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　６ 年　 ６ 月 １１ 日現在

機関番号：１３９０１
研究種目：基盤研究(C)（一般）
研究期間：2021～2023
課題番号：２１Ｋ１１８８６

研究課題名（和文）サイドチャネル攻撃の包括的安全性評価を目的とした漏洩情報量計算手法の開発

研究課題名（英文）Comprehensive security evaluation for side-channel attacks by evaluating the amount of information leakage

研究代表者
楫　勇一（KAJI, Yuichi）

名古屋大学・情報学研究科・教授

研究者番号：７０２６３４３１

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：サイドチャネル攻撃は，機器から漏洩する電磁波や入力データに対する処理時間等，情報システムが意図せず発出する副次的な情報を手がかりとして実行される攻撃手法であり，システム内部で使用されている暗号鍵の特定等，重大な脅威となることが知られている．本研究では，副次的情報が持つ情報量に着目し，サイドチャネル攻撃に対する安全性評価の手法について各種の検討を行った．
具体的な成果としては，古典的な（非量子的な）枠組みにおいて漏洩情報量を評価し，削減するための技術開発を行った．また，量子計算機の実用化を考慮に入れ，耐量子暗号技術や量子アルゴリズムの計算量評価等に関し，先駆的な知見を得ることができた．

研究成果の学術的意義や社会的意義
実用的なシステムやプログラムを対象として漏洩情報量を具体的に計算することは，きわめて難しい．本研究では，自然に導かれる前提条件から計算機の動作を数学的にモデル化し，同モデルに基づいて漏洩する情報の量を定量化・具体化することに成功している．また，キャッシュ攻撃等のサイドチャネル攻撃への対策提案，符号ベース暗号に関するアルゴリズム開発等，周辺の関連分野に対しても貢献を行うことができた．さらに，ポスト量子時代を見据え，耐量子安全な暗号関連技術の開発や量子アルゴリズムの計算量評価等にも取り組み，研究開始時点からの社会状況の変化等に対し柔軟に対応し，次世代の研究の礎となる結果を与えることができた．

研究成果の概要（英文）：A side-channel attack focuses on side information emitted from the system unintentionally and is regarded as a serious threat to many practical computer systems. For the comprehensive evaluation of security against side-channel attacks, this study develops a means to evaluate the amount of information that leaks out from the system.
Investigations are made to derive formulas for the amount of leaked information in a classic (non-quantitative) framework, and some measures are proposed to reduce the amount in several side-channel attacks. The study also focuses on the relationship between the subject and quantum computers and investigates post-quantum crypt techniques and quantum algorithms also.

研究分野：情報セキュリティ

キーワード：サイドチャネル攻撃　漏洩情報量　情報理論　耐量子暗号技術　ハッシュベース署名　ハッシュパズル　量子アルゴリズム

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

暗号や情報セキュリティの歴史は，より安全とされる新しい技術の開発と，その技術を破る新しい攻撃手法の発見の繰り返しにより構成されてきた．当然のことながら，セキュリティ技術を開発するものは，その技術が破られることのないよう万全の注意を払っている．しかし，技術開発の段階において想定できるのは既知の攻撃手法のみであり，未知の攻撃手法の全てを想定して安全性を検討することは，通常のアプローチでは不可能である．このため，個々の攻撃手法に対して安全性を論じるのでは十分ではなく，包括的に安全性を評価する枠組みが強く求められている．暗号やプロトコル等の基礎的技術に対しては，証明可能安全性，形式的手法を用いた安全性検証，UC(汎用的結合可能）安全性といった用語に代表される取り組みが進められている．その一方，基礎技術の実装を与える情報システムやコンピュータプログラムの安全性を包括的に評価するための技術は確立されておらず，経験的な安全性評価と，想定外の攻撃による脆弱性の発見とが繰り返されているのが研究開始当初の状況であり，本報告書執筆の段階でも，その状況は大きく変わっていない．

その一方，個々の攻撃手法を具体的に想定するのではなく，情報システムが意図的に，あるいは偶発的に発出する情報の総量でもって，攻撃者が入手しうる情報量の上限を測るアプローチが模索されている．たとえば，情報理論的安全性の研究では，情報の持つ統計的な性質や情報量に着目することで，たとえ無限の計算能力を持つ攻撃者であっても，攻撃対象から意味ある情報を引き出せないという立場での安全性を議論する．もう少し具体的な量的情報流解析では，情報システムやプログラムの出力を介して漏洩する入力の情報量（漏洩情報量）を定量的に評価し，未知の攻撃に対する安全性の検証に活用することを考える．すなわち，攻撃者がどのような攻撃手段を取ったとしても，漏洩した量より多くの情報を得ることは情報理論的に不可能であることを利用して安全性の評価につなげる．このアプローチは近年猛威を振るうサイドチャネル攻撃の安全性評価において有用であり，情報システム等に対する包括的な安全性評価の実現に貢献すると期待されている．

実用的な場面において量的情報流解析的なアプローチを取るためには，情報システムで利用されている複雑なプログラム等に対し，漏洩情報の量を具体的に計算できることが必須条件となる．しかしながら，現実の情報システムやコンピュータプログラムは非常に複雑であるため，漏洩情報の量を具体的に計算することはきわめて難しい．また，暗号分野において近年大きな話題となっている量子コンピュータとの関係性が明確でなく，ポスト量子の時代における量的情報流解析や情報理論的安全性評価等，より大きな視点からの取り組みが強く待たれている．

２．研究の目的

本研究の目的は，サイドチャネル攻撃への包括的な安全性評価を可能とするため，今日の時点で実用的な，あるいは，近く実用化されると想定される情報システムにおいて，漏洩情報量を具体的に計算するための手法を開発することである．

先述のとおり，実用的なシステムやプログラムを対象として漏洩情報量を具体的に計算することは，きわめて難しい．研究代表者は，本研究課題開始以前の予備的な検討において，数千ビットの鍵長を持つ RSA 復号プログラムのタイミング攻撃から得られる漏洩情報量の正確な導出に成功しているが，同手法を他のプログラムに適用し，包括的な安全性評価が可能となるプログラムのクラスを拡大することが可能かどうかは明らかでない．また，プロセッサキャッシュへのアクセス時間に着目して計算過程の類推を行うキャッシュ攻撃の危険性が指摘されて久しいが，キャッシュ攻撃には，攻撃者による主体的な操作によりキャシュ情報の漏洩が生じるという側面があるため，情報の統計量だけに着目する静的な解析では，漏洩情報量の評価が困難であると考えられる．これら具体的な課題を解決することが本研究における第１の目的となる．

また，今日の暗号・セキュリティ分野の研究では，急速に実用化の進む量子コンピュータの影響を無視することができない．古典計算機を前提として安全性が確保された暗号技術の危殆化が懸念されており，その代替とすべく，耐量子安全な暗号関連技術が数多く提案されている．これら耐量子安全な技術についてはまだ十分な知見が蓄積されておらず，多方面からの取り組みが待たれているところである．本研究の第２の目的は，耐量子安全な暗号技術の開発やその振る舞いの解析，各種の量子アルゴリズムの計算量評価を通じ，ポスト量子の時代の安全性の包括的評価の礎を築くことである．

３．研究の方法

本課題における取り組みでは，大きく２つの方向性に沿って研究を進めることとした．

第１の方向性では，量子コンピュータの存在はいったん横に置き，いわゆる古典計算機における各種計算に着目して漏洩情報量評価につながる取り組みを行う．具体的には ① 代表的な楕円曲線暗号である楕円 ElGamal 暗号の復号実行時間から漏洩する情報量の精密な評価，② Flush+Reload キャッシュ攻撃における漏洩情報量削減手法の提案，③ 格子ベース暗号や符号ベ

ース暗号，準同型暗号等に応用可能性を持つ多元線形符号の復号アルゴリズムの開発の 3 つの課題に取り組む．

第 2 の方向性では，量子コンピュータおよび耐量子安全な暗号関連技術に焦点を定め，④ ハッシュベース署名において証明可能な最適性を持つ指紋関数開発，⑤ 暗号通貨等で用いられるハッシュパズルの量子計算量の解明の 2 つの課題を設定する．

４．研究成果

4.1 楕円 ElGamal 暗号復号実行時間からの漏洩情報量評価

ElGamal 暗号は離散対数問題を利用して実現される公開鍵暗号の一種であり，実用上は，楕円曲線上で定義される巡回群を用いて構成される楕円曲線 ElGamal 暗号として広く利用されている．通常の巡回群の演算においてべき乗剰余計算の実行時間差がタイミング攻撃の実行を許すのと同様，楕円曲線 ElGamal 暗号では，主として点加算操作の実行時間差が内部情報に関する情報漏洩の原因となる．本研究では，いくつかも自然な仮定の下で実行時間の定式化を行い，構築された実行時間モデルを用い，実行時間を通じて漏洩する情報量を正確に示す数式を導出した．この数式によると，鍵長を 256 ビットとするとき，1 回の復号実行時間から漏出する情報量は約 2.78 ビットであり，鍵長 1024 ビットの RSA 暗号の復号時間から漏出する情報量 6.01 ビットの半分以下であることがわかった．タイミング攻撃への耐性という視点からは，RSA 暗号よりも楕円曲線 ElGamal 暗号のほうが有利であることが明らかとなった．

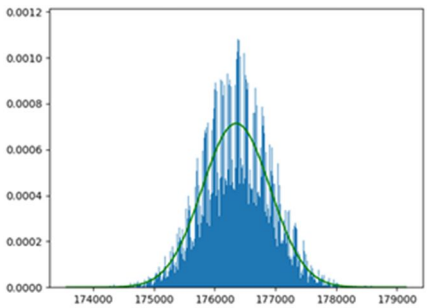

図 1: 楕円 ElGamal 暗号の復号時間分布

4.2 キャッシュ攻撃に対する漏洩情報量削減手法の提案

実用的なプロセッサでは，多段に配置されたキャッシュを利用することで，データアクセス時間の節約を行っている．今日のキャッシュ管理の仕組みは非常に洗練されており，異なるユーザや異なるプロセスがメモリの同一ページを参照する場合であっても，実際に保持されるキャッシュページは 1 枚だけとされることも多い．Flush+Reload 攻撃は，この仕組みを悪用したサイドチャネル攻撃の一種である．Flush+Reload 攻撃では，プログラムコードの動作において鍵となるメモリページをキャッシュから掃き出し，一定時間の経過後に再び同じメモリページにアクセスして，その実行時間の長短から，同ページがキャッシュに格納されているかどうか推測を行う．いちど掃き出したはずのページがキャッシュに格納されているということは，他のプロセスがプログラムコードの該当箇所を実行したことを示唆している．この現象を利用し，プログラム内部で使用されている変数の値を推測することが可能となる．Flush+Reload および関連するキャッシュ攻撃における情報漏洩を抑止するため，プログラムの動作を変えない範囲でプログラムコードの自動改変を行う仕組みを構築し，プロセス間でのキャッシュ共有を禁止する仕組みの構築を行った．自動改変はプログラムのアセンブリコードレベルで実行され，コードのサイズや実際の実行時間に対し，ほとんど影響を与えないことが確認された．現在広く利用されているコンピュータシステムやオペレーティングシステムに手を入れることなく，保護したいプログラムだけを狙って提案手法を適用することが可能となっているため，導入も比較的容易であるとのメリットも生じる．

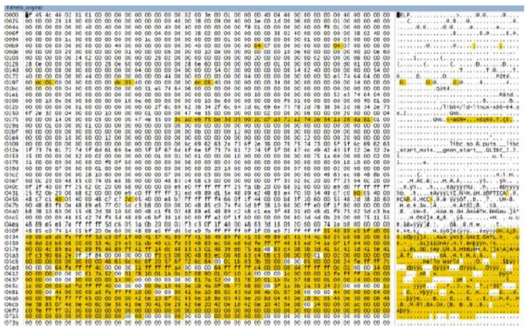
図 2: コード自動改変によるキャッシュ攻撃防止

4.3 多元線形符号の復号アルゴリズムの開発

公開鍵暗号の構成に誤り訂正符号（線形符号）を利用するアプローチは古くから行われており，MacElice 暗号等が広く知られている．符号ベース暗号は耐量子暗号を構成する有力なアプローチであると同時に，線形符号に関する各種のアルゴリズムは，格子ベース暗号や準同型暗号の実現においても重要な役割を果たす．これら，暗号分野における符号の利用においては，デジタル通信等で利用される 2 元符号ではなく，多元の符号に焦点が当てられることが多い．一方，多元符号に対する強力な復号アルゴリズムの研究は十分とはいえず，情報理論的な見地からの取り組みが必要と考えられる．このような状況を改善するため，2 元符号に対する効率的な復号アル

ゴリズムである適応的再帰最尤復号アルゴリズム（aRMLD）をベースに，任意の多元線形符号に適用できるよう拡張を行った．多元 aRMLD では，符号の持つ代数的構造を利用することで冗長な計算の実行を抑制しており，かなり小さな計算量で軟判定最尤復号を実現することができる．本研究期間の終了時点でアルゴリズムの実装まで進めることができており，今後のフォローアップにおいて，暗号学的な用途への適用を実施する予定である．

4.4 ハッシュベース署名向け最適指紋関数の開発

現在広く利用されている公開鍵暗号や電子署名では，離散対数問題や素因数分解等の数論的問題が効率的に解けないことを利用して落とし戸付き一方向性関数が実現されている．一方，これらの問題を効率的に解く量子アルゴリズムが広く知られており，量子コンピュータの実用化が進むと，いま利用されている暗号技術の多くが危殆化し，利用できなくなることが懸念されている．この問題に対処するため，古典計算機だけでなく，量子計算機に対しても耐性を有する暗号関連技術の開発が熱心に進められている．ハッシュベース署名は，量子耐性を持つ電子署名方式の一つであり，米国 NIST による PQC 標準化対象の一つにも選定される等，実用的にも重要な技術である．ハッシュベース署名の中核を構成するのは Winternitz 方式と呼ばれるワンタイム署名方式（WOTS と略す）であり，安全性を損なうことなく WOTS の効率を改善することは，長年にわたり解決されていない問題であった．既存研究では，ハッシュ関数の適用で構成されるグラフ構造を改良することにより効率改善が試みられてきた．これに対し本研究では，WOTS の安全性がチェックサムと呼ばれる補助情報の付加により生み出されていることを示し，安全性を保ったまま効率を改善する指針を示すことに成功した．この指針に基づき「中間和指紋関数」と呼ばれる新しい指紋計算の仕組みを開発し，この関数が効率改善に資することを示した（表１）．また，数学でいう順序論の成果を適用し，中間和指紋関数が最適な指紋関数であること，すなわち，この関数よりも効率を改善する指紋関数が存在しないことを数学的に証明した．一連の成果は理論的に興味深いだけでなく，PQC 標準化を通じ，現実世界の実用的な技術の効率改善にもつながる大きな成果ととらえることができる．

表 1: WOTS および既存方式と提案法の性能比較

w	key/sig size	Winternitz			ZS-OTS			MS-OTS (proposed)		
	wL	l	KeyGen	Sig./Ver.	b	KeyGen	Sig./Ver.	l	KeyGen	Sig./Ver.
67	17,152	16	1,005	502	8	1,072	536	16	1,005	502
55	14,080	32	1,705	852	14	1,540	770	28	1,485	742
45	11,520	64	2,835	1,417	29	2,610	1,305	59	2,610	1,305
39	9,984	128	4,953	2,476	55	4,290	2,145	111	4,290	2,145
34	8,704	256	8,670	4,335	113	7,684	3,842	227	7,684	3,842
31	7,936	512	15,841	7,920	194	12,028	6,014	389	12,028	6,014
28	7,168	1,024	28,644	14,322	376	21,056	10,528	752	21,028	10,514
26	6,656	2,048	53,222	26,611	637	33,124	16,562	1,275	33,124	16,562
24	6,144	4,096	98,280	49,140	1,185	56,880	28,440	2,370	56,856	28,428

4.5 ハッシュパズルの量子計算量の解明

ビットコインをはじめとする暗号通貨では，Proof of Work の仕組みを実現するため，ハッシュパズルの問題が広く利用されている．ハッシュパズルとは，ハッシュ値が一定の条件を満たす原像を発見する問題であり，暗号学的に安全なハッシュ関数が使われる限りにおいて，総当たり的な探索が必要になるとされてきた．ハッシュパズルは原像計算問題の一般化であり，原像計算問題に対しては，古典アルゴリズムよりも効率の良い量子アルゴリズム（グローバーアルゴリズム）が存在することが知られている．グローバーアルゴリズムを一般化することで，ハッシュパズルを解く量子アルゴリズムを構成することも可能であるが，その場合，計算に失敗する確率が無視できなくなってしまう．一般化されたグローバーアルゴリズムの計算失敗を補償するためには，モンテカルロ的な乱択法を繰り返し実行してラスベガス的な乱択法に変換するのと同様，計算に成功するまでグローバーアルゴリズムを繰り返し実行する必要がある．本研究では，グローバーアルゴリズムの計算成功確率をハッシュパズルの正解数により定式化し，ハッシュパズルを解く最適な量子アルゴリズムの計算量について検討を行った．古典的な枠組みでは，ハッシュパズル求解の計算量と正解数との間には負の相関が成り立つ（逆に，不正解の数との間に正の相関が成り立つ）が，量子的な枠組みでは，そのような単純な相関が成り立たないことが明らかになった．すなわち，正解数を減らしてパズルを難しくしたにも関わらず，量子計算機を利用すれば，より効率的に正解を求めることが可能になる場合が存在する．図３は，ハッシュパズルの不正解の数を横軸に，ハッシュパズル求解に必要となる計算量の期待値を縦軸に取って両者の関係を示したグラフである．古典的な枠組み（classic で示すグラフ）の場合，不正解の個数が増えると計算量も単調に増加することが了解できるが，量子的な枠組み（$C(j_{min})$で示すグラフ）においては，計算量が減少する領域（B から C の区間）があったり，グラフに滑らかでない点（点 B）が存在したりするすることがわかる．このことはきわめて興味深い結果であり，ポスト量子

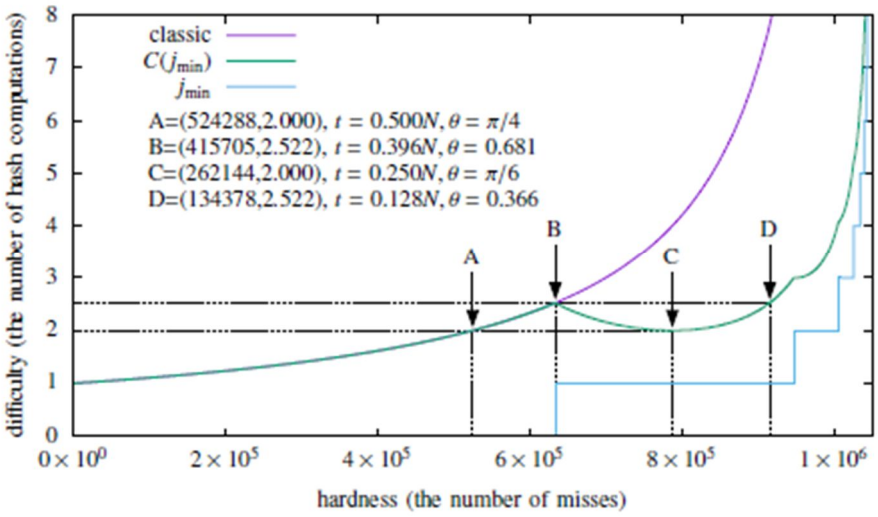

図 3: ハッシュパズル不正解の数と求解計算量の関係

の時代における Proof of Work のあり方，暗号通貨への影響等について，未解決な問題が多く残されていることが示唆される．

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1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 Tomonori Hirata, Yuichi Kaji	４．巻 E106-A
２．論文標題 Information Leakage Through Passive Timing Attacks on RSA Decryption System	５．発行年 2023年
３．雑誌名 IEICE Transactions on Fundamentals	６．最初と最後の頁 406-413
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2022TAP0006	査読の有無 有
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 －

〔学会発表〕　計12件（うち招待講演　0件／うち国際学会　3件）

１．発表者名 Motonari Honda, Yuichi Kaji
２．発表標題 Optimum Fingerprinting Function for Winternitz One-Time Signature
３．学会等名 2024 IEEE International Symposium on Information Theory（国際学会）
４．発表年 2024年

１．発表者名 Honda Motonari、Kaji Yuichi
２．発表標題 Improvement of Winternitz OTS with a Novel Fingerprinting Function
３．学会等名 Proceedings of the 20th International Conference on Security and Cryptography（国際学会）
４．発表年 2023年

１．発表者名 山口夏生，楫勇一
２．発表標題 二次元コードによる安全でオフライン実行可能な暗号鍵共有
３．学会等名 マルチメディア，分散，協調とモバイル(DICOMO2023)シンポジウム
４．発表年 2023年

１．発表者名
本多志成，楫勇一

２．発表標題
Winternitz署名の最適化:Median-sum署名方式

３．学会等名
電子情報通信学会 情報セキュリティ研究会

４．発表年
2023年

１．発表者名
Motonari Honda, Yuichi Kaji

２．発表標題
Optimum Fingerprinting Function for Winternitz One-Time Signature

３．学会等名
第46回情報理論とその応用シンポジウム予稿集

４．発表年
2023年

１．発表者名
山口 夏生，楫 勇一

２．発表標題
可視相互通信を用いた暗号鍵共有による端末間ファイル転送の安全性強化

３．学会等名
情報処理学会 コンピュータセキュリティ研究発表会 予稿集

４．発表年
2023年

１．発表者名
井戸田くりす，楫勇一

２．発表標題
Boyer量子アルゴリズムの再構成とハッシュパズルへの適用

３．学会等名
電子情報通信学会 情報セキュリティ研究会

４．発表年
2024年

１．発表者名
Yuichi Kaji

２．発表標題
Improved Upper-bound of the Entropy of Multinomial Distribution

３．学会等名
IEICE RE:BIT 2022（国際学会）

４．発表年
2022年

１．発表者名
本多志成，楫勇一

２．発表標題
ゼロサム指紋関数の導入によるWinternitz署名の改良

３．学会等名
コンピュータセキュリティシンポジウム 2022

４．発表年
2022年

１．発表者名
島田祐希，楫勇一

２．発表標題
実行ファイル改変によるキャッシュ攻撃への対策手法の検討

３．学会等名
情報処理学会 コンピュータセキュリティ研究発表会

４．発表年
2022年

１．発表者名
Bo Wang, Ako Suzuki, Yuichi Kaji

２．発表標題
Efficient Machine Learning Method for Protocol Fuzzing: Improvement of Sequence-to-Sequence Model and Refined Training Data

３．学会等名
暗号と情報セキュリティシンポジウム 2022

４．発表年
2022年

１．発表者名 Bo Wang, Ako Suzuki, Yuichi Kaji
２．発表標題 Efficient Machine learning Method for Protocol Fuzzing: Improvement of Sequence-to-Sequence Model and Refined Training Data
３．学会等名 情報処理学会 ソフトウェア工学研究発表会
４．発表年 2022年

〔図書〕　計0件

〔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

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関