New Result in Quantum Cryptograp...

Howard E. Brandt
U.S. Army Research Laboratory
Adelphi, MD 20783-1197
Phone: (301) 394-4143
email: hbrandt@lamp0.arl.army.mil

Abstract

In the entangled translucent eavesdropping scenario of key generation in quantum cryptography, I demonstrate that the unsafe error rate based on standard mutual information comparisons is equivalent to the maximum allowable error rate based on perfect mutual information for the eavesdropper. In this case, the unsafe error rate is not in fact overly conservative, as is commonly supposed.

Introduction

In a popular scheme for entangled translucent eavesdropping in quantum cryptography, the key generation procedure involves the transmission, interception, and reception of nonorthogonal photon polarization states [1]. The eavesdropping is translucent in the sense that it results in only a small perturbation on the carrier, following quantum entanglement between the carrier and the probe states. At the receiving end, a POVM (positive operator valued measure) is employed in the measurement process. The eavesdropping involves an ordinary information-maximizing von Neumann-type projective measurement. It is conventional to refer to the transmitter as Alice, the receiver as Bob, and the eavesdropper as Eve. It is commonly assumed that in any eavesdropping scenario of key generation in quantum cryptography, the transmission is unsafe if the mutual information in the Alice-Bob channel, I_{AB}, is less than the minimum of the mutual information in the Alice-Eve channel, I_{AE}, and the mutual information in the Bob-Eve channel, I_{BE}, namely [1],

$$I_{AB} \le \min(I_{AE}, I_{BE}) \ . \tag{1}$$

This criterion is commonly supposed to be overly conservative (overcautious) [1,2]. Here and in the following, any mutual information is understood to be maximal. I define the unsafe error rate to be the smallest error rate, Q, in the Alice-Bob channel, such that the equality in Eq. (1) is satisfied, namely,

$$Q_u = \text{smallest } Q \text{ such that } I_{AB} = \min(I_{AE}, I_{BE}) \ . \tag{2}$$

Here, the dependence of mutual information on Bob's error rate Q (the error rate in the Alice-Bob channel) is implicit.

The maximum allowable error rate, $Q_{\max}$, is the value of the error rate in the Alice-Bob channel, for which the mutual information in the Bob-Eve channel is unity, namely [1],

$$Q_{\max} = Q \text{ such that } I_{BE} = 1 \ . \tag{3}$$

This corresponds to perfect information for the eavesdropper.

I recently obtained new closed-form algebraic expressions for the error rates and mutual information, expressed only in terms of the POVM receiver error rate, Q, and the angle θ between the carrier polarization states [3,4]. To do this, I employed the quantum mechanical unitarity conditions that must be satisfied by the eavesdropping device parameters, together with known expressions for the error rates and mutual information, expressed in terms of unknown parameters characterizing the apparatus of the eavesdropper. I showed that the error rate in the Alice-Eve channel is given by [4]

$$Q_{AE}(Q,\theta) = \frac{1}{2} - \left(\frac{1}{2} - Q\right)\left(1 - F(Q,\theta)^2\right)^{1/2} \ , \tag{4}$$

where

$$F(Q,\theta) = \frac{2Q(1-Q) - [Q(1-Q)]^{1/2}\cos\theta}{[Q(1-Q)]^{1/2}\cos\theta\,\{2[Q(1-Q)]^{1/2}\cos\theta - 1\}} \ . \tag{5}$$

The corresponding mutual information in the Alice-Eve channel is

$$I_{AE}(Q_{AE}) = 1 + Q_{AE}\log_2 Q_{AE} + (1 - Q_{AE})\log_2(1 - Q_{AE}) \ . \tag{6}$$

In the Bob-Eve channel, one has [4]

$$Q_{BE}(Q,\theta) = \frac{1}{2} - \frac{1}{2}\left(1 - F(Q,\theta)^2\right)^{1/2} \tag{7}$$

and

$$I_{BE}(Q_{BE}) = 1 + Q_{BE}\log_2 Q_{BE} + (1 - Q_{BE})\log_2(1 - Q_{BE}) \ . \tag{8}$$

One also has the well-known expression for the mutual information, $I_{AB}(Q)$, in the Alice-Bob channel in terms of the error rate, Q, in the Alice-Bob channel [1],

$$I_{AB}(Q) = 1 + Q \log_2 Q + (1 - Q)\log_2(1 - Q) \ . \quad (9)$$

In the present work, I prove a significant new result, namely, that in the entangled translucent eavesdropping scenario, the unsafe error rate based on Eq. (2) is equivalent to the maximum allowable error rate based on Eq. (3). In this case, the unsafe error rate is not in fact overly conservative, as is commonly supposed.

Maximum Allowable Error Rate

First define

$$\alpha = \frac{\pi}{4} - \frac{\theta}{2} \ . \quad (10)$$

Next, evaluating Eq. (7) for $Q = \sin^2\alpha$, one obtains

$$Q_{BE}(\sin^2\alpha, \theta) = 0 \ . \quad (11)$$

If one next substitutes Eq. (11) in Eq. (8), one obtains

$$I_{BE}(Q_{BE}(\sin^2\alpha, \theta)) = 1 \ . \quad (12)$$

Therefore, comparing Eqs. (12) and (3), one concludes that

$$Q_{\max} = \sin^2\alpha \ , \quad (13)$$

in agreement with Eq. (41) of Ekert et al [1]. The maximum allowable error rate is given by Eqs. (13) and (10) in terms of the angle between the two photon polarization states.

Proof that Unsafe Error Rate is Maximum Allowable Error Rate

Evaluating Eq. (4) for $Q = \sin^2\alpha$, one obtains

$$Q_{AE}(\sin^2\alpha, \theta) = \sin^2\alpha \ . \quad (14)$$

If one next substitutes Eq. (14) in Eq. (6), one obtains

$$I_{AE}(Q_{AE}(\sin^2\alpha, \theta)) = 1 + \sin^2\alpha \log_2(\sin^2\alpha) + \cos^2\alpha \log_2(\cos^2\alpha) \ . \quad (15)$$

Next, using Eq. (9), one obtains

$$I_{AB}(\sin^2\alpha) = 1 + \sin^2\alpha \log_2(\sin^2\alpha) + \cos^2\alpha \log_2(\cos^2\alpha) \ . \quad (16)$$

Comparing Eq. (16) with Eq. (15), one can conclude that

$$I_{AE}(Q_{AE}(\sin^2\alpha, \theta)) = I_{AB}(\sin^2\alpha) \ . \quad (17)$$

Using Eq. (12), one obtains

$$\begin{aligned} &\min(I_{AE}(Q_{AE}(\sin^2\alpha, \theta)), I_{BE}(Q_{BE}(\sin^2\alpha, \theta))) \\ &\quad = \min(I_{AE}(Q_{AE}(\sin^2\alpha, \theta)), 1) \\ &\quad = I_{AE}(Q_{AE}(\sin^2\alpha, \theta)) \ . \end{aligned} \quad (18)$$

Therefore, substituting Eq. (17) in Eq. (18), one has

$$\min(I_{AE}(Q_{AE}(\sin^2\alpha, \theta)), I_{BE}(Q_{BE}(\sin^2\alpha, \theta))) = I_{AB}(\sin^2\alpha) \ . \quad (19)$$

Next comparing Eq. (19) with Eq. (2), one can conclude that

$$Q_u = \sin^2\alpha \ . \quad (20)$$

Finally, comparing Eqs. (13) and (20), one has

$$Q_u = Q_{\max} \ , \quad (21)$$

which was the claim. If one substitutes Eq.(10) in Eqs. (20) and (21), one obtains

$$Q_u = Q_{\max} = \frac{1}{2}(1 - \sin\theta) \ , \quad (22)$$

written explicitly in terms of the angle between the photon polarization states.

Conclusion

I conclude that for the entangled translucent eavesdropping scenario of Ekert et al [1], the unsafe error rate defined by Eq. (2) is in fact equal to the maximum allowable error rate defined by Eq. (3). These rates are given by Eq. (22).

For this scenario, the unsafe error rate is not in fact overly conservative, as is commonly supposed.

References

1. A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, *Eavesdropping on Quantum-Cryptographical Systems*, Phys. Rev. A **50**, 1047 (1994).

2. U. M. Maurer, *Secret Key Agreement by Public Discussion from Common Information*, IEEE Trans. Information Theory **39**, 733 (1993).

3. H. E. Brandt, J. M. Myers, and S. J. Lomonaco, Jr., *Entangled Translucent Eavesdropping in Quantum Cryptography*, presented at Symposium on Quantum Computing, Memory and Communications, abstract published in Program, OSA Annual Meeting, 20–24 October 1996, Rochester, NY, Optical Society of America (1996).

4. H. E. Brandt, J. M. Myers, and S. J. Lomonaco, Jr., *New Results in Entangled Translucent Eavesdropping in Quantum Cryptography*, to appear in Proceedings of SPIE Conference, Photonic Quantum Computing, 21–25 April 1997, Orlando, FL, S. P. Hotaling and A. R. Pirich, editors (1997).

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: New Result in Quantum Cryptography

B. DATE Report Downloaded From the Internet 1/5/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **U.S Army Research Laboratory**
Howard E. Brandt (301) 394-4143
2800 Powder Mill Road
Adelphi, MD 20783

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: VM_ **Preparation Date**: 1/5/99__

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.