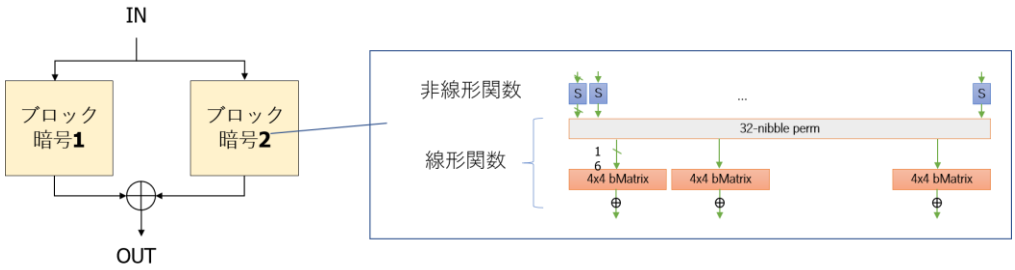

図4：2-branch Dual Construction

低回路規模暗号に関しては、ストリーム暗号において必要なレジスタサイズを抑える技術である Double key filtering と呼ばれる技術を開発した。これは、2 種類の key scheduling function を用いることで、レジスタサイズが小さい暗号に対する安全性を向上させる技術である。この技術を用いた暗号として、ストリーム暗号アルゴリズム Atom を設計した（図 5）。Atom は 128 bit security のストリーム暗号としては、世界最軽量を達成し、ToSC 2020 に採録された。

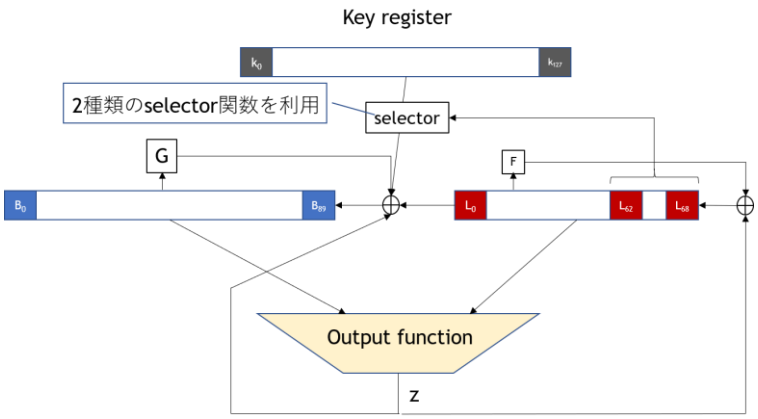

図 5：Double Key Filtering

低消費電力暗号に関しては、IoT 向けの低消費電力暗号の設計理論を確立した。ハードウェア実装において任意ラウンド関数を展開して実装（アンロール実装）した際に、各演算のクリティカルパスの長さが均一になる Perfect Tree と呼ばれる構造を多く持たせることでクリティカルパスの最小化が可能であることを示した。この理論を用いたストリーム暗号 Triad-LE を設計し、低消費電力性能で世界最小を達成したアルゴリズム Triad-LE を設計した。

■　研究テーマ C「軽量暗号安全性評価」

共通鍵暗号に対する代表的な攻撃手法である差分攻撃、線形攻撃、積分攻撃、代数攻撃、不能差分攻撃に関して、混合整数線形計画法のソルバーを用いた自動の安全性評価ツールを作成した。具体的には各種攻撃で用いる統計的な性質を求める問題を混合整数線形計画における目的関数に変換し、暗号の構造を制約式でうまくモデリングすることで実現した。すべての攻撃ツールは独立なものであり、合計５通りの安全性評価ツールの作成を、言語は C++、Solver は Gurobi optimizer を用いて実施した。自動評価ツールであるため、特定の暗号アルゴリズムに対して動くのではなく、あらゆる暗号構造に適用可能な汎用ツールとして設計した(図 6)。

評価ツールの最適化と有用性を確認するために、IoT 向け暗号である Friet, SNOW, Keccak, LowMC, Lesamnta, Rasta, RIMPE-MD, Chagri に適用し、未知の脆弱性や性質の発見に成功し,暗号分野のトップ会議 CRYPTO, EUROCRYPT, ASIACRYPT 等に採録された。

次に、IoT 向けのスペースハード暗号の新しい攻撃モデル Hybrid Code Lifting モデルを考案した。この攻撃モデルでは、攻撃者は物理的な攻撃と通常のブラックボックス攻撃を組み合わせて利用するもので、実際の IoT 機器への攻撃もこのモデルで表現することが可能である(図 7)。このより実用的なモデルにおいて、既存の暗号である Yoroi や SPNbox の安全性を厳密に評価した. 本成果は、共通鍵暗号のトップジャーナル FSE 2023 に採録され、Best Paper Award も受賞した[代表的論文3]。

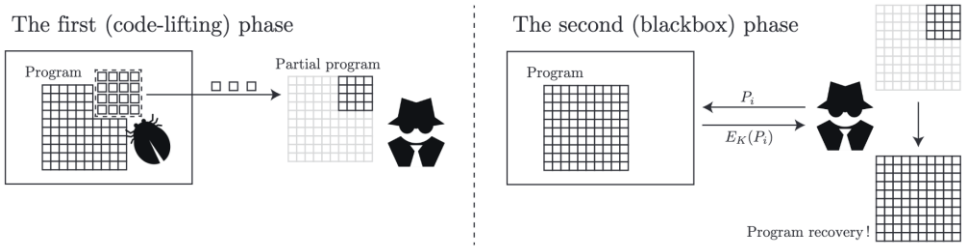

図 6: Hybrid Code Lifting Attack

■　さきがけ研究領域内外の研究者や産業界との連携

産業界との連携に関しては、研究テーマ A のホワイトボックス暗号では NTT, テーマ B では NEC と KDDI 総合研究所、テーマ C では三菱電気と共同研究契約を締結し、研究を推進した。テーマ B に関しては、Beyond 5G 用に発展させる研究課題において、GMO サイバーセキュリティと共同で NICT beyond 5G のシーズ創出プログラムに応募し、採択された。以上のように、社会実装を見据えて企業等の共同研究を積極的に推進した。

さきがけ領域内ではハードでの軽量化や省電力技術に専門性のある新津先生と共同研究プロジェクトをスタートし、研究費のプロポーサルを行っており、来年度から本格的に共同研究を実施する予定である。またさきがけ外では、スイスの EPFL, ドイツのワイマール大学、マンハイム大学、インドのインド工科大学と共同での研究を推進し、国際的なネットワークを構築した。

3. 今後の展開

＜目的の達成状況＞

当初予定していた Beyond 共通鍵暗号である“複製困難性を持つホワイトボックス暗号”に関しては、暗号の設計理論や実際の暗号アルゴリズムの開発が完了し、全ての目標は達成することができた。さらに、その設計の過程で得た技術をベースに、IoT 向けの軽量暗号の設計や安全性解析に関する研究も推進し、当初の想定にはないプラスαの結果を上げることができた。質的にも、期間内に暗号分野のトップ会議 CRYPTO, ASIACRYPT, EUROCRYPT, FSE, CHES の 5 つに全て採録させることができ、学術的にもインパクトのある結果を創出できた。

＜研究の進め方（研究実施体制及び研究費執行状況）＞

進め方に関しては、コロナの状況もあり海外に直接行くことが難しいため、その予算を計算機サーバの拡充やプログラム作成や数値計算のための人件費に投入した。これにより、私自身がコア技術やアイデアを考え、その検証や実験を計算機や学生のアルバイトにアウトソースする体制を構築することでき、効果的に研究を推進することができた。また、国内の電機メーカの研究者とも積極的に共同研究を実施することで、自分と異なる専門性を持つ研究者とチームを組んで研究を推進することができ、人的リソースが多く必要となる暗号設計プロジェクトを複数推進することができた。

4. 自己評価

＜目的の達成状況＞

当初予定していた Beyond 共通鍵暗号である“複製困難性を持つホワイトボックス暗号”に関しては、暗号の設計理論や実際の暗号アルゴリズムの開発が完了し、全ての目標は達成することができた。さらに、その設計の過程で得た技術をベースに、IoT 向けの軽量暗号の設計や安全性解析に関する研究も推進し、当初の想定にはないプラスαの結果を上げることができた。質的にも、期間内に暗号分野のトップ会議 CRYPTO, ASIACRYPT, EUROCRYPT, FSE, CHES の 5 つに全て採録させることができ、学術的にもインパクトのある結果を創出できた。

＜研究の進め方（研究実施体制及び研究費執行状況）＞

進め方に関しては、コロナの状況もあり海外に直接行くことが難しいため、その予算を計算機サーバの拡充やプログラム作成や数値計算のための人件費に投入した。これにより、私自身がコア技術やアイデアを考え、その検証や実験を計算機や学生のアルバイトにアウトソースする体制を構築することでき、効果的に研究を推進することができた。また、国内の電機メーカの研究者とも積極的に共同研究を実施することで、自分と異なる専門性を持つ研究者とチームを組んで研究を推進することができ、人的リソースが多く必要となる暗号設計プロジェクトを複数推進することができた。

＜研究成果の科学技術及び社会・経済への波及効果＞

学術的には、CRYPTO, ASIACRYPT, EUROCRYPT, FSE, CHES などのトップ会議に採録されるとともに、共通鍵暗号分野のトップ会議 FSE のベストペーパーを 2 年連続で受賞、また末松安晴賞, 文部科学大臣表彰若手科学者賞なども受賞でき、暗号や情報セキュリティ分野の発展や日本のプレゼンス向上に貢献することができた。

社会、経済への波及効果としては、複数の企業と共同研究することで、実際に設計した暗号技術の社会実装も積極的に進めた。特に、KDDI や NEC では社内サービスやプロダクトで利用されている。また標準化活動も KDDI や GMO と共同で進めている。

5. 主な研究成果リスト

(1)代表的な論文(原著論文)発表

研究期間累積件数: 39件

1. Yuji Koike and Takanori Isobe, "Yoroi: Updatable Whitebox Cryptography", IACR Transactions on Cryptographic Hardware and Embedded Sytems (TCHES), no.4, pp.587-617, 2021.	1.
ホワイトボックス暗号ではテーブル内に鍵隠すため、鍵取得は困難であるが、テーブル自体の取得による暗号化機能の複製は防ぐことが困難である。本研究では、困難性を付加する技術として、暗号化関数としての機能を維持したまま、セキュアにテーブルを更新可能な”Updatable Whitebox Cryptography”の理論を構築し。この技術では、テーブルの前後に非線形関数を加えることでテーブル自体を更新するが、前後のテーブルにその逆関数を加えることで、暗号関数全体の機能は維持する構成をとっている。これにより、テーブルの取得、複製を困難にできる。この理論をもとに、実際のホワイトボックス暗号アルゴリズム Yoroi を設計した。	
2. Subhadeep Banik, Takanori Isobe, Fukang Liu, Kazuhiko Minematsu and Kosei Sakamoto, "Orthros: A Low-Latency PRF", IACR Trans. Symmetric Cryptol (ToSC/FSE), 2021, issue 1, pp.37-77, 2021.	2.
IoT 社会の発達にともない, より少ない遅延で暗号化が実行可能な 128 ビット低遅延擬似ランダム関数が求められている。本研究で提案する擬似ランダム置換 Orthros は 128 ビットの鍵を持つ。Orthros の全体構造は、Branch1 とBranch2 と呼ばれる 2 つの SPN 型の鍵付き置換の排他的論理で構成されている。Orthros のラウンド関数は、Midori に基づいており低遅延暗号に適しているが、新しい線形層と S-box を採用することで遅延をさらに最小化した。結果として既存の暗号である Midori や QARMA よりも暗号化に必要な Latency の値が小さくなりかつ、消費電力に関して既存技術からの大幅な削減に成功した。	
3. Yosuke Todo and Takanori Isobe, "Hybrid Code Lifting on Space-Hard Block Ciphers", IACR Trans. Symmetric Cryptol (ToSC/FSE), 2022, issue 3, pp. 368-402, 2022.	3.
IoT 向けのスペースハード暗号の新しい攻撃モデル Hybrid Code Lifting モデルを考案した。この攻撃モデルでは、攻撃者は物理的な攻撃と通常のブラックボックス攻撃を組み合わせて利	

用するもので、実際の IoT 機器への攻撃もこのモデルで表現することが可能である。このより実用的なモデルにおいて、既存の暗号である Yoroi や SPNbox の安全性を厳密に評価した。

(2)特許出願

研究期間全出願件数:0 件(特許公開前のものは件数にのみ含む)

1	発明者	
	発明の名称	
	出願人	
	出願日	
	出願番号	
	概要	
2	発明者	
	発明の名称	
	出願人	
	出願日	
	出願番号	
	概要	

(3)その他の成果(主要な学会発表、受賞、著作物、プレスリリース等)

- 第9回(令和4年度)末松安晴賞, 2023
- 令和 5 年度 文部科学大臣表彰若手科学者賞, 2023
- International Association for Cryptographic Research, Fast Software Encryption 2023 Best Paper Award, 2023
- International Association for Cryptographic Research, Fast Software Encryption 2022 Best Paper Award, 2022
- 日本セキュリテイ・マネジメント学会 第 7 回 辻井重男セキュリティ論文賞 優秀賞, 2022