



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

سمیرا مرشدی^۱، فرامرز اسمعیلی 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 به‌کارگیری 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 به‌دست 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

¹Phsyscis 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.

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

۱- مقدمه

در سال ۱۹۹۲ پروتکل B92 بر گرفته از پروتکل BB84 است که تنها دو پایه نامتعامد $|0\rangle$ و $|+\rangle$ را به کار می برد [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 مدل های حمله ساده را محافظت می کرد [3]. اگرچه برای نشان دادن امنیت BB84 باید به شنودگر اجازه دهیم تا هر عملی را که مکانیک کوانتومی مجاز می داند 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 شیوه ای متفاوت ارائه کردند [5-8].

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

در این مقاله، با به کار گیری اصول مکانیک کوانتومی تغییری در پروتکل BB84 ایجاد کرده ایم و با بیان جزئیات نشان داده ایم که تقریب زدن یک حالت دو کیوبیتی درهم تنیده با حالت های ضربی دو کیوبیتی مشکلاتی برای شنودگر پنهانی ایجاد می کند.

۲- بهینه سازی حالت های کوانتومی در یک پیام

رمز شده نوری

در این بخش پروتکل را که بر پایه پروتکل BB84 بنا شده را تحلیل می کنیم. پروتکل ما در مرحله های زیر با پروتکل BB84 متفاوت است:

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

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

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

ب) سپس U را بر کیوبیت ها اعمال می کند. ج) آنگاه کیوبیت ها را یکی یکی می فرستد. آلیس پیش از فرستادن هر کیوبیت منتظر می ماند تا باب به او خبر دهد که کیوبیت پیشین را دریافت کرده است.

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

الف) تا هنگامی که همه N کیوبیت را دریافت نکرده است، اندازه گیری های مورد نیاز پروتکل BB84 را انجام نمی دهد.

ب) فوراً پس از دریافت هر کیوبیت به آلیس خبر می دهد. ج) با دریافت دنباله N کیوبیتی، تبدیل $U^{-1} = U^\dagger$ را بر آن ها اعمال می کند و آنگاه همانند آنچه در پروتکل BB84 داشتیم روی آن ها اندازه گیری انجام می دهد.

تبدیل U را می توان بسطی برای پروتکل BB84 در نظر گرفت. شنودگر کاملاً از U آگاه است، زیرا به طور همگانی اعلام می شود. چون باب به محض دریافت هر کیوبیت آلیس را آگاه می کند، شنودگر بر هر حالت N -کیوبیتی دسترسی یک به یک دارد. در پروتکل ما آلیس کیوبیت هایی از حالت $|\psi_{a_1, a_2, \dots, a_N}\rangle$ را یک به یک برای باب می فرستد.

اگر U به شکل زیر باشد:

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

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

اگر U به گیت های تک-کیوبیتی تجزیه پذیر باشد، حالت N -کیوبیتی فرستاده شده، حالتی ضربی است. شنودگر می تواند U را بی اثر کند و به کیوبیت های نا درهم تنیده حمله کرده و با $U_j^\dagger$ و U_j حالت فرستاده

¹ Entanglement Distribution Protocol: EDP

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

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

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

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

مقدارهای r_{α_j} را می‌توان با سه زاویه $\bar{\theta} = (\theta_1, \theta_2, \theta_3)$ که نشان دهنده نقاط روی سطح یک کره چهار بعدی هستند را 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 دایره را نمایش می‌دهند که نقطه‌های بر روی محیط آن‌ها را با زاویه‌های 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:

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

که در آن تابع G که شنودگر کوشش می‌کند آنرا بیشینه کند و آلیس و

باب می‌خواهند آن بیشینه را کمینه کنند به صورت زیر بیان می‌شود:

$$\begin{aligned} G(\bar{\theta}, \bar{\alpha}, \Phi, \Omega, \bar{\phi}, \bar{\omega}) &:= \cos \Phi [\cos \Omega \cos(\alpha_1 - \phi_1 - \omega_1) \cos \theta_1 \\ &+ \sin \Omega \cos(\alpha_2 - \phi_1 - \omega_2) \sin \theta_1 \cos \theta_2] \\ &+ \sin \Phi [\cos \Omega \cos(\alpha_3 - \phi_2 - \omega_1) \sin \theta_1 \sin \theta_2 \cos \theta_3 \\ &+ \sin \Omega \cos(\alpha_4 - \phi_2 - \omega_2) \sin \theta_1 \sin \theta_2 \sin \theta_3] \end{aligned} \quad (16)$$

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

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

$$U \neq U_1 \otimes U_2 \otimes \dots \otimes U_N \quad (3)$$

است. پس آلیس 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 اندیشه به کارگیری یک گیت N -کیوبیتی درهم تنیده در پروتکل BB84 روی دقتی که یک حالت دو کیوبیتی درهم تنیده می‌تواند با حالتی از دو کیوبیت ضربی تقریب زده شود، تحلیلی انجام دادیم که در آن مقدار N به ۲ محدود شده است. این تحلیل نشان می‌دهد که پروتکل محدودیتی ذاتی برای شنودگر ایجاد می‌کند فرض کنید شنودگر برای تقریب زدن حالت بهنجار $|\psi\rangle \in \mathbb{C}^{2^N} = H^N$ که آلیس در هر زمان یکی از کیوبیت‌های آن را برای باب فرستاده است، حالت زیر را بسازد:

$$\bigotimes_{i=1}^N |\psi_i\rangle, \quad |\psi_i\rangle \in \mathbb{C}^2 = H^1, \quad \|\psi_i\| = 1 \quad (4)$$

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

$$E_{mm} := \max_{|\psi\rangle} \min_{\{|\psi_i\rangle\}} \left\| |\psi\rangle - \bigotimes_{i=1}^N |\psi_i\rangle \right\| \quad (5)$$

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

۳-۱- فرضیه برای تعیین E_{mm}

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

$$|\psi\rangle = (r_{\alpha_1} e^{i\alpha_1} \quad r_{\alpha_2} e^{i\alpha_2} \quad r_{\alpha_3} e^{i\alpha_3} \quad r_{\alpha_4} e^{i\alpha_4})^T \quad (6)$$

و حالت‌های شنودگر به صورت زیر است:

$$|\psi_1\rangle = (r_{\phi_1} e^{i\phi_1} \quad r_{\phi_2} e^{i\phi_2})^T \quad (7)$$

$$|\psi_2\rangle = (r_{\omega_1} e^{i\omega_1} \quad r_{\omega_2} e^{i\omega_2})^T \quad (8)$$

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

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

چون آلیس و باب می‌خواهند در معادله (۵) مقدار را بیشینه کنند کافی است بیشینه‌سازی را با سه فاز ثابت α_j (که تغییر آن‌ها نمی‌تواند مقدار کمینه را افزایش دهد) انجام داد. باید گفته شود که اولاً فاز کلی جفت $|\psi\rangle$ 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 کیوبیتی دیگری را بر $|\psi_1\rangle$ و $|\psi_2\rangle$ اعمال کند

۳-۲ تعیین E_{mm} با روش جستجوی تصادفی

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

۴- نتیجه‌های تحلیل

با حل این معادله به روش ذکر شده مشاهده شده که $E_{mm} = 0.781$ است. این مقدار با گزینش $\alpha_4 = 628$ و مقدارهای $\bar{\theta}$ برابر با 0.628 ، صفر و $1/885$ به‌دست آمده است. برای تأیید بیش‌تر نتیجه می‌توان بیشینه‌سازی را روی پارامترهای شنودگر نیز انجام داد و همچنین مقدارهای اولیه بسیار متفاوتی را آزمایش کرد. همه این روش‌ها و مقدارهای اولیه آزمایش شده بیشینه هم‌اندازی را برای G ارائه می‌دهند بنابراین می‌توان گفت مله ازای مقدارهای $\bar{\theta}$ و $\bar{\alpha}$ داده شده یک بیشینه کلی برای G به‌دست آورده‌ایم. مقدارهای بهینه به‌دست 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 به‌عنوان مثال، بهترین گزینش شنودگر برای این حالت $|\psi\rangle$ را با حالت‌های ندرهم تنیدم‌اش تقریب بزنه از مقادیر زیر برای این زوایه‌ها

$$\omega_1, \omega_2, \phi_2, \phi_1, \Omega, \Phi$$

$$\omega_1 = -0.28, \omega_2 = -0.67, \phi_2 = 0.19, \phi_1 = -0.79,$$

$$\Omega = 1.585, \phi = -0.521$$

این تقریب بر حالت زیر منطبق است:

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

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

۵- نتیجه‌گیری

در این مقاله با استفاده از اصول مکانیک کوانتمی و روش جستجوی تصادفی با حل خطای بیشینه-کمینه نشان داده شده که درصد خطای شنودگر برای تقریب زدن حالت‌های درهم تنیده توسط حالت‌های ضریب افزایش می‌یابد. از یافته‌های تحلیل انجام شده می‌توان نتیجه گرفت که شنودگر هر چقدر هم تلاش کند قادر نیست به حالت‌هایی که فرستنده ارسال می‌کند دست یابد. به بیان دیگر، با توجه به افزایش خطا در تقریب زدن حالت فرستنده آنچه شنودگر به‌دست 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. Phys. 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, Tzoneh 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.