科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１３　日現在

機関番号：　１２４０１
研究種目：　挑戦的萌芽研究
研究期間：　2011～2013
課題番号：　２３６５０００４

研究課題名（和文）量子暗号理論と古典暗号理論の互換技法の開発

研究課題名（英文）Interchangeable techniques between classical and quantum cryptography

研究代表者
小柴　健史（KOSHIBA, Takeshi）

埼玉大学・理工学研究科・准教授

研究者番号：６０４００８００

交付決定額（研究期間全体）：（直接経費）　　2,500,000円、（間接経費）　　750,000円

研究成果の概要（和文）：一般的に観測ベース量子計算モデルで議論されるブラインド量子計算の特別形として観測に適した系と計算に適した系が存在し観測は観測系でのみ行う計算モデルとして補助キュービット駆動量子計算がある．当該モデルにおいてブラインド量子計算が可能であるための十分条件を導出し，実際にその十分条件を満たす方法を与えた．暗号理論においては，他のプロトコルの部品として利用しても安全性を維持する性質は汎用結合可能性と呼ばれる．ブラインド量子計算の方式には様々な方式があるが，クライアントが観測を行うタイプのFujii-Morimae方式は汎用結合可能であることを証明した．

研究成果の概要（英文）：Quantum blind computation can be discussed in the measurement-based quantum computation model. As a special case, ancilla-driven quantum computation is defined as computation where measurements are made only on the measurement system and computation is carried on the computational system and those two system are separated. In the ancilla-driven computation model, we derive sufficient conditions for the blindness and show a bind protocol. In cryptography, the universal composability guarantees that a prococol can be used as a part of larger cryptosystems. We show that Fujii-Morimae blind computation, where only the client makes measurements, is universally composable.

研究分野：　情報学基礎

科研費の分科・細目：　量子計算

キーワード：　量子計算　量子暗号　代理計算　暗号プロトコル　暗号理論

１．研究開始当初の背景

1990年代前半にOstrovsky, Venkatesan & Yung により，汎用ハッシュ関数を対話的に用いる手法（インタラクティブハッシュ）が提案され，様々な暗号プロトコル（紛失通信，ビット委託，ゼロ知識対話証明など）の設計に応用されている．ビット委託方式について言及すると，インタラクティブハッシュの性質（インタラクティブハッシュ定理）が研究されるに連れて，より一般化されたインタラクティブハッシュ定理が得られている．それに伴って構成されるビット委託方式の実現に必要な計算量仮定を弱めることに成功している．具体的にはNaor ら (CRYPTO 1992) が一方向性置換に基づく方法(NOVY 方式)を，Haitner ら (EUROCRYPT 2005)が特殊な一方向性関数に基づく方法(HHKKMS 方式)を，その後，Haitner ら (SIAM J. Comput., Vol.39, 2009)が任意の一方向性関数に基づく方法(HNORV 方式)の提案している．別の研究の流れとして，Dumais, Mayers & Salvail (EUROCRYPT 2000)は BB84 量子状態を利用して量子一方向性置換から量子ビット委託方式(DMS 方式)を示していた．応募者らは古典プロトコルである NOVY 方式と量子プロトコルである DMS 方式の類似性を見出し，HHKKMS 方式の量子版(KO 方式)の構築(Koshiba & Odaira, TQC 2009)に成功している．これを契機にして古典暗号プロトコルと量子暗号プロトコルの構築技術の等価性が単なる一事例ではなく普遍化できるかもしれないという着想を得る．

２．研究の目的

量子暗号プロトコルは量子力学的な効果を利用することにより，古典暗号プロトコルよりも効率的あるいは安全にできる可能性がある．また，量子暗号プロトコル開発は古典暗号研究分野とは独立に遂行されていることが多く，効率等を犠牲にしても同等な機能を古典技術で実装できるならば実効化が容易となる．本研究課題では，古典暗号プロトコルの設計手段と量子暗号プロトコルの設計手段の間の等価性を見出し，古典暗号プロトコルの設計論と量子暗号プロトコルの設計論が相互に援用できる方法論を提案することを目標とする．同等の機能を持つプロトコルならば量子プロトコルは構造が比較的観点であり，プロトコル設計論として「まず量子暗号プロトコルを設計し，その後，古典プロトコル化する」という新しい方法論の確立を目指す．

３．研究の方法

一方向性置換および一方向性関数からの統計的秘匿ビット委託方式を構成するために用いられている技術的道具であるインタラクティブハッシュ定理(Naor, Ostrovsky, Venkatesan & Yung, CRYPTO 1992)およびその精緻化(Haitner & Reingold, CCC 2007)をもとに，インタラクティブハッシュと統計的秘匿量子ビット委託方式(Dumais, Mayers & Salvail, EUROCRYPT 2000)における量子状態送付との類似・相違をもとに一般化量子非対話ハッシュ定理を導出する．この量子非対話ハッシュ定理を量子暗号プロトコルの構成法に利用できることを示すために，インタラクティブハッシュを利用したビット委託･紛失通信･ゼロ知識証明をもとにして，対応する量子暗号プロトコルを構成する．さらには，既存の量子暗号プロトコルの中で安全性保証が量子非対話ハッシュ定理に依存していそうなものを模索し，古典暗号プロトコル化できるか検討する．

また，セキュア計算の枠組みにおいて，量子計算の優位性を示す事例（量子ブラインド計算）が近年提案された(Broadbent, Kashefi & Fitzsimons, FOCS 2009)．情報理論的な意味で安全な代理計算を可能にするもので，古典暗号理論では計算量理論的な方法しか知られていない．量子ブラインド計算は観測ベース量子計算モデルで実現される方式であるが，基本的に量子回路モデルにおける計算プロセスと１対１対応の関係にある．また，古典暗号理論において，セキュア計算を実現する方法としてGarbled 回路と呼ばれる技法があり，Garbled は論理回路を素子単位で何を実行しているのか分からなくする技術である．素子単位でセキュア計算を実行するという観点は，量子サイドの研究でも古典サイドの研究でも符合している．また，安全性の強化方法などに技術的な親和性が見られるため，この点についても互換技術を検討す

る．

さらに，観測ベース量子計算は新しく提案された計算モデルであるため，その計算モデルの可能性や限界が十分に究明されていないので，それについても合わせて研究する．観測ベース量子計算モデルの基本的な取り扱い方の知見を得ることで，互換技術を研究するための基盤も整える．

４．研究成果

暗号理論において代理計算と呼ばれる二者間プロトコルがあり，クライアントの入力や計算結果をサーバに秘匿したままで，サーバに代理計算を行わせることができる．古典暗号理論においては，Garbled 回路と呼ばれる方法論があり，量子暗号理論においては，ブラインド量子計算と呼ばれる手法がある．それぞれの領域で，安全性を強化する方法が知られているが，それらの技術はお互いに応用できる関係にあることを見出すことができた．

互換技法を研究するに辺り，それぞれの領域を深める研究も行った．ブラインド量子計算は観測ベース量子計算と呼ばれる計算モデル上で議論するのが一般的であるが，物理的な実装を考慮すると，観測に適した系と計算に適した系が存在し，観測は観測系でのみ行う計算モデルとして補助キュービット駆動量子計算と呼ばれる計算モデルがある．観測ベース量子計算の特殊な形であるため，ブラインド量子計算が可能であるための十分条件を導出し，実際にその十分条件を満たす方法を与えた．

暗号理論においては，プロトコルを単体で用いることは少なく，他のプロトコルの部品として利用されることが一般的であり，そのような状況においても安全性を維持する性質は汎用結合可能性と呼ばれる．ブラインド量子計算の方式には様々な方式があるが，クライアントが観測を行うタイプの Fujii-Morimae 方式は汎用結合可能であることを証明した．この証明は，Fujii-Morimae 方式が一方向通信しか行わないという性質を利用したもので，従来証明手法(Dunjko, Fitzsimons, Portmann & Rennar, arXiv:1301.3662, 2013)を大幅に簡略化するとともに，no-signaling 仮定だけで証明が可能であるという意味で従来よりも安全性が高いプロトコルになっていることを示したものである．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 3 件）

① M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama, T. Koshiba, Practical packing method in somewhat homomorphic encryption, *Lecture Notes in Computer Science* **8247**, pp.34-50, 2014, 査読有

② M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama, T. Koshiba, Packed homomorphic encryption based on ideal lattices and its application to biometrics, *Lecture Notes in Computer Science* **8128**, pp. 55-74, 2014, 査読有

③ T. Sueki, T. Koshiba, T. Morimae, Ancilla-driven universal blind quantum computation, *Physical Review A* **87**, 2013, 60301 (5pages, Rapid Communication), 査読有

〔学会発表〕（計 4 件）

① T. Koshiba, S. Sawada, On unidirectional public discussion in secure message transmission, 1st International Conference on Energy, Environment and Human Engineering (ICEEHE 2013), 2013 年 12 月 21 日, Kandawgyi Palace Hotel, Yangon, Myanmar

② T. Morimae, T. Koshiba, Composable security of measuring-Alice blind quantum computation, 7th International Conference on Information Theoretic Security (ICITS 2013), 2013 年 11 月 29 日, NangYang Technological University, Singapore

③ T. Koshiba, Composable security of blind computation, Quantum Science Symposium ASIA (QSS-ASIA 2013), 2013年11月26日, Tokyo Univ., Tokyo,

Japan, **招待講演**

④ M. Yasuda, T. Shimoyama, J. Kogure, H. Yokoyama, T. Koshiba, Secure pattern matching using somewhat homomorphic encryption, 2013 ACM Workshop on Cloud Computing Security, 2013 年 11 月 8 日, Berlin, Germany

〔図書〕（計 1 件）

① T. Koshiba, Quantum Cryptography, Chapter 45 in Handbook of Natural Computing, Springer, 23p, 2012.

６．研究組織

(1)研究代表者

小柴　健史（KOSHIBA, Takeshi）
埼玉大学・大学院理工学研究科・准教授
研究者番号：60400800