（ 続紙 1 ）

京都大学	博士（情報学）	氏名	Quan Yuan
論文題目	A Study on Hash-based Signature Schemes （ハッシュ関数に基づく署名方式の研究）		

（論文内容の要旨）

ディジタル署名は現代暗号の基本機能の一つである認証機能を提供する暗号技術である。多くの実用的な情報システムにディジタル署名が用いられており、情報社会を支える重要な基盤技術となっているが、近年では量子計算機による攻撃能力の向上に備えた「ポスト量子（計算機）安全（Post-Quantum Secure）」なディジタル署名方式の開発が求められている。ポスト量子安全なディジタル署名の構成に関しては、格子理論、同種写像、多変数多項式などに基づく、量子計算機での効率的な解法が知られていない構造を利用するアプローチが検討されている。加えて、特定の構造に拠らず、抽象化されたハッシュ関数のみを利用して構成する署名方式はハッシュベース署名と呼ばれ、ポスト量子安全な署名方式を構成する有望なアプローチの一つと考えられている。ハッシュベース署名には、一つの具体的なハッシュ関数の安全性が損なわれた場合でも他のハッシュ関数で代替して署名方式としての安全性を維持できるという設計上の柔軟性や、演算が単純で高速なハッシュ関数を利用して効率を上げられるなどの優位点があり、古くから古典的な安全性概念の下で効率化の研究が行われてきたが、ポスト量子安全性に関しては基礎理論の充実と、より効率の良い具体的な方式の開発が望まれている。本論文は、ハッシュベース署名に関して、基礎的な安全性概念の検討から具体的構成の提案まで広範なテーマに取り組み、構成部品であるハッシュ関数のポスト量子安全性の解析、ステート付き署名の安全性概念の定式化、量子クエリに対応した強い安全性概念の下での具体的ハッシュベース署名の安全性解析、という三つの課題における研究結果について述べたものである。

本論文は全六章で構成されている。

第一章では研究の背景と結果の概要が述べられている。ハッシュベース署名の概説に続き、ブラックボックス構成の概念を説明し、本論文第三章から五章で述べる三つの課題と結果について概説している。

第二章では、第三章以降で用いられる記法や用語の定義のほか、解析に必要な擬似ランダム関数などの定義を与えている。

第三章では、ハッシュ関数のサブセット耐性に関する三つの結果を述べている。サブセット耐性ハッシュ関数族（SRH）はサブセット耐性という安全性を満たすハッシュ関数の族であり、HORS等のワンタイム署名の構成に用いられているが、そのポスト量子安全性については十分に研究されていない。本章では、まず、量子計算機によるサブセット耐性に対する一般的な攻撃方法を提案し、その効率を解析する。次に、よく知られた概念である決定的衝突困難性とサブセット耐性の関係を解析し、SRHの存在は決定性衝突困難性を満たすハッシュ関数の存在を意味することを示す。最後に、より一般的な仮定である一方向性置換からSRHをブラックボックス的に構成することが不可能であることを証明する。

第四章では、ステートフル署名方式の安全性の定式化と他の安全性概念との関係を論じている。ステートフル署名は署名を発行する毎に署名者が保持するステートと呼ばれる情報を更新する必要がある署名方式であり、多くのハッシュベースの署名方式で採用されている構成である。ステートフル署名に対する古典的な安全性概念は、ステートが攻撃者に見えないことを前提としているが、現実の運用ではそのような仮定は

必ずしも成立しない。本章では、ステートが攻撃者に漏洩する、あるいは攻撃者がステートを変更できるといった状況における安全性を定式化し、それらの概念間の関係を示している。
第五章では、ステートのないハッシュベース署名方式における量子アクセス安全性を解析している。従来、ディジタル署名方式の安全性は、選択メッセージ攻撃に対して安全であることが妥当と考えられてきた。すなわち、多項式時間（量子）攻撃者は、攻撃者が任意に選んだメッセージに署名できる署名オラクルが与えられても、新たなメッセージに対する署名を偽造することはできない、という安全性である。この署名オラクルは古典的なものであり、署名を要求する各クエリに対して1つのメッセージにしか署名できない。ところが、署名オラクルが量子計算機である場合、量子状態のメッセージに直接署名できるため、一つのクエリが一つのメッセージに対応するとは限らない。このような量子署名オラクルへのアクセスを攻撃者に許す強い攻撃モデルに関して、本章では以下の結果を示している。まず、回数限定のステートレスハッシュベース署名に対して、古典的安全性と量子アクセス安全性を含む一般的な安全性を示す。次に、既存の（回数限定でない）ステートレスハッシュベース署名方式に対する量子アクセス攻撃の効率を解析する。この解析から、古典的な選択メッセージ攻撃よりもはるかに小さな時間計算量で攻撃が成功し、これらの方式にとって量子アクセス攻撃が古典的な攻撃よりも大きな脅威であることを示す。最後に、具体的なハッシュベース方式であるSPHINCS+を改良し、その量子アクセス攻撃に対する安全性を証明する。提案の方式は量子アクセス攻撃に対する安全性が証明された初めてのステートレスハッシュベース署名方式である。
第六章は、上記三つの課題に対する結果が示唆する安全性解析とより強い安全性モデルの重要性を訴えるとともに、今後の研究の方向性を示す未解決の課題について述べている。

（続紙 ２ ）

（論文審査の結果の要旨）

本論文の主題であるディジタル署名は情報化社会において安全なデータ流通を可能にする基盤技術であり、マイナンバーをはじめ実社会の様々な情報システムで利用されている。ある時点で安全とされた方式であっても、計算リソースの増大やネットワークの高度化による攻撃者の能力向上に対応してその安全性は再評価されねばならず、新たな脅威に対応して安全なディジタル署名方式を開発することは情報化社会の維持発展に不可欠である。将来予想される量子計算機が実現すると現在普及しているディジタル署名方式は多項式時間で破れることが知られている。本論文では、量子計算機に対しても安全なディジタル署名を構成する幾つかの有力なアプローチのうち、ハッシュベース署名を研究対象としている。ハッシュベース署名はNIST（米国立標準技術研究所）が進めるポスト量子安全なディジタル署名の標準化においても有力な候補の一つであり、その安全性の探求は社会的に意義がある研究課題であると言える。本論文第一章ではハッシュベース署名の重要性が社会的・技術的観点で述べられており、研究動機が明確に示されている。

本論文では、ハッシュベース署名の安全性に関する三つの課題に取り組んでいる。まず第三章では、ハッシュベース署名を構成する基本部品であるハッシュ関数に求められる安全性の一つであるサブセット耐性について、量子計算機による攻撃を想定して解析を行い、すでによく知られた決定的衝突困難性や一方向性置換との帰着・分離係関を解明している。これらは、サブセット耐性という安全性概念がどの程度の妥当性を持つかについて新たな知見を与える結果である。

第四章では、既存の多くのハッシュベース署名が準ずるステートフル構成の安全性を論じている。ステートは本来署名者が安全に保管すべき内部状態であり、従来の安全性概念では攻撃者に対して秘匿されていることが前提であった。本論文では、一つの署名プロセスの内部状態が他のプロセスと共有される、あるいは悪意あるプロセスの影響を受けるなどの状況を細分化して安全性概念に定式化し、それらの間の関係性を示すことで、より高度かつ妥当な安全性の概念を提唱している。これはより安全なステートフルハッシュベース署名の設計に貢献する結果であると認められる。

第五章では、量子計算機が攻撃ではなく正当な署名生成に使われるようになる将来の状況における署名の安全性を検討している。攻撃者が量子状態のメッセージに対する署名を入手できる環境では、既存のステートレスハッシュベース署名SPINCS+がより偽造されやすくなることを示し、署名サイズの増大と引き換えに安全性を高めた新たな方式を提案している。この結果は既存の標準化候補方式に対して新たな安全性評価をもたらす結果であり、理論と実用の両面で意義のある結果である。

以上、本研究の結果はハッシュベース署名の基礎的な安全性概念から具体的構成方法まで広範囲の課題に対する研究を進展させ、ポスト量子安全な署名方式の実現に貢献するものであると言える。

以上により、本論文は博士（情報学）の学位論文として価値あるものと認める。また、令和４年８月１日に実施した論文内容とそれに関連した口頭試問の結果、合格と認めた。なお、本論文の令和５年９月２５日以降のインターネットでの全文公表についても支障がないことを確認した。

要旨公開可能日： 2022 年 10 月 1 日以降