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 １１ 日現在

機関番号：１３９０１
研究種目：基盤研究(C)（一般）
研究期間：2015～2018
課題番号：１５Ｋ００００１７

研究課題名（和文）漏洩情報の量に基づくセキュリティ解析を可能とする情報量指標の開発

研究課題名（英文）Quantitative Information Measure for Security Analisys of Information Leakage

研究代表者
楫　勇一（KAJI, Yuichi）

名古屋大学・情報連携統括本部・教授

研究者番号：７０２６３４３１

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：情報システムの副次的出力（実行時間等）から漏洩する情報を定量的に測ることは，サイドチャネル攻撃等のリスク評価の精密化に不可欠である．この問題に対処するため，本研究では２つの課題に取り組んだ．最初の課題は，サイドチャネル攻撃のモデルにおいて頻出する多項分布のエントロピーを精密に評価する限界式を導出することであり，非漸近的なパラメータについても有効で漸近的に収束する限界式の導出に成功した．２つ目の課題は，実用的なプログラムから漏洩する情報量の具体的計算手段の確率であり，RSA復号アルゴリズムを対象に，情報量計算のベースとなる公式を導出した．また，関連する周辺分野についても多くの知見を得た．

研究成果の学術的意義や社会的意義
悪意を持った攻撃者は，プログラムの実行時間等，誰もが観測できる情報を手がかりに，システム内部に隠された秘密情報を推測しようと試みる可能性がある．本研究では，そのような「意図せずシステムから漏洩する情報」の量を数値として測るための技術について検討を行った．最初の大きな研究成果は，既存研究で知られていなかった数学的な公式を導出したことである．これにより，漏洩情報量を正確に見積もることが可能となった．二つ目の大きな成果は，実用的なプログラムの具体的な分析手法を開発したことである．これにより，漏洩情報量の量的評価に関する研究が，より一層実用的なものとなった．

研究成果の概要（英文）：The focus of this study is the quantitative measuring of information leakage through side-information of security systems. Two concrete problems are tackled, and contributions are made for both problems. In the first problem, the study derived converging bound formulas for the entropy of multinomial distributions that are common and essential in various side-channel attacks. In the second problem, well-defined formulas are derived that are to determine the information leakage through practical RSA decryption algorithms. Additional results are also obtained for related research subjects.

研究分野：情報セキュリティ

キーワード：情報セキュリティ　情報理論的安全性　量的情報流評価　情報理論　エントロピー　RSA暗号　サイドチャネル攻撃　タイミング攻撃

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

情報システムのセキュリティを議論する際に問題となるのは，攻撃者の能力や攻撃手法について，事前には予測できないという点である．既知の攻撃手法に対して万全の対策を取っても，想定外の新しい攻撃に対する安全性までは保証できない．いわゆる情報理論的安全性の議論が適用できれば，未知の攻撃に対する安全性まで保証することができるが，複雑な情報システムを適切にモデル化し，証明を与えることは容易ではない．

この問題に対する一つのアプローチとして，量的情報流解析の研究が注目されている．量的情報流解析では，プログラム実行等の「計算」から漏洩する情報の量を，隠された入力（たとえば，プログラム中に埋め込まれた秘密の暗号鍵）Xと観測可能な出力（明示的な出力だけでなく，実行時間や消費電力等の副次的な出力も含まれる）Yの間の相互情報量$I(X;Y)$により測定する．たとえ無限の計算能力を持つ攻撃者が出現しても，$I(X;Y)$ビット以上の情報をYから引き出すことはできないため，未知の攻撃者に対する安全性を議論することが可能となる．$I(X;Y)=0$のときが情報理論的に安全なケースに相当し，その意味で，量的情報流解析は，情報理論的安全性の議論を定量的に一般化する試みであると考えることもできる．実行時間等，計算の副次的な出力をYと考えればサイドチャネル攻撃の脅威分析にも応用可能であり，実用上の効果も大きい．

量的情報流解析の概念は非常にシンプルであるが，実際に漏洩情報量の計算を行うことには大きな困難が伴う．この困難さは，主として２つの要因によりもたらされている．最初の要因は，実用的な場面で頻出する多項分布に対し，効率よくエントロピーを計算するための手段が確立されていないことである．いわゆる計算公式が存在しないため，エントロピーを求めるためには非現実的な規模の数値計算を実行する必要がある．漏洩情報量の計算を困難にする２番目の要因は，実用的なプログラムの入出力間の条件付きエントロピーの導出が非常に煩雑であり，難しいという点である．プログラムの内部では，計算過程で複雑に変化する変数値に基づき，条件分岐や繰り返し処理が行われる．プログラム入出力間の統計的な関係を導き出すことは解析的にも実験的にも困難であるため，既存研究では条件付きエントロピーを無視し，非常にルーズな限界式の議論に留まっていたのが実情である．

２．研究の目的

本研究の主たる目的は，概念的なレベルに留まっていた量的情報流解析のアプローチにおいて，漏洩情報の量を実際に計算するための効率的で具体的な手段を確立することにある．この目的を達成するため，２つの目標を定める．

① 多項分布に従う確率変数のエントロピーについて，近似式または限界式を導出する．

サイドチャネル攻撃の攻撃者は，攻撃対象となる情報システムの動作を複数回観測し，観測された結果からシステム内部の秘密情報を類推する．各試行における情報システムの動作が独立であり，システムの出力結果が各試行で同一の分布に従う場合，出力結果の順序に意味はなく，相対頻度のみが実質的な意味を持つ．すなわち，攻撃者は多項分布に従う確率変数の実現値を１つだけ得て，この値から秘密情報を推測することになる．実用的なシナリオでは，攻撃者の試行回数は数百回から数千回程度となることが予想され，この場合，確率変数の値域は天文学的なサイズとなる．すべての実現値に対して網羅的に確率を計算し，数値計算によりエントロピーを求めることは現実的でないため，数学的，解析的な手段により，エントロピーの値を見積もる手段を確立する．

② 実用的なプログラムについて，入出力間の条件付きエントロピーを定式化する．

RSA 復号アルゴリズムに対して動的な（すなわち，復号アルゴリズムに入力する暗号文を攻撃者が自由に選択できる前提で）タイミング攻撃を行えば，比較的小さな計算量で秘密の復号鍵を特定できることが知られている．そのような結果を受け対策が進められた結果，動的タイミング攻撃の実行は困難になりつつあり，静的な（すなわち，復号アルゴリズムへの入力暗号文が攻撃者から秘匿された状態での）タイミング攻撃のリスク評価が重要となりつつある．静的タイミング攻撃は情報理論的に取り扱いやすい枠組であるが，プログラム入出力間のエントロピーを求めるためには，秘密鍵と実行時間の相互関係を明確にする必要がある．条件分岐や繰り返し処理の影響を考慮に入れて RSA 復号アルゴリズムの動作を分析し，同アルゴリズムの入出力間の統計的な関係を記述する数学的モデルを構築する．

また，上記の２つの目標を追求する過程で得られる各種知見についても精力的に検討・拡張を行い，本研究周辺分野の開拓にも積極的に取り組む．

３．研究の方法

課題①については数学的な解析が主となる．多項分布の特別な場合である二項分布に対しては，Jacquet らにより，漸近的な場合にのみ有効なエントロピーの近似式が提案されている．また，Jacquet とは全く異なるアプローチを採用することにより，多項分布のエントロピーの漸近的な近似式が Cichon らにより提案されている．これらの結果は興味深いものであるが，真値と近似値の関係が不明であること，非漸近的な領域では明らかな異常値が得られること等の問題が存在している．量的情報流解析の議論では，数百から数千といった非漸近的なパラメータ値が重要となり，また，真値との関係が不明な近似値ではなく，漏洩情報量の上界を与えるような限界式が強く求められる．そこで本研究では，エントロピーの定義式の多項式上界・多項式下界を導出し，二項分布に従う確率変数の単項式の期待値の代数和により，求めるエントロピーの上界および下界を与えることを検討する．

課題②について，ターゲットとなるプログラム，具体的には，RSA 復号アルゴリズムの実装をいくつか考え，アルゴリズム内に秘匿される復号鍵と，プログラムの実行時間の関係を明らかにする．一般に，RSA 復号計算の実行時間は，復号鍵だけでなく，復号対象となる暗号文の値によっても変化する．復号過程の計算において暗号文に操作が加えられ，操作の結果得られた値により，異なった分岐処理・繰り返し処理が実行される．最初に与えられる暗号文が一様に分布すると仮定しても，復号過程で得られる中間的な結果の確率分布は一様になるとは限らず，プログラムの振る舞いを確率的・統計的に記述することは非常に困難である．この問題に対処するため，プログラム中の変数値を厳密に追跡するのではなく，変数値が単純な統計モデルに従うという仮定を置くことで，プログラムの動作を説明する簡潔なモデルを構成する．

また，課題①，②に関する取り組みと並行し，シャノンエントロピー以外の情報量尺度の検討，耐量子安全性・量子情報理論とセキュリティ技術，ブロックチェーン技術と情報理論といった視点から積極的に情報収集を行い，周辺分野の開拓を心がける．

４．研究成果

４．１．多項分布のエントロピーの限界式の導出

m,nを非負整数とし，$\mathcal{T}_{m,n}=\{(t_1,\dots,t_m): t_1+\cdots+t_m=n, t_i\in\{0,\dots,n\}\}$と定義する．また，$p_1,\dots,p_m$を，$p_1+\cdots+p_m=1$となる非負実数値とする．$\mathcal{T}_{m,n}$を標本空間とする確率変数$T_{m,n}$の確率分布が

$$P_{T_{m,n}}\big((t_1,\dots,t_m)\big)=\frac{n!}{t_1!\dots t_m!}p_1^{t_1}\dots p_m^{t_m}$$

であるとき，$T_{m,n}$は次数$m-1$の多項分布に従うという．$T_{m,n}$のエントロピーは

$$H\big(T_{m,n}\big)=-\sum_{(t_1,\dots,t_m)\in T_{m,n}} P_{T_{m,n}}\big((t_1,\dots,t_m)\big)\ln P_{T_{m,n}}\big((t_1,\dots,t_m)\big)$$

として定義されるが，$T_{m,n}$はパラメータm,nに対して指数的な個数の要素を含むため，m,nが非常に小さい場合を除いて，この定義式に従いエントロピーを計算することは現実的でない．一方，エントロピーの定義式において対数の真数部分を展開し，式を整理すると

$$H\big(T_{m,n}\big)=-\ln n!-n\sum_{i=1}^{m}p_i\ln p_i+\sum_{i=1}^{m}\sum_{j=2}^{n}\pi_{n,j}^{[p_i]}\ln j! \qquad (1)$$

となる．ここで

$$\pi_{n,j}^{[p_i]}=n!/(j!\,(n-j)!)p^j(1-p)^{n-j}$$

は二項確率である．式(1)の第３項について検討を進めるため，関数$f(\mathrm{x})$に対し

$$E_s^{n,p}[f(X)]=\sum_{j=s}^{n}\pi_{n,j}^{[p_i]}f(j)$$

と定義する．式(1)の第３項は$E_2^{n,p}[\ln X!]$として書くことができる．$s=0$のとき，$E_0^{n,p}[f(X)]$は確率変数Xが二項分布に従うときの$f(X)$の期待値であり，$s>0$の場合，$E_s^{n,p}[f(X)]$は$E_0^{n,p}[f(X)]$から$\pi_{n,o}^{[p]}f(0)+\cdots+\pi_{n,s-1}^{[p]}f(s-1)$ を引き去ることで得ることができる．詳細な説明は省略するが，$f(x)$が多項式であれば$E_2^{n,p}[f(X)]$を閉じた式として正確に書き下すことができる．しかし，多項式でない$\ln x!$については，簡潔な式により$E_2^{n,p}[\ln X!]$を表現することができない．式(1)のエントロピーの限界式を与えるためには，$E_2^{n,p}[\ln X!]$に対する精度の良い限界式が必要となる．

この問題に対処するため，$\ln x!$の上界，下界を与える多項式限界を導出し，その限界式に対して$E_2^{n,p}[\cdot]$を計算することで$E_2^{n,p}[\ln X!]$の上界および下界を導き出す．はじめに，Stirling の公式により与えられる$\ln x!$の上界および下界を考える．

$$\left(x+\frac{1}{2}\right)\ln x - x + \frac{1}{2}\ln 2\pi \le \ln x! \le \frac{1}{12x} + \left(x+\frac{1}{2}\right)\ln x - x + \frac{1}{2}\ln 2\pi.$$

この上界式，下界式の中には単項式となっていない項$\ln x$と$1/\mathrm{x}$が存在するため，このままでは$E_2^{n,p}[\cdot]$の計算を行うことができない．単項式を除去するため，$\ln x$および$1/\mathrm{x}$の Taylor 級数展開を考え，場合によっては微修正を加えることで多項式限界を導出する．最終的に得られる限界式は非常に複雑であるため，本報告書には記載しないが，上記のアプローチで計算を進めた結果$E_2^{n,p}[\ln X!]$の上界および下界を導き出すことができ，その上界，下界を用いることで，エントロピー$H(T_{m,n})$の上界，下界を導出することができた．得られた上界と下界は漸近的に収束することが確認でき，これにより，多項分布のエントロピーの精細な上界式，下界式を得ることが出来た．

４．２．RSA 復号アルゴリズムの入出力関係モデル化

公開鍵暗号の復号操作では，秘密の復号鍵を用いた計算が行われる．安直な実装では，復号計算の実行時間が復号鍵に依存して変化するため，復号に要する実行時間を注意深く観測すれば，秘密の復号鍵に関する情報を入手できる場合がある．とくに，復号装置に入力する暗号文を攻撃者が制御可能な場合（いわゆる動的タイミング攻撃が可能な場合），比較的小さな計算量で復号鍵の特定が可能となる．これに対処するため，復号装置への入力に先立って暗号文をブラインド化し，復号計算の後にブラインド化を解除する方法が検討されている．この場合，攻撃者は，復号装置に実際に入力される値を制御したり知ったりすることができず，未知の復号鍵と未知の暗号文に対して動作する復号装置の振る舞いのみから，秘密の復号鍵を推測することになる．この種の静的タイミング攻撃の危険性については十分議論されているとは言えず，その理解について，さらなる取組が待たれるところである．

本研究では，RSA 暗号の典型的な復号アルゴリズムであるバイナリ法，モンゴメリ法の２つの復号アルゴリズムを対象として選び，鍵の選択が復号操作の実行時間に及ぼす影響について統計的に分析する．具体的には，鍵と実行時間との間の条件付き確率を導出し，その条件付き確率を用いて，鍵と実行時間の間の相互情報量を定式化する．本報告書では，簡単のため，比較的シンプルなバイナリ法に対する取り組みの概要を説明する．

RSA 暗号の復号計算を実行するバイナリ法は，以下のような擬似コードで記述される．

入力：暗号文c，復号鍵dおよびn．ただしdの 2 進数表記を$(d_{t-1},\dots,d_0)$とし，$d_{t-1}=1$とする
出力：$m = c^d \bmod n$を満たす平文m
1. $m = c$
2. **for** $i = t-2$ to 0 **do**
3. 　　$m = m^2 \bmod n$
4. 　　**if** $d_i = 1$ **then**
5. 　　　　$m = mc \bmod n$
6. 　　**end if**
7. **end for**
8. **return** m

鍵，平文，暗号文等がlビットで表現される場合，m^2やmcのような乗算には$O(l^2)$の計算量が必要となる．また，$x \bmod n$の形の剰余計算について，$x < n$であればとくに計算は必要ないが，$x \ge n$の場合は剰余還元（除算を行い剰余を求める計算）のため$O(l^2)$の計算量が必要となる．乗算と剰余還元以外の処理は定数時間で実行されるため，バイナリ法の実行時間は，概ね乗算と剰余還元の実行回数に依存して定まる．

擬似コードから明らかなとおり，3 行目の乗算は必ず$t-1$回実行される．また，5 行目の乗算は$d_i = 1$のときのみ実行されるため，鍵のハミング重みをwとすると，乗算実行回数の合計は$(t-1)+(w-1)$回となる（最上位の非ゼロビットであるd_{t-1}に対しては 5 行目の計算が不要であるため，5 行目の乗算実行回数は$w-1$回である点に注意）．

一方，剰余還元の回数は，擬似コードの構文から単純に決定することができない．剰余「計算」の回数であれば，上述の乗算回数の分析と同様に導き出すことができるが，剰余「演算」が発生するのは$x \bmod n$において$x \ge n$の場合のみであるため，厳密な議論を行うためには，計算過程におけるm^2やmcの値を分析する必要がある．一般的な整数環$\mathbf{Z}$では，計算過程におけるm^2やmcの系列は平方数の数列や等比数列により特徴づけられるが，剰余類環$\mathbf{Z}/n\mathbf{Z}$においては，これら数列を簡潔に特徴づけることはできない．この問題を回避するため，本研究ではまず 3 行目の剰余計算に着目し，「mが$\mathbf{Z}/n\mathbf{Z}$において一様に分布するならば，$m^2 \bmod n$も$\mathbf{Z}/n\mathbf{Z}$において一様に分布する」と仮定する．この場合，$m^2 \ge n$となる確率は$1-\sqrt{n}/n = 1-1/\sqrt{n}$により与えられるため，実用的な$n$の値（2 進数で数千ビット）に対しては，この確率はほぼ 1

であると考えられる．すなわち，3 行目の剰余計算では，ほぼ確実に剰余還元が実行されることになる．5 行目の剰余計算についても同様の議論を行うことができるが，$mc \geq n$となる確率はcの値にも依存するため，若干複雑な議論が必要となる．たとえば，$c = 0$の場合，$mc \geq n$となる確率は 0 であり，5 行目で実行される剰余還元の回数の期待値も 0 である．一方，$c > 0$の場合$mc \geq n$の確率は$1/c$であり，5 行目で実行される剰余還元の回数の期待値は$1 - (w-1)/c$により与えられる．全てのcが一様に与えられると仮定すると，これら「剰余還元回数の期待値」の期待値は$w - 1$に漸近する．すなわち，5 行目の剰余計算においても，ほぼ確実に剰余還元が実行されることになる．以上の議論より，バイナリ法で実行される剰余還元の回数は，$(t-1) + (w-1)$により近似することができる．この近似値は数値実験の結果とよく一致しており，この結果を用いて後続の議論を続行することも妥当であると言える．

以上の議論より，バイナリ法の実行時間は，鍵の実行ビット長tおよびハミング重みwから（ほぼ）一意に定まることが明らかになった．すなわち，実行時間を確率変数Z，鍵の実行ビット長とハミング重みを確率変数T, Wで表す場合，

$$P_{Z|T,W}(z|t,w) = \begin{cases} 1 & (t = c_m\big((t-1)+(w-1)\big) + c_r\big((t-1)+(w-1)\big)\text{のとき}) \\ 0 & \text{（上記以外のとき）} \end{cases}$$

であり，これから$H(Z|T,W) = 0$が得られ，$I(Z;T,W) = H(Z) - H(Z|T,W) = H(Z)$も導かれる．また，情報理論におけるデータ処理補題の特殊な場合から$I(Z;K) = I(Z;T,W)$を示すことができ，したがって，バイナリ法の実行時間を通じて漏洩する復号鍵の情報量は$I(Z;K) = H(Z)$となることがわかる．$H(Z)$の計算には実行時間Zの確率分布P_Zが必要になるが，これは確率分布$P_{Z|T,W}$を周辺化することで得ることができる．これらの結果をまとめることにより，$I(Z;K)$を数式により書き下すことが可能となった．

４．３．周辺分野への貢献

本研究では，主たる課題の周辺分野についても多大な知見を得ることができた．とくに，安全で効率の良いハッシュベース署名の構成法に関する一連の結果は，証明可能な安全性を備え，耐量子安全性も有する軽量な署名方式となっており，理論的にも実用的にも興味深いものとなっている．また，ブロックチェーン技術を様々な応用に適用する研究についても先駆的な結果が得られており，今後，それぞれ独立した研究課題としての発展が期待される．

５．主な発表論文等

〔雑誌論文〕（計 6 件）

[1]. J.P. Cruz, Y. Kaji, N. Yanai, RBAC-SC: Role-Based Access Control Using Smart Contract, IEEE Access, 6, pp.12240-12251, 2018.（査読あり）

[2]. J.P. Cruz, Y. Kaji, E-voting System Based on the Bitcoin Protocl and Blind Signatures, 情報処理学会（トランザクション）数理モデル化と応用，10, pp.14-22, 2017.（査読あり）

[3]. J.P. Cruz, Y. Kaji, The Bitcoin Network as Platform for Trans-Organizational Attribute Authentication, 情報処理学会（トランザクション）数理モデル化と応用，9, pp.41-48, 2016.（査読あり）

[4]. Y. Takeda, Y. Kaji, M. Ito, On the Computational Complexity of the Linear Solvability of Information Flow Problem with Hierarchy Constraint, IEICE Transactions on Fundamentals of Electronics, Communication and Computer Sciences, E99-A, pp.2211-2217, 2016.（査読あり）

[5]. Y. Kaji, Performance Evaluation of Index-Less Indexed Flash Codes for Non-Uniform Write Operations, 情報処理学会（トランザクション）数理モデル化と応用，8, pp.1-6, 2015.（査読あり）

[6]. 熊谷，楫，動的なセグメントを用いたフラッシュ符号の構成，電子情報通信学会論文誌 A, 8, pp.398-401, 2015.（査読あり）

〔学会発表〕（計 13 件）

[1]. T. Hirata, Y. Kaji, The Amount of Information Leakage of Decryption Keys Through Timing Attacks on RSA Decryption System, 電子情報通信学会情報セキュリティ研究会，2019.（査読なし）

[2]. 柏倉，楫，署名鍵のパンクチャによる Winternitz OTS の改良，電子情報通信学会情報セキュリティ研究会，2018.（査読なし）

[3]. Y. Kaji, J.P. Cruz, Y. Yatani, Hash-Based Signature with Constant-Sum Fingerprinting and Partial Construction of Hash Chains, 15th International Conference on Security and Cryptography, Porto, Portugal, pp.297—304, 2018.（査読あり）

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

[4]. J.P. Cruz, Y. Yatani, Y. Kaji, Constant-Sum Fingerprinting for Winternitz One-Time Signature, 2016 International Symposium on Information Theory and Its Applications, Monterey, CA, 2016.（査読あり）
[5]. Y. Yatani, J.P. Cruz, Y. Kaji, Improvement of Winternitz One Time Signature, 2016 International Symposium on Information Theory and Its Applications, poster session, Monterey, CA, 2016.（査読あり）
[6]. Y. Kaji, Converging Bounds of the Entropy of Multinomial Distributions, 2016 International Symposium on Information Theory and Its Applications, Monterey, CA, 2016.（査読あり）
[7]. 弥谷，クルーズ，揖，改良型 Winternitz One Time 署名の提案と安全性評価，電子情報通信学会情報セキュリティ研究会，2016.（査読なし）
[8]. J.P. Cruz, Y. Kaji, E-voting System Based on the Bitcoin Protocl and Blind Signatures, 2016 暗号と情報セキュリティシンポジウム，2016.（査読なし）
[9]. Y. Takeda, Y. Kaji, M. Ito, On the Computational Complexity of the Solvability of Information Flow Problem with Hierarchy Constraint, 53rd Annual Allerton Conference on Communication, Control and Computing, Monticello, IL, 2015.（査読あり）
[10]. J.P. Cruz, Y. Kaji, The Bitcoin Network as Platform for Trans-Organizational Attribute Authentication, The Third International Conference on Building and Exploring Web Based Environment, Rome, Italy, 2015.（査読あり）
[11]. Y. Kaji, Bound on the Entropy of Multinomial Distribution, 2015 IEEE International Symposium on Information Theory, Hong Kong, China, 2015.（査読あり）
[12]. Y. Kaji, Converging Bounds of the Entropy of Multinomial Distributions, 第 38 回情報理論とその応用シンポジウム，2015.（査読なし）
[13]. 武田，揖，伊東，階層制約のある情報フロー問題に関する計算理論的考察，電子情報通信学会情報理論研究会，2015.（査読なし）

６．研究組織

(1)研究分担者
なし

(2)研究協力者
なし

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。