様式 C-19

科学研究費補助金研究成果報告書

平成 21 年　6 月 19 日現在

研究種目：若手研究(B)
研究期間：2006～2008
課題番号：１８７０００１６
研究課題名（和文）　各種量子暗号方式に対する安全性の定式化およびその証明手法

研究課題名（英文）　Formalization and proof of the security for quantum key distribution

研究代表者
渡辺 曜大（WATANABE YODAI）
国立情報学研究所・情報学プリンシプル研究系・助教
研究者番号：70360675

研究成果の概要：本研究では，盗聴者の情報がハッシュ関数に依存しうる状況にも適用可能な秘匿性増強の安全性証明を与えた．その結果，最終鍵に関する盗聴者の相互情報量は若干増加するが，既存の結果と同じ圧縮率で安全な秘匿性増強が構成できることがわかった．さらに，Jensen の作用素不等式を用いることによって，既存の古典の結果と一致する鍵生成レートを持つ量子秘匿性増強の安全性証明を与えた．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００６年度	1,300,000	0	1,300,000
２００７年度	1,200,000	0	1,200,000
２００８年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,500,000	300,000	3,800,000

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，盗聴者に漏れた鍵に関する情報量を推定し，その情報量に応じて鍵を圧縮しなければならない．この圧縮過程を秘匿性増強とよぶ．圧縮関数としてユニバーサル・ハッシュ関数を用いた秘匿性増強に関してはすでに詳しく調べられていて，盗聴者の鍵に関するレニー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，安全な秘匿性増強が構成できることが知られている[BBCM95]．しかし，この結果をそのまま量子鍵配送における秘匿性増強に適用することはできない．これは，量子鍵配送では秘匿性増強に用いられるハッシュ関数が公開された後に盗聴者が観測を行うことができるため，一般に盗聴者の情報がハッシュ関数と独立とは限らないためである．

２．研究の目的

こうした背景をふまえ，本研究では，

(1) 量子鍵配送においてユニバーサル・ハッシュ関数を用いた秘匿性増強は可能か，

(2) 可能な場合，ハッシュ関数の圧縮率および最終鍵に関する盗聴者の情報量はどうなるか，

の 2 点について考察し，最終的に，量子鍵配送に適用可能な秘匿性増強法を構成することを目的とする．

３．研究の方法

通常，量子鍵配送の安全性証明では線形符号を用いた秘匿性増強を考えるが，本研究ではユニバーサル・ハッシュ関数を用いた秘匿性増強を扱う．ここで，ユニバーサル・ハッシュ関数の定義は以下で与えられる．

G を有限集合 A から有限集合 B への関数の集合とし，G を G 上の一様分布にしたがう確率変数とする．任意の $a_0, a_1 \in A$ に対して $a_0 \neq a_1$ ならば $Pr[G(a_0) = G(a_1)] \leq 1/|B|$ が成り立つとき，G はユニバーサルであるという．

例えば，A から B へのすべての関数の集合，$\{0,1\}^n$ から $\{0,1\}^r$ へのすべての 線形関数の集合などはユニバーサルである．ユニバーサル・ハッシュ関数のクラスは圧縮関数として線形符号のクラスよりも真に広く，実際，線形符号よりも効率的な（必要とする乱数のサイズが小さい）ユニバーサル・ハッシュ関数族が存在することが知られている．

４．研究成果

圧縮関数としてユニバーサル・ハッシュ関数を用いた秘匿性増強に関しては，以下の結果が知られている．

定理[BBCM95]．T および S を有限集合とする．X を T 上の確率変数とし，W を

$$Pr[R(X|W=w) \geq \lambda] \geq 1-\varepsilon$$

なる条件をみたす確率変数とする．ここで，R はレニーエントロピー

$$R(X|W=w) = -\log_2 \sum_x Pr[X=x|W=w]^2$$

をあらわしている．さらに，G を X および W と独立な T から S へのユニバーサル・ハッシュ関数の集合上の一様分布にしたがう確率変数とする．このとき，次が成り立つ．

$$H(G(X)|G,W) \geq (1-\varepsilon)\log_2|S| - \frac{\delta}{\ln 2},$$

ただし，$\delta = |S| \exp_2(-\lambda)$ とおいた．

この定理では，確率変数 G（ハッシュ関数）と W（盗聴者に漏れた鍵に関する情報量）が独立であると仮定されている．一方，量子鍵配送では，秘匿性増強に用いられるハッシュ関数が公開された後に盗聴者が観測を行うことができるため，一般に盗聴者の情報がハッシュ関数と独立とは限らない．したがって，この結果をそのまま量子鍵配送の秘匿性増強に用いることはできない．そこで本研究では，この定理を一般化して，以下の結果を得た．

主結果． T および S を有限集合とする．X を T 上の確率変数とし，W を

$$Pr[R(X|W=w) \geq \lambda] \geq 1-\varepsilon$$

なる条件をみたす確率変数とする．ここで，R はレニーエントロピー

$$R(X|W=w)$$
$$=-\log_2 \sum_x Pr[X=x|W=w]^2$$

をあらわしている．さらに，G を X と独立な T から S へのユニバーサル・ハッシュ関数の集合上の一様分布にしたがう確率変数とする．このとき，次が成り立つ．

$$H(G(X)|G,W)$$
$$\geq (1-\varepsilon)\log_2|S| - \frac{\delta+\varepsilon}{\ln 2},$$

ただし，$\delta = |S|\exp_2(-\lambda)$ とおいた．

上記2つの結果を比べると以下のことが分かる．まず，前者では確率変数 X と W の独立性を仮定していたが，後者では仮定していない．したがって，後者は前者の一つの一般化になっている．一方，後者の条件付エントロピー $H(G(X)|G,W)$ の下界は，前者に比べて $\varepsilon/\ln 2$ だけ減少している．なお，この結果を量子鍵配送に適用する場合，パラメータ ε は十分小さい値をとる（鍵のサイズに関して指数関数的に減少する）ことに注意しておく．

結局．本研究では以下の成果を得た．まず，盗聴者の情報がハッシュ関数に依存しうる状況にも適用可能な秘匿性増強の安全性証明を与えた．その結果，(1) 量子鍵配送においてユニバーサル・ハッシュ関数を用いた秘匿性増強は可能であり，(2) 最終鍵に関する盗聴者の相互情報量は若干増加するが，既存の結果と同じ圧縮率で安全な秘匿性増強が構成できることが分かった．

さらに，上記成果とは別に，Jensen の作用素不等式を用いることによって，既存の古典の結果と一致する鍵生成レートを持つ量子秘匿性増強の安全性証明を与えた．

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 2 件）

① Yodai Watanabe: Privacy amplification for quantum key distribution, Journal of Physics A: Mathematical and Theoretical, 40, F99-F104, (2007). 査読あり

② Yodai Watanabe: Differential geometry on diffeomorphism groups and Lagrangian stability of viscous flows, Physica D, 225, 197-203, (2007). 査読あり

〔学会発表〕（計 3 件）

① 渡辺曜大：量子秘匿性増強の鍵生成レートについて, 第 31 回情報理論とその応用シンポジウム予稿集， SITA2008，pp. 715-718, (2008)．査読なし

② 渡辺曜大: 量子暗号における秘匿性増強, 第 7 回代数幾何・数論及び符号・暗号研究集会報告集，pp.58-69, (2006)．査読なし

③ 渡辺曜大：量子鍵配送における秘匿性増強, 第 29 回情報理論とその応用シンポジウム予稿集， SITA2006， pp.673-674, (2006). 査読なし

〔図書〕（計 0 件）

なし

〔産業財産権〕

○出願状況（計 1 件）

名称：量子鍵配送方法および通信装置
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：11/814,619
出願年月日：2007 年 07 月 24 日
国内外の別：外国

○取得状況（計 1 件）

名称：量子鍵配送方法および通信装置
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 4231926 号
取得年月日：2008 年 12 月 19 日
国内外の別：国内

〔その他〕

ホームページ等

６．研究組織

(1)研究代表者

渡辺 曜大 (WATANABE YODAI)

国立情報学研究所・情報学プリンシプル研究系・助教
研究者番号： 70360675

(2)研究分担者
なし

(3)連携研究者
なし

様式C-19（記入例）

科学研究費補助金研究成果報告書

平成　　年　　月　　日現在

研究種目：基盤研究（A）
研究期間：2004～2007
課題番号：１６０００００００
研究課題名（和文）　○○○○○○○○○に関する研究

研究課題名（英文）　ＡＡＡＡＡＡＡＡＡＡＡＡ

研究代表者
学振　太郎（GAKUSHIN TARO）
○○大学・大学院理工学研究科・教授
研究者番号：

研究成果の概要：○○

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００４年度	10,000,000	3,000,000	13,000,000
２００５年度	10,000,000	3,000,000	13,000,000
２００６年度	10,000,000	3,000,000	13,000,000
２００７年度	10,000,000	3,000,000	13,000,000
年度			
総　計	40,000,000	12,000,000	52,000,000

研究分野：
科研費の分科・細目：
キーワード：

１．研究開始当初の背景

(1) ○○

(2) ○○○

２．研究の目的

(1) ○○

(2) ○○

３．研究の方法

(1) ○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○

(2) ○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○

４．研究成果

(1) ○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○

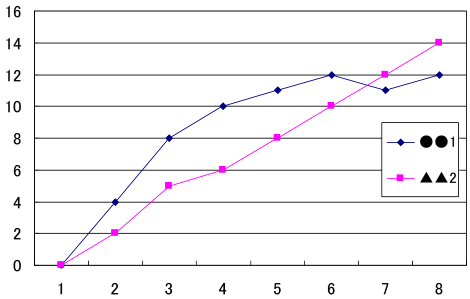

図1 ○○○○○

(2) ○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○

(3) ○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○

(4) ○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○

(5) ○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○

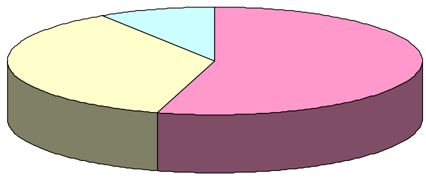

図2 ○○○○○

(6) ○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○

(7)○○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○○

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１０件）

① 学振太郎、半蔵門一郎、学振花子、論文名、掲載誌名、巻、最初と最後の頁、発表年（西暦）、査読の有無
② 学振太郎、論文名、掲載誌名、巻、最初と最後の頁、発表年（西暦）、査読の有無
③ 学振花子、論文名、掲載誌名、巻、最初と最後の頁、発表年（西暦）、査読の有無

〔学会発表〕（計５件）

①

②

③

〔図書〕（計２件）

①

②

〔産業財産権〕
○出願状況（計□件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計◇件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等
http://○○○○○○○○○○○○○○○○

６．研究組織
(1)研究代表者
学振　太郎（GAKUSHIN　TARO）
○○大学・大学院理工学研究科・教授
研究者番号：
(2)研究分担者
学振　花子（GAKUSHIN　HANAKO）
○○大学・大学院理工学研究科・教授
研究者番号：
学振　次郎（GAKUSHIN　JIRO）
○○大学・大学院理工学研究科・教授
研究者番号：
学振　三郎（GAKUSHIN　SABURO）
○○大学・大学院理工学研究科・教授
研究者番号：

(3)連携研究者
学振　四郎（GAKUSHIN　SHIRO）
○○大学・大学院理工学研究科・教授
研究者番号：