2023年度共同利用研究報告書

2023年12月01日

所属・職名 筑波大学・システム情報系・教授
國廣 昇

		整理番号	2023a003	
1.研究計画題目	現代暗号に対する安全性解析・攻撃の数理			
2.新規・継続	新規			
3.種別	一般研究			
4.種目	研究集会（Ｉ）			
5.開催方法	ハイブリッド開催			
6.研究代表者	氏名	國廣 昇		
	所属部局名	筑波大学・システム情報系	職名	教授
7.研究実施期間	2023年09月20日(水曜日)～2023年09月22日(金曜日)			
8.キーワード	暗号理論，安全性評価			
9.参加者人数	159人			

10.本研究で得られた成果の概要

本研究集会は，暗号の安全性解析・攻撃の数理に関する最新の成果やアイデアを研究者間で共有することを目的として企画された．以下で説明するように，当初の目的は十分に達成できたと考える．

講演は次の4つのカテゴリに基づき行われ，合計10件の講演が行われた．
カテゴリ1: ハードウェアの安全性（3件），カテゴリ2: 共通鍵暗号の安全性（2件），カテゴリ3: 量子計算機に対する安全性（3件），カテゴリ4: サイドチャネル攻撃に対する安全性（2件）．

1件あたり1時間（学生の発表は30分）の講演時間であり，講演は，基本的な事柄から始まり，最新の研究成果までカバーされていた．質疑応答および休憩時間では，活発に議論が行われていた．件数及び時間の観点で安全性解析の各トピックを網羅的にバランスよく講演があったと考えている．いずれの講演も，内容はトップレベルの国際会議で採択されている研究の一端，もしくは最先端の研究の一端であり，情報と示唆の多い充実した研究集会となった．

全10件の講演中，企業からの講演が6件あり，産業界からの暗号の安全性解析に対する成果の講演があった．具体的には，NEC，NTT，三菱電機，富士通という活発に研究活動をしている国内企業，および，フランスのCryptoExpertsに所属する研究者からの講演も行われた．

参加者についての成果を説明する．本研究集会は159名の参加登録があった．若手研究者からシニアの研究者まで幅広い年齢層の参加があった．産業界からは73名（46%），学からは73名（46%），官及びその他からは13名（8%）であった．特に産業界からの参加者も多く，学と同数の参加者であった．そのため，本研究集会の目的は十分に達成できたと考える．また，学の参加者のうち半数近くは学生であり，若い世代への啓蒙活動にも成功している．さらに，7名は海外からの参加者であり，国際的な連携という点でも十分に成果をあげるのに成功している．

2023 年 11 月 1 日

2023 年九州大学マス・フォア・インダストリ研究所共同利用研究集会(I)

現代暗号に対する安全性解析・攻撃の数理

(Mathematics of Security Analysis for Modern Cryptography)

成果報告書

組織委員

筑波大学・教授	國廣昇（代表者）
九州大学・IMI・助教	池松 泰彦
富士通・シニアディレクター	伊豆 哲也
青森大・教授	穴田 啓晃
九州大・IMI・教授	縫田 光司

ウェブサイト

https://joint.imi.kyushu-u.ac.jp/research-reports/year-2023/

https://joint.imi.kyushu-u.ac.jp/post-9072/

本報告書は，2023 年の共同利用研究集会(I)で採択頂いた上記の表題の研究集会を開催して得られた成果を簡潔に報告することを目的とする．

はじめに，参加者についての成果を説明する．本研究集会は 159 名の参加登録があった．参加人数の内訳を，年齢別及び産学官別でそれぞれ表 1 及び表 2 に示す．**表 1** から，若手研究者からシニアの研究者まで幅広い年齢層の参加があったことがわかる．また表 2 から，産業界からは 73 名（46%），学からは 73 名（46%），官及びその他からは 13 名（8%）であったことがわかる．特に産業界から多くの参加があり，学と同数の参加者であった．そのため，本研究集会の目的は十分に達成できたと考える．また，学の参加者のうち半数近くは学生であり，若い世代への啓蒙活動に成功している．さらに，7 名は海外からの参加者である（このうち，2 名は対面での講演者である）．国際的な連携という点でも十分に成果をあげるのに成功している．

表 1　参加人数内訳．年齢別

	40 歳以上	40 歳未満	35 歳以下	合計
人数	66	19	74	159
比率	41%	12%	47%	100%

表 2　参加人数内訳．産学官別

	産	学	官	その他	合計
人数	73	73 （うち学生 31）	9	4	159
比率	46%	46%	6%	2%	100%

次に，研究内容の成果を説明する．次ページに実施された講演の一覧を示す．講演は次の 4 つのカテゴリに分類される．

- カテゴリ 1: ハードウェアの安全性　　：講演 1) 2) 3)
- カテゴリ 2: 共通鍵暗号の安全性　　：講演 4) 5)
- カテゴリ 3: 量子計算機に対する安全性　　：講演 6) 7) 8)
- カテゴリ 4: サイドチャネル攻撃に対する安全性　：講演 9) 10)

このことから，本研究集会の研究題目「現代暗号に対する安全性解析・攻撃の数理」に関し，件数及び時間の観点で安全性解析の各トピックを網羅的にバランスよく講演頂けたものと考えている．

講演内容について説明する．ハードウェアの安全性に関して 3 件，共通鍵暗号の安全性に関して 2 件，量子計算機に対する安全性に関して 3 件，サイドチャネル攻撃に対する安全性に関して 2 件，合計 10 件の講演を頂いた．3 日間の開催であり，1 件あたり 1 時間（学生の発表は 30 分）の講演時間とし，基本的な事柄からスタートし，最新の研究成果まで，十分に講演いただけるようにするとともに，十分な質疑応答ができるようにした．いずれの講演も，内容はトップレベルの国際会議で採択されている一連の研究の一端，もしくは最先端の研究の一端であった．そのため，情報と示唆の多い充実した研究集会となった．

全 10 件の講演中，企業からの講演が 6 件あり，産業界からの暗号に対する安全性解析に対する成果を講演頂いた．特に，国内企業では，NEC，NTT，三菱電機，富士通という活発に研究活動をしている企業から講演を頂いた．海外からは，フランスの CryptoExperts に所属する研究者から講演を頂いた．

最後に，本研究集会の開催に当たっては，九州大学マス・フォア・インダストリ研究所から支給頂いた予算を用いた．ここに深く申し上げる．

（以上）

2023 年 11 月 1 日

実施された講演の一覧

第 1 日：9 月 20 日（水）

1) 13:10-14:10
林優一（奈良先端科学技術大学院大学）
現代暗号を含むハードウェアからの電磁的情報漏えいの数理

2) 14:25-15:25
上野嶺（東北大学）
メモリ暗号化のための暗号技術とハードウェアアーキテクチャ

3) 15:40-16:40
Abdul Rahman Taleb (CryptoExperts and Sorbonne University)
Towards Achieving Provable Side-Channel Security in Practice

第 2 日：9 月 21 日（木）

4) 10:00-11:00
井上明子（NEC）
共通鍵暗号の認証暗号利用モードの安全性と攻撃について

5) 11:15-12:15
藤堂洋介（NTT）
キャッシュランダム化関数の安全性モデルと SCARF の設計・安全性評価

6) 13:45-14:45
大西健斗（三菱電機）
効率的な近似量子フーリエ変換を利用した Shor アルゴリズム

7) 15:00-16:00
山口純平（富士通）
素因数分解問題に対する新しい量子アルゴリズム SQIF の実装と解析

8) 16:10-16:40
田口 廉（東京大学）
バイナリ ECDLP を解く Shor のアルゴリズムにおける楕円曲線加算の量子リソース削減

第 3 日：9 月 22 日（金）

9) 10:00-11:00
草川恵太（TII）
格子ベースの鍵カプセル化方式に対するサイドチャネル攻撃を利用した鍵回復攻撃

10) 11:20-12:20
伊東燦（NTT）
深層学習に基づくサイドチャネル攻撃とその対策

現代暗号に対する安全性解析・攻撃の数理

開催日程：9/20(水) - 9/22(金)
開催場所：JR 博多シティ 9 階会議室 1

9/20（水）

13:00-13:10 Opening

Session 1: ハードウェアの安全性

13:10-14:10 林優一（奈良先端科学技術大学院大学）
現代暗号を含むハードウェアからの電磁的情報漏えいの数理
【アブストラクト】
本講演では、現代暗号を含むハードウェアからの電磁的情報漏えいメカニズムに着目し、漏えい源となる暗号モジュールから電磁波を通じてモジュール内部の秘密鍵が機器外部に漏えいする過程を数理モデルにより説明する。また、電磁気学の相反性から、機器外部から到来した電磁波によって暗号モジュールから秘密鍵が漏えいする過程も同様のモデルで説明できることを概説する。

14:25-15:25 上野嶺 (東北大学)
メモリ暗号化のための暗号技術とハードウェアアーキテクチャ
【アブストラクト】
CPU の外部に配置されるメインメモリは盗聴や改ざんなどの脅威に晒されうるため，それに対抗するためにメモリ暗号化が用いられる．特に近年では，不揮発メモリ (NVM) の高性能化や大容量化に伴い，データセンタや IoT 機器，さらに現代の CPU において省消費電力化や高性能化を目的として不揮発メモリ (NVM) の採用例が増えている．一方で，NVM はそのデータの永続性から盗聴や改ざんのリスクが DRAM に比べて高まる．そこで，大容量の NVM をリアルタイムで暗号化・認証するメモリ暗号化技術が強く求められる．本講演では，セキュア NVM のための暗号化技術およびそのハードウェアアーキテクチャについて，講演者らによる最新の成果を交えながら概説する．

15:40-16:40　Abdul Rahman Taleb (CryptoExperts and Sorbonne University)

Towards Achieving Provable Side-Channel Security in Practice

Abstract:
Physical side-channel attacks are powerful attacks that exploit a device's physical emanations to break the security of cryptographic implementations. Many countermeasures have been proposed against these attacks, especially the widely-used and efficient masking countermeasure. Nevertheless, proving the security of masked implementations is challenging. Current techniques rely on empirical approaches to validate the security of such implementations. On the other hand, the theoretical community introduced leakage models to provide formal proofs of the security of masked implementations. Meanwhile, these leakage models rely on physical assumptions that are difficult to satisfy in practice, and the literature lacks a clear framework to implement proven secure constructions on a physical device while preserving the proven security.

9/21(木)

Session 2: 共通鍵暗号の安全性

10:00-11:00 井上明子（NEC）
共通鍵暗号の認証暗号利用モードの安全性と攻撃について
【アブストラクト】
認証暗号は平文の秘匿と暗号文の改ざん検知が同時に実現できる共通鍵暗号方式である．その安全性は，2000 年に秘匿と改ざん検知の 2 つとして正式に定義されたが，その後，これらの安全性を満たす認証暗号が実装上の過失により破れる場合があることや，認証暗号を用いるプロトコルが，秘匿と改ざん検知以上の安全性を認証暗号に要求している場合があることが攻撃により示されている．本発表では，ブロック暗号等の固定長入出力暗号部品を用いた認証暗号構成を中心の話題として，基本的な認証暗号の安全性及びそれに対する攻撃，そして上記のように基本の安全性を超えた攻撃や，それらを考慮した認証暗号の拡張された安全性について紹介する．

11:15-12:15 藤堂洋介（NTT）
キャッシュランダム化関数の安全性モデルと SCARF の設計・安全性評価
【アブストラクト】
キャッシュ攻撃とはキャッシュとメモリの遅延差を利用したサイドチャネル攻撃である。キャッシュ攻撃を防ぐ方法としてキャッシュランダム化が注目されている。Usenix

Security2023 で、キャッシュランダム化関数の安全性モデル、調整可能暗号を用いた設計理論、具体的な関数 SCARF を設計・発表した。本講演では、この安全性モデルの解説、実際の SCARF の設計プロセス、SCARF に対する具体的な暗号解読の取り組みを紹介する。

Session 3: 量子計算機に対する安全性

13:45-14:45 大西健斗（三菱電機）
効率的な近似量子フーリエ変換を利用した Shor アルゴリズム
【アブストラクト】
本発表では，素因数分解問題を解く Shor アルゴリズムの効率化手法について議論する．現在利用されている主な公開鍵暗号として，RSA 暗号や楕円曲線暗号があり，素因数分解問題や離散対数問題に安全性の基盤を置いている．Shor アルゴリズムは，これらの問題を多項式時間で解く量子アルゴリズムである．現在の公開鍵暗号が危殆化する時期を見積もるため，Shor アルゴリズムの計算コスト評価は極めて重要である．本発表では，近似量子フーリエ変換に基づく Shor アルゴリズムについて議論する．特に，本発表では，将来実現しうる大規模な耐故障性量子計算機を考慮し，耐故障性を持つ Shor アルゴリズムについて計算コストの削減方法を議論する．

15:00-16:00 山口純平（富士通）
素因数分解問題に対する新しい量子アルゴリズム SQIF の実装と解析
【アブストラクト】
2022 年 12 月に Shor よりも少ない量子ビットで素因数分解可能とする
新しい量子アルゴリズム SQIF(Sublinear-resource Quantum Integer Factorization)が提案された．SQIF は平方差法をベースとしており，特に平方差法の関係式計算を組み合わせ最適化問題に帰着し， その近似解を量子アルゴリズム QAOA を用いて計算することで関係式を得る．本講演では，2023 年 5 月の CSEC で発表した「格子と最適化手法を用いた素因数分解法の実験報告」の詳細を紹介する．まず SQIF の詳細を紹介し，関係式が数個しか計算できないという問題点を指摘する．次に，十分な数の関係式が計算可能な拡張 SQIF を提案し，その実験結果を紹介する．実験を大規模にするため QAOA の代わりに古典的なアニーリング計算を使用し， 11 から 55 ビットの合成数の素因数分解に成功した．最後に，2048 ビット合成数の分解に必要な量子ビット数および計算量の見積もりを与える．

16:10-16:40 田口 廉 (東京大学)
バイナリ ECDLP を解く Shor のアルゴリズムにおける楕円曲線加算の量子リソース削減
【アブストラクト】

離散対数問題を多項式時間で解く Shor のアルゴリズムの実装に係る量子リソース評価の研究が数多く行われており，バイナリ楕円曲線では量子逆元計算が主要な計算であることが知られている．その中でも我々は Toffoli ゲート数と深さの面でより有効な量子 FLT 逆元計算に着目する. 我々は, 既存の量子 FLT 逆元計算アルゴリズムを純粋に改良する量子 FLT 逆元計算アルゴリズムを提案し，量子ビット数をさらに削減できることを示す.

9/22(金)

Session 4: サイドチャネル攻撃に対する安全性

10:00-11:00 草川恵太（TII）
格子ベースの鍵カプセル化方式に対するサイドチャネル攻撃を利用した鍵回復攻撃
【アブストラクト】
量子計算機の開発の進展を受け、耐量子計算機暗号（PQC）の標準化や実装が盛んになっている。大きな影響を持つ NIST の PQC 標準化では、サイズ・速度・安全性といった観点から鍵カプセル化方式（KEM）として格子暗号の Kyber が選ばれた。一方、標準化される暗号は様々な機器で実装されることから、サイドチャネル攻撃耐性も重要視される。本発表では Kyber を中心とした格子暗号に対するサイドチャネル攻撃を利用した鍵回復攻撃を、紹介する。特に、サイドチャネル攻撃を用いて平文判定オラクルや復号オラクルを構築した後の、攻撃の効率化について紹介する。

11:20-12:20 伊東燦（NTT）
深層学習に基づくサイドチャネル攻撃とその対策
【アブストラクト】
暗号モジュールから副次的に発生する消費電力・漏洩電磁波（サイドチャネル情報）を用いることで、暗号モジュール内の秘密鍵を推定する攻撃をサイドチャネル攻撃という。本講演では、近年高い注目を集めているニューラルネットワークを用いたサイドチャネル攻撃（DL-SCA)について解説を行う。DL-SCA では、あらかじめ攻撃対象モジュールのサイドチャネル情報について学習することで、従来よりも強力な攻撃が可能なことが知られている。また、サイドチャネル攻撃に対する代表的な対策手法であるマスキング対策と、その理論的な安全性についても紹介し、マスキング対策が DL-SCA に対しても有効であることを説明する。

12:20-12:30 Closing

13:00-15:00 Free Discussion