



اصلاحیه‌ای بر پروتکل BB84 برای افزایش امنیت حالت‌های کوانتومی در یک پیام رمز شده نوری

سمیرا مرشدی^۱، فرامرز اسماعیلی سراجی^۲ و منصور رضایی مرساق^۱

^۱گروه فیزیک، دانشگاه آزاد اسلامی، تهران شمال، حکیمیه، تهران

^۲گروه مخابرات نوری، مرکز تحقیقات مخابرات ایران (پژوهشگاه)، تهران

چکیده- در این مقاله، با به کارگیری اصول مکانیک کوانتومی تغییری در پروتکل BB84 ایجاد کرده‌ایم و با استفاده از روش جستجوی تصادفی نشان داده شده که تقریب زدن یک حالت دو کیوبیتی درهم تنیده با حالت‌های ضربی دو کیوبیتی مشکلاتی برای شنودگر پنهانی ایجاد می‌کند. نتیجه‌های به دست آمده می‌تواند در رمزگذاری اطلاعات سری در سیستم‌های مخابرات کوانتومی مورد استفاده قرار گیرد.

کلید واژه- کیوبیت، روش جستجوی تصادفی، درهم تنیده، امنیت

A Correction on BB84 Protocol for Enhancement of Quantum State Security in an Encoded Optical Message

Samira Morshedi¹, Faramarz E. Seraji², M. Rezaie Mersagh¹

¹Phsycis Gorup, Islamic Azad Univ., Tehran Shomal Branch, Hakimieh, Tehran

Abstract- In this paper, using quantum mechanics principles, a change is made in BB84 protocol, then by utilizing random search method, we have shown that approximation of entangled two-Qbit state with two-Qbit multiplication state, makes eavesdropper confuse in decoding the secured information. The obtained results can be used in encoding of covert information in quantum communication systems.

Kerwords: Q-bit, Random search method, Entanglement, Security.

که همگان می‌توانند از این تبدیل یکانی $U : H^N \rightarrow H^N$ آگاه شوند.

۲- کارهایی که آلیس در اینجا انجام می‌دهد با پروتکل BB84 به دلایل زیر متفاوت است: (الف) تا هنگامی که همه N کیوبیت را تولید نکند، فرستادن کیوبیت‌ها را به تعویق می‌اندازد.^۲

(ب) سپس U را برکیوبیت‌ها اعمال می‌کند. (ج) آنگاه کیوبیت‌ها را یکی یکی می‌فرستد. آلیس پیش از فرستادن هر کیوبیت منتظر می‌ماند تا باب به او خبر دهد که کیوبیت پیشین را دریافت کرده است.

۳- کارهایی که باب اینجا انجام می‌دهد با پروتکل BB84 متفاوت است زیرا او:

(الف) تا هنگامی که همه N کیوبیت را دریافت نکرده است، اندازه‌گیری‌های مورد نیاز پروتکل BB84 را انجام نمی‌دهد.

(ب) فوراً پس از دریافت هر کیوبیت به آلیس خبر می‌دهد. (ج) با دریافت دنباله N کیوبیتی، تبدیل U^{-1} را بر آن‌ها اعمال می‌کند و آنگاه همانند آنچه در پروتکل BB84 داشتیم روی آن‌ها اندازه‌گیری انجام می‌دهد.

تبدیل U را می‌توان بسطی برای پروتکل BB84 در نظر گرفت. شنودگر کاملاً از U آگاه است، زیرا به طور همگانی اعلام می‌شود. چون باب به محض دریافت هر کیوبیت آلیس را آگاه می‌کند، شنودگر بر هر حالت N -کیوبیتی دسترسی یک به یک دارد. در پروتکل ما آلیس کیوبیت‌هایی از حالت $\langle \psi_{a_1, a_2, \dots, a_N} \rangle$ را یک به یک برای باب می‌فرستد.

اگر U به شکل زیر باشد:

$$U = U_1 \otimes U_2 \otimes \dots \otimes U_N \quad (1)$$

$$\begin{aligned} U(\lvert a_1 \rangle \otimes \lvert a_2 \rangle \otimes \dots \otimes \lvert a_N \rangle) &= (U_1 \otimes U_2 \otimes \dots \otimes U_N)(\lvert a_1 \rangle \otimes \lvert a_2 \rangle \otimes \dots \otimes \lvert a_N \rangle) \\ &= U_1 \lvert a_1 \rangle \otimes U_2 \lvert a_2 \rangle \otimes \dots \otimes U_N \lvert a_N \rangle \\ &= \lvert \psi_{a_1, a_2, \dots, a_N} \rangle \end{aligned} \quad (2)$$

اگر U به گیتهای تک-کیوبیتی تجزیه پذیر باشد، حالت N -کیوبیتی فرستاده شده، حالتی ضربی است. شنودگر می‌تواند U را بی اثر کند و به کیوبیت‌های نادرهم تنیده حمله کرده و با U^\dagger و U حالت فرستاده

۱- مقدمه

در سال ۱۹۹۲ پروتکل BB84 بر گرفته از پروتکل BB84 است که تنها دو پایه نامتعادم $|+\rangle$ و $|-\rangle$ را به کار می‌برد [1]. سپس هوونگ لو با سازگار کردن BB84 بر پایه عملگرهای x, y, z به پروتکل ۶ حالتی دست یافت [2]. نخستین پیشنهاد برای BB84 تنها امنیت در برابر مدل‌های حمله ساده را محافظت می‌کرد [3]. اگرچه برای نشان دادن امنیت BB84 باید به شنودگر اجازه دهیم تا هر عملی را که مکانیک کوانتمی مجاز می‌داند انجام دهد. امنیت بی قید و شرط پروتکل BB84 برای نخستین بار در سال ۱۹۹۶ به اثبات رسید. [4]. پس از آن گروهی دیگر اثبات دیگری را با استفاده از شیوه‌ای متفاوت ارائه کردند [5-8].

در سال ۱۹۹۹، اثبات ساده‌ای از کلیدهای رمزگذاری کوانتمی ارائه شد [9] که به یک پروتکل گلچین کننده اطلاعات درهم تنیده^۱ مربوط می‌شد [10]. اخیراً رمزگذاری کوانتمی تنیده در فضای آزاد در فاصله بیش از ۱۵ کیلومتر آزمایش شده است که در آن از پروتکل BB84 استفاده شده است [11]. در سال‌های اخیر، امنیت رمزگذاری سیستم‌های کوانتمی مورد توجه ویژه محققان قرار گرفته و با استفاده از پروتکل BB84 جنبه‌های مختلف آن بررسی شده است [12, 13]

در این مقاله، با به کار گیری اصول مکانیک کوانتمی تغییری در پروتکل BB84 ایجاد کرده‌ایم و با بیان جزئیات نشان داده‌ایم که تقریب زدن یک حالت دو کیوبیتی درهم تنیده با حالت‌های ضربی دو کیوبیتی مشکلاتی برای شنودگر پنهانی ایجاد می‌کند.

۲- بهینه‌سازی حالت‌های کوانتمی در یک پیام

رمز شده نوری

در این بخش پروتکل را که بر پایه پروتکل BB84 بنا شده را تحلیل می‌کنیم. پروتکل ما در مرحله‌های زیر با پروتکل BB84 متفاوت است:

۱- پیش از هر چیز آلیس (فرستنده) و باب (گیرنده) برای توزیع کلید روی یک تبدیل یکانی توافق می‌کنند به طوری

¹ Entanglement Distribution Protocol: EDP

از بهنجارش بردارها در رابطه‌های (۶) تا (۸)، داریم:

$$r_{\alpha_1}^2 + r_{\alpha_2}^2 + r_{\alpha_3}^2 + r_{\alpha_4}^2 = 1 \quad (9)$$

$$r_{\omega_1}^2 + r_{\omega_2}^2 = 1 \quad (10)$$

$$r_{\phi_1}^2 + r_{\phi_2}^2 = 1 \quad (11)$$

مقادرهای r_α را می‌توان با سه زویه $\bar{\theta} = (\theta_1, \theta_2, \theta_3)$ که نشان دهنده نقاط روی سطح یک کره چهار بعدی هستند، به صورت زیر بیان می‌کنیم:

$$\begin{cases} r_{\alpha_1} = \cos \theta_1 \\ r_{\alpha_2} = \sin \theta_1 \cos \theta_2 \\ r_{\alpha_3} = \sin \theta_1 \sin \theta_2 \cos \theta_3 \\ r_{\alpha_4} = \sin \theta_1 \sin \theta_2 \sin \theta_3 \end{cases} \quad (12)$$

همچنین مدول‌های کیوبیت‌های شنودگر دو دلیه را نمایش می‌دهند که نقطه‌های بر روی محیط آن‌ها را بازویه‌های Φ و Ω نمایش داد:

$$r_{\phi_1} = \cos \Phi, \quad r_{\phi_2} = \sin \Phi \quad (13)$$

$$r_{\omega_1} = \cos \Omega, \quad r_{\omega_2} = \sin \Omega \quad (14)$$

حال با جایگذاری r_{α_j} در بردارهای (۶) تا (۸)،

رابطه E_{mm} به صورت زیر به دست می‌آید:

$$\begin{aligned} E_{mm} &= \max_{|\psi\rangle} \min_{\{|\psi_i\rangle\}} \left\| |\psi\rangle - \bigotimes_{i=1}^N |\psi_i\rangle \right\| \\ &= \left\| \begin{pmatrix} \cos \theta_1 e^{i\alpha_1} \\ \sin \theta_1 \cos \theta_2 e^{i\alpha_2} \\ \sin \theta_1 \sin \theta_2 \cos \theta_3 e^{i\alpha_3} \\ \sin \theta_1 \sin \theta_2 \sin \theta_3 e^{i\alpha_4} \end{pmatrix} - \begin{pmatrix} \cos \Phi e^{i\phi_1} \cos \Omega e^{i\omega_1} \\ \cos \Phi e^{i\phi_1} \sin \Omega e^{i\omega_2} \\ \sin \Phi e^{i\phi_2} \cos \Omega e^{i\omega_1} \\ \sin \Phi e^{i\phi_2} \sin \Omega e^{i\omega_2} \end{pmatrix} \right\| \quad (15) \\ &= \left\{ 2 \left[1 - \min_{\bar{\theta}, \bar{\alpha}} \max_{\Phi, \Omega, \bar{\phi}, \bar{\omega}} G(\bar{\theta}, \bar{\alpha}, \Phi, \Omega, \bar{\phi}, \bar{\omega}) \right] \right\}^{1/2} \end{aligned}$$

$$\begin{aligned} &\text{که در آن تابع } G \text{ که شنودگر کوشش می‌کند آنرا بیشینه کند و آليس و بلب می‌خواهند آن بیشینه را کمینه کنند به صورت زیر بیان می‌شود:} \\ &G(\bar{\theta}, \bar{\alpha}, \Phi, \Omega, \bar{\phi}, \bar{\omega}) := \cos \Phi [\cos \Omega \cos(\alpha_1 - \phi_1 - \omega_1) \cos \theta_1 \\ &+ \sin \Omega \cos(\alpha_2 - \phi_1 - \omega_1) \sin \theta_1 \cos \theta_2] \\ &+ \sin \Phi [\cos \Omega \cos(\alpha_3 - \phi_2 - \omega_1) \sin \theta_1 \sin \theta_2 \cos \theta_3 \\ &+ \sin \Omega \cos(\alpha_4 - \phi_2 - \omega_1) \sin \theta_1 \sin \theta_2 \sin \theta_3] \quad (16) \end{aligned}$$

$$\begin{aligned} \bar{\alpha} &= (\alpha_1, \alpha_2, \alpha_3, \alpha_4); \\ \bar{\phi} &= (\phi_1, \phi_2); \\ \bar{\omega} &= (\omega_1, \omega_2) \quad (17) \end{aligned}$$

شده را باز سازی کند. آليس و باب باید U را چنان برگزینند که یک حالت N -کیوبیتی درهم تنیده تولید کند، یعنی به این مفهوم است که:

$$U \neq U_1 \otimes U_2 \otimes \dots \otimes U_N \quad (18)$$

است. پس آليس و باب با استفاده از U نا موضعی، درهم تنیدگی را به کار گرفته و مانع می‌شوند که شنودگر به طور کامل به کیوبیت‌های فرستاده شده دسترسی یابد.

۳- تقریب حالت ضربی از یک جفت کیوبیت درهم تنیده

برای درک آندیشه به کارگیری یک گیت N -کیوبیتی درهم تنیده در پروتکل BB84 روی دقیقی که یک حالت دو کیوبیتی درهم تنیده می‌تواند با حالتی از دو کیوبیت ضربی تقریب زده شود تحلیل اجام دادهایم که در آن مقدار N به ۲ محدود شده است. این تحلیل نشان می‌دهد که پروتکل محدودیتی ذاتی برای شنودگر ایجاد می‌کند فرض کیبد شنودگر برای تقریب زدن حالت پنهنجار $|\psi\rangle \in C^{2^N} = H^N$ که آليس در هر زمان یکی از کیوبیت‌های آن را برای باب فرستاده است، حالت زیر را بازسازد:

$$\bigotimes_{i=1}^N |\psi_i\rangle, \quad |\psi_i\rangle \in C^2 = H^1, \quad \|\psi_i\| = 1 \quad (19)$$

در این تقریب شنودگر کوشش می‌کند که خطرا کمینه کند در حالی که آليس و باب می‌کوشند با گرینش مناسب $|\psi\rangle$ خطای شنودگر را بیشینه کنند. این خطای بیشینه-کمینه به صورت زیر است:

$$E_{mm} := \max_{|\psi\rangle} \min_{\{|\psi_i\rangle\}} \left\| |\psi\rangle - \bigotimes_{i=1}^N |\psi_i\rangle \right\| \quad (20)$$

در اینجا جمله $\left\| |\psi\rangle - \bigotimes_{i=1}^N |\psi_i\rangle \right\|$ همان فاصله ردي بین ماتریس چگالی‌های مربوط به $|\psi\rangle$ و $\bigotimes_{i=1}^N |\psi_i\rangle$ است.

۴- فرضیه برای تعیین E_{mm}

فرض می‌کنیم که آليس و باب $N=2$ را برگزیده‌اند که در این صورت حالت آليس با زابطه زیر بیان می‌شود:

$$|\psi\rangle = (r_{\alpha_1} e^{i\alpha_1} \quad r_{\alpha_2} e^{i\alpha_2} \quad r_{\alpha_3} e^{i\alpha_3} \quad r_{\alpha_4} e^{i\alpha_4})^T \quad (21)$$

و حالت‌های شنودگر به صورت زیر است:

$$|\psi_1\rangle = (r_{\phi_1} e^{i\phi_1} \quad r_{\phi_2} e^{i\phi_2})^T \quad (22)$$

$$|\psi_2\rangle = (r_{\omega_1} e^{i\omega_1} \quad r_{\omega_2} e^{i\omega_2})^T \quad (23)$$

تأکید می‌کنیم که اگر آلیس و باب مطابق حالتی که در معادله (۱۸) آمده، اقدام کنند، خطای تقریب شنودگر حداقل برابر با $E_{mm} = 0.781$ می‌شود.

۵- نتیجه‌گیری

در این مقاله با استفاده از اصول مکلیک کوانتمی و روش جستجوی تصادفی با حل خطای بیشینه-کمینه نشان داده شده که درصد خطای شنودگر برای تقریب زدن حالت های درهم تبیه توسط حالت‌های ضربی افزایش می‌بلد از یافته‌های تحلیل انجام شده می‌توان نتیجه گرفت که شنودگر هر چقدر هم تلاش کند قدر نیست به حالت‌هایی که فرستنده ارسال می‌کند دست یابد به بیان دیگر، با توجه به افزایش خطای تقریب زدن حالت فرستنده آنچه شنودگر بدهست می‌آورد نادرست است.

مراجع

- [1] C. Bennett. "Quantum cryptography using any two non-orthogonal states". Phys. Rev. Lett., 68:003121, 1992.
- [2] H.-K. Lo. "Proof of unconditional security of six-state quantum key distribution scheme. Quantum Information and Computation", 1(1):81, 2001.
- [3] C. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing", Proc. Int. IEEE Conf. Computers, Sys. Signal Processing, pages 175–179, Bangalore, India, 1984.
- [4] D. Mayers. "Quantum key distribution and string oblivious transfer in noisy channels. Proc. Crypto '96, pages 343–357, New York, 1996. Springer-Verlag.
- [5] E. Biham, M. Boyer, P. Boykin, T. Mor, and V. Roychowdhury. "A proof of the security of quantum key distribution. In Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing", New York, ACM Press, 2000.
- [6] CAO Hai-Jing, CHEN Jing, and SONG He-Shan, "A New Quantum Communication Scheme by Using Bell States", Commun. Theor. Phys. (Beijing, China) Vol. 45, pp. 271–274, 2006.
- [7] Yin, Zhen-Qiang, et al. "A study of BB84 protocol in a device-independent scenario: from the view of entanglement distillation", Quant. Info. Comput. 13.9-10: 827-832, 2013.
- [8] Fengli Yan and Xiaoqiang Zhang, "Secure direct communication using Einstein-Podolsky-Rosen pairs and teleportation", The Euro. Phy. J. B, Vol. 41, pp.75, 2004.
- [9] H.-K. Lo and H.F. Chau. "Unconditional security of quantum key distribution over arbitrarily long distances", Science, 283:2050–2056, 1999.
- [10] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters. "Mixed state entanglement and quantum error correction", Phys. Rev. A, 54:3824–3851, 1996.
- [11] Yuan Cao et al. "Entanglement-based quantum key distribution with biased basis choice via free space", Opt. Exp., Vol. 21, Issue 22, pp. 27260-27268, 2013.
- [12] Song-Kong Chong, Tzonelih Hwang, "Quantum key agreement protocol based on BB84", Opt. Commun., Vol. 283, Issue 6, 15 pp. 1192-1195, 2010.
- [13] Sano, Yousuke, Ryutaroh Matsumoto, and Tomohiko Uyematsu, "Secure key rate of the BB84 protocol using finite sample bits", J. Phys. A: Mathematical and Theoretical 43.49: 495302, 2010.

با توجه به کرانهای G می‌توان کرانهای E_{mm} را نیز بدهست آورد

$$-1 \leq G \leq 1 \Rightarrow 0 \leq E_{mm} \leq 2$$

چون آلیس و باب می‌خواهند در معادله (۵) مقدار رایشینه کنند کافی است بیشینه سازی را با سه فاز ثابت α_j (که تغیر آن‌ها نی تواند مقدار کمینه را افزایش دهد) انجام داد باید گفته شود که اولاً فاز کلی جفت $(\psi_1 | \psi_2)$ پیشنهاد می‌کند که آلیس و باب هیچ برتری نسبت به هم ندارند همان‌گونه که شنودگر می‌تواند این فاز را مستقیماً باز تولید کند و ثانیاً شنودگر می‌تواند هر گیت تک کیوپیتی دیگری را بر $(\psi_1 | \psi_2)$ اعمال کند

۲-۳ تعیین E_{mm} با روش جستجوی تصادفی

با در نظر گرفتن $\bar{\theta} = \alpha_1 = \alpha_2 = \alpha_3 = 0$ و با بهینه‌سازی روی α_4 و $\bar{\theta}$ ، جوابی برای E_{mm} ارائه می‌دهیم که برای آن از روش جستجوی تصادفی استفاده کردیم. مقدارهای مختلف $\theta_1, \theta_2, \theta_3$ بین π و $-\pi$ و مقدار بهینه $\bar{\theta}, \Phi, \bar{\omega}, \bar{\phi}$ را با بهره‌گیری از روش جستجوی تصادفی بدهست آورده و سپس با α_4 و مقدارهای مختلف $\theta_1, \theta_2, \theta_3$ ، مقدار G بهینه را بدهست می‌آوریم و آنگاه با انتخاب این مقادیر، مقدار E و $(\psi | \psi)$ بهینه را بدهست می‌آوریم

۴- نتیجه‌های تحلیل

با حل این معادله به روش ذکر شده مشاهده شده که $E_{mm} = 0.781$ است. این مقدار با گرینش $\alpha_4 = 62.8^\circ$ و مقدارهای $\bar{\theta} = 62.8^\circ$ ، صفر و $\psi = 1/88.5^\circ$ بدهست آمده است. برای تأیید بیشتر نتیجه می‌توان بیشینه‌سازی را روی پارامترهای شنودگر نیز انجام داد و همچنین مقدارهای اولیه بسیار متغیری را آزمایش کرد همه این روش‌ها و مقدارهای اولیه آزمایش شده بهینه همانندی را برای G ارائه می‌دهند بنابراین می‌توان گفت مبلغ از مقدارهای $\bar{\theta}$ و $\bar{\alpha}$ داده شده یک بهینه کلی برای G بدهست آورده‌ایم. مقدارهای بهینه بدهست آمده برای $\bar{\theta}$ و $\bar{\alpha}$ تقریباً بر حالت زیر منطبق هستند:

$$|\psi\rangle = (0.99 \quad 0.31 \quad 0.00 \quad 0.00)^T \quad (18)$$

همچنین به عنوان مثال، بهترین گرینش شنودگر برای این که حالت $(\psi | \psi)$ را با حالت‌های نادرهم تبیه کند بزرگتر از مقداری زیر برای این زوایها استفاده می‌کند:

$$\omega_1 = -0.28, \omega_2 = -0.67, \phi_2 = 0.19, \phi_1 = -0.79, \Omega = 1.585, \varphi = -0.521$$

این تقریب بر حالت زیر منطبق است:

$$|\psi_1\rangle \otimes |\psi_2\rangle = (0.01 + 0.01i \quad 0.01 - 0.01i \quad 0.09 - 0.89i \quad -0.44 + 0.23i)^T \quad (19)$$