Privacy amplification for quantum key distribution

2007 J. Phys. A: Math. Theor. 40 F99

(http://iopscience.iop.org/1751-8121/40/3/F03)

IOP FTC
INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND THEORETICAL

J. Phys. A: Math. Theor. **40** (2007) F99–F104 doi:10.1088/1751-8113/40/3/F03

FAST TRACK COMMUNICATION

Privacy amplification for quantum key distribution

Yodai Watanabe

National Institute of Informatics, Research Organization of Information and Systems 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 1018430, Japan

Received 7 November 2006, in final form 28 November 2006
Published 20 December 2006
Online at stacks.iop.org/JPhysA/40/F99

Abstract

This paper examines classical privacy amplification using a universal family of hash functions. In quantum key distribution, the adversary's measurement can wait until the choice of hash functions is announced, and so the adversary's information may depend on the choice. Therefore the existing result on classical privacy amplification, which assumes the independence of the choice from the other random variables, is not applicable to this case. This paper provides a security proof of privacy amplification which is valid even when the adversary's information may depend on the choice of hash functions. The compression rate of the proposed privacy amplification can be taken to be the same as that of the existing one with an exponentially small loss in secrecy of a final key.

PACS numbers: 89.70.+c, 03.67.Dd

Quantum key distribution [1, 2] allows two parties, say Alice and Bob, to share a secret key (random number) in the presence of an adversary, say Eve, with unlimited resources for computation. To make quantum key distribution secure, Alice and Bob have to distill highly secret shared information (final key) from only partially secret shared information (raw key). The art of this distillation is called privacy amplification. Remember here that the Shannon entropy is a measure of uncertainty of a random variable and takes its maximum if and only if the random variable has a uniform distribution (see e.g. [5]). Therefore, the standard way to prove the security of privacy amplification is to show that the Shannon entropy of the final key conditioned on Eve's information is maximal except for a small loss.

To perform privacy amplification, it is necessary to estimate Eve's information about a raw key and then compress it with a rate determined by the estimation. Now, to illustrate a simple example of privacy amplification, let us consider the following situation: Alice and Bob share two random bits $r_1 r_2 \in_R \{0, 1\}^2$ and they estimate that Eve knows only one bit e of the shared two bits (i.e. $e = r_1$ or $e = r_2$), where the estimation succeeds with probability $1 - \epsilon$. They choose a function g which compresses the raw key $r_1 r_2$ to generate a final key $g(r_1 r_2)$. Here, to agree on which function is to be used, they communicate with each other through an authenticated public channel, which is accessible to all parties including Eve. Now, let g be the function which takes two bits as input and outputs the exclusive OR (XOR) of the input two bits (i.e. $g(b_1 b_2) = b_1 \oplus b_2$ for $b_1, b_2 \in \{0, 1\}$). Then it is easy to see that the privacy

amplification using g to compress a raw key $r_1 r_2$ is secure when ε is negligible. In fact, we can show that the Shannon entropy $H(g(r_1 r_2)|e, g)$ of the finale key $g(r_1 r_2)$ conditioned on Eve's information e and g is lower bounded by $1 - \epsilon$.

In proving the security of quantum key distribution, it is conventional to apply privacy amplification using a family of linear codes for the compression (see e.g. [6, 9]). Instead, in this paper, we consider privacy amplification using a universal family of hash functions [4]. It should be noted that the universal families of hash functions are strictly lager than the families of linear codes. In fact, there are families in the former which are more efficient than all in the latter [4, 10].

Privacy amplification using a universal family of hash functions has already been investigated in detail by Bennett *et al* [3]. They proved the security of privacy amplification in which the Rényi entropy of a raw key given Eve's information is used to determine the compression rate. However, this result is not applicable to proving the security of quantum key distribution. This is because in the security proof of [3], Eve's information is assumed to be independent of the choice of hash functions, while in the actual situation of quantum key distribution, Eve's measurement can wait until the choice of hash functions is announced and so Eve's information (extracted by her measurement) may depend on the choice. To solve this problem, Renner and König [8] developed privacy amplification which is secure even when Eve is allowed to keep her information in the form of a quantum state. More precisely, the privacy amplification does not require Eve to extract classical information by measuring her quantum state, which is independent of the choice of hash functions, but it allows Eve to keep her state as quantum information. In this privacy amplification, the compression rate of hash functions is determined by using the quantum version of the (smooth) Rényi entropy of a raw key given Eve's information. Here, we note that the state transformation induced by a measurement is doubly stochastic (i.e. trace-preserving and unital). Thus, the classical Rényi entropy of a raw key is lower bounded by the corresponding quantum Rényi entropy (see [7]), and so the former could give a better compression rate than the latter. Therefore it is of interest to ask (i) whether or not secure privacy amplification is possible in the classical framework when Eve's information may depend on the choice of hash functions, and if possible, then (ii) how to determine the compression rate of hash functions. The aim of this paper is to answer these questions.

We begin by providing some definitions and notations which will be used later. Let X and Y be random variables over finite sets $\mathcal{X}$ and $\mathcal{Y}$, respectively. Then the Shannon entropy of X, $H(X)$, and the (second-order) Rényi entropy of X, $R(X)$, are defined by

$$H(X) = -\sum_{x\in\mathcal{X}} \Pr[X = x] \log_2 \Pr[X = x], \tag{1}$$

$$R(X) = -\log_2 \sum_{x\in\mathcal{X}} \Pr[X = x]^2 \tag{2}$$

respectively, where $\log_2$ denotes the logarithm to the base 2. We also use the notation $\exp_2(x) = 2^x$. By definition, it can be shown that

$$H(X) \leqslant \log_2 |\mathcal{X}|, \tag{3}$$

where $|\mathcal{X}|$ denotes the number of elements in the range of X, with equality if and only if X has a uniform distribution over $\mathcal{X}$ (see e.g. [5]). The conditional Shannon entropy of X given $Y = y$, $H(X|Y = y)$, and the Shannon entropy of X conditioned on Y, $H(X|Y)$, are defined by

$$H(X|Y = y) = -\sum_{x\in\mathcal{X}} \Pr[X = x|Y = y] \log_2 \Pr[X = x|Y = y], \tag{4}$$

$$H(X|Y) = \sum_{y\in\mathcal{Y}} \Pr[Y = y] H(X|Y = y) \tag{5}$$

respectively. The conditional Rényi entropies $R(X|Y = y)$ and $R(X|Y)$ are defined in the same way.

Let $\mathcal{A}$ and $\mathcal{B}$ be finite sets and $\mathcal{G}$ be a family of functions from $\mathcal{A}$ to $\mathcal{B}$. Let G be the random variable uniformly distributed over $\mathcal{G}$. Then $\mathcal{G}$ is called universal if

$$\Pr[G(a_0) = G(a_1)] \leqslant \frac{1}{|\mathcal{B}|} \tag{6}$$

for every distinct $a_0, a_1 \in \mathcal{A}$ [4]. For example, the family of all functions from $\mathcal{A}$ to $\mathcal{B}$ is universal. A more useful universal family is that of all linear functions from $\{0,1\}^n$ to $\{0,1\}^m$ [4]. More efficient families, which can be described using $O(n+m)$ bits and have polynomial-time evaluating algorithms, are discussed in [4, 10].

Having provided definitions and notations, we now consider privacy amplification which can be applied to quantum key distribution.

Theorem 1. *Let $\mathcal{X}$ and $\mathcal{S}$ be finite sets. Let X be a random variable over $\mathcal{X}$, and G be the random variable, independent of X, uniformly distributed over a universal family of hash functions from $\mathcal{X}$ to $\mathcal{S}$. Let W be a random variable such that*

$$\Pr[R(X|W = w) \geqslant \lambda] \geqslant 1 - \epsilon. \tag{7}$$

Then

$$H(G(X)|G, W) \geqslant (1-\epsilon)\log_2 \frac{(1-\epsilon)|\mathcal{S}|}{1+\delta} \geqslant (1-\epsilon)\log_2 |\mathcal{S}| - \frac{\delta+\epsilon}{\ln 2}, \tag{8}$$

where $\delta = |\mathcal{S}| \exp_2(-\lambda)$.

Here we note that the above theorem does not assume the independence between G and W.

Proof. We begin with

$$\Pr[G(X) = s|G = g, W = w] = \sum_x p(x|g, w)\delta(g(x) = s) \tag{9}$$

for every $s \in \mathcal{S}$, where $p(g, x, w) = \Pr[G = g, X = x, W = w]$ and

$$\delta(g(x) = s) = \Pr[g(x) = s|G = g, X = x] = \begin{cases} 1 & \text{if} \quad g(x) = s, \\ 0 & \text{if} \quad g(x) \neq s, \end{cases} \tag{10}$$

for short. Let X' be a random variable, independent of X and G, with the same distribution as X. Then the Shannon entropy of $G(X)$ conditioned on G and W, $H(G(X)|G, W)$, can be written as

$$H(G(X)|G, W) = -\sum_s \sum_{g,x,w} p(g, x, w)\delta(g(x) = s)\log_2 \sum_{x'} p(x'|w)\delta(g(x') = s). \tag{11}$$

It is now convenient to define the event E by

$$E = [w \in \{w|R(X|W = w) \geqslant \lambda\}]. \tag{12}$$

Since $p(g, x, w) \geqslant p(E)p(g, x, w|E)$ and $p(E) \geqslant 1 - \epsilon$,

$$H(G(X)|G, W) \geqslant -(1-\epsilon) \sum_{s,g,x,w} p(g, x, w|E)\delta(g(x) = s)\log_2 \sum_{x'} p(x'|w)\delta(g(x') = s). \tag{13}$$

Further, Jensen's inequality gives

$$H(G(X)|G,W) \geqslant -(1-\epsilon)\log_2 \sum_{s,g,x,x',w} p(g,x,w|E)\delta(g(x)=s)p(x'|w)\delta(g(x')=s)$$
$$\geqslant -(1-\epsilon)\log_2 \frac{1}{1-\epsilon}\sum_{w:E}\sum_{g,x,x'} p(g,x,w)p(x'|w)\delta(g(x)=g(x')), \quad (14)$$

where the last step follows from

$$p(g,x,w|E) = \frac{p(g,x,w,E)}{p(E)} \leqslant \frac{p(g,x,w)}{1-\epsilon}. \quad (15)$$

Now we divide the sum in the last line of (14) into two parts:

$$\sum_{w:E}\sum_{g,x,x'} p(g,x,w)p(x'|w)\delta(g(x)=g(x'))$$
$$= \sum_{w:E}\sum_{g,x,x':x=x'} p(g,x,w)p(x'|w)\delta(g(x)=g(x'))$$
$$+\sum_{w:E}\sum_{g,x,x':x\neq x'} p(g,x,w)p(x'|w)\delta(g(x)=g(x')). \quad (16)$$

The first part can be bounded as

$$\sum_{w:E}\sum_{g,x,x':x=x'} p(g,x,w)p(x'|w)\delta(g(x)=g(x'))$$
$$= \sum_{g,w:E} p(g,w)\sum_x p(x|w)^2$$
$$\leqslant \exp_2(-\lambda). \quad (17)$$

Also the second part can be bounded as

$$\sum_{w:E}\sum_{g,x,x':x\neq x'} p(g,x,w)p(x'|w)\delta(g(x)=g(x'))$$
$$= \sum_{w:E}\sum_{g,x,x':x\neq x'} p(g,x,w)p(x'|g,x,w)\delta(g(x)=g(x'))$$
$$\leqslant \sum_{w}\sum_{g,x,x':x\neq x'} p(g,x,x',w)\delta(g(x)=g(x'))$$
$$= \sum_{x,x':x\neq x'} p(x,x')\sum_g p(g)\delta(g(x)=g(x'))$$
$$\leqslant \frac{1}{|\mathcal{S}|}. \quad (18)$$

Inequality (8) readily follows from the above inequalities, and from

$$\log_2(1+x) \leqslant \frac{x}{\ln 2} \qquad \text{and} \qquad -(1-x)\log_2(1-x) \leqslant \frac{x}{\ln 2} \quad (19)$$

for $0 \leqslant x \leqslant 1$ (with the convention $0\log_2 0 = 0$). This completes the proof. □

As an example of application of this theorem, let us consider the BB84 protocol [2]. In this case, we may take X and $W = (Y, Z)$ so that X represents Alice's information used for the key, Y represents Bob's information resulting from his 'fictive' measurement and Z represents Eve's information resulting from her measurement. Further, the condition of the form $\Pr[R(X|Y=y, Z=z) \geqslant \lambda] \geqslant 1-\epsilon$ with ε exponentially small can be derived from

observed errors between Alice's information used for the test and Bob's information resulting from his 'real' measurement (for details of Bob's measurements, see [6]). Here it should be stated that, in contrast to Shannon entropy, Rényi entropy can increase when it is conditioned on a random variable. That is, $R(X|Y) > R(X)$ is possible. This is the reason why an auxiliary random variable Y is introduced. For a detailed discussion on auxiliary random variables, see [3].

Let us now estimate the conditional Shannon entropy $H(G(X)|G, Z)$ when $\Pr[R(X|Y = y, Z = z) \geqslant \lambda] \geqslant 1 - \epsilon$. It readily follows from the above theorem that

$$\begin{aligned} H(G(X)|G, Z) &\geqslant H(G(X)|G, Y, Z) \\ &\geqslant (1 - \epsilon)\log_2|\mathcal{S}| - \frac{\delta + \epsilon}{\ln 2}. \end{aligned} \tag{20}$$

On the other hand, if Z and G are independent, we have

$$H(G(X)|G, Z) \geqslant (1 - \epsilon)\log_2|\mathcal{S}| - \frac{\delta}{\ln 2} \tag{21}$$

for the same parameters as above [3]. By comparing these inequalities, we see that the lower bound in (20) is smaller than that in (21) by $\epsilon/\ln 2$, which can be taken exponentially small in quantum key distribution (see e.g. [6]). This decrease in the lower bound comes from inequality (15). We now explain this in more detail. In the above proof, it is essential to use inequality (6), which describes the property of a universal family of hash functions. However, this inequality requires that G is uniformly distributed over the universal family. If G is independent of W (and X), then

$$p(g, x, w|E) = p(g)p(x, w|E), \tag{22}$$

and thus this requirement is automatically satisfied. However, the above theorem allows W to depend on G, and so the conditional probability distribution $p(g|E)$ is not uniform in general. Hence, in the above proof, we use inequality (15) to ensure that G is uniformly distributed in (18), the last step of which follows from inequality (6). This completes the explanation why the decrease in the lower bound occurs.

In conclusion, we have examined classical privacy amplification using a universal family of hash functions. In quantum key distribution, Eve's measurement can wait until the choice of hash functions is announced, and so Eve's information Z may depend on the choice G of hash functions. Therefore the existing result [3] on privacy amplification is not applicable to this case. In this paper, we provided a security proof of privacy amplification which is valid even when Eve's information Z may depend on the choice G. Since the proposed privacy amplification is applicable to more general situations than the existing privacy amplification, it follows that the former cannot exceed the latter in efficiency and security. However, this disadvantage is negligible; in fact, the compression rate of the former can be taken to be the same as that of the latter with a negligible (exponentially small) loss of the lower bound on the conditional Shannon entropy $H(G(X)|Z, G)$.

We close this paper by mentioning a future problem. Let ρ be a quantum state, and X be a random variable resulting from a measurement on ρ. Since the state transformation induced by a measurement is doubly stochastic, it follows that

$$S_2(\rho) \leqslant R(X), \tag{23}$$

where S_2 denotes the (second-order) quantum Rényi entropy (see [7]). Note here that, in quantum key distribution, Eve's state can depend on Alice's information but Eve's measurement cannot; thus the equality in (23) does not hold in general. Therefore privacy amplification using R can have a better compression rate than that using S_2 at least in the

region of finite length (although they may asymptotically coincide). On the other hand, the same observation shows that the latter can have stronger security than the former at least in the region of finite length. Investigating this tradeoff between efficiency and security will be the subject of future work.

Acknowledgments

This work was supported in part by MEXT, Grant-in-Aid for Encouragement of Young Scientists (B) No 18700016.

References

[1] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[2] Bennett C H and Brassard G 1984 *Proc. IEEE Conf. on Computers, Systems and Signal Processing* (Bangalore India) (Piscataway, NJ: IEEE) p 175
[3] Bennett C H, Brassard G, Crépeau C and Maurer U M 1995 *IEEE Trans. Inform. Theory* **41** 1915
[4] Carter J L and Wegman M N 1979 *J. Comput. Syst. Sci.* **18** 143
[5] Cover T M and Thomas J A 2006 *Elements of Information Theory* 2nd edn (New York: Wiley)
[6] Mayers D 2001 *J. Assoc. Comput. Mach.* **48** 351
[7] Nislsen M A 2002 Lecture Note (Online at http://www.qinfo.org/talks/2002/maj/book.ps)
[8] Renner R and König R 2005 *Proc. Theory of Cryptography Conf.* (*Lecture Notes in Computer Science* vol 3378) (Berlin: Springer) p 407
[9] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[10] Wegman M N and Carter J L 1981 *J. Comput. Syst. Sci.* **22** 265