

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号
特表2024-539876
(P2024-539876A)

(43)公表日 令和6年10月31日(2024.10.31)

(51)国際特許分類
H 0 4 L 9/32 (2006.01)

F I
H 0 4 L 9/32 2 0 0 C

審査請求 未請求 予備審査請求 未請求 (全19頁)

(21)出願番号	特願2024-522578(P2024-522578)	(71)出願人	524140499
(86)(22)出願日	令和4年10月26日(2022.10.26)		ピーキューシー ピーティーイー リミテ
(85)翻訳文提出日	令和6年6月5日(2024.6.5)		ッド
(86)国際出願番号	PCT/SG2022/050769		シンガポール国 シンガポール 0 3 8 9
(87)国際公開番号	WO2023/080842		8 7 テマセック ブールバード 7 ナン
(87)国際公開日	令和5年5月11日(2023.5.11)		バー 1 2 - 0 7 サンテック タワー ワン
(31)優先権主張番号	10202112269T	(74)代理人	100120891
(32)優先日	令和3年11月5日(2021.11.5)		弁理士 林 一好
(33)優先権主張国・地域又は機関	シンガポール(SG)	(74)代理人	100165157
			弁理士 芝 哲央
(81)指定国・地域	AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA	(74)代理人	100205659
	,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(		弁理士 齋藤 拓也
	AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,A	(74)代理人	100126000
	T,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR		弁理士 岩池 満
	,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,	(74)代理人	100185269
	最終頁に続く		最終頁に続く

(54)【発明の名称】 デジタル署名を保護するための方法およびシステム

(57)【要約】

データを耐量子デジタル署名するための方法、秘密鍵を検証することによってデータのソースを認証するための耐量子デジタル署名を検証するための方法、および耐量子デジタル署名システムが提供される。耐量子デジタル署名システムは、デジタル署名システムおよび耐量子保護レイヤを含む。デジタル署名システムは、公開鍵および秘密鍵を含み、公開鍵は秘密鍵と関連付けられている。デジタル署名システムはまた、データおよび秘密鍵に応答して生成されるデジタル署名を含む。耐量子保護レイヤは、デジタル署名システムに適用され、署名当事者によって提供される、秘密鍵の事前イメージの知識の量子安全証明を含む。

【選択図】 図 2

Algorithm 2: Quantum-resistant ECDSA signing $Sign_q$.

```
1 begin
2    $G \leftarrow$  ECC base point;  $P \leftarrow$  ECC order;
3    $\rho \leftarrow$  secret pre-image;
4    $M \leftarrow$  message;
5   Generate signature random  $r$ ;
6   Compute  $r^{-1}$  where  $r \cdot r^{-1} \equiv 1 \bmod P$ ;
7   Compute  $R = (R_x, R_y)$  where  $R \equiv r \cdot G \bmod P$ ;
8   Compute hash of message  $H(M)$ ;
9   Enumerate ZKBoo proof  $\pi \leftarrow$  begin
10    Zero-knowledge computation of private key  $K_s$  where  $K_s = H(\rho)$ ;
11    Zero-knowledge computation of public key  $K_p$  where
12      $K_p \equiv K_s \cdot G \bmod P$ ;
13    Compute  $s$  where  $s \equiv r^{-1} \cdot (H(M) + R_x \cdot K_x) \bmod P$ ;
14    Commit  $R_x, s$  in the proof;
15  end
16  destroy  $r, r^{-1}, K_s$ ;
17  return  $\sigma = \{R_x, s\}, \pi$ ;
end
```

200 FIG. 2

【特許請求の範囲】**【請求項 1】**

公開鍵および秘密鍵を含むデジタル署名システムであって、前記公開鍵が前記秘密鍵に関連付けられ、前記デジタル署名システムは、データおよび前記秘密鍵に応答して生成されるデジタル署名を含む、デジタル署名システムと、

前記デジタル署名システムに適用される耐量子保護レイヤであって、署名当事者によって提供される、前記秘密鍵の事前イメージの知識の量子安全証明を含む、耐量子保護レイヤと、

を含む、耐量子デジタル署名システム。

【請求項 2】

前記秘密鍵の計算は、崩壊ハッシュ関数を含む、請求項 1 に記載の耐量子デジタル署名システム。

【請求項 3】

所定の強度の暗号鍵は、前記公開鍵および前記秘密鍵の両方を生成する、請求項 1 または請求項 2 に記載の耐量子デジタル署名システム。

【請求項 4】

前記署名当事者によって提供される、前記秘密鍵の前記事前イメージの知識の量子安全証明は、ゼロ知識証明を含む、請求項 1 ～ 3 のいずれか一項に記載の耐量子デジタル署名システム。

【請求項 5】

前記署名当事者によって提供される、前記秘密鍵の前記事前イメージの知識の量子安全証明は、部分的知識証明を含む、請求項 1 ～ 3 のいずれか一項に記載の耐量子デジタル署名システム。

【請求項 6】

前記署名当事者によって提供される、前記秘密鍵の前記事前イメージの知識の量子安全証明は、前記秘密鍵の少なくとも一部に応答して生成される、請求項 1 ～ 5 のいずれか一項に記載の耐量子デジタル署名システム。

【請求項 7】

前記耐量子保護レイヤは、前記秘密鍵の前記事前イメージの知識の複数の証明を提供することにより、複数の当事者をサポートし、前記秘密鍵の前記事前イメージの知識の前記複数の証明は、予め定義された証明書階層を有する、請求項 1 ～ 6 のいずれか一項に記載の耐量子デジタル署名システム。

【請求項 8】

データを耐量子デジタル署名するための方法であって、

セキュリティパラメータに応答して公開鍵および事前イメージパラメータを生成するステップと、

秘密鍵を生成するステップであって、前記秘密鍵は、前記事前イメージパラメータに
応答して生成され、前記公開鍵と関連付けられる、ステップと、

前記データおよび前記秘密鍵に
応答して署名を生成するステップと、

前記事前イメージパラメータの知識の証明を生成するステップと、

前記署名および前記事前イメージパラメータの知識の前記証明の両方を用いて前記データをデジタル署名するステップと、

を含む、方法。

【請求項 9】

前記データをデジタル署名するステップは、並列検証のためにゼロ知識証明とは別に前記署名を記憶することを含む、請求項 8 に記載の方法。

【請求項 10】

前記秘密鍵を生成するステップは、崩壊ハッシュ関数を使用して前記秘密鍵を生成することを含む、請求項 8 または請求項 9 に記載の方法。

【請求項 11】

前記セキュリティパラメータは、所定の強度の暗号鍵を含む、請求項 8 ～ 10 のいずれか一項に記載の方法。

【請求項 12】

前記事前イメージパラメータの知識の前記証明は、ゼロ知識証明を含む、請求項 8 ～ 11 のいずれか一項に記載の方法。

【請求項 13】

前記事前イメージパラメータの知識の前記証明は、部分的知識証明を含む、請求項 8 ～ 11 のいずれか一項に記載の方法。

【請求項 14】

前記事前イメージパラメータの知識の前記証明は、前記秘密鍵の少なくとも一部に応答して生成される、請求項 8 ～ 13 のいずれか一項に記載の方法。

【請求項 15】

前記秘密鍵を生成するステップは、前記事前イメージパラメータに対してハッシュ鍵導出を実行することによって前記秘密鍵を生成すること、前記事前イメージパラメータに対して一方向性関数鍵導出を実行することによって前記秘密鍵を生成すること、または前記事前イメージパラメータに対して対称鍵導出を実行することによって前記秘密鍵を生成することのうちの 1 つまたは複数を含む、請求項 8 ～ 14 のいずれか一項に記載の方法。

【請求項 16】

前記公開鍵および前記事前イメージパラメータを生成するステップは、前記事前イメージパラメータに対してハッシュ鍵導出を実行することによって前記公開鍵を生成すること、前記事前イメージパラメータに対して一方向性関数鍵導出を実行することによって前記公開鍵を生成すること、または前記事前イメージパラメータに対して対称鍵導出を実行することによって前記公開鍵を生成することのうちの 1 つまたは複数を含む、請求項 8 ～ 15 のいずれか一項に記載の方法。

【請求項 17】

前記データはメッセージを含み、前記方法は、前記デジタル署名されたメッセージを送信するステップをさらに含み、前記事前イメージパラメータの知識の前記証明が、前記メッセージの受信者によってアクセス可能である、請求項 8 ～ 16 のいずれか一項に記載の方法。

【請求項 18】

前記デジタル署名されたメッセージを送信するステップは、(i) 前記事前イメージパラメータの知識の前記証明、または (ii) 前記事前イメージパラメータの知識の前記証明にアクセス可能なデジタル記憶場所を特定するための位置情報の一方または両方と共に、前記デジタル署名されたメッセージを送信することを含む、請求項 17 に記載の方法。

【請求項 19】

前記公開鍵を送信するステップをさらに含み、前記公開鍵を送信するステップは、前記公開鍵と共に前記デジタル署名されたメッセージを送信すること、または前記公開鍵をデジタル記憶場所へ送信することを含み、前記デジタル記憶場所が、認証局またはパブリックリポジトリを含む、請求項 17 または請求項 18 に記載の方法。

【請求項 20】

秘密鍵を検証することにより、データのソースを認証するための耐量子デジタル署名を検証するための方法であって、前記方法は、

前記秘密鍵に関連付けられた公開鍵、および前記データに対応するデジタル署名が前記秘密鍵に応答して生成されることを検証するための事前イメージパラメータの知識の証明の両方を使用して検証することによって、前記データのの前記ソースを認証するステップを含む、方法。

【請求項 21】

前記事前イメージパラメータの知識の前記証明は、ゼロ知識証明を含む、請求項 20 に記載の方法。

【請求項 22】

前記認証するステップは、前記公開鍵を使用した検証および前記事前イメージパラメータの知識の前記証明を使用した検証を並行して処理することを含む、請求項 20 または請求項 21 に記載の方法。

【請求項 23】

前記公開鍵を使用した検証および前記事前イメージパラメータの知識の前記証明を使用した検証を並行して処理することは、

前記公開鍵を第 1 のデジタル記憶場所から検索するステップと、

前記事前イメージパラメータの知識の前記証明を第 2 のデジタル記憶場所から検索するステップと

を含む、請求項 22 に記載の方法。

10

【請求項 24】

前記データの前記ソースを認証するステップは、前記デジタル署名が前記秘密鍵に応答して生成されたと判定され、前記事前イメージパラメータの知識の前記証明が前記事前イメージパラメータから計算された有効な証明であると判定された場合に、およびそれらの両方の場合にのみ、前記データの検証を承諾することを含む、請求項 20 ~ 23 のいずれか一項に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

【優先権の主張】

20

本出願は、2021 年 11 月 05 日に提出されたシンガポール特許出願第 10202112269T 号からの優先権を主張する。

【0002】

本発明は、概して、デジタル署名に関し、より具体的には、量子能力のある (quantum-capable) 敵対者からデジタル署名を保護するための方法およびシステムに関する。

【背景技術】

【0003】

非対称鍵暗号は、デジタル領域における当事者間の信頼を維持するために世界中のシステムで使用されているツールである。デジタル署名の使用により、通信当事者は互いを認証し、交換されたデータの完全性を確認し、否認された状況においてデータの出所を証明することができる。3つの古典的なデジタル署名アルゴリズムがアメリカ国立標準技術研究所 (NIST) のデジタル署名標準に記載されており、離散対数暗号に基づくデジタル署名アルゴリズム (DSA)、リベストーシャミア エーデルマン (Rivest-Shamir Adelman) (RSA) アルゴリズム、および楕円曲線デジタル署名アルゴリズム (ECDSA) を含み、ECDSA は楕円曲線暗号 (ECC) に基づいている。DSA および ECDSA の安全性は、非常に大きな数の有限体上の離散対数を解くことに基づいており、一方、RSA の安全性は、非常に大きな数の有限体上の素因数分解の難しさに基づいている。

30

【0004】

しかしながら、大型のフォールト・トレラント (fault-tolerant) 量子コンピュータの出現は、これらの古典的なデジタル署名アルゴリズムを使用するシステムに大きなリスクをもたらした。ショア (Shor) のアルゴリズムは、DSA および ECDSA がベースとなっている離散対数問題、および RSA がベースとなっている素因数分解問題の両方を、 $O(\log N)$ 多項式時間で解く能力を有する。これは、十分に大型の量子コンピュータを所有するいずれかの敵対者が、ユーザの公開鍵が与えられたときに、ユーザの秘密署名鍵を数時間で計算することができ、それによって、ユーザになりすますための有効なデジタル署名を生成することができることを意味する。さらに、以前にユーザによって署名されたデータは、もはや真正かつ信頼できるものであることを証明することができない。

40

50

【0005】

業界は、新しいデジタル署名標準が進化するにつれて、新しいシステムの実装を検討することを奨励する可能性が高いが、既存のシステムまたは今後のシステムに対する課題は、デジタル署名に特有の以下の問題を提起する：量子コンピュータがデジタル署名を無効にする能力に直面して、既にデジタル署名された文書はどのように信頼性を維持できるのか？これらの文書には新しいアルゴリズムで対署名（counter-signed）をする必要があるのか？対署名者（counter-signer）は取引の利害関係のない第三者かもしれないので、対署名者は検証当事者に対してどのような責任を負うのか？移行できないレガシーシステムについてはどうするのか？検証当事者はいつ新しいアルゴリズムを検証する準備ができていると予想するのか？既存の非量子安全（non-quantum-secure）署名は検証に合格したが、検証当事者が新しい量子安全（quantum-secure）署名を検証できなかった場合、検証当事者にはどのような法的な影響があるのか？デジタル署名を使用するシステムオペレータは、業界の標準化を待つのではなく、ステートフルハッシュベースの（stateful hash-based）署名への暗号移行に着手すべきか？

10

【0006】

したがって、現在のデジタル署名システムの欠点を克服し、量子能力のある敵対者からデジタル署名を保護するデジタル署名のシステムおよび方法に対する必要性が存在する。さらに、他の望ましい特徴および特性は、添付の図面および本開示のこの背景と併せて考慮される、後続の詳細な説明および添付の特許請求の範囲から明らかになるであろう。

20

【発明の概要】

【0007】

本実施形態の少なくとも1つの態様によれば、耐量子（quantum resistant）デジタル署名システムが提供される。耐量子デジタル署名システムは、デジタル署名システムおよび耐量子保護レイヤを含む。デジタル署名システムは、公開鍵および秘密鍵を含み、公開鍵は秘密鍵と関連付けられている。デジタル署名システムはまた、データおよび秘密鍵に応答して生成されるデジタル署名を含む。耐量子保護レイヤは、デジタル署名システムに適用され、署名当事者によって提供される、秘密鍵の事前イメージの知識の量子安全証明を含む。

【0008】

本実施形態の別の態様によれば、データを耐量子デジタル署名するための方法が提供される。この方法は、セキュリティパラメータに応答して公開鍵および事前イメージパラメータを生成するステップと、秘密鍵を生成するステップとを含み、秘密鍵は、事前イメージ（pre-image）パラメータに応答して生成され、公開鍵と関連付けられる。この方法はさらに、データおよび秘密鍵に応答して署名を生成するステップと、事前イメージパラメータの知識の証明を生成するステップと、署名および事前イメージパラメータの知識の証明の両方を用いてデータをデジタル署名するステップとを含む。

30

【0009】

本実施形態のさらなる態様によれば、秘密鍵を検証することによってデータのソースを認証するための耐量子デジタル署名を検証するための方法が提供される。この方法は、秘密鍵に関連付けられた公開鍵、およびデータに対応するデジタル署名が秘密鍵に応答して生成されることを検証するための事前イメージパラメータの知識の証明の両方を使用して検証することによってデータのソースを認証するステップを含む。

40

【図面の簡単な説明】

【0010】

添付の図面は、同様の参照数字が別の図面全体を通して同一または機能的に類似の要素を示し、以下の詳細な説明と共に本明細書に組み込まれ、本明細書の一部を構成し、様々な実施形態を例示し、本実施形態に従って様々な原理および利点を説明するのに役立つ。

【0011】

【図1】本実施形態による例示的な耐量子（quantum-resistant）EC

50

D S A 鍵生成アルゴリズム $KeyGen_q$ を示す。

【図 2】本実施形態による例示的な耐量子 E C D S A 署名アルゴリズム $Sign_q$ を示す。

【図 3】本実施形態による例示的な耐量子 E C D S A 検証アルゴリズム $Verify_q$ を示す。

【図 4】テスト中の本実施形態による耐量子デジタル署名方式の実際の実装のユースケースを示すプロセス図を示す。

【図 5】本実施形態による耐量子デジタル署名方式の実際の実装における、予め定義された証明書階層を例示するウィンドウの画像を示す。

【図 6】本実施形態による耐量子デジタル署名方式の実際の実装における、タイムスタンプクライアントによる検証を例示するウィンドウの画像を示す。

10

【0012】

図面の要素は単純化および明確化のために示されており、必ずしも縮尺通りに描かれていないことを当業者は理解するであろう。

【発明を実施するための形態】

【0013】

以下の詳細な説明は、本質的に単なる例示であり、本発明または本発明の適用および用途を限定することを意図するものではない。さらに、本開示の先行する背景または以下の詳細な説明に提示されたいかなる理論にも拘束される意図はない。本実施形態がなければ、量子コンピュータを使用する敵対者に対して脆弱である可能性のある、R S A / D S A / E C D S A および他のデジタル署名アルゴリズムを使用するシステムに対して、耐量子保護レイヤを追加する新規手段を提示することが、本実施形態の意図である。本実施形態によれば、量子安全ゼロ知識証明 (quantum-secure zero-knowledge proof) の使用が適用されて、署名当事者は、秘密鍵が確かに署名当事者によって生成され、量子コンピュータを使用して解読されていないことの証明を含めることを要求する。これは、本実施形態の方法およびシステムに従って、署名当事者が、検証当事者に送信されるメッセージにデジタル署名する際に、秘密鍵から生成されたデジタル署名と共に、秘密鍵の事前イメージ (プレイメージ。プレ画像。事前画像。pre-image) の知識の量子安全ゼロ知識証明を署名プロセス中に含めることによって達成される。このように、本実施形態は、R S A / D S A / E C D S A および他のデジタル署名アルゴリズムを使用するシステムが、デジタル署名の使用を認める既存の検証当事者の実装および立法 (legislature) との後方互換性を維持しながら、量子コンピュータに対する保護を有利に達成することを可能にする。

20

30

【0014】

本実施形態による方法およびシステムは、十分に大型の量子コンピュータが構築された後でも、既存のデジタル署名が耐量子を維持できるのであれば、移行 (トランジション。transition) に関連する多くの後方互換性の問題を回避できるという前提に基づいて形成される。新しいアルゴリズムへの移行 (マイグレーション。migration) タイムラインは、対抗者に依存することが少なくなり、既存のデジタル署名された文書は、ポスト量子時代においても、それらの真正性を有利に保持する。本実施形態は、秘密署名鍵の事前イメージの量子安全ゼロ知識証明を署名と共に重ねる (層化する。layer) ことによって、既存のシステムが互換性の問題に直面することを有利に防止し、その結果、以下の技術的効果が得られる。(a) デジタル署名方式を拡張して、後方互換性の特性を有する耐量子デジタル署名方式を構築する、(b) デジタル署名に含まれるゼロ知識証明を使用して耐量子デジタル署名方式を実現して、デジタル署名を耐量子にする、(c) 既存の Adobe PDF Acrobat Reader DC v2021.x と互換性のある X.509 v3 証明書を用いて耐量子 E C D S A タイムスタンプデジタル署名を発行するための RFC 3161 互換タイムスタンプサーバを提供する Adobe (登録商標) PDF デジタル署名ソリューションを含む現実世界の実装を展開する。

40

【0015】

50

デジタル署名は、デジタル通信において完全性、真正性、および否認不可（non-repudiation）を提供する。例として、アリス（Alice）およびボブ（Bob）は通信当事者である。アリスは、ボブに送信すべきメッセージMを有し、ボブがメッセージを変更せずに確実に受信し（完全性）、それがアリスからのメッセージであること（真正性）を知ることが望んでいる。ボブは、そのメッセージが本当にアリスからのものであることを第三者に証明できるようにすること（否認不可）を望んでいる。

【0016】

デジタル署名方式は、多項式時間アルゴリズムであるKeyGen、Sign、およびVerifyの三重として定義される。アルゴリズムKeyGenは、所定の強度nの暗号鍵強度を定義するセキュリティパラメータ 1^n を取り込み、秘密鍵 K_s および対応する公開鍵 K_p を出力する。アルゴリズムSignは、メッセージMおよび秘密鍵 K_s を取り込み、署名 σ を出力する。そして、アルゴリズムVerifyは、メッセージM、公開鍵 K_p 、および署名 σ を取り込み、 σ が $\text{Sign}(M, K_s)$ によって生成された有効な署名である場合およびその場合に限り、「承諾（アクセプト。accept）」を出力する。これらの関係を式（1）、（2）、および（3）に示す。

10

【数1】

$$\text{KeyGen}(1^n) \Rightarrow \{K_s, K_p\} \quad (1)$$

$$\text{Sign}(M, K_s) \Rightarrow \{\sigma\} \quad (2)$$

20

$$\text{Verify}(M, K_p, \sigma) \Rightarrow \{\text{結果}\} \quad (3)$$

【0017】

アリスおよびボブの例では、署名当事者であるアリスが、KeyGenを呼び出して $\{K_s, K_p\}$ を生成する。 K_p は公開され、ボブおよび他の当事者が K_p にアクセスできるようになる。次いでアリスは、秘密鍵 K_s を用いてSignを呼び出し、メッセージMに署名し、署名 σ を生成する。アリスは、 $\{M, \sigma\}$ をボブに送信する。検証当事者であるボブは、メッセージMについての署名 σ を検証するために、アリスの公開鍵 K_p を用いてVerifyを呼び出す。Verifyが「承諾」を返すと、ボブはアリスから変更されていないメッセージMおよび署名証明 σ を正常に受信したことになる。

30

【0018】

ゼロ知識証明は、命題の正確さ以外に追加の知識を伝達しない証明として定義される。ゼロ知識証明の具体的な実現例は多く存在するが、耐量子非インタラクティブ（非対話型。non-interactive）ゼロ知識証明は、ZKStarkベースの証明、またはMPC-in-the-head（Multi-party computation in-the-head）ベースの証明のいずれかである。部分的知識証明（partial-knowledge proof）は、命題の正確さに加えて何らかの知識を伝達する証明である。

【0019】

MPC-in-the-head証明では、証明者はコミットメントを有するn個の分岐のブール（Boolean）計算回路を作成しなければならない、そのうちn-1個のビュー（views）が知識の証明として検証者に明らかにされ得る。証明を非インタラクティブにするために、証明者は、フィアット-シャミール（Fiat-Shamir）のヒューリスティック（heuristic）を使用して、どのn-1個のビューを検証者に送信するかを確定的に、しかし予測不可能に決定することができる。次いで検証者は、その命題が誤りである確率を $1/n$ としてn-1個のビューを調査する（ウォークする。walk）。このように証明者が回路を計算し、ビューを提供しなければならないラウンド数を（異なるランダムな入力パラメータで）増やすことによって、証明者が誤った主張をする統計的確率は指数関数的に減少する。

40

50

【0020】

量子コンピュータ上でのショア (Shor) のアルゴリズムは、素因数分解問題、離散対数問題、および楕円曲線離散対数問題を破っているので、十分に大型の量子コンピュータが構築された場合、敵対者は公開鍵 K_p が与えられれば、全ての $RSA/DSA/ECDSA$ 秘密鍵 K_s を実行可能に計算できると確実に想定することができる。しかしながら、対称鍵およびハッシュベースの暗号は比較的耐量子がある。例えば、量子コンピュータ上でのグローバー (Grover) のアルゴリズムは、ブルートフォースサーチ (力まかせ探索。brute-force search) を実行した場合、

【数2】

$$O(\sqrt{N})$$

10

の二次高速化 (平方的高速化。quadratic speedup) しか達成できず、これが最適であることが証明されている。

【0021】

したがって、本実施形態によれば、署名プロセスは、署名を保護するために、秘密鍵の事前イメージの知識のゼロ知識証明において重ねるように拡張される。次いで、拡張された検証プロセスは、この証明を検証して、署名が量子能力のある敵対者ではなく、秘密鍵の所有者によって真に作成されたものであることを確認することができる。後方互換性のために、既存の検証プロセスは、耐量子保証を失うものの、証明なしでデジタル署名を依然として検証することができる。

20

【0022】

本実施形態による有利な解決策を実装するために、古典的なデジタル署名方式の三重多項式時間アルゴリズム (すなわち、式 (1)、(2) および (3)) を拡張する。本実施形態による拡張された耐量子デジタル署名方式は、多項式時間アルゴリズムである $KeyGen_q$ 、 $Sign_q$ 、および $Verify_q$ の三重として定義される。アルゴリズム $KeyGen_q$ は、 n の暗号鍵強度を定義するセキュリティパラメータ 1^n を取り込み、秘密の事前イメージパラメータである事前イメージ p 、および公開鍵 K_p を出力する。 K_p は秘密鍵 $H(p)$ に関連付けられた公開鍵であり、秘密鍵の計算である $H()$ は、崩壊 (折り畳み。コラプシング。collapsing) ハッシュ関数である。アルゴリズム $Sign_q$ は、メッセージ M および秘密の事前イメージ p を取り込み、 $Sign(M, H(p))$ を使用して計算された署名 σ 、および耐量子ゼロ知識証明 π を出力し、ここで、 $H(p)$ は p から計算され、 σ は $H(p)$ から計算され、耐量子ゼロ知識証明 π は、秘密鍵 $H(p)$ の少なくとも一部に応答して生成される。秘密鍵 $H(p)$ は、事前イメージ p に対してハッシュ鍵導出を行うか、事前イメージ p に対して一方向性関数鍵導出を行うか、または事前イメージ p に対して対称鍵導出を行うことによって生成することができる。公開鍵 K_p は秘密鍵 $H(p)$ に関連付けられるので、公開鍵 K_p は、事前イメージ p に対してハッシュ鍵導出を行うか、事前イメージ p に対して一方向性関数鍵導出を行うか、または事前イメージ p に対して対称鍵導出を行うことによって生成することもできる。

30

40

【0023】

検証のために、アルゴリズム $Verify_q$ は、メッセージ M 、公開鍵 K_p 、および署名 σ を取り込み、 $Verify(M, K_p)$ が承諾を返し、 π が、 p から σ が計算されたことの知識の有効なゼロ知識証明である場合およびその場合に限り、メッセージ M のソース (source) を認証するために「承諾」を出力する。これらの関係は、式 (4)、(5) および (6) に示される。

【数3】

50

$$\text{KeyGen}_q(1^n) \Rightarrow \{\rho, K_p\} \quad (4)$$

$$\text{Sign}_q(M, \rho) \Rightarrow \{\sigma, \pi\} \quad (5)$$

$$\text{Verify}_q(M, K_p, \sigma, \pi) \Rightarrow \{\text{結果}\} \quad (6)$$

【0024】

直感的に、本実施形態によるデジタル署名方式は、秘密鍵に耐量子の付加的なレイヤを配置して、古典的なデジタル署名方式の古典的なセキュリティ特性を継承している。Sign_qから得られる追加の情報は、秘密の事前イメージρまたは秘密鍵K_s = H(ρ)を明らかにしないゼロ知識証明であるため、古典的な敵対者は、署名当事者と対話する際にVerify_qの健全性を危うくすることはできない。

10

【0025】

このように、本実施形態による耐量子デジタル署名方式は、署名σおよび証明πを検証するためにVerify_qが使用されるならば、Sign_qを使用して生成されたデジタル署名に対して、さらなる耐量子を有利に提供することを理解でき、ここで、証明πは、署名当事者によって提供される、秘密鍵の事前イメージρの知識の量子安全証明であり、したがって、証明πは、検証者によってアクセス可能であり、デジタル署名σがρから計算されることを量子安全に証明するために使用される。

20

【0026】

本実施形態によるデジタル署名方式に対するさらなる耐量子は、量子能力のある敵対者が、K_pからH(ρ)を復元するためにショアのアルゴリズムを使用することができると仮定することによって示すことができる。H(ρ)を使用することで、敵対者は、Verifyによって承諾される有効な署名σを、Signを使用して任意に生成することができる。しかしながら、H()は崩壊ハッシュ関数であり、量子コンピュータからのものであっても、事前イメージ攻撃には耐性があるので、署名ρの値は秘密鍵H(ρ)の計算から復元できないため、敵対者は証明πを生成することはできない。したがって、Verify_qは量子能力のある敵対者に対して耐性がある。

30

【0027】

さらに、本実施形態によるデジタル署名方式のKeyGen_qおよびSign_qを使用する署名当事者は、古典的なデジタル署名方式のVerifyアルゴリズムを使用する検証当事者と後方互換性のある署名σを有利に生成することが理解できる。

【0028】

本実施形態による耐量子デジタル署名方式の後方互換性は、Sign_qによって戻される署名σが、H(ρ)が効果的にK_sと等しい同じアルゴリズムSignを使用して生成されるという事実によって証明される。したがって、Verifyを使用する任意の検証当事者は、πを無視し、MおよびK_pに関する署名σの有効性を確認するためにVerifyを呼び出し続けることができる。

40

【0029】

このように、本実施形態による耐量子デジタル署名方式を実現するために、デジタル署名アルゴリズム、ハッシュ関数、およびゼロ知識証明システムが含まれることを理解することができる。

【0030】

DSAまたはECDSAのいずれかは、本実施形態による耐量子デジタル署名方式のデジタル署名アルゴリズムとして容易に使用することができる。これは、DSAおよびECDSAの秘密鍵ジェネレータは、本質的に、有限体上で生成される予測不可能な乱数であり、これは、有利なことに、一方向ハッシュ関数H()の出力とうまく一致するからである。RSAを署名アルゴリズムとして使用することは、より複雑で面倒である。なぜなら

50

、鍵の生成には、ハッシュ関数の出力と、RSAモジュラス(modulus)を計算するために使用される2つ以上の予測不可能な素数との照合(matching)が含まれるからである。可能な技術には、ハッシュ出力を非常に大きな素数の順序付きリストにマッピングすること、または素数が見つかるまで乱数を繰り返しハッシュ(またはマイニング)することが含まれる。より単純な実装のために、ECDSAが使用される。なぜならこれは最小の証明サイズに変換される最小の鍵サイズを有するからであり、選択される可能性のある曲線は、本明細書における実施態様の例に使用されるsecp256r1(またはprime256v1)である。

【0031】

本実施形態に従って使用され、本明細書における実施態様の例に使用されるハッシュ関数はSHA-256である。なぜならこれは崩壊であり、出力がsecp256r1曲線に十分に適合するからである。

【0032】

本実施形態による耐量子デジタル署名方式で使用されるゼロ知識証明システムは、ポスト量子安全でなければならない。そのようなゼロ知識証明システムの1つがZKBooであり、これは3分岐MPC-in-the-headの実現であり、既にSHA-256の実装が整っている。したがって、ZKBooは、本明細書における実施態様の例についてのゼロ知識証明システムとして利用される。

【0033】

図1を参照すると、本実施形態による例示的な耐量子ECDSA鍵生成アルゴリズムKeyGen_q100が示される。鍵生成アルゴリズムKeyGen_q100は、公開鍵K_pを計算する前に秘密事前イメージpをハッシュするために実行される追加ステップ110(ステップ4を参照のこと)を除いて、KeyGenと非常に同様に機能する。

【0034】

図2を参照すると、本実施形態による例示的な耐量子ECDSA署名アルゴリズムSign_q200が示される。秘密鍵H(p)を使用してECDSA署名を計算する以外に、Sign_q関数は、H(p)の事前イメージの知識のゼロ知識証明、公開鍵K_pがH(p)から計算されることのゼロ知識証明、およびH(M)が署名されるメッセージであることのコミットメントを含むZKBoo証明πを戻す。

【0035】

ステップ210(ステップ10)における本実施形態による実装は、GiacomelliのSHA-256コードを使用する。証明πの計算ステップの数によって秘密鍵K_sが明らかになる可能性があるため、次のステップ220(ステップ11)を符号化するには特に注意が必要である。例えば、秘密鍵K_sが生成された後に公開鍵K_pを計算する場合、楕円曲線暗号(ECC)の式は、 $K_p = K_s \cdot G \bmod P$ であり、ここで、Gは楕円曲線上の既知のベースポイントであり、Pは曲線の次数である。通常の計算下では、GはK_s倍されたドット積となる。K_sは1から 2^{256} の値であり、乗算にはビットシフト法が使用されるため、K_pを得るためには1から256のドット積乗算を実行する必要がある。MPC-in-the-headのゼロ知識証明下では、K_pを計算するのに必要な回路のゲート数が証明に示され、これは、誰かが証明回路のサイズを解析すれば、K_sの値が明らかになることを意味する。したがって、本実施形態に従い、秘密鍵K_sの値をさらに有利に遮蔽／隠蔽するために、K_sの値に関係なく、予め定義された数のドット積乗算を実行する回路を作成し、それによって公開鍵計算の回路数を固定したままにする。本実施態様では、楕円曲線がsecp256r1曲線であるため、予め定義された計算回数は256回である。さらに、楕円曲線乗算を実行する場合、モンゴメリ・ラダー・ダブル・アンド・アッド・オールウェイズ(Montgomery ladder double-and-add always)技術を有利に実装することで、セキュリティレベルをさらに高め、タイミング攻撃および電力サイドチャネル攻撃(すなわち、攻撃者が秘密鍵から公開鍵を計算する際の時間または消費電力を測定する場合)を防ぐ。

【0036】

図3を参照すると、本実施形態による例示的な耐量子E C D S A検証アルゴリズムV e r i f y_q 3 0 0が示される。

【0037】

耐量子E C D S A検証アルゴリズムV e r i f y_q 3 0 0は、2つの部分から構成され、第1の部分310（ステップ5からステップ12まで）は、V e r i f yと同様のE C D S A署名検証であり、一方、第2の部分320（ステップ14からステップ20まで）は、本実施形態による耐量子ゼロ知識証明の追加検証である。

【0038】

本実施形態による耐量子デジタル署名方式の例示的な実装は、Cで実装され、64ビットのM i c r o s o f t W i n d o w s 1 0上でC y g w i n端末を実行する、8 C P Uコアおよび8 G BのR A Mを備えたI n t e l I 5 - 8 2 5 0 U第8世代マシンでテストされた。オペレーティングシステムレベルのC P Uスケジューリングまたは調整は行わなかった。Z K B o oのラウンド数を50から250まで50刻みで変化させた場合のS i g n_qおよびV e r i f y_qの実行時間、ならびに証明サイズを測定した。ラウンド数を増やすと、証明のビット強度は増加するが、表1に示すように、証明サイズおよび実行時間も不注意に増加する。

【0039】

【表1】

ZKBooラウンド	50	100	150	200	250
証明サイズ（キロバイト）	1,978	3,956	5,934	7,912	9,890
Sign _q 実行時間（秒）	20.9	45.9	72.9	95.1	118.2
Verify _q 実行時間（秒）	19.6	45.0	71.0	93.2	115.7

表1

【0040】

一見したところ、250ビットの強度の証明について測定されたオーバーヘッドは、約10 M Bのサイズの非常に大きな証明を示し、S i g n_qまたはV e r i f y_qのいずれかを実行するためにほぼ2分かかる。しかしながら、本明細書以下で論じられる本実施形態による耐量子デジタル署名方式の実際の展開実装は、証明を非同期的に生成し、証明書とは別に記憶する（すなわち、証明を第1のデジタル場所に記憶し、証明書を第2のデジタル場所に記憶する）ことができるため、ユーザエクスペリエンスへの影響を低減することができる。これにより、並列処理または非同期検証を有利に行うことができ、ユーザエクスペリエンスへの影響をさらに低減することができる。

【0041】

後方互換性および耐量子への移行に関連する問題を研究するために、耐量子デジタル署名方式の実際の展開実装として、既存の（変更されていない）A d o b e A c r o b a t R e a d e r D Cを使用して耐量子タイムスタンプ署名付きP D Fを要求しながら、本実施形態による耐量子デジタル署名方式をタイムスタンプサーバに展開した。展開は、クライアントおよびサーバの両方に64ビットのM i c r o s o f t W i n d o w s 1 0を実行する、8 C P Uコアおよび8 G B R A Mを備えたI n t e l I 5 - 8 2 5 0 U第8世代マシンを搭載したラップトップで実行された。セットアップには、タイムスタンプクライアントおよびタイムスタンプサーバが含まれた。タイムスタンプクライアントには、A d o b e A c r o b a t R e a d e r D C v 2 0 2 1 . xを使用した。なぜならこのクライアントは既にE C D S Aをサポートしており、変更せずに使用することができたからである。タイムスタンプサーバには、P i e r r e - F r a n c o i s C a r p e n t i e rによるオープンソースのタイムスタンプサーバ（<https://github.com/kakwa/uts-server>から）を、コードを変更せずに使用した。

【0042】

暗号ライブラリとして、タイムスタンプサーバは、OpenSSL v1.1.xを使用して、サーバ証明書の認証局（CA）発行のオペレーションを実行し、さらにRFC3161に従ったデジタル署名を実行する。OpenSSL v1.1.1bのバージョンは、X.509証明書の発行およびタイムスタンプの両方についての拡張されたデジタル署名方式を実行するように変更された。ZKBoo証明を非同期的に生成しながら、OpenSSLがECDSA署名を戻すように最適化を行った。これにより、ZKBoo証明が完全に生成されるのを待たずに、ECDSA署名付きタイムスタンプをクライアントに戻すことができるようになった。したがって、証明は証明書とは別に記憶された。

【0043】

証明書およびタイムスタンプについての耐量子256ラウンドZKBoo証明は各々10メガバイトであったため、それらはクライアントに容易に送信することができなかった。そのため、署名されたX.509証明書または呼び出しプログラムに戻されたPKCS#7タイムスタンプにURLリンクを埋め込みながら、OpenSSLの修正バージョンは、証明をDropbox (www.dropbox.com) に書き込んだ。

【0044】

図4を参照すると、プロセス図400は、テスト中の本実施形態による耐量子デジタル署名方式の実際の実装のユースケースを示す。上記に示したように、この実装により、エンドユーザ401がタイムスタンプクライアントとしてAdobe Acrobatリーダー402を使用することが可能であった。この実装には、証明書の発行およびタイムスタンプにOpenSSL 406を使用するタイムスタンプサーバ404も含まれており、OpenSSL 406は証明をDropbox 408に書き込む。

【0045】

1回のみ行われるセットアップフェーズ410では、OpenSSL 406を使用してルートCA証明書についての鍵および証明書を生成し（412）、さらにOpenSSL 406を使用してタイムスタンプサーバ証明書についての鍵および証明書を生成する（414）。図5の画像500のウィンドウ510、520に示されるように、中間CAを必要とせずにルートCAがサーバ証明書を証明する、本実施形態に従って定義される証明書階層（certificate hierarchy）が採用される。どちらの証明書も、Dropbox 408の耐量子証明を指すデジタル記憶場所情報として、X.509機関情報アクセス（Authority-Information-Access）拡張下でリンク416、418を含む。運用上、デジタル記憶場所（location）は、認証局またはデジタル記憶場所情報を使用して検証者がアクセス可能なパブリックリポジトリ（public repository）であり得る。ルートCA証明書は、エンドユーザ401にダウンロードされ（420）、次いでAdobe Acrobat 402にインポートされて（422）、信頼へのルート（root-to-trust）を確立する。

【0046】

RFC3161フェーズ430では、PDF文書は、エンドユーザ401がPDFを開いた後（432）に、Adobe Acrobat 402からタイムスタンプサーバ404へのリクエストを開始すること（434）によって、タイムスタンプを付与することができる。タイムスタンプサーバ404は、リクエスト436をOpenSSL 406に送信し、ECDSA署名付きPKCS#7タイムスタンプを受信し（438）、これはAdobe Acrobat 402に提供される（440）。タイムスタンプ署名証明442も同様に、タイムスタンプに埋め込まれたURLリンクと共にDropbox 408に記憶される。このタイムスタンプは、Adobe Acrobat 402によって検証され（444）、エンドユーザ401による後の認証446のためにPDFに保存され得る。検証の例を図6の画像600に示す。修正されていないAdobe Acrobatは、ECDSA署名付きタイムスタンプおよび証明書チェーンのみを検証し、ZKBoo証明は検証しないため、エンドユーザが経験する待ち時間に変化がないことに留意

10

20

30

40

50

されたい。

【0047】

アップグレード後のフェーズ450では、Verify_qを実行できる任意の検証当事者は、証明書／署名ブロックに見出されるリンクをたどって(452)、耐量子ECDSA検証アルゴリズム300(図3)に従った完全な署名検証のための耐量子証明をダウンロードすることができる(454)。

【0048】

耐量子デジタル署名方式に徐々に移行するシステムへの影響を理解するために、移行の異なる段階における署名当事者および検証当事者について、異なる結果を表2に列挙する。表2から分かるように、本実施形態に従った耐量子のレイヤ(階層化、layer)への適切な移行戦略は、まず署名当事者をアップグレードして署名に耐量子証明を含めるようにし、その後、検証当事者をアップグレードして証明を検証できるようにすることである。早期にアップグレードすることを選択した検証当事者に関して、まだアップグレードしていない可能性のある署名当事者との互換性を維持するために、本明細書上に論じた古典的なデジタル署名方式に従ってVerify機能を含めることが推奨される。

【0049】

【表2】

	検証当事者	
	定義1 ¹	定義2 ²
署名当事者	定義1 ¹ これが「現状のまま」のシナリオである。署名された文書は、ポスト量子時代には偽造に対して脆弱である。	署名付きの書類には耐量子証明は含まれない。検証当事者は、文書を拒否するか、または署名当事者に移行を実行するように通知しながら、Verifyを使用して署名を確認するかのいずれかを選択する。
	定義2 ² これが移行プロセスの適切な「ステップ1」である。署名された文書には、耐量子証明も含まれる。署名当事者は、このステップを実行する前に、検証当事者が移行するのを待つ必要はない。検証当事者は、耐量子証明を無視しながら署名の検証を続ける。	これが「将来」の状態であり、移行プロセスの適切な「ステップ2」である。署名当事者が移行し、耐量子証明を含む署名付き文書の送信を開始した後、検証当事者はシステムをアップデートして署名および証明を検証し、移行プロセスを完了することができる。

¹まだ移行されていない。依然として定義1のKeyGen、Sign、およびVerifyを使用する。

²移行が完了した。定義2のKeyGen_q、Sign_q、およびVerify_qを使用してアップグレードした。

表2

【0050】

本実施形態による耐量子デジタル署名方式の利点は、当業者には容易に明らかであり、今日の技術で制定することができる。より強力な量子コンピュータがオンラインになるにつれて、ポスト量子期限(post-quantum deadline)が迫っており、本実施形態による耐量子デジタル署名方式の利点は、安全で認証可能な通信のために必要不可欠となるであろう。ポスト量子期限の参考として、NISTは、2030年までに、10億ドルの予算でRSA-2048の暗号解読が可能な量子コンピュータを構築できる可能性が高いことに言及した報告書を提供している。この問題に対処するために、NISTは適切な量子安全デジタル署名および鍵交換アルゴリズムを選択するポスト量子標準化作業に着手している。最終的な選択はまもなく完了し、新しい標準は2024年までに公表される予定であると予測される。これとは別に、NISTはまた、2つのステートフ

ルハッシュベースの署名、すなわち `Leighton-Micali` 署名および `extended-Merkle` 署名方式を条件下でのポスト量子使用に推奨している。

【0051】

2024年以降の新しいシステム実装では、業界は新しいデジタル署名標準の採用を検討するよう奨励する可能性が高いが、既存または今後のシステムには異なる課題が予想される。

【0052】

デジタル署名を量子的に安全なものにするための直感的なアプローチは、量子的に安全な代替アルゴリズムまたは追加アルゴリズムを使用することである。NISTのポスト量子標準化作業により、現在、2つの格子ベースのアルゴリズムである、`Dilithium` および `Falcon`、ならびに1つの多変量ベースのアルゴリズムである、`Rainbow` が3つの最終候補のデジタル署名アルゴリズムとして特定されている。3つの代替アルゴリズム、すなわち、多変量ベースの `GeMSS`、ゼロ知識ベースの `Picnic`（これは、`ZKB++` を作成するための基礎となる証明システムとして、本実施形態の実装で説明されているゼロ知識証明システムである `ZKBoo` も使用する）、およびステートレスハッシュベースの `SPHINCS+` が候補に挙がっているが、2024年の期限を超えてさらなる評価を受ける予定である。理想的には、ソフトウェアライブラリまたはハードウェアセキュリティモジュールの形式で「ドロップイン交換 (`drop-in replacement`)」を使用して、`RSA/DSA/ECDSA` を標準化される新しいアルゴリズムと入れ替えるか、または増強する。しかし、これらのアルゴリズムの各々は、固有のリソース、パフォーマンス、およびプラットフォームに関する考慮事項を有し、異なるキーセレモニープロセス (`key ceremony processes`) およびプロトコルと相まって、移行プレイブックを設計し、実行する必要がある可能性が高い。

【0053】

別のアプローチは、漏洩した場合に通常の署名鍵を上書き（オーバーライド。 `override`）できるバックアップ鍵を使用することである。1つの提案は、耐量子ステートフルハッシュベースの `WOTS+` バックアップ鍵を使用することであり、このバックアップ鍵は、鍵生成プロセス中に作成され、元の鍵が漏洩または紛失した場合にフォールバック (`fallback`) 手順として使用することができる。このようなバックアップデジタル署名鍵のアプローチは、認証関連プロトコルのアカウント回復メカニズムとして機能するが、データの長期的な否認防止が必要な日常的な非インタラクティブデジタル署名のユースケースには適していない。

【0054】

タイムスタンプのユースケースに特化すると、順方向または逆方向のいずれかで連鎖させる一連のハッシュの使用は、長期的な、おそらく量子安全な、タイムスタンプを提供するための周知のアプローチであり、これは、線形ハッシュチェーンを通じて、またはマール (`Merkle`) ツリーを通じて、タイムスタンプされる文書のシーケンスをリンクすることによって、デジタルタイムスタンプを含むことができる。今日、イーサリウム (`Ethereum`) のようなブロックチェーンは既にタイムスタンプのスマートコントラクトをサポートしており、ブロックチェーン上の分散型タイムスタンププロトコルを提供し得ることにより、事前／事後の日付を防ぐことができる。これらの技術は典型的に、特定の発生時刻を決定するために公開された検証可能なチェーンに依存しているため、一般的にデジタル署名を保護するための耐量子メカニズムとしては適用可能ではない。また、パブリックブロックチェーンは、実行されたトランザクション (`transactions`) の数およびトランザクションが行われたタイミングが公開されているため、プライバシーに関する懸念にも直面する。

【0055】

このように、本実施形態は、安全で認証可能な通信における既存および今後の脆弱性に有利かつ効率的に対処する現在の解決策を提供する耐量子デジタル署名方式を提供することを理解することができる。本実施形態による耐量子デジタル署名方式は、ポスト量子デ

10

20

30

40

50

デジタル署名の実装において異なるアプローチをとる。異なる量子安全デジタル署名アルゴリズムに置き換えるか、または追加する代わりに、本実施形態による耐量子デジタル署名方式は、より長期的な耐量子を達成しながら、古典的なRSA、DSA、またはECDSAデジタル署名アルゴリズムを使用することを継続することを可能にする。これは、デジタル署名に加えて、秘密鍵の事前イメージの知識のゼロ知識証明を重ねることによって達成される。本実施形態による耐量子デジタル署名方式では、量子への対応を進めたいデジタル署名実装は、既存のアプリケーションとの後方互換性を維持し続けることができる。これは、異なるシステムが、量子対応への移行がいつ行われるかについて異なるタイムラインおよびスケジュールを有する可能性がある一方で、本実施形態による耐量子デジタル署名方式は、アップグレードしたアプリケーションとアップグレードしていないアプリケーションとの間でシームレスな動作を確保（ensure）できるため、非常に有利である。

10

【0056】

例示的なPDF文書タイムスタンプ方式に関して本明細書で上述した本実施形態による耐量子デジタル署名方式を適用したが、耐量子を重ねるために本実施形態によるデジタル署名方式を利用することができるブロックチェーン、セキュア電子メール、およびトランスポートレイヤセキュリティなどの他のアプリケーションもある。

【0057】

本実施形態の前述の詳細な説明において例示的な実施形態を提示したが、膨大な数の変形例が存在することを理解されたい。さらに、例示的な実施形態は例示に過ぎず、本発明の範囲、適用性、動作、または構成を何ら限定することを意図していないことを理解されたい。むしろ、前述の詳細な説明は、本発明の例示的な実施形態を実装するための便利なロードマップを当業者に提供するものであり、添付の特許請求の範囲に記載された本発明の範囲から逸脱することなく、例示的な実施形態に記載されたステップの機能および配置、ならびに動作方法において様々な変更がなされ得ることが理解される。

20

【図面】

【図1】

アルゴリズム1：耐量子ECDSA鍵生成 $KeyGen_q$

```
1 開始
2  $G \leftarrow$  ECCベースポイント;  $P \leftarrow$  ECCオーダー;
3 秘密事前イメージ $\rho$ を生成する;
4 秘密鍵 $K_s = H(\rho)$ を計算する;
5 公開鍵 $K_p = (x, y)$ を計算する ここで、 $K_p \equiv K_s \cdot G \bmod P$ ;
6  $K_s$ を破壊する;
7  $\rho, K_p$ に戻る;
8 終了
```

100

【図2】

アルゴリズム2：耐量子ECDSA署名 $Sign_q$

```
1 開始
2  $G \leftarrow$  ECCベースポイント;  $P \leftarrow$  ECCオーダー;
3  $\rho \leftarrow$  秘密事前イメージ;
4  $M \leftarrow$  メッセージ;
5 署名ランダム $r$ を生成する;
6  $r^{-1}$ を計算する ここで、 $r \cdot r^{-1} \equiv 1 \bmod P$ ;
7  $R = (R_x, R_y)$ を計算する ここで、 $R \equiv r \cdot G \bmod P$ ;
8 メッセージのハッシュ $H(M)$ を計算する;
9 ZKBooの証明を列挙する $\pi$ を開始
10 秘密鍵 $K_s$ のゼロ知識計算 ここで、 $K_s = H(\rho)$ ;
11 公開鍵 $K_p$ のゼロ知識計算 ここで、 $K_p \equiv K_s \cdot G \bmod P$ ;
12  $s$ を計算する ここで、 $s \equiv r^{-1} * (H(M) + R_x * K_s) \bmod P$ ;
13 証明において $R_x, s$ をコミットする;
14 終了
15  $r, r^{-1}, K_s$ を破壊する;
16  $\sigma = \{R_x, s\}, \pi$ を戻す;
17 終了
```

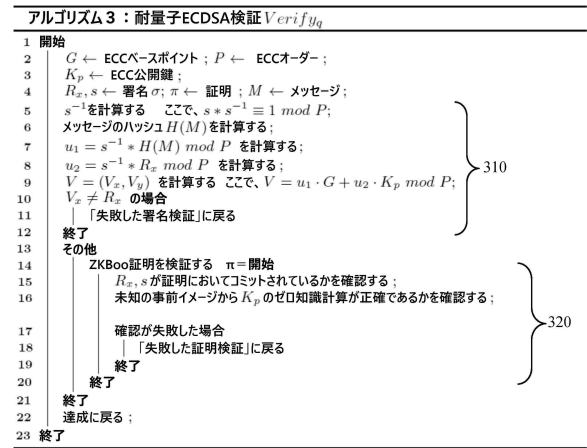
200

30

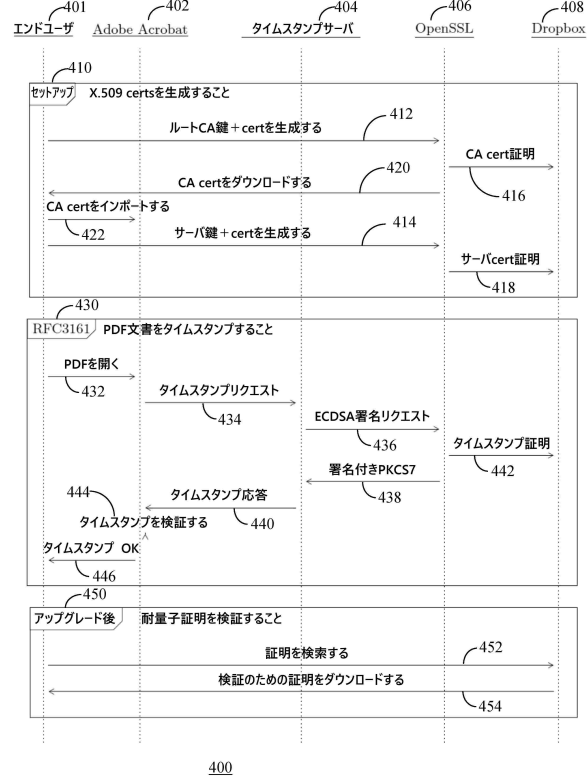
40

50

【図 3】



【図 4】



【図 5】



【図 6】



10

20

30

40

50

【国際調査報告】

INTERNATIONAL SEARCH REPORT		International application No. PCT/SG2022/050769
A. CLASSIFICATION OF SUBJECT MATTER H04L 9/32 (2006.01) G06F 21/64 (2013.01) According to International Patent Classification (IPC)		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) H04L; G06F Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) FAMPAT: signature, signing, 签名, 签字, 签章, 签署, 署名, proof of knowledge, zero knowledge, statement of proof, ZKP, 知识证明, 语句证明, private key, secret key, key, 私钥, 密钥, 钥, pre-image, seed, hash, 原像, 种子, 哈希, original, pre, previous, prior, before, map, 原, 前, value, function, parameter, 值, 参数, validate, verify, check, confirm, 确认, 证明, 鉴证, quantum, 量子, adversary, attack, hack, malicious, intrusion, safe, resistant, protect, 攻击, 破解, 恶意, 侵扰 and similar terms; IEEE: quantum, attack, adversary, hack, intrusion, safe, resistant, signature, key, proof, ZKP, pre-image		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2021/0297255 A1 (WAN Z. ET AL.) 23 September 2021 Par. [0065]-[0077]	1 – 24
A	WO 2021/102443 A1 (XX LABS SEZC) 27 May 2021 Pages 2 and 14-16; Figures 1 and 5	1 – 24
A	Tan T.G. et al. A Survey of Digital Signing in the Post Quantum Era. 1 December 2019 [Retrieved on 2023-05-24 from https://eprint.iacr.org/archive/2019/1374/20191201:205800] Whole document	1 – 24
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
*Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "D" document cited by the applicant in the international application "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 24/05/2023 (day/month/year)		Date of mailing of the international search report 05/06/2023 (day/month/year)
Name and mailing address of the ISA/SG  Intellectual Property Office of Singapore 1 Paya Lebar Link, #11-03 PLQ 1, Paya Lebar Quarter Singapore 408533 Email: pct@ipos.gov.sg		Authorized officer Teo Ailing (Dr) IPOS Customer Service Tel. No.: (+65) 6339 8616

INTERNATIONAL SEARCH REPORT
Information on patent family membersInternational application No.
PCT/SG2022/050769

Note: This Annex lists known patent family members relating to the patent documents cited in this International Search Report. This Authority is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2021/0297255 A1	23/09/2021	WO 2020/114240 A1 CN 110781521 A CN 109614820 A	11/06/2020 11/02/2020 12/04/2019
WO 2021/102443 A1	27/05/2021	CN 115552397 A US 2023/0006836 A1 EP 4062299 A1	30/12/2022 05/01/2023 28/09/2022

10

20

30

40

50

フロントページの続き

MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,N
E,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,
CV,CV,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,IR,IS,I
T,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,
MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,
SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

弁理士 小菅 一弘

(72)発明者 タン テイク グアン
シンガポール 038987 テマセック ブールバード 7 ナンバー12-07 サンテック タウ
ー ワン

(72)発明者 チョウ ジャンイン
シンガポール 487372 ソマパー ロード 8