様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 24 年　6 月　8 日現在

機関番号：21602
研究種目：若手研究(B)
研究期間：2009～2011
課題番号：21700021
研究課題名（和文）　量子暗号と量子状態の対称性に関する研究

研究課題名（英文）　Quantum cryptography and symmetry of quantum states

研究代表者
渡辺 曜大（WATANABE YODAI）
会津大学・コンピュータ理工学部・准教授
研究者番号：70360675

研究成果の概要（和文）：乱数抽出とは，与えられた情報源から，情報源と相関を持つ副情報に対してほぼ一様に分布する鍵を抽出する技術である．本研究では，量子状態に関する最大化に基づく通常の平滑化を用いずに定義された条件付き衝突エントロピーの量子版によって抽出鍵の長さが与えられる量子副情報に対する乱数抽出を与えた．さらに，量子副情報がある種の対称性をもつとき(量子条件付き衝突エントロピーの定義に現れる２つの演算子が交換するとき)，その評価が容易になることを実際に示した．

研究成果の概要（英文）：Randomness extraction against side information is the art of distilling from a given source a key which is almost uniform conditioned on side information. This work provided randomness extraction against quantum side information whose extractable key length is given by a quantum generalization of the conditional collision entropy defined without the conventional smoothing based on the maximization with respect to quantum states. Moreover, it was demonstrated that the evaluation of the quantum conditional collision entropy becomes drastically easy when the two operators in its definition commute.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,300,000	390,000	1,690,000
2010 年度	1,000,000	300,000	1,300,000
2011 年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,300,000	990,000	4,290,000

研究分野：総合領域
科研費の分科・細目：情報学・情報学基礎
キーワード：量子暗号，量子鍵配送，情報量的安全性

１．研究開始当初の背景

現在標準的に用いられている多くの暗号技術の安全性は，桁数の大きい素因数分解問題や離散対数問題を解くのが難しいといういわゆる計算量的な仮定にもとづいている．このような計算量的な仮定にもとづく暗号は，計算機能力の向上やアルゴリズムの発展に伴い，長い期間にわたってその安全性を確保することが難しくなってきている．さらに，量子コンピュータが実現したり，多くの研究者の予想に反して P=NP が示されたりすると安全性そのものがまったく保証されないと

いう事態になってしまう．

これに対して，量子暗号の主要な目的は，計算量的な仮定によらない暗号技術を構成することであり，「無条件の安全性」と呼ばれる極めて強い安全性を保証することのできる暗号技術として現在注目されている．実際，量子暗号の中で現在最も実用化に近いと考えられている量子鍵配送は，盗聴者の計算能力によらず（すなわち無限の計算資源をもつ盗聴者に対しても）安全性の保証された鍵配送方式である．

量子鍵配送の安全性を証明するためには，攻撃者のもつ量子状態を推定し，これを副情報とする乱数抽出を行う必要がある．抽出に用いる圧縮関数としてユニバーサル・ハッシュ関数を用いた乱数抽出（秘匿性増強）に関してはすでに詳しく調べられていて，攻撃者の量子状態の条件付き最少エントロピーあるいは衝突エントロピーにもとづいて圧縮率を決めることによって，安全な鍵が生成できることが知られている[Renner05]．ここで，上記条件付き最少エントロピーおよび衝突エントロピーは，量子状態に関する最大化に基づく平滑化を用いて定義されている．しかし，この最大化のために，これら条件付きエントロピーの評価は，一般に容易ではない．

２．研究の目的

上記，研究の背景をふまえ，量子状態に関する最大化に基づく通常の平滑化によらない条件付き衝突エントロピーの量子版を導入し，これを抽出鍵長とする乱数抽出を構成することを本研究の目的とする．

３．研究の方法

本研究では，先行研究と同様に，抽出に用いる圧縮関数としてユニバーサル・ハッシュ関数を用いる．ただし，圧縮率を与える条件付きエントロピーとして，量子状態に関する最大化に基づく通常の平滑化によらない条件付き衝突エントロピーの量子版を導入する．また，合成系(S,ρ)と(U,ρ)の距離（次節参照）は，量子相対エントロピーにより測る．

４．研究成果

いま，Xを確率変数とし，ρを量子状態とする．このとき，副情報ρに対する情報源Xからの乱数抽出とは，合成系(S,ρ)と(U,ρ)の距離が（ほぼ）0となる鍵Sを生成する技術をいう．ただし，Uはρと独立に一様に分布する確率変数である．

まず，条件付き衝突エントロピーの量子版 $R_\epsilon(X|\rho)$ を下式により定義する．

$$R_\epsilon(X|\rho) = \sup_\lambda \{\lambda|\mathrm{Tr}\left[\{\Lambda_{X\rho} - 2^{-\lambda}\rho_*^2 \le 0\}\rho_*\right] \ge 1-\epsilon\}$$

ただし，

$$\Lambda_{X\rho} = \sum_x (p_x\rho_x)^2 \quad \text{and} \quad \rho_* = \sum_x p_x\rho_x$$

とおいた．明らかに，$R_\epsilon(X|\rho)$の定義は

1. （陽に）量子状態に関する最大化を含まない
2. ただ 2 つの演算子$\Lambda_{X\rho}$およびρ_*により記述される

ことがわかる．したがって，特にわれわれの興味が鍵長有限の場合にあるとき，$R_\epsilon(X|\rho)$は既存の量子条件付きエントロピーよりも有用で扱いやすいということが期待できるかもしれない．実際，演算子$\Lambda_{X\rho}$およびρ_*が交換する場合は，$R_\epsilon(X|\rho)$の評価が大幅に容易になることが確かめられる[1]．

さらに，$R_\epsilon(X|\rho)$を抽出鍵長とする乱数抽出を構成することができる．実際，2-ユニバーサル・ハッシュ関数Gを圧縮関数として用いることによって，一様からの距離$D(S|G,\rho)$に対する上界を以下のように与えることができる．

$$D(S|G,\rho) \le \epsilon\log_2\left(\frac{d|S|}{\epsilon}\right) + \frac{\delta+\epsilon+\epsilon^{1/2}}{\ln 2}$$

ただし，

$$S = G(X), d = \mathrm{rank}\rho_* \text{ and } \delta = |S|2^{-R_\varepsilon(X|\rho)}$$

とおいた[1]．

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 0 件）

[1] Yodai Watanabe: Randomness extraction via a quantum generalization of the conditional collision entropy, submitted.

〔学会発表〕（計 0 件）

〔図書〕（計 0 件）

〔産業財産権〕

○出願状況（計 0 件）

○取得状況（計 4 件）

名称：量子鍵配送方法および通信装置
発明者：松本渉，渡辺曜大
権利者：三菱電機株式会社，理化学研究所
種類：特許
番号：特許第 4290401 号
取得年月日：2009.04.10
国内外の別：国内

名称：量子鍵配送方法および通信装置
発明者：松本渉，渡辺曜大
権利者：三菱電機株式会社，理化学研究所
種類：特許
番号：特許第 4346929 号
取得年月日：2009.07.24
国内外の別：国内

名称：Quantum key distribution method and communication device
発明者：Wataru Matsumoto, Yodai Watanabe
権利者：Mitsubishi Denki Kabushiki Kaisha
種類：United States Patent
番号：7,609,839
取得年月日：October 27, 2009
国内外の別：国外

名称：量子鍵配送方法、通信システムおよび通信装置
発明者：渡辺曜大
権利者：情報・システム研究機構
種類：特許
番号：特許第 4862159 号
取得年月日：2011.11.18
国内外の別：国内

〔その他〕
なし

６．研究組織
(1)研究代表者
渡辺 曜大（WATANABE YODAI）
会津大学・コンピュータ理工学部・准教授
研究者番号：70360675

(2)研究分担者
なし

(3)連携研究者
なし