International Journal of Theoretical Physics
Volume 56, Issue 7, 1 July 2017, Pages 2231-2242

The Probe Attack on the Bennett-Brassard 1984 Protocol in the Presences of Noisy Amplitude Damping Channel (Article)

Abdel-Hameed, H.F.[ab], Zidan, N.[a], Wahiddin, M.R.[c]

[a]Department of Mathematics, Faculty of Science, Sohag University, Sohag, Egypt
[b]Department of Mathematics, Faculty of Science and Education, Al-Khurma Branch, Taif University, Al-Khurma, Saudi Arabia
[c]Department of Computer Science, Faculty of ICT, International Islamic University Malaysia (IIUM), P.O. Box 10, Kuala Lumpur, Malaysia

Abstract

View references (23)

In this contribution, we investigate the effect of the generalized amplitude damping as Eve's strategy to cause an error on the received signal during generating a quantum key distribution between Alice and Bob using Bennett-Brassard 1984 (BB84) protocol. For small values of the channel strength and larger values of the decay parameter, the entanglement decays gradually. The phenomena of the sudden changes of entanglement are observed for smaller and larger values of the willing initial error. These changes of entanglement decay gradually when Alice prepares her qubit in horizontal-vertical basis. While the sudden changes are depicted if the initial state is prepared in the diagonal-anti-diagonal basis. Bob will get his measurement with an error, where the probability of this error depends on the initial polarized angle, the initial desired error and the channel parameters. © 2017, Springer Science+Business Media New York.

Author keywords

Bennett-Brassard 1984 protocol Eve-Alice entanglement Eve's strategy

ISSN: 00207748
DOI: 10.1007/s10773-017-3370-2
Source Type: Journal
Document Type: Article
Original language: English
Publisher: Springer New York LLC

References (23)

View in search results format

All Export Print E-mail Save to PDF Create bibliography

1 Bennett, C.H., Brassard, G.
(1984) *Proceeding of IEEE international Conference on Computers, systems and Signal Processing*, 175. IEE, New York: Bangaloare

2 Bennett, C.H., Brassard, G., Mermin, N.D.
Quantum cryptography without Bell's theorem
(1992) *Physical Review Letters*, 68 (5), pp. 557-559. Cited 1321 times.
doi: 10.1103/PhysRevLett.68.557
View at Publisher

3 Bennett, C.H.

Quantum cryptography using any two nonorthogonal states

(1992) *Physical Review Letters*, 68 (21), pp. 3121-3124. Cited 1819 times.
doi: 10.1103/PhysRevLett.68.3121

View at Publisher

4 Fuchs, C.A., Peres, A.

Quantum-state disturbance versus information gain: Uncertainty relations for quantum information

(1996) *Physical Review A - Atomic, Molecular, and Optical Physics*, 53 (4), pp. 2038-2045. Cited 206 times.
doi: 10.1103/PhysRevA.53.2038

View at Publisher

5 Fuchs, C.A., Gisin, N., Griffiths, R.B., Niu, C.-S., Peres, A.

Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy

(1997) *Physical Review A - Atomic, Molecular, and Optical Physics*, 56 (2), pp. 1163-1172. Cited 357 times.
doi: 10.1103/PhysRevA.56.1163

View at Publisher

6 Slutsky, B.A., Rao, R., Sun, P.-C., Fainman, Y.

Security of quantum cryptography against individual attacks

(1998) *Physical Review A - Atomic, Molecular, and Optical Physics*, 57 (4), pp. 2383-2398. Cited 94 times.
doi: 10.1103/PhysRevA.57.2383

View at Publisher

7 Brandt, H.E.

Quantum-cryptographic entangling probe

(2005) *Physical Review A - Atomic, Molecular, and Optical Physics*, 71 (4), art. no. 042312. Cited 27 times.
http://oai.aps.org/oai/?verb=ListRecords&metadataPrefix=oai_apsmeta_2&set=journal:PRA:71
doi: 10.1103/PhysRevA.71.042312

View at Publisher

8 Kim, T., Stork Genannt Wersborg, I., Wong, F.N.C., Shapiro, J.H.

Complete physical simulation of the entangling-probe attack on the Bennett-Brassard 1984 protocol

(2007) *Physical Review A - Atomic, Molecular, and Optical Physics*, 75 (4), art. no. 042327. Cited 12 times.
http://oai.aps.org/oai?verb=GetRecord&Identifier=oai:aps.org:PhysRevA.75.042327&metadataPrefix=oai_apsmeta_2
doi: 10.1103/PhysRevA.75.042327

View at Publisher

9 Herbauts, I.M., Bettelli, S., Hübel, H., Peev, M.

On the optimality of individual entangling-probe attacks against BB84 quantum key distribution

(2008) *European Physical Journal D*, 46 (2), pp. 395-406. Cited 7 times.
doi: 10.1140/epjd/e2008-00002-x

View at Publisher

10 Bennett, C.H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J.A., Wootters, W.K.
Purification of noisy entanglement and faithful teleportation via noisy channels

(1996) *Physical Review Letters*, 76 (5), pp. 722-725. Cited 1757 times.
doi: 10.1103/PhysRevLett.76.722

View at Publisher

11 Bennett, C.H., DiVincenzo, D.P., Smolin, J.A., Wootters, W.K.
Mixed-state entanglement and quantum error correction

(1996) *Physical Review A - Atomic, Molecular, and Optical Physics*, 54 (5), pp. 3824-3851. Cited 3196 times.
doi: 10.1103/PhysRevA.54.3824

View at Publisher

12 Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C., Popescu, S., Sanpera, A.
Quantum privacy amplification and the security of quantum cryptography over noisy channels

(1996) *Physical Review Letters*, 77 (13), pp. 2818-2821. Cited 802 times.
doi: 10.1103/PhysRevLett.77.2818

View at Publisher

13 Metwally, N.
More efficient entanglement purification

(2002) *Physical Review A - Atomic, Molecular, and Optical Physics*, 66 (5), pp. 054302/1-054302/4. Cited 12 times.

View at Publisher

14 Metwally, N., Obada, A.-S.
More efficient purifying scheme via controlled-controlled NOT gate

(2006) *Physics Letters, Section A: General, Atomic and Solid State Physics*, 352 (1-2), pp. 45-48. Cited 8 times.
doi: 10.1016/j.physleta.2005.11.040

View at Publisher

15 Metwally, N., Abdelaty, M., Obada, A.-S.F.
Quantum teleportation via entangled states generated by the Jaynes-Cummings model

(2004) *Chaos, Solitons and Fractals*, 22 (3), pp. 529-535. Cited 11 times.
doi: 10.1016/j.chaos.2004.02.045

View at Publisher

16 Metwally, N., Al-Amin, A.A.
(2009) *Physica E*, 41, p. 722.

17 Jeong, Y.-C., Kim, Y.-S., Kim, Y.-H.
Effects of depolarizing quantum channels on BB84 and SARG04 quantum cryptography protocols

(2011) *Laser Physics*, 21 (8), pp. 1438-1442. Cited 9 times.
doi: 10.1134/S1054660X11150126

View at Publisher

18 Loura, R., Almeida, A.J., André, P.S., Pinto, A.N., Mateus, P., Paunković, N.

Noise and measurement errors in a practical two-state quantum bit commitment protocol

(2014) *Physical Review A - Atomic, Molecular, and Optical Physics*, 89 (5), art. no. 052336. Cited 10 times.
http://harvest.aps.org/bagit/articles/10.1103/PhysRevA.89.052336/apsxml
doi: 10.1103/PhysRevA.89.052336

View at Publisher

19 Siomau, M., Kamli, A.A.

Defeating entanglement sudden death by a single local filtering

(2012) *Physical Review A - Atomic, Molecular, and Optical Physics*, 86 (3), art. no. 032304. Cited 12 times.
http://oai.aps.org/filefetch?identifier=10.1103/PhysRevA.86.032304&component=fulltext&description=markup&format=xml
doi: 10.1103/PhysRevA.86.032304

View at Publisher

20 Srikanth, R., Banerjee, S.

Squeezed generalized amplitude damping channel

(2008) *Physical Review A - Atomic, Molecular, and Optical Physics*, 77 (1), art. no. 012318. Cited 39 times.
http://oai.aps.org/oai?verb=GetRecord&Identifier=oai:aps.org:PhysRevA.77.012318&metadataPrefix=oai_apsmeta_2
doi: 10.1103/PhysRevA.77.012318

View at Publisher

21 Montealegre, J.D., Paula, F.M., Saguia, A., Sarandy, M.S.

One-norm geometric quantum discord under decoherence

(2013) *Physical Review A - Atomic, Molecular, and Optical Physics*, 87 (4), art. no. 042115. Cited 56 times.
http://oai.aps.org/filefetch?identifier=10.1103/PhysRevA.87.042115&component=fulltext&description=markup&format=xml
doi: 10.1103/PhysRevA.87.042115

View at Publisher

22 Metwally, N.

Single and double changes of entanglement

(2014) *Journal of the Optical Society of America B: Optical Physics*, 31 (4), pp. 691-696. Cited 7 times.
http://www.opticsinfobase.org/view_article.cfm?gotourl=http%3A%2F%2Fwww%2Eopticsinfobase%2Eorg%2FDirectPDFAccess%2FFA2E26A7-EB33-3187-EAC02E678469C807_281179%2Fjosab-31-4-691%2Epdf%3Fda%3D1%26id%3D281179%26seq%3D0%26mobile%3Dno&org=Elsevier%20Inc
doi: 10.1364/JOSAB.31.000691

View at Publisher

23 Karpat, G., Gedik, Z.

Correlation dynamics of qubit-qutrit systems in a classical dephasing environment

(2011) *Physics Letters, Section A: General, Atomic and Solid State Physics*, 375 (47), pp. 4166-4171. Cited 41 times.
doi: 10.1016/j.physleta.2011.10.017

View at Publisher

Zidan, N.; Department of Mathematics, Faculty of Science, Sohag University, Sohag, Egypt;
email:nazidan@yahoo.com