APPEARS IN *PROCEEDINGS OF 26TH SYMPOSIUM ON INFORMATION THEORY IN THE BENELUX* (2005) 189–196.

GENERIC SECURITY PROOF OF QUANTUM KEY EXCHANGE USING SQUEEZED STATES

Karin Poels* Pim Tuyls† Berry Schoenmakers*
k.j.p.m.poels@tue.nl pim.tuyls@philips.com berry@win.tue.nl

In [4], a Quantum Key Exchange (QKE) protocol that uses squeezed states was presented by Gottesman and Preskill. In this paper we give a generic security proof for this protocol, based on the work by Christiandl, Renner and Ekert ([1]).

INTRODUCTION

In a QKE protocol there are three parties; Alice and Bob who want to exchange a secret key and a malicious third party, Eve. Eve has access to unlimited quantum computational power and she can monitor but not alter all public communication between Alice and Bob. Alice and Bob transmit quantum states over a (lossless) quantum communication channel. They perform measurements on their respective quantum states following the QKE protocol. From the measurements they extract bit values. By communication over an authenticated public channel, Alice and Bob agree which bits will be used for secret key generation. They estimate the bit error rate ε of these key bits with another round of public communication. Alice and Bob then apply information reconciliation and privacy amplification to the key bits so that they end with a shared bit string K.

In [1], a generic security proof is proposed by which the security of a wide class of QKE protocols is proved. It is based on the fact that privacy amplification is equally secure when an adversary's memory for data storage is quantum rather than classical ([2]). It gives Alice and Bob a threshold d for the bit error rate ε. This means that if $\varepsilon \leq d$, then K is unconditionally secure. The generic security proof is applicable to QKE protocols that involve quantum systems with a finite number of degrees of freedom (in [1] it was proved that BB84 is secure for $\varepsilon \leq 11\%$). It does not immediately apply however to QKE protocols using quantum systems with an infinite number of degrees of freedom.

In [4], a QKE protocol, which we denote by GP00, was presented that resembles BB84 but works with squeezed states which are infinite-dimensional. The

* Technische Universiteit Eindhoven, Eindhoven, The Netherlands.

† Information Security Systems, Philips Research Eindhoven, Eindhoven, The Netherlands.

squeezing parameter r determines the amount of squeezing of a squeezed state. In [4] it was proved that the protocol is secure if $\varepsilon \leq 11\%$ hence if $r \geq 0.289$. In this paper we apply the generic security proof to GP00 and find the same thresholds. We will further discuss some security issues of GP00.

SQUEEZED STATES

Let $\alpha \in \mathbb{C}$ and $\zeta = re^{i\varphi}$ with $r \in \mathbb{R}$ and $\varphi \in [0, \pi)$. The squeezed state corresponding to ζ, α is denoted by $|\zeta, \alpha\rangle$. It satisfies the Heisenberg uncertainty relation with equality for the position and momentum operators x and p if and only if $\varphi = 0$ so $\zeta = r \in \mathbb{R}$. That is, $\sigma_x \sigma_p = \frac{1}{2}$. In fact, if we measure the position or the momentum of the squeezed state $|\zeta = r, \alpha\rangle$, then the measured value x or p is distributed according to a Gaussian distribution with variance equal to respectively $\sigma_x^2 = \frac{1}{2}e^{2r}$ or $\sigma_p^2 = \frac{1}{2}e^{-2r}$. We say that r is the squeezing parameter and that $|r, \alpha\rangle$ is a minimum uncertainty squeezed state. If $r < 0$, then $\sigma_x^2 < \sigma_p^2$ and the squeezed state is "squeezed" in x. If $r > 0$, then the squeezed state is "squeezed" in p. After a measurement of position value x or momentum value p, the squeezed state collapses to respectively a position eigenstate $|x\rangle$ or a momentum eigenstate $|p\rangle$.

BIT ENCODING AND DECODING SCHEME FOR GP00

Fix $\hat{r} > 0$. All squeezed states are squeezed with squeezing parameter $r = -\hat{r}$ (squeezing in x) or $r = \hat{r}$ (squeezing in p). We divide the real numbers into two sets of intervals $\mathcal{L}_0$ and $\mathcal{L}_1$ as in Fig. 1. Alice samples $a \in \mathbb{R}$ from the Gaussian $P_A(a)$ with mean 0 and variance $\frac{1}{2}e^{2\hat{r}}$:

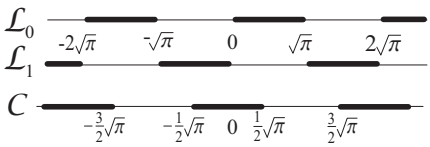

Figure 1: Encoding and Decoding intervals

$$P_A(a) = \frac{1}{\sqrt{\pi e^{2\hat{r}}}} \exp\left[-\frac{a^2}{e^{2\hat{r}}}\right]. \tag{1}$$

If $a \in \mathcal{L}_0$, Alice extracts bit 0, otherwise she extracts bit 1. She prepares a squeezed state squeezed in x or p at random. If she squeezes in x, she sends to Bob

$$|-\hat{r}, \alpha\rangle \text{ with } \begin{cases} \langle x \rangle & = a' = a\sqrt{1 - e^{-4\hat{r}}} \\ \langle p \rangle & = 0 \end{cases}$$

If she squeezes in p, she sends to Bob the squeezed state

$$|\hat{r}, \alpha\rangle \text{ with } \begin{cases} \langle x \rangle & = 0 \\ \langle p \rangle & = a' = a\sqrt{1 - e^{-4\hat{r}}} \end{cases}$$

For every squeezed state Alice computes and announces $\varphi = a \bmod \sqrt{\pi}$ where $0 \leq \varphi < \sqrt{\pi}$. Note that there exists an $n_a \in \mathbb{Z}$ such that $a = n_a\sqrt{\pi} + \varphi$. Every value for φ should be equally likely because then $P(a \in \mathcal{L}_0|\varphi) = P(a \in \mathcal{L}_0) = 0.5$ such that φ leaks no information to Eve (we further discuss this in the final section).

For every squeezed state Bob decides at random to measure the position or the momentum. Suppose that the outcome of his measurement is b where $b = a + \delta$ for some $\delta \in \mathbb{R}$. Note that $b - \varphi = n_a\sqrt{\pi} + \delta$. Bob extracts bit value 0 if $b - \varphi = n_a\sqrt{\pi} + \delta$ rounded to the nearest integer multiple of $\sqrt{\pi}$ is an even multiple of $\sqrt{\pi}$ and bit value 1 otherwise. If we define the decoding interval $\mathcal{C}$ as in Fig. 1, then Alice and Bob find the same bit if $\delta = b - a \in \mathcal{C}$. This is because if $\delta \in \mathcal{C}$, then $n_a\sqrt{\pi} + \delta$ rounded to the nearest integer multiple of $\sqrt{\pi}$ is equal to $n_a\sqrt{\pi}$. They find different bits if $\delta = b - a \notin \mathcal{C}$.

BIT EXTRACTION PROBABILITIES FOR GP00

If Alice and Bob use different bases, then the value measured by Bob has a Gaussian distribution centered at 0. This distribution is shown as the graph on the left in Fig. 2 for $a = \frac{1}{2}\sqrt{\pi}$. The marked area represents the probability that Alice and Bob find the same bit and equals 0.5 if $a = \frac{1}{2}\sqrt{\pi}$. In fact, this probability is maximal if $a = 2n\sqrt{\pi}$, is equal to 0.5 if $a = (2n + \frac{1}{2})\sqrt{\pi}$ and is minimal if $a = (2n + 1)\sqrt{\pi}$. This means that if all values for φ are equally likely, then the bit extracted by Bob is random. The corresponding cases in the protocol can therefore be discarded. If Alice and Bob use the same basis, then the probability that they find the same bit is dependent on the distance between a and a', the mean value of Bob's squeezed state. This is illustrated in the graph on the right in Fig. 2 for $a' - a = \frac{1}{4}\sqrt{\pi}$. For illustration, this probability is 0.89 if $\hat{r} = 0.289$ and if $\hat{r} \to \infty$ it will approach 1. Note that if Alice and Bob use the same basis then, in contrast to BB84, they find the same bit with probability smaller than 1. This means that because of the squeezed states, additional quantum noise is introduced (ε_s).

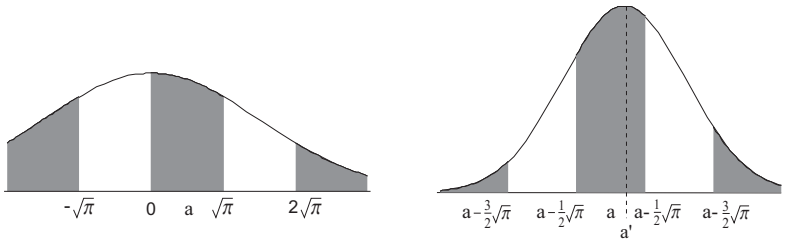

Figure 2: Bit correct probability if a) different basis are used and $a = \frac{1}{2}\sqrt{\pi}$ and b) the same basis is used and $a' - a = \frac{1}{4}\sqrt{\pi}$.

THE PROTOCOL GP00

We give the description of the protocol. At the end of the protocol, just before information reconciliation and privacy amplification, Alice and Bob each have an n-bit string respectively X and Y. After information reconciliation and privacy amplification they have a shared secure key K of length $k < n$.

1. Alice prepares approximately $4n$ squeezed states. For every squeezed state she decides to squeeze it in x or in p at random. She prepares the squeezed states according to the encoding scheme described in the previous sections. For every squeezed state she extracts a bit value. She sends the squeezed states to Bob.
2. For each squeezed state, Bob decides to measure the position or the momentum at random.
3. Bob confirms having received the squeezed states. Alice and Bob announce which bases they used.
4. Alice and Bob discard the cases where they did not use the same basis. From the remaining approximately $4n/2 = 2n$ bits Alice chooses n to serve as check bits and n to serve as key bits. For the squeezed states corresponding to these check and key bits, Alice computes φ. Alice sends all φ's to Bob with which Bob extracts check bits and key bits from his measured values. Alice and Bob's resulting key bit strings are X and Y.
5. Alice and Bob announce their check bits to estimate the bit error rate ε.
6. If $\varepsilon \leq 11\%$, then information reconciliation and privacy amplification follow such that Alice and Bob end with a shared secret key K.

The main difference between GP00 and BB84 is that Bob needs additional information φ about the squeezed states to extract bit values from his measured

values. Noise (ε) is not only caused by the channel or by Eve, but also by the natural noise of squeezed states (ε_s). If $\hat{r} \to \infty$, then $\varepsilon_s \to 0$ and GP00 becomes the continuous version of $BB84$.

THE GENERIC SECURITY PROOF

The generic security proof [1] can be applied to a generic QKE protocol equivalent to an entanglement based protocol. Let the measurements that Alice and Bob randomly apply to their received quantum states be the POVM's $\mathcal{F}$ and $\mathcal{G}$ and the bit error rate of the bits extracted from the measurements be ε. Let $\mathcal{R}$ be the set of all density operators $\tilde{\varrho}$ (describing the quantum state of two systems) for which it holds that if $\tilde{\varrho}$ is measured with respect to $\mathcal{F} \otimes \mathcal{F}$ or $\mathcal{G} \otimes \mathcal{G}$, then the two bits extracted from the measurement have bit error probability ε. Thus $\mathcal{R}$ is the set of all possible density operators describing the mutual state of Alice and Bob, given that the bit error rate is equal to ε. Let $\mathcal{Z}$ be a projective measurement on the density operator $\tilde{\varrho} \in \mathcal{R}$ with outcome described by the random variable Z. Let X and Y be random variables such that Alice's and Bob's bit strings consist of n realizations of these variables. The secret key rate R is now given by ([1])

$$R = H(X) - H(X|Y) - \arg_{\tilde{\varrho} \in \mathcal{R}} \max H(Z). \tag{2}$$

The rate might be improved by conditioning on additional information W gained during privacy amplification. The rate then becomes

$$R = H(X|W) - H(X|Y) - \arg_{\tilde{\varrho} \in \mathcal{R}} \max H(Z|W). \tag{3}$$

The generic security proof consists in finding the maximum error rate ε such that R is still positive and hence the extracted secret key K is secure.

ENTANGLEMENT BASED VERSION OF GP00

To be able to apply the generic proof to GP00, we regard it as an entanglement based protocol. The entangled states prepared by the dealer (given in both position eigenstates and momentum eigenstates) are as follows ([4])

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{\pi}} \int\int \exp\left[-\frac{\tilde{\Delta}^2}{2} x_a^2\right] \exp\left[-\frac{1}{2\tilde{\Delta}^2}\left(x_b - \sqrt{1-\tilde{\Delta}^4} x_a\right)^2\right] |x_a, x_b\rangle dx_b dx_a \\ &= \frac{1}{\sqrt{\pi}} \int\int \exp\left[-\frac{\tilde{\Delta}^2}{2} p_a^2\right] \exp\left[-\frac{1}{2\tilde{\Delta}^2}\left(p_b + \sqrt{1-\tilde{\Delta}^4} p_b\right)^2\right] |p_a, p_b\rangle dp_b dp_a \end{aligned}$$

where $0 < \tilde{\Delta}^2 \leq 1$. For $\tilde{\Delta}^2 < 1$, $|\psi\rangle$ is an entangled state.

Alice and Bob both get a part of this entangled state. If Alice measures the position of her part, she measures position value x_a with probability $P_x(x_a) = \frac{\tilde{\Delta}}{\sqrt{\pi}} \exp\left[-\tilde{\Delta}^2 x_a^2\right]$. By this measurement, she prepares for Bob the state

$$\frac{1}{(\pi\tilde{\Delta}^2)^{1/4}} \int \exp\left[-\frac{1}{2\tilde{\Delta}^2}\left(x_b - \sqrt{1-\tilde{\Delta}^4}x_a\right)^2\right]|x_b\rangle dx_b,$$

which is a squeezed state squeezed in x with mean position value $\sqrt{1-\tilde{\Delta}^4}x_a$ and mean momentum value 0.
If Alice measures the momentum of her part, she measures p_a with probability $P_p(p_a) = P_x(p_a)$. By this measurement, she prepares for Bob a squeezed state squeezed in p with mean momentum value $-\sqrt{1-\tilde{\Delta}^4}p_a$ and mean position 0.

If we choose $\tilde{\Delta}^2 = e^{-2\hat{r}}$, then the entanglement based protocol is equivalent to GP00; from Eq. 1 we see that $P_x(x_a) = P_p(x_a) = P_A(x_a)$ and the squeezed states produced by Alice's measurements in the entanglement based version are equal to the squeezed states sent by Alice in GP00. Note that in the entanglement based version, the mean momentum value is $-\sqrt{1-\tilde{\Delta}^4}p_a$ rather than $\sqrt{1-\tilde{\Delta}^4}p_a$. This means that Alice extracts a bit value and calculates φ from $-p_a$ rather than from p_a if she measured the momentum and from x_a if she measured the position. Alice and Bob find the same bit if $x_b - x_a \in \mathcal{C}$ or $p_b - (-p_a) = p_b + p_a \in \mathcal{C}$.

GENERIC SECURITY PROOF OF GP00

Let ε be the bit error probability of the check bits. Let the density operator $\tilde{\varrho} \in \mathcal{R}$; if of both parts of $\tilde{\varrho}$ the position is measured or the momentum, then the probability that the extracted bits differ is equal to ε. This can be formulated by

$$\int_{-\infty}^{\infty}\int_{x\in\mathcal{C}} \langle x_a, x_a+x|\tilde{\varrho}|x_a, x_a+x\rangle dx dx_a = 1-\varepsilon \quad (4)$$

$$\int_{-\infty}^{\infty}\int_{x\in\mathcal{C}^c} \langle x_a, x_a+x|\tilde{\varrho}|x_a, x_a+x\rangle dx dx_a = \varepsilon \quad (5)$$

$$\int_{-\infty}^{\infty}\int_{p\in\mathcal{C}} \langle p_a, -p_a+p|\tilde{\varrho}|p_a, -p_a+p\rangle dp dp_a = 1-\varepsilon \quad (6)$$

$$\int_{-\infty}^{\infty}\int_{p\in\mathcal{C}^c} \langle p_a, -p_a+p|\tilde{\varrho}|p_a, -p_a+p\rangle dp dp_a = \varepsilon \quad (7)$$

where e.g. $\langle x_a, x_a+x|\tilde{\varrho}|x_a, x_a+x\rangle$ is the probability that Alice measures position value x_a and Bob measures position value $x_a + x$.

As projective measurement $\mathcal{Z}$ we choose the continuous Bell measurement which is given by the projectors $\{|\psi(x,p)\rangle\langle\psi(x,p)||x,p\in\mathbb{R}\}$ with

$$|\psi(x,p)\rangle \;=\; \int_{-\infty}^{\infty} e^{ipx_a}|x_a,x_a+x\rangle dx_a \;=\; \int_{-\infty}^{\infty} e^{ixp_a}|p_a,-p_a+p\rangle dp_a.$$

If we define $p_{xp}=\langle\psi(x,p)|\tilde{\varrho}|\psi(x,p)\rangle$, then p_{xp} is the probability that if Alice and Bob both measure the position, then the difference of their outcomes is x and if they both measure the momentum, then the sum of their outcomes equals p. If x or $p\in\mathcal{C}$, then Alice and Bob extract the same bit and if x or $p\notin\mathcal{C}$ they extract different bits. We therefore group the probabilities p_{xp} in the following way

$$\lambda_1=\int_{p\in\mathcal{C}}\int_{x\in\mathcal{C}} p_{xp}dxdp \qquad \lambda_3=\int_{p\in\mathcal{C}}\int_{x\in\mathcal{C}^c} p_{xp}dxdp$$

$$\lambda_2=\int_{p\in\mathcal{C}^c}\int_{x\in\mathcal{C}} p_{xp}dxdp \qquad \lambda_4=\int_{p\in\mathcal{C}^c}\int_{x\in\mathcal{C}^c} p_{xp}dxdp.$$

For illustration, λ_2 is the probability that if Alice and Bob both measure the position, they find the same bit and if they both measure the momentum, they find different bits. We rewrite Eqs. (4,5,6,7) as

$$\lambda_1+\lambda_2 \;=\; 1-\varepsilon \qquad \lambda_3+\lambda_4 \;=\; \varepsilon \qquad \lambda_1+\lambda_3 \;=\; 1-\varepsilon \qquad \lambda_2+\lambda_4 \;=\; \varepsilon$$

With these relations, λ_1,λ_2 and λ_3 can be expressed in terms of λ_4. The entropy $H(Z)=-\sum_{i=1}^{4}\lambda_i\log_2\lambda_i$ is maximized for $\lambda_4=\varepsilon^2$ and then $H(Z)=2h(\varepsilon)$. The secret key bit rate becomes (Eq. 2) $R=1-h(\varepsilon)-2h(\varepsilon)=1-3h(\varepsilon)$. This rate is positive for $\varepsilon\leq 6.1\%$.

We improve the rate by using the additional information $W=X+Y$ gained during privacy amplification. It holds that

$$\begin{aligned} H(Z|W) &= \textstyle\sum_{i\in\{0,1\}} P(W=i)H(Z|W=i) \\ &= (1-\varepsilon)h\left(\tfrac{\lambda_1}{1-\varepsilon}\right)+\varepsilon h\left(\tfrac{\lambda_3}{\varepsilon}\right) \;=\; H(Z)-h(\varepsilon). \end{aligned}$$

The entropy $H(Z|W)$ is maximized for $\lambda_4=\varepsilon^2$ and then $H(Z|W)=h(\varepsilon)$. The rate R becomes (Eq. 3) $R=1-h(\varepsilon)-h(\varepsilon)=1-2h(\varepsilon)$ which is positive for $\varepsilon\leq 11\%$. This means that GP00 is secure if $\varepsilon\leq 11\%$. Because the noise generated by squeezed states (ε_s) is a part of ε, we have $\varepsilon_s\leq\varepsilon$. Calculations show that $\varepsilon_s\leq 11\%$ if $\hat{r}\geq 0.289$. This means that GP00 can only be secure if squeezed states are squeezed with squeezing parameter $\hat{r}\geq 0.289$.

RANDOMIZATION ISSUE OF φ.

In GP00, Alice announces $\varphi = a \bmod \sqrt{\pi}$. For unconditional security it has to hold that $P(a \in \mathcal{L}_0|\varphi) = P(a \in \mathcal{L}_0) = 0.5$. The probability $P(a \in \mathcal{L}_0|\varphi)$ is maximal at $\varphi = 0$, equal to 0.5 if $\varphi = \frac{1}{2}\sqrt{\pi}$ and minimal at $\varphi = \sqrt{\pi}$. For $\hat{r} = 0.289$ we find e.g. that $P(a \in \mathcal{L}_0|\varphi = 0) = 0.745$ which is rather high; it means that φ leaks a significant amount of information to Eve about the bit extracted by Alice. One way to solve this poblem, is to enlarge the lower bound for $\hat{r}$. For example, if $\hat{r} \geq 1.5$, then $P(a \in \mathcal{L}_0|\varphi = 0) = 0.5$ and no information leaks to Eve.

Another solution could be to make a discrete approximation of Alice's sampling distribution $P_A(a)$ as in Fig. 3. It then holds that every value for φ is equally likely, the value φ does not leak information to Eve and if Bob or Eve measures the squeezed state in the incorrect basis, the extracted bit is random. The catch, however, is that the resulting protocol has no entanglement based equivalent anymore such that the generic security proof [1] cannot be applied to it.

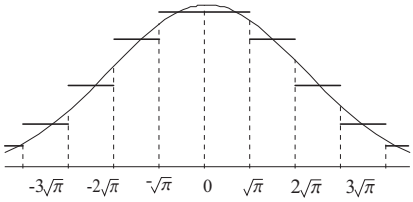

Figure 3: Discrete approximation of $P_A(a)$.

It seems that for unconditional security, the bit encoding and/or decoding strategy should be changed such that every value of φ becomes equally likely while the sampling distribution $P_A(a)$ and the squeezed states sent to Bob remain the same. In this way, the resulting protocol has an entanglement based equivalent. An idea to do this is to choose $\varphi = |a| \bmod \sqrt{\pi}$ instead of $\varphi = a \bmod \sqrt{\pi}$. At the moment, we are still studying this randomization issue of φ.

REFERENCES

[1] M. Christiandl, R. Renner & A. Ekert, "A Generic Security Proof for Quantum Key Distribution," 2004, quant-ph/0402131.

[2] R. König, U. Maurer & R. Renner; "On the power of quantum memory,"2003, quant-ph/0305154.

[3] C.H. Bennett & G. Brassard; "Quantum Cryptography; Public key distribution and coin tossing," 1984, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179, IEEE, New York.

[4] D. Gottesman & J. Preskill, "Secure quantum key exchange using squeezed states," 2000, quant-ph/0008046.