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　４ 年　 ６ 月 １４ 日現在

機関番号：１３９０１
研究種目：基盤研究(C)（一般）
研究期間：2018～2021
課題番号：１８Ｋ１１１６２

研究課題名（和文）ハッシュベース電子署名方式の開発および性能限界の解明

研究課題名（英文）Comprehensive Study of Hash-Based Digital Signature

研究代表者
楫　勇一（KAJI, Yuichi）

名古屋大学・情報連携推進本部・教授

研究者番号：７０２６３４３１

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：耐量子安全性が期待されるハッシュベース署名方式について，各種方式のベースとなるWinternitzワンタイム署名の安全性要件を詳細に検討した上で，主要な性能指標のすべてにおいてWinternitz方式よりも優れた効率を有する改良方式を開発した．改良方式においては，定数和指紋関数，ゼロサム指紋関数と呼ばれる新しい指紋関数を導入し，署名情報が流用されることを防止している．Winternitz方式のチェックサムを効率よく代替できるようになっており，強存在的偽造不可能性を維持したまま，効率の改善が可能となった．

研究成果の学術的意義や社会的意義
ハッシュベース暗号は，耐量子安全性を実現する有望な基礎技術であるが，その効率の悪さがしばしば指摘されてきた．本研究では，代表的なハッシュベース暗号として広く使用されているWinternitz方式の効率改善に成功しており，耐量子安全な技術の実用化に大きく貢献することが期待される．また，本研究においては，ハッシュベース署名で使用する指紋関数の値域が備えるべき条件について詳細に検討を行っており，比較不能部分集合の概念を明確に定義している．比較不能部分集合は，情報理論・符号理論的な見地からも興味深い対象であり，関連研究の発展への動機づけを与える可能性がある．

研究成果の概要（英文）：Hash-based signatures are expected to have post-quantum security, and improving their efficiency has been a focal point in recent years. This study improves widely recognized Winternitz one-time signature (OTS) and proposes novel schemes that are more efficient than Winternitz OTS while preserving the provable security notion of the strongly existential unforgeability. A crucial point is an introduction of constant-sum and zero-sum fingerprinting functions that involve the check-sum mechanism of Winternitz OTS and contribute to prevent one valid signature to be used maliciously to forge another signatures that pass the signature verification.

研究分野：情報セキュリティ

キーワード：ハッシュベース署名　耐量子安全性　Winternitzワンタイム署名　強存在的偽造不可能生　指紋関数　比較不能部分集合

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

電子署名は，今日の情報化社会の安全性確保に必要不可欠な技術である．現在広く使用されている電子署名の多くは，離散対数問題や素因数分解問題等，数論的な問題を効率的に解く方法が知られていないことに安全性の根拠を依拠している．その一方，現在のコンピュータとは全く異なる原理に基づいて計算を実行する量子計算機の研究が以前より行われており，量子計算機を使えば（正確には，量子計算機向けのアルゴリズムである Shor のアルゴリズム[17]を使えば），公開鍵暗号や電子署名等で利用されている数論的な問題も効率よく解けることが既に知られている[1]. 実用的な量子計算機が出現するまでには非常に長い年月がかかると予想されていたが，近年急速に量子計算機の実用化研究が進みつつあり，数論的な問題に依拠する暗号技術の安全性に大きな懸念が示されている．それほど遠くない将来に，現在広く利用されている暗号技術が利用できなくなる（安全でなくなる）可能性も否定できないため，量子計算機に対しても耐性を持つ暗号技術，すなわち，耐量子安全性を有する暗号技術の開発が急がれている．

耐量子安全性を追求するにあたっては，いくつかの異なるアプローチが検討されている．現在最も有力なのは，組合せ論的な問題の難しさに依拠してトラップドア付き一方向計算を実現するアプローチであり，格子ベース暗号や符号ベース暗号等が本範疇に分類される．また，これとは異なるアプローチとして，対称鍵暗号や暗号学的ハッシュ関数等，ランダム関数のように振る舞う操作を活用する研究も多く行われており，本研究で取り組むハッシュベース署名も，このアプローチからの技術として分類される．ランダム関数の逆像計算は Shor のアルゴリズムで解くことができず，Grover 法として知られる別の量子アルゴリズムを利用する必要があるが，Grover 法を利用しても逆像計算の計算量は$O(2^{n/2})$までしか削減されず，古典計算機と同様，指数オーダーの計算量が必要となる. このことから, ランダム関数を利用した暗号学的な仕組みは，量子計算機に対しても一定の安全性を有すると考えられている．

ハッシュベース署名の歴史は古く，1980 年代にまで遡ることができる[13]．その当時は耐量子安全の概念もなく，ハッシュベース署名は，数論ベース技術において必要となる数千ビットの大規模計算を回避するための手段として検討が行われてきた．比較的小さな計算量で各種の操作が実現できる点が評価され，1990 年代から 2000 年代にかけては，無線センサネットワークや各種の組込機器，M2M システム等で使用される小型省電力装置での利用に関する研究が盛んに行われた．ハッシュベース署名においては，その原理上，特定のルールに従って秘密情報の一部を開示することにより電子署名を構成するため，署名作成鍵・署名検証鍵の組は 1 度しか利用することができず，いわゆるワンタイム署名（One-Time Signature, OTS）しか実現することができない．ただし，Merkle 木[14]に代表されるよう，複数の鍵組を効率よく管理する方法が早くから知られているため，OTS であることが実用上の支障となることは少なく，SPHINCS[2]や XMSS[8]といった実用的な署名方式の内部においてもハッシュベース OTS が利用されている．とくに，ハッシュベース署名の研究初期に提案された Winternitz OTS 署名はシンプルで効率が良いため，SPHINCE, XMSS を含め，その後に出現した多くの改良方式，発展方式のベースとして利用されている[10,12].

２．研究の目的

本研究の目的は，Winternitz OTS の安全性や使い勝手の良さを維持したままで，より効率の良いハッシュベース署名を実現することである．Winternitz OTS より優れたハッシュベース署名を目指し，いくつかの研究が行われている．たとえば Bleichenbacher らは，Winternitz OTS で使用されている単純なハッシュ連鎖ではなく，木や DAG（directed acyclic graph）といった複雑なグラフ構造をハッシュ計算により定義し，同グラフ上で署名機能を実現することを検討している[3,4]．ハッシュグラフを構成する以外のアプローチでは， bins and balls 問題とハッシュ関数を組み合わせた BiBa[15]，BiBa[16]の拡張となる HORS 等が提案されている．いずれの方式も，一部の性能指標においては Winternitz OTS より優れているものの，それ以外の性能指標が犠牲となっており，すべての側面において Winternitz OTS を真に改良する方式は知られていない．本研究では，鍵サイズ，署名サイズ，鍵生成の計算量，署名作成の計算量，署名検証の計算量のすべての性能指標において，Winternitz OTS と同等以上の性能を有するハッシュベース署名方式を実現する．

３．研究の方法

Winternitz OTS のシンプルな構成は，各種計算量の削減や安全性証明の構成において有利であるため, 本研究においても, 複数のハッシュ連鎖を利用する Winternitz OTS 方式を踏襲する．このアプローチでは, 長さlのハッシュ連鎖をw本準備し，その連鎖中のハッシュ値を鍵および署名として利用する（lおよびwの選択は，方式の安全性と効率に直結するが，本稿では説明を割愛する）．研究の方法について述べるため，はじめに，Winternitz OTS の概要について紹介する．

Winternitz OTS では，任意長のメッセージを固定長の指紋に変換する指紋関数fと，暗号学的なハッシュ関数hを使用する．以下では説明を簡潔にするため，f, hのいずれも 160 ビット長であると仮定する．この仮定の下で$l^{w_1} \geq 2^{160}$となるよう整数パラメータw_1, lを定め，また，$2^{w_2} \geq w_1(k-1)$となるよう整数パラメータw_2を定めたうえで，$w = w_1 + w_2$とする．署名作成鍵は，ハ

ッシュ関数hの値域からランダムに選択されたw個の値$k_s=(s_1,\dots,s_w)$であり，署名検証鍵は，k_sの各要素にhを$l-1$回作用させて得られるw個のハッシュ値$k_v=(v_1,\dots,v_w), v_i=h^{l-1}(s_i)$である．メッセージ$m$に対する署名を計算するには，はじめに$f(m)$を計算して$m$の指紋値を求め，その指紋値を$w_1$桁の$l$進数$(f_1,\dots,f_{w_1})$に変換する．さらに，$C=w_1(l-1)-\sum f_i$として指紋のチェックサム$C$を計算し，これを$w_2$桁の$l$進数$(f'_1,\dots,f'_{w_2})$に変換したうえで，$f=(f_1,\dots,f_w)=(f_1,\dots,f_{w_1},f'_1,\dots,f'_{w_2})$としてチェックサム付き$l$進指紋を計算する．メッセージ$m$に対する署名は，$\sigma=(\sigma_1,..,\sigma_w), \sigma_i=h^{f_i}(s_i)$として求められる．署名検証は$m$と$\sigma$を受け取り，署名作成時と同じ計算により，チェックサム付きl進指紋$f=(f_1,\dots,f_w)$を計算する．この値を用い，すべての$1\le i\le w$において$v_i=h^{l-1-f_i}(\sigma_i)$が成立すれば署名は正しいものとし，一つでも不一致があれば署名は不正であるとする．

各種操作を実現するのに必要となるハッシュ関数hの実行回数を計算コストと呼び，計算コストにより，各種操作の計算複雑さを測ることとする．Winternitz OTS では，1 本のハッシュ連鎖を計算するのに$l-1$回のハッシュ関数hの計算が必要となるため，鍵生成コストは$w(l-1)$となる．署名作成および署名検証のコストは指紋値により変動するが，いずれも$w(l-1)$以下となり，署名作成コストと署名検証コストの和は必ず$w(l-1)$と一致する．指紋関数fが衝突困難性を有し，ハッシュ関数hが衝突困難性と一方向性を有するとき，Winternitz OTS は強存在的偽造不可能[6,11]であることが知られている[7]．

Winternitz OTS における重要なポイントは，異なるチェックサム付きl進指紋が必ず比較不能となっている点である．w桁のl進数$f=(f_1,\dots,f_w), f'=(f'_1,\dots,f'_w)$に対し，すべての$1\le i\le w$において$f_i\le f'_i$となるとき，$f\le f'$と書くことにする．もし$f<f'$であるならば，$f$に対応する署名の各要素にハッシュ関数$h$を適当な回数だけ作用させることで，$f'$に対応する署名を計算することができてしまう．Winternitz OTS では，最初のw_1桁とは逆進的に作用するw_2桁のチェックサムが存在するため，2 つの異なるチェックサム付きl進指紋f,f'に対し，$f<f'$となることも$f<f'$となることもなく，一つの正答な署名を手がかりとして他の署名が偽造されることを防止している．逆にいうと，任意の異なる$f,f'\in FS$に対し$f<f'$となるよう指紋空間$FS=\{(f_1,\dots,f_w): 0\le f_i<l, 1\le i\le w\}$が構成されていれば，最終的には安全なハッシュベース署名を構成することが可能となる．本研究では，与えられたパラメータ l,wに対し，指紋空間FSができるだけ大きくなるような指紋関数の構成方法を検討することで，Winternitz OTS の改良を模索する．

４．研究成果

Winternitz OTS の改良となる 2 つの方式を開発した．最初の方式は，定数和指紋関数の導入とハッシュ連鎖の部分構成により実現される方式であり，パラメータを適切に選択すれば，すべての性能指標において Winternitz OTS と同等以上の性能を確保することが可能である．ただし，この方式では，ハッシュ連鎖のうち構成されていない部分が参照されるのを避けるため，定数和指紋回数を複数回にわたって計算する必要が生じる可能性がある．そのような隠れコストの存在を考慮すると，あらゆる面において Winternitz OTS より優れているとは言い難い部分があるため，定数和指紋関数を改良することで新たにゼロサム指紋関数を定義し，ハッシュ連鎖の部分構成を必要としない第 2 の方式を開発した．

4.1 第 1 の方式[9]

この方式では，Winternitz OTS と同様，長さlのハッシュ連鎖をw本準備して使用する．ただし，w,lを選択するための制約条件は Winternitz OTS とは異なり，また，長さlのハッシュ連鎖については，その一部のみ（たとえば，連鎖の後半 1/2 の部分のみ）を構成すれば良い．説明を簡潔にするため，はじめに長さlのハッシュ連鎖の全体を構成するプレ方式を導入し，プレ方式を改良することで，第 1 の方式の全体像を述べる．

以下のように$T_{l,w}$を定め，これを定数和集合と呼ぶ．

$$T_{l,w}=\{(t_1,\dots,t_w): t_i\in\{0,\dots,l\}, t_1+\cdots+t_w=l\}.$$

定数和集合は，総和がlとなるような非負整数w個の組の集合であり，その要素数は$|T_{l,w}|=\frac{(l+w-1)!}{l!(w-1)!}$となることが知られている．ここでは，$|T_{l,w}|\ge 2^{160}$となるよう$l,w$の値を定めるものとする．定数和指紋関数は，その値域が定数和集合となっているような指紋関数である．定数和指紋関数をゼロから構成することも可能であるが，既存の指紋関数の出力と定数和集合の間に単射を定義することで，元の指紋関数の持つ統計的性質を引き継ぐ形で定数和指紋関数を構成することができる．この場合，元の指紋関数が衝突困難であれば定数和指紋関数も衝突困難となる．詳細は割愛するが，$|T_{l,w}|$に関する再帰的な関係を利用すれば，既存の指紋関数が生成する指紋値（一般には整数値と解釈される）から$T_{l,w}$の要素を一意的に決定することは容易であり，きわめて効率よく定数和指紋を計算することができる．以下では，そのようにして構成された衝突困難な定数和指紋関数をfと表記する．

提案方式における署名作成鍵, 署名検証鍵の構成方法は, Winternitz OTS とほぼ同様である．すなわち，ランダムに選択されたw個のハッシュ値の組$k_s=(s_1,\dots,s_w)$を署名作成鍵とし，k_sの各要素にhをl回作用させて得られるw個のハッシュ値$k_v=(v_1,\dots,v_w), v_i=h^l(s_i)$を署名検証鍵とする．署名作成では，定数和指紋関数$f$を用いてメッセージの定数和指紋$f=(f_1,\dots,f_w)$を求め，$\sigma=(\sigma_1,..,\sigma_w), \sigma_i=h^{l-f_i}(s_i)$として署名を決定する．署名検証では，検証対象メッセージの定数和指紋に応じて署名の各要素のハッシュ値を計算し，署名検証鍵と一致するか確認することで，

署名の正しさを検証する．ここで述べた方式では，鍵の生成にあたりlw回のハッシュ計算が必要となるため，鍵生成コストはlw回である．また，署名の作成および検証には，それぞれ$wl-l, l$回のハッシュ計算が必要となるため，これらの値が両操作の計算コストとなる．

ここで注意しなければならないのは，$|T_{l,w}| \geq 2^{160}$となるようl, wを選ぼうとすると，Winternitz OTS のl, wよりも大きな値となってしまう傾向があるという点である．たとえば，Winternitz OTS で$l = 256, w = 22$とすると指紋関数の空間サイズが2^{160}以上となるが，提案方式において$w = 22$として指紋関数の空間サイズを2^{160}以上にしようとすると，$l = 1695$として値を定める必要がある．すなわち，安全性レベルとハッシュ連鎖の本数を同じに揃えようとすると，ここで紹介した方式では Winternitz OTS に比べ 6 倍以上長い連鎖を準備する必要が生じ，鍵生成，署名作成の計算量が大きくなってしまう．

この問題を回避するため，ハッシュ連鎖を部分的に構成することを考える．ランダムに選ばれたメッセージに対し指紋値が一様に分布するとき，定数和指紋$f = (f_1, \dots, f_w)$の各要素の期待値は$\frac{l}{w}$に近づくこととなる．もう少し詳細に分析すると，f_iの値が比較的小さくなる確率は相対的に大きく，f_iの値が大きくなる確率は非常に小さくなることを示すことができる．たとえば，$f_1 = l$となる定数和指紋は$(l, 0, \dots, 0)$の 1 つしかなく，ハッシュ連鎖の先頭にあるs_1（署名作成鍵の第 1 要素）が指紋の一部として利用されることは，ほとんど無いと言っても過言ではない．この場合，s_1を起点として長さlのハッシュ連鎖を構成するのではなく，$h(s_1)$に相当するハッシュ値をランダムに定め，この値を 起点として長さ$l-1$のハッシュ連鎖を構成したとしても，多くの場合，支障等は生じない．この考え方をさらに進め，$\theta \leq l$となるパラメータを適当に選択し，本来は長さlであるハッシュ連鎖の後半部分，θ個のハッシュ値による連鎖の部分のみを構成することを考える．もし定数和指紋の要素f_iの値がθ以下であれば，ハッシュ連鎖の中の「構成しなかった前半部分」が参照されることはないため，署名の作成にも検証にも支障は生じないことになる．一方，$f_i > \theta$となる要素が存在した場合は，「構成しなかった前半部分」を参照する必要があるため，そのままでは署名を計算することができなくなってしまう．この問題を回避するため，メッセージから定数和指紋を計算する際に追加の情報を入力し，その追加情報の値を調整することで，定数和指紋のすべての要素をθ以下になるよう制御する．たとえば，メッセージmとランダムな nonce rを使用し，$(f_1, \dots, f_w) = f(m||r)$として定数和指紋を計算することを考える．すべての$1 \leq i \leq w$に対し$f_i \leq \theta$であれば nonce rを採用し，一つでもθを超える要素が存在すれば，別の nonce をランダムに選んで再度の試行を行う．メッセージ，署名に加え，採用された nonce をあわせて送信することで，受信側では効率よく署名の正しさを確認することができる．どのような nonce に対し，どのような指紋値が得られるかは予測できないため，一般には，複数の nonce を生成し，定数和指紋関数を複数回計算する必要が生じることになる．θの値が大きければ試行回数は比較的小さく，θの値が小さくなると，より多くの試行回数が必要となる．何回の試行が必要になるかは，包除計算により求めることが可能であり[5]，たとえば上述の$w = 22, l = 1695$の場合，$\theta = 272, 232, 209$としたときに試行回数の期待値が 2, 4, 8 回となることが確認できる．

ハッシュ連鎖の部分構成を採用した場合の鍵生成コストは$w\theta$，署名作成コストは$\theta w - l$，署名検証コストはlであり，$w = 22$（鍵サイズや署名サイズをハッシュ値 22 個分と同じ長さ$22 \times 160 = 3520$ビットに定めることに相当する）としたときの Winternitz OTS，提案手法のコストを表に示し比較すると，下表のようになる．$\theta = l = 1695$は，ハッシュ連鎖の全体を構成する方式に相当し，鍵生成および署名作成に膨大なコストが必要となることが確認できる．この表から，θの値を小さく取ることで，Winternitz OTS よりも効率が改善されていることを確認することができる．ただし，定数和指紋関数の計算を複数回実行することが暗黙のうちに想定されているため，この表に示されていない隠れコストが存在しているという点について十分配慮が必要である．

Winternitz					提案方式 1				
l	鍵生成	署名作成	署名検証	w	l	θ	鍵生成	署名作成	署名検証
256	5,610	≤ 5,610	≤ 5,610	22	1,695	1,695	37,290	35,595	1,695
					1,695	272	5,984	4,289	1,695
					1,695	232	5,104	3,409	1,695
					1,695	209	4,598	2,903	1,695

4.2 第 2 の方式

定数和指紋は，指紋空間の各要素を比較不能とするのに有効であるが，指紋値の要素が広範に分布するため，一般には非常に長いハッシュ連鎖を準備する必要が生じる．ハッシュ連鎖の部分構成等の工夫で計算量を抑制することも可能であるが，nonce を試行錯誤的に生成し，定数和指紋関数を複数回計算する必要がある等の手間が追加で発生することになる．指紋値の要素を一定範囲に制限することができれば，この問題を回避することが可能になると期待されるため，定数和指紋の概念を少し変更し，ゼロサム指紋を導入してハッシュベース署名の構成に利用することを考える．正整数wと整数v, wに対し，下記のように集合$D_{w,b}^{v}$を定義する．

$$D_{w,b}^{v} = \{(t_1, \dots, t_w) : t_i \in \{-b, \dots, b\}, t_1 + \cdots + t_w = v\}.$$

$D^v_{w,b}$は，総和がvとなるようなw個の整数の組の集合であるが，各整数の値が$-b$から$+b$の範囲に制限されている点が一般の定数和集合と異なる．$D^0_{w,b}$を値域とする指紋関数を，ゼロサム指紋関数と呼ぶ．ゼロサム指紋関数が十分なサイズの値域を持つためには，$\left|D^0_{w,b}\right| \geq 2^{160}$となるよう$w, b$の値を設定する必要があるが，そのためには$\left|D^v_{w,b}\right|$の値を計算する必要がある．閉じた式により$\left|D^v_{w,b}\right|$を示すことは難しいが，下記の再帰式を利用し，具体的な数値を計算することが可能である．

$$\left|D^v_{1,b}\right| = \begin{cases} 1 & \text{if } v \in \{-b, \ldots, b\} \\ 0 & \text{otherwise} \end{cases}$$

$$\left|D^v_{w,b}\right| = \sum_{i=-b}^{b} \left|D^{v-i}_{w-1,b}\right|$$

この式を用い$\left|D^0_{w,b}\right| \geq 2^{160}$となる$w, b$を求めると，たとえば$w = 22, b = 104$とのパラメータ選択が可能となることがわかる．

第２の方式における鍵生成では，長さ$2b + 1$のハッシュ連鎖を用いることにより，署名作成鍵と署名検証鍵を構成する．ゼロサム指紋値の第i要素がf_iであるとき，署名作成においては$\sigma_i = h^{b-f_i}(s_i)$として計算を行い，署名検証においては$v_i = h_i^{b+f_i+1}(\sigma_i)$として署名の正しさを確認する．鍵生成コストは$w(2b + 1)$となり，署名作成および署名検証のコストは，それぞれ$wb, w(b + 1)$となる．$w = 22, b = 104$の場合，鍵生成，署名作成，署名検証のコストは，それぞれ 4,598, 2,288, 2,310 となり，第１の方法の$\theta = 209$の場合と同等のコストになることが確認できる．この第２の方法では nonce の利用等も必要なく．いわゆる隠れコストが存在していないため，より実用生が高いと判断することができる．

4.3 提案方式の安全性

第１の方式については，Winternitz OTS と同様，定数和指紋関数fが衝突困難性を有し，ハッシュ関数hが衝突困難性と一方向性を有するとき，強存在的偽造不可能が保証されることを証明済みである．第２の方式についても，同様のアプローチで安全性証明を与えることが可能と強く予想しており，本報告書執筆時点において，証明内容の最終的な確認を行っている段階である．

参考文献

[1] Bernstein, D.J, Buchmann, J., Dahmen, E., Post-Quantum Cryptography, Springer, 2009.

[2] Bernstein, D.J., Hopwood, D., Hulsing, et al.,SPHINCS: Practical Stateless Hash-Based Signatures, EUROCRYPT 15, pp.368–397, 2015.

[3] Bleichenbacher, D., Maurer, U., Optimal Tree-Based One-Time Digital Signature Schemes, Symp. on Theoretical Aspects of Comp. Sci., pp.363–374, 1996.

[4] Bleichenbacher, D., Maurer, U., On the Efficiency of One-Time Digital Signature Schemes, ASIACRYPT 96, pp.145–158, 1996.

[5] Bollinger, R.C., Burchard, C.L., Lucas's Theorem and Some Related Results for Extended Pascal Triangles, The American Math. Monthly, 97, 3, pp.198–204, 1990.

[6] Boneh, D., Shen, E.,Waters, B., Strongly Unforgeable Signatures Based on Computational Diffie-Hellman, Intl. Conf. on Theory and Practice of Public-Key Cryptography, pp.229–240, 2006.

[7] Buchmann, J., Dahmen, E., Ereth, S., et al., On the Security of the Winternitz One-Time Signature Scheme, AFRICACRYPT 11, pp.363–378, 2011.

[8] Buchmann, J., Dahmen, E., Hulsing, XMSS—A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions, Intl. Conf. on Post-Quantum Cryptography, pp.117–129, 2011.

[9] Cruz, J.P., Yatani, Y., Kaji, Y., Constant-Sum Fingerprinting for Winternitz One-Time Signature, 2016 Intl. Symp. on Inf. Theory and Its Applications, pp.703-707, 2016.

[10] Dods, C., Smart, N., Stam, M., Hash Based Digital Signature Schemes, Intl. Conf. on Cryptography and Coding 2005, pp.96–115, 2005.

[11] Goldwasser, S., Bellare, M., Lecture Notes on Cryptography, https://cseweb.ucsd.edu/~mihir/papers/gb.pdf, accessed March 30, 2022.

[12] Hulsing, A., W-OTS+ — Shorter Signatures for Hash-Based Signature Schemes, AFRICACRYPT 13, pp.173–188, 2013.

[13] Lamport, L., Constructing Digital Signatures from a One-Way Function, Technical Report SRI-CSL-98, SRI Intl. Computer Sci. Lab., 1979.

[14] Merkle, R., A Certified Digital Signature, CRYPTO 89, pp.218–238, 1990.

[15] Perrig, A., The BiBa One-Time Signature and Broadcast Authentication Protocol, ACM Conf. on Computer and Communications Security, pp.28–37, 2001.

[16] Reyzin, L., Reyzin, N., Better than BiBa: Short One-Time Signatures with Fast Signing and Verifying, Intl. Inf. Security and Privacy Conference, pp.1–47, 2002.

[17] Shor, P.W., Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. of Computing, 26, 5, pp.1484–1509, 1997.

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　0件）

１．著者名 Kaji Yuichi、Paul Cruz Jason、Yatani Yoshio	４．巻 1
２．論文標題 Hash-Based Signature with Constant-Sum Fingerprinting and Partial Construction of Hash Chains	５．発行年 2018年
３．雑誌名 15th International Conference on Security and Cryptography	６．最初と最後の頁 297-304
掲載論文のDOI（デジタルオブジェクト識別子） 10.5220/0006828202970304	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計10件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 Tomonori Hirata, Yuichi Kaji
２．発表標題 Information Leakage through Passive Timing Attacks on RSA Decryption System
３．学会等名 Proceedings of 2020 International Symposium on Information Theory and Its Applications（国際学会）
４．発表年 2020年

１．発表者名 Tomonori Hirata, Yuichi Kaji
２．発表標題 Information leakage through passive timing attacks on ElGamal Elliptic Curve Cryptography
３．学会等名 暗号と情報セキュリティシンポジウム 2021
４．発表年 2021年

１．発表者名 Bo Wang, Ako Suzuki, Yuichi Kaji
２．発表標題 A Real-Time Bluetooth Protocol Fuzzing System
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 2021年

１．発表者名
平田智紀，楫勇一

２．発表標題
RSA復号プログラムへのタイミング攻撃により得られる秘密鍵の漏洩情報量評価

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
2019年

１．発表者名
Atsuki Momose, Jason Paul Cruz, Yuichi Kaji

２．発表標題
BLDAG: Generalization of the Blockchain into Bi-Layered Directed Acyclic Graph

３．学会等名
コンピュータセキュリティシンポジウム 2019

４．発表年
2019年

１．発表者名
Tomonori Hirata, Yuichi Kaji

２．発表標題
Information leakage through passive timing attacks on RSA decryption system

３．学会等名
コンピュータセキュリティシンポジウム 2019

４．発表年
2019年

１．発表者名
山中隆太郎，王博，鈴木亜香，楫勇一

２．発表標題
遺伝的アルゴリズムを用いたBluetoothファジングの検討

３．学会等名
暗号と情報セキュリティシンポジウム 2020

４．発表年
2020年

１．発表者名
柏倉祐吉，楫勇一

２．発表標題
署名鍵のパンクチャと定数和指紋を利用したハッシュベース署名

３．学会等名
暗号と情報セキュリティシンポジウム 2020

４．発表年
2020年

１．発表者名
柏倉祐吉，楫勇一

２．発表標題
署名鍵のパンクチャによるWinternitz OTSの改良

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
2018年

１．発表者名
Tomonori Hirata, Yuichi Kaji

２．発表標題
The amount of information leakage of decryption keys through timing attacks on RSA decryption system

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
2019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