論 文 の 内 容 の 要 旨

論文題目　　分散台帳向けセキュリティ・プライバシ技術の研究
(Security and Privacy Enhancing Technologies for Blockchain Systems)

氏　　名　　長沼　健

1. はじめに

近年、Bitcoin、Ethereum をはじめとする暗号通貨、及びそのコア技術であるブロックチェーンが新しい金融決済システムとして大きな注目を浴びている。これらブロックチェーンベースの暗号通貨の特徴として、銀行などの中央機関を必要とせず、低い手数料でトランザクションの決済処理を行える点があげられる。一方、エンタープライズ分野では、Hyperledger に代表される特定のノードのみが 分散合意に基づくトランザクション承認処理を行う、許可型分散台帳（以下、 プライベート/コンソーシアム型ブロックチェーンとも称する）の利用が進んでいる。どちらのブロックチェーンシステムにおいても、複数のノード間で台帳情報が共有されるため「誰が誰に送金を行ったか」といった機微な情報が漏洩するプライバシ問題が存在する。また ブロックチェーンシステムでは、公開鍵暗号方式に基づく電子署名によるユーザ認証を利用しているが、署名生成に使用する秘密鍵を紛失すると、ブロックチェーン上の資産も失う問題が存在する。非中央集権型のブロックチェーンでは、特に秘密鍵の安全な管理が大きな課題となっている。

本論文では、上述の台帳情報のセキュリティ・ プライバシ問題に対して、以下の４つ貢献を報告する。

1. 台帳情報のプライバシ問題に対して、ゼロ知識証明を用いた解決方法、特に量子計算機耐性を有する算術回路向けzk-SNARK方式を提案する。
2. 既存の幾つかのゼロ知識証明方式は、信頼できる第3者(TTP)をSetup時に必要とする課題があるが、TTP無しでゼロ知識証明を構成する一般的な方法を提案する。
3. 秘密鍵紛失の課題に対して、生体認証技術を利用した解決方法を提案する。
4. コンソーシアムブロックチェーン上でプライバシを保ちつつネッティング決済を実行するプロトコルを提案する。

2. 分散台帳向けゼロ知識証明技術の研究1

現在、ブロックチェーン分野では、zk-SNARKと呼ばれるゼロ知識証明方式と、そのライブラリlibsnarkの利用が一般的である。このライブラリはペアリング暗号(離散対数問題)を安全性のベースとしているため量子計算機に対する耐性を有していない事が知られている。量子計算機耐性を有するzk-SNARK方式として2018年にGennaroらはSSPs(Square Span Programs)をベースとするdesignated-verifier型のzk-SNARKを提案した。しかし、この方式はブール回路で表現された命題のみを対象としているため、libsnarkで利用されている算術回路との互換性が無い。量子計算機耐性を持ち、かつ算術回路を対象としたzk-SNARKの構成が未解決問題となっていた。

本論文では、QAPs/SAPs表現された算術回路を対象としたdesignated-verifier型のzk-SNARKを3方式提案した。QAPs(Quadratic Arithmetic Programs)とは、算術回路の1つの表現方法で、深さ1の掛算と複数の制約式で回路を表現する。SAPs(Square Arithmetic Programs)は, QAPsの特殊な場合で、掛算が全て2乗の掛算となっている。提案方式の特徴は以下の通りである。

提案方式1の特徴：

提案方式1は、Zcash等の既存方式で最も利用されているPinocchio型のデータフォーマットを流用しQAPベースで構成した。結果、既存システムへの実装が他の方式に比べ容易な点が特徴である。また他の提案方式に比べ、より標準的な仮定で安全性証明が可能な点があげられる。

提案方式2の特徴：

提案方式2はGroth型のzk-SNARK方式を参考に同じくQAPをベースに構成した。特徴としては、ゼロ知識証明値のサイズが比較的小さく(LWE暗号文3つ)、ゼロ知識証明の生成が最も高速な点があげられる(通常, zk-SNARKでは証明の生成がボトルネックとなる)。例えば、Gennaroらの既存方式に比べ、同じ回路サイズに対してゼロ知識証明値の生成が3倍程度高速である。

提案方式3の特徴：

提案方式3はSAPベースに構成した。特徴としてゼロ知識証明値のサイズがより小さい(LWE暗号文2つ)点があげられる。またこの方式は最近Nitulescuによって提案されたzk-SNARKの構成に類似している。

3. 分散台帳向けゼロ知識証明技術の研究2

現在、Pinocchio方式などのゼロ知識証明方式がブロックチェーンでは利用されているが、Pinocchio方式では、信頼できる第3者機関がシステムパラメータを生成しなくてはならない問題がある。例えばZcashでは運営団体がシステムパラメータを生成・公開している。このシステムパラメータ生成時に使用する乱数情報はマスターキーの役割を持ち、万が一漏洩した場合、誰でもfake proofが生成できてしまうため、システム全体の更新が必要となる。また、漏洩しない場合においても第3者機関は自由にfake proofを生成できるため、ブロックチェーンが本来持つ非中央集権性に反する問題があげられる。

Chiesaらは、対話型証明方法の一種であるAlgebraic holographic proofとpolynomial commitment方式からuniversal (証明する回路が変更可能)なzk-SNARKを構成する方法を示した。Polynomial commitment方式とは、暗号化した多項式を検証者に渡し、その多項式のある1点での評価値をゼロ知識証明する技術の総称である。

本論文では、特定の条件を満たすvector commitment方式から、polynomial commitment方式を構成する一般的な方法を示した。代表的なvector commitment方式であるPedersen commitment方式(離散対数問題をベースとする)、Ajtai commitment方式(格子問題をベースとする)は、この条件を満たしている。結果として、Chiesaらの結果と合わせ離散対数問題、格子問題をベースとするuniversalなゼロ知識証明が構成可能となった。

また、この構成方法の特徴として、元々のvector commitment方式が信頼できる第3者機関無し(trustless)で構成可能な場合、それをベースとする方式自体もtrustlessで構成可能な点があげられる。一方で、ゼロ知識証明のデータサイズが、既存方式では定数であったのに対して、提案方式では、回路サイズnに対して$O(\log n)$となる課題がある。

4. 生体認証を用いた秘密鍵管理技術の研究

一般に、ブロックチェーン上のトランザクションの正当性は、ユーザがトランザクションに公開鍵暗号方式をベースとする電子署名を付与し、その正当性をトランザクション検証者が検証することで担保されている。このため、万が一、ユーザが電子署名用の秘密鍵を紛失、漏えいした場合は、ブロックチェーン上の資産損失や、なりすましによる不正取引被害といった問題が発生する。本論文では、このブロックチェーンシステムにおける秘密鍵管理の課題に対して、生体情報から電子署名を生成するPublic Biometrics Infrastructure(PBI)技術を用いた解決方法を提案した。PBIを利用する事で、生体情報を秘密鍵として利用できるため、秘密鍵をストレージに保存する必要が無くなり、秘密鍵の紛失、漏えいといったリスクを軽減する事が可能である。

5．許可型分散台帳向けセキュアネッティングプロトコルの研究

コンソーシアム型ブロックチェーンOSSであるHyperledger Fabricのチャネル機能を用いた非中央集権型のネッティングプロトコルを提案した。提案プロトコルでは、チャネル機能を用いる事で、取引情報の送受信者、金額を秘匿し、更に乱数を用いたマルチパーティー型のネッティングプロトコルを用いる事でネッティングの計算尻も秘匿した。また提案方式は中央サーバなどの特定の中央機関を設置する必要が無く、P2Pにネッティング決済を実行可能である。

6．結論

以上、本論文の主要な成果は以下の 4 点である。

1. 算術回路を対象とした、量子計算機耐性を持つzk-SNARK方式を提案した。計算機実験の結果、既存方式に比べ2～3倍程度、処理性能が改善した。
2. Vector commitment方式からuniversal かつtrustlessなゼロ知識証明を構成する一般的な方法を示した。結果として信頼できる第3者機関無しで、ゼロ知識証明の利用が可能となった。
3. ブロックチェーンにおける秘密鍵管理問題に対して、生体認証を利用した解決方法を提案した。提案システムでは、秘密鍵管理デバイス/サーバを必要としないため、よりセキュアな利用が可能となる。
4. コンソーシアムブロックチェーン向けに、銀行間の非中央集権型のネッティングプロトコルを提案した。提案方式は、中央銀行機関を必要とせず、かつ秘匿性を保ったままネッティング処理が可能である。