SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

QMA に対する Certified Everlasting ゼロ知識証明
Certified Everlasting Zero-Knowledge Proof for QMA

廣岡　大河 * 森前　智行 * 西巻　亮 † 山川　高志 †
Taiga Hiroka Tomoyuki Morimae Ryo Nishimaki Takashi Yamakawa

キーワード 理論計算機科学、量子暗号、量子ゼロ知識証明 、量子ビットコミットメント

あらまし

ゼロ知識証明とは、ある数学的な命題が真であることを示すのに命題が真であること以外のなんの情報も与えることなく証明できる手法である。検証者と証明者がお互いに量子操作を行えない場合はゼロ知識性と健全性の両方を統計的に満たした NP 問題に対するゼロ知識証明は、多項式階層が崩壊しない限り、存在しないことが知られている。検証者と証明者が量子操作を行える場合でも、ゼロ知識性と健全性の両方を統計的に満たした NP 問題に対するゼロ知識証明は構成できないと考えられている。実際、これまで知られている構成方法はゼロ知識性と健全性のどちらか一方は計算量的安全性である。

本稿では、Certified Everlasting ゼロ知識性という、統計的ゼロ知識性を緩和した、新しい安全性を提案する。Certified Everlasting ゼロ知識性において、検証者はプロトコルの実行中に受け取った量子情報を消去したことを証明する証明書を発行できる。証明書が有効な場合には、証明書を発行した後に検証者の計算能力が無制限になり計算量的仮定が後から破れたとしても検証者は数学的な命題が正しいという情報以外なんの情報も得ることが出来ない。Certified Everlasting ゼロ知識性は検証者が証明書を発行することを拒んだ場合や証明書を発行するまでの間に計算量的仮定が破れた場合の安全性を保証しない。したがって、Certified Everlasting 安全性は統計的ゼロ知識性を含まない。そのため、統計的健全性を満たし Certified Everlasting ゼロ知識性を満たした NP 問題に対するゼロ知識証明が構成できたとしても、これまでの不可能性の結果に矛盾しない。本稿では統計的健全性を満たし Certified Everlasting ゼロ知識性を満たした QMA 問題に対するゼロ知識証明を構成する。（QMA とは NP を含んだ計算量クラスのことで、NP を量子一般化したものである。）

これを構成するために、統計的拘束性を満たし Certified Everlasting 秘匿性を満たした量子ビットコミットメントを構成する。ここで Certified Everlasting 秘匿性とは受信者が発行した証明書が有効な場合には、受信者が証明書を発行した後に計算能力が無限大になり計算量的仮定が破れたとしても、コミットされた値の情報が受信者に漏れないことを保証した安全性である。本稿では Broadbent と Islam によって構成された Certified Deletion 付きワンタイム秘密鍵暗号と、統計的拘束性を満たし計算量的秘匿性を満たしたビットコミットメントを構成要素としてブラックボックス的に用いることで、統計的拘束性を満たし Certified Everlasting 秘匿性を満たした量子ビットコミットメントを構成する。我々の構成方法は量子ランダムオラクルモデルの下に Certified Everlasting 安全性を満たす。

本稿で構成する新しいゼロ知識証明は、検証者と証明者が完全に古典的な情報処理しか行えない場合には、構成できないと考えられる。なぜなら、古典的な検証者に対する Certified Everlasting ゼロ知識性は明らかに正直な検証者に対する統計的ゼロ知識性と等しいため、古典の世界においては Certified Everlasting ゼロ知識性は統計的ゼロ知識性と等しい。そのため、健全性を統計的に満たしたままで Certified Everlasting ゼロ知識性を満たした NP 問題に対するゼロ知識証明は、多項式階層が崩壊しない限り、不可能である。したがって、本結果は古典の不可能性を量子の性質を用いて乗り越えた新たな例である。

* 京都大学基礎物理学研究所, 〒 605-8502 京都市左京区北白川追分町, Yukawa Institute for Theoretical Physics, Kyoto University, Kitashirakawa-Oiwakecho, Sakyo-Ku, Kyoto 606-8502, Japan
† 日本電信電話株式会社, 〒 100-8116 東京都千代田区大手町一丁目 5 番 1 号 大手町ファーストスクエア イーストタワー, NTT corporation, Otemachi First Square, East Tower, 5-1, Otemachi 1-Chome, Chiyoda-ku, Tokyo 100-8116, Japan