Zero-Knowledge Protocols for Code-Based Public-Key Encryption and Their Applications

胡, 荣

https://doi.org/10.15017/1543929

出版情報：九州大学, 2015, 博士（数理学）, 課程博士
バージョン：

（様式６－２）

氏　　名	胡　荣
論　文　名	Zero-Knowledge Protocols for Code-Based Public-Key Encryption and Their Applications (符号ベース公開鍵暗号に対するゼロ知識証明とその応用)
論文調査委員	主査　九州大学　教授　　高木　剛 副査　九州大学　准教授　溝口 佳寛 副査　九州大学　准教授　脇 隼人 副査　台湾大学　准教授　鄭 振牟

論　文　審　査　の　結　果　の　要　旨

本論文では、符号理論に基づく暗号プロトコルの構築と安全性の評価を行った。FOCS 1994 において Shor は、量子計算モデルにより素因数分解問題と離散対数問題が多項式時間で計算可能なアルゴリズムを発表した。Shor のアルゴリズムにより現在普及している暗号（RSA 暗号、楕円曲線暗号、ペアリング暗号など）は危殆化するため、それに代わる量子計算機による攻撃に対して耐性のあるポスト量子暗号を構成する必要がある。ポスト量子暗号の候補の一つとして、符号理論に基づく暗号に関して幾つかの研究結果が報告されてきている。実際、符号理論に基づく基本的な暗号プロトコルとしては、McEliece と Niederreiter による公開鍵暗号方式、Courtois, Finiasz, Sendrier によるディジタル署名、Stern によるユーザ認証方式などが知られている。本博士論文では、これらの基本的な暗号方式だけでなく、更なる高機能な符号理論に基づく暗号プロトコルを提案することを目標としている。

CRYPTO 1993 において Stern はハミング重みがある定数以下となる 2 値ベクトルの 3-pass ゼロ知識証明を構成し、それを応用したユーザ認証プロトコルを提案した。更に、SAC 2010 において Cayrel, Veron, Alaoui は、q 元符号に基づく 5-pass プロトコルを構成した。本博士論文では、直接的に Stern の 2 値方式を q 元 Stern ユーザ認証プロトコルとして拡張し、鍵サイズや計算及び通信コストなどの性能評価を行った。特に、$q=3, 4$ である場合の提案方式は、Cayrel らのユーザ認証プロトコルより効率的であることを示した。実際、$q=3$ の場合に、健全性エラー確率 2^{-16} の 80 ビット安全性を持つ提案方式の通信コストは 4.8 キロバイトとなり、Cayrel らの方式と比較して 36%の効率化を達成した。

一方、本論文では、Stern プロトコルを用いることにより、Niederreiter 公開鍵暗号方式の平文知識証明プロトコルが構成できることを示した。平文知識証明プロトコルでは、他の参加者に対して指定された暗号文が対応する平文の知識を有することを証明可能であるが、平文自体と暗号化者の秘密鍵に関しての情報を取得できない性質を持つ。本博士論文では、Asiacrypt 2012 において Jain らが発表した方式を利用して、McEliece 公開鍵暗号方式の平文知識証明プロトコルと暗号化された平文知識証明プロトコルを構築した。この平文知識証明プロトコルの安全性証明には、ランダムオラクルを利用しない標準モデルにおいて行った。

更に、提案した平文知識証明プロトコルを用いて、McEliece 公開鍵暗号方式に基づく検証可能公開鍵暗号(verifiable encryption)、符号理論に基づく検証者指定ディジタル署名(designated confirmer signature)を構築した。ProvSec 2010 において El Aimani は、準同型暗号化を利用した検証者指定ディジタル署名の一般的な構成方法を提案している。しかし、McEliece 公開鍵暗号方式は準同型暗号化ではないため、本博士論文では符号理論に基づいた署名確認プロトコル(confirmation protocol)と署名否認プロトコル(deniable protocol)により構築した。特に、提案方式では、署名否認プロトコルを構築するために新しいゼロ知識証明プロトコルを提案した。

本博士論文の結果は、査読付き国際会議 The 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2013)および The 8th Asia Joint Conference on Information Security (AsiaJCIS 2013)において発表を行い、予稿集論文とし公表済である。また、同論文の Full paper は、IEICE Transactions on Fundamentals on Fundamentals of Electronics, Communications and Computer Sciences に投稿中である。

以上の結果は、シンドローム復号などの符号理論により公開鍵暗号で用いるゼロ知識証明を考察したものであり、暗号理論において価値のある業績と認められる。

よって、本研究者は博士（数理学）の学位を受ける資格があるものと認める。