УДК 003.26:621.39

Є.В. Васіліу, канд. фіз.-мат. наук,
Одес. нац. акад. зв'язку ім. О.С. Попова,
Л.М. Васіліу, фізик-теоретик,
Одес. нац. політехн. ун-т

ОПТИМІЗАЦІЯ НЕКОГЕРЕНТНОЇ АТАКИ НА КВАНТОВИЙ ПРОТОКОЛ РОЗПОДІЛЕННЯ КЛЮЧІВ З ПЕРЕДАВАННЯМ КУТРИТІВ

Е.В. Василиу, Л.Н. Василиу. **Оптимизация некогерентной атаки на квантовый протокол распределения ключей с передачей кутритов.** Численной оптимизацией найдены параметры квантовой пробы подслушивающего агента, при которых его информация о ключе максимальна в широком интервале уровня ошибок между легитимными пользователями. Показано, что протокол с передачей кутритов более стойкий к оптимальной некогерентной атаке, чем протоколы BB84 с шестью состояниями и Экерта

E.V. Vasiliu, L.N. Vasiliu. **Optimization of incoherent attack against quantum key distribution protocol with qutrits transfer.** By numerical optimization the parameters of eavesdropper's quantum probe are found, at which its information on a key is maximal in a wide interval of a disturbance level between legitimate users. It is shown, that the protocol with qutrits transfer is more robust against optimal incoherent attack, than the BB84 protocol, the protocol with six states and the Ekert's protocol.

Бурхливий розвиток телекомунікаційних систем, а також автоматизованих засобів зберігання та обробки інформації потребує розробки нових криптографічних методів, що забезпечують захист при передачі та зберіганні даних. Квантова криптографія є новим етапом розвитку криптологічної науки, що швидко розвивається в останні два десятиріччя [1, 2]. Основною перевагою квантових шифрувальних протоколів є принципова можливість виявити присутність спостерігача, що за традицією називають Євою, в каналі комунікації, тому що при підслуховуванні він змушений вносити збурювання в повідомлення, якими обмінюються легітимні користувачі (Аліса та Боб).

Одним з розділів квантової криптографії є квантові протоколи розподілення секретних ключів. Для реалізації таких протоколів необхідно закодувати сигнал у квантові стани, що відносяться до неортогональних базисів, як у запропонованому першим в 1984 р. протоколі BB84 [1, 2]. Пізніше була запропонована схема, у якій безпека квантової криптографії базується на квантових кореляціях (переплутаності) пари двовимірних квантових систем — кубітів [3]. У цій схемі ключ зашифровується в несумісні базиси кубітів, які максимізують порушення локального реалізму, тобто максимально порушують нерівності Белла.

Нещодавно було запропоновано узагальнення схеми Екерта [3] на тривимірні квантові системи — кутрити [4]. Зважаючи на те, що трит містить більше інформації, ніж біт, протокол з передаванням переплутаних кутритів має більшу ефективність, ніж первісна схема Екерта. Було розглянуто деякі аспекти безпеки запропонованого протоколу, зокрема розглянута симетрична некогерентна атака з використанням квантових проб [4]. Але оптимізація атаки за параметрами проб не проводилась, тому питання надійності протоколу з передаванням кутритів залишилось відкритим. З метою визначення стійкості цього протоколу проведемо детальний аналіз та оптимізацію симетричної некогерентної атаки на протокол.

Розглянемо коротко схему протоколу з передаванням кутритів [4]. Квантовий канал містить джерело *S*, що випромінює два кутрити *A* і *B*, у максимально переплутаному стані $|\psi\rangle = \frac{1}{\sqrt{3}}\sum_{k=0}^{2}|k\rangle_A \otimes |k\rangle_B$, де $|k\rangle_A$ і $|k\rangle_B$ є *k*-м базисним станом кутритів *A* і *B* відповідно (рис. 1). Кутрит *A* прямує до Аліси, а кутрит *B* — до Боба. Кожний з них має симетричний 6-

портовий світлодільник T та по три детектори фотонів D (див. рис. 1). Перед кожним вхідним портом світлодільника T розташовано фазообертач φ_i, що контролюється Алісою або Бобом.

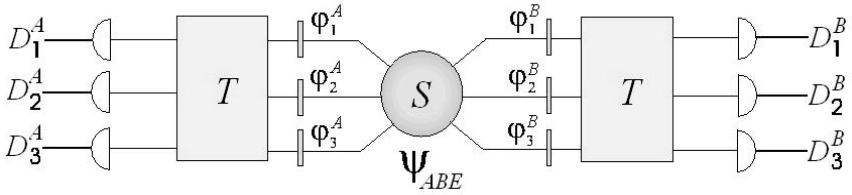

Рис. 1. Схема протоколу з передаванням переплутаних кутритів

Якщо позначити три фазові зсуви для кожного кутрита через $\vec{\varphi} = (\varphi_1,\ \varphi_2,\ \varphi_3)$, то перетворення, виконувані фазообертачем Аліси, можна записати у вигляді: $\vec{\varphi}_1^A = (0,0,0)$, $\vec{\varphi}_2^A = \left(0, \frac{\pi}{3}, -\frac{\pi}{3}\right)$ і $\vec{\varphi}_3^A = (\pi, 0, -\pi)$, а фазообертачем Боба: $\vec{\varphi}_1^B = \left(0, \frac{\pi}{6}, -\frac{\pi}{6}\right)$, $\vec{\varphi}_2^B = \left(0, -\frac{\pi}{6}, \frac{\pi}{6}\right)$ і $\vec{\varphi}_3^B = (\pi, 0, -\pi)$. Для кожного кутрита Аліса і Боб випадково та незалежно один від одного вибирають один із трьох вищенаведених векторів зсуву фаз, а тоді виконують вимір стану кутрита в базисі $|0\rangle_x$, $|1\rangle_x$, $|2\rangle_x$ $(x = A,\ B)$.

Після закінчення передачі Аліса і Боб публічно повідомляють вектори зсуву фаз, які вони вибирали для кожного окремого кутрита, і розділяють проведені виміри на дві підмножини: *перша* — коли вони використовували $\vec{\varphi}_1^A$, $\vec{\varphi}_2^A$, та $\vec{\varphi}_1^B$, $\vec{\varphi}_2^B$, і *друга*, коли вони використовували $\vec{\varphi}_3^A$, $\vec{\varphi}_3^B$ (тільки друга підмножина вимірів використовується для генерації ключа). Тоді Аліса і Боб публічно повідомляють результати своїх вимірів, але тільки тих, які становлять першу підмножину. Це дозволяє їм виявити підслуховування, перевіряючи порушення нерівностей Белла. Вони повинні знайти квантово-механічну кореляційну функцію S, яка є лінійною комбінацією коефіцієнтів кореляцій між результатами вимірів Аліси та Боба у першій підмножині [4]. Якщо нерівності Белла порушуються, що означає відсутність збурювання станів кутритів, то величина S повинна дорівнювати $\frac{2}{3}(2+\sqrt{3})$. Якщо ж виявляється, що $S < \frac{2}{3}(2+\sqrt{3})$, то збурювання приписується атаці Єви. Таким чином, Аліса і Боб мають додаткову можливість виявити підслуховування, використовуючи першу підмножину своїх вимірів (крім можливості оцінити рівень помилок у другій підмножині вимірів).

Однак найбільш цікавим є випадок, коли нерівності Белла порушуються, але Єва все-таки може одержати часткову інформацію про ключ за рахунок внесення помилок у послідовність трит, які одержать Аліса і Боб. У цьому випадку стійкість протоколу залежить від величини взаємної шеннонівської інформації між Алісою та Євою $I_{AE}(D)$, де D — середній рівень помилок, що вносить Єва у просіяний ключ внаслідок підслуховування [1].

Щоб завершити опис протоколу, відзначимо, що після посилення таємності Аліса і Боб одержать випадковий тернарний ключ, наприклад, якщо рядок Аліси має вигляд (0, 1, 0, 2, 2, 0, ...), то в Боба буде (0, 2, 0, 1, 1, 0, ...). Щоб ключі стали однаковими, один з них повинен зробити заміну $1 \leftrightarrow 2$ у своєму рядку. При необхідності тернарний ключ може бути перетворений у бінарний.

Розглянемо найбільш загальну некогерентну атаку, при якій Єва контролює джерело часток, тобто може приготувати усі пари кутритів, які потім прямують до Аліси та Боба. При цьому Єва переплутує кожну пару кутритів окремо зі своєю пробою. Виміри станів проб виконуються Євою після публічного оголошення зсувів фаз і тільки для тих випадків, коли Аліса і Боб використали $\vec{\varphi}_3^A$ та $\vec{\varphi}_3^B$ відповідно.

Найбільш загальний переплутаний стан пари кутритів і проби Єви [4]

$$|\Psi_{ABE}\rangle = \sqrt{\frac{F}{3}}(|00\rangle|E_{00}\rangle + |11\rangle|E_{11}\rangle + |22\rangle|E_{22}\rangle) + \sqrt{\frac{G}{6}}(|01\rangle|E_{01}\rangle + |10\rangle|E_{10}\rangle + |20\rangle|E_{20}\rangle + |02\rangle|E_{02}\rangle + |12\rangle|E_{12}\rangle + |21\rangle|E_{21}\rangle), \quad (1)$$

де $\{|kl\rangle\}$ — базисні стани пари кутритів;

$\{|E_{kl}\rangle\}$ — стани проб;

$k, l = 0\ldots2$;

F, G — нормувальні множники, які є параметрами проб Єви.

Відзначимо, що умова нормування вимагає $F + G = 1$, тому тільки один з цих параметрів є вільним. Виберемо як вільний параметр нормувальний множник F.

Позначаючи через λ скалярні добутки $\langle E_{kk}|E_{ll}\rangle$, для середнього рівня помилок між Алісою і Бобом та для взаємної інформації між ними можна записати відповідно [4]:

$$D = \frac{2}{3}(1 - F\lambda), \quad (2)$$

$$I_{AB}(F,\lambda) = 2\log_2 3 + \frac{1}{3}(1+F\lambda)\{\log_2(1+F\lambda) - \log_2 9\} + \frac{2}{3}(1-F\lambda)\{\log_2(1-F\lambda) - \log_2 9\}. \quad (3)$$

Тут і далі інформація вимірюється в бітах.

Вираз для взаємної інформації між Алісою та Євою має вигляд [4]

$$I_{AE}(F,\lambda) = \log_2 3 - 3\left\langle \tilde{E}_{00}\middle|\tilde{E}_{00}\right\rangle \log_2 \left\langle \tilde{E}_{00}\middle|\tilde{E}_{00}\right\rangle - 6\left\langle \tilde{E}_{11}\middle|\tilde{E}_{11}\right\rangle \log_2 \left\langle \tilde{E}_{11}\middle|\tilde{E}_{11}\right\rangle -$$
$$-\left[-3\left\langle \tilde{E}_{00}\middle|\tilde{E}_{00}\right\rangle W_1 \log_2\left(\left\langle \tilde{E}_{00}\middle|\tilde{E}_{00}\right\rangle W_1\right) - 6\left\langle \tilde{E}_{00}\middle|\tilde{E}_{00}\right\rangle (1-W_1)^2 \log_2\left(\left\langle \tilde{E}_{00}\middle|\tilde{E}_{00}\right\rangle (1-W_1)^2\right) - \right. \quad (4)$$
$$\left. -6\left\langle \tilde{E}_{11}\middle|\tilde{E}_{11}\right\rangle W_2 \log_2\left(\left\langle \tilde{E}_{11}\middle|\tilde{E}_{11}\right\rangle W_2\right) - 12\left\langle \tilde{E}_{11}\middle|\tilde{E}_{11}\right\rangle (1-W_2)^2 \log_2\left(\left\langle \tilde{E}_{11}\middle|\tilde{E}_{11}\right\rangle (1-W_2)^2\right)\right],$$

де $\tilde{E}_{kk}$ — стани проб після виміру.

При цьому

$$\left\langle \tilde{E}_{00}\middle|\tilde{E}_{00}\right\rangle = \frac{1+2F\lambda}{9}, \qquad \left\langle \tilde{E}_{11}\middle|\tilde{E}_{11}\right\rangle = \frac{1-F\lambda}{9}. \quad (5)$$

Величини W_1 та W_2 в (4) даються формулами [4]

$$W_1 = \left(\frac{1}{3}\sqrt{1+2\tilde{\lambda}_1} + \frac{2}{3}\sqrt{1-\tilde{\lambda}_1}\right)^2, \qquad W_2 = \left(\frac{1}{3}\sqrt{1+2\tilde{\lambda}_2} + \frac{2}{3}\sqrt{1-\tilde{\lambda}_2}\right)^2, \quad (6)$$

де

$$\tilde{\lambda}_1 = \frac{1}{2}\frac{3F + 4F\lambda - 1}{1+2F\lambda}, \qquad \tilde{\lambda}_2 = \frac{1}{2}\frac{3F - 2F\lambda - 1}{1-F\lambda}. \quad (7)$$

В (2), (3), (5) і (7) величини F та λ є параметрами проб Єви, які вона може вибирати на свій розсуд. Але для порушення нерівностей Белла потрібно, щоб виконувалась нерівність [4]

$$F\lambda \geq \frac{6\sqrt{3} - 9}{2} \approx 0{,}69615. \quad (8)$$

Таким чином, щоб не бути виявленою при перевірці порушень нерівностей Белла, Єва повинна вибирати F та λ так, щоб їхній добуток був більший, ніж 0,69615.

Щоб визначити стійкість протоколу з передаванням кутритів до некогерентної атаки, необхідно знайти залежності $I_{AB}(D)$ та $I_{AE}(D)$, які не були отримані в [4]. Перший вираз легко одержати підстановкою $F\lambda$ з (2) в (3)

$$I_{AB}(D) = 2\log_2 3 + \left(\frac{2}{3} - \frac{D}{2}\right)\left\{\log_2\left(2 - \frac{3}{2}D\right) - \log_2 9\right\} + D\left\{\log_2\left(\frac{3}{2}D\right) - \log_2 9\right\}. \qquad (9)$$

Що стосується I_{AE}, то з (2) та (4)…(7) видно, що ця величина, крім залежності від середнього рівня помилок D між Алісою і Бобом, також буде залежати від одного з параметрів проб Єви (F або λ), що надає Єві можливість максимізувати інформацію про ключ вибором одного з параметрів своєї проби. Для цього Єва повинна спочатку вибрати середній рівень помилок D, який вона буде створювати при перехваті, так, щоб він не сильно перевищував природний рівень шумів в каналі, а тоді вибрати F (або λ) так, щоб величина I_{AE} була максимальною. Другий параметр при цьому буде однозначно визначатися з (2) для кожного фіксованого D, а Єва повинна також стежити за тим, щоб параметри її проби задовольняли умові (8).

Залежність I_{AE} від параметра F можна одержати, виразивши λ з (2) і підставивши цю величину послідовно в (7), (6), (5) і нарешті в (4). Вираз для $I_{AE}(D,F)$, який при цьому виходить, дуже громіздкий і тут не наводиться.

З нашого аналізу випливає, що $I_{AE}(D,F)$ залежить від параметра F монотонно (рис. 2). Зазначимо, що для задоволення нерівності (8), Єва змушена створювати деякий мінімальний рівень помилок D при кожному значенні F, що відображено на рисунку 2. Вертикальна штрихова лінія на рисунку 2 відповідає $D = 0{,}20257$, яке одержано підстановкою $F\lambda$ з (8) у (2).

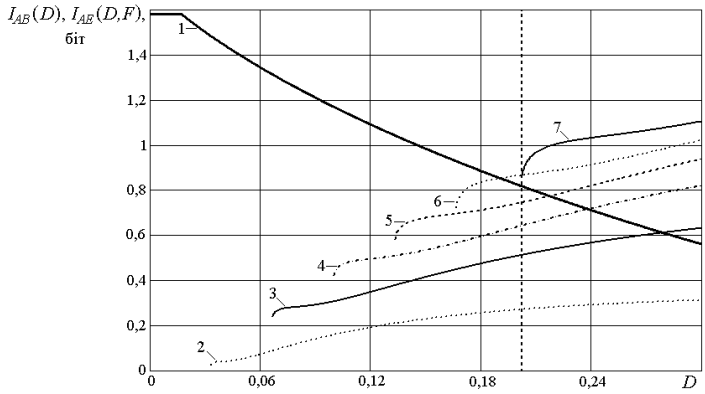

Рис. 2. Взаємна інформація $I_{AB}(D)$ (крива 1) та $I_{AE}(D,F)$ для значень параметра F: 0,95 (крива 2), 0,9 (крива 3), 0,85 (крива 4), 0,8 (крива 5), 0,75 (крива 6), 0,69615 (крива 7)

Одержимо тепер вираз для $I_{AE}(D,\lambda)$. Для цього підставимо F з (2) в (7), а далі одержані вирази для $\tilde{\lambda}_1$ та $\tilde{\lambda}_2$ підставимо в (6). Тоді

$$W_1(D,\lambda) = \frac{1}{9(1-D)}\left[\frac{1{,}5D-1}{\lambda} - 3D + 4 + 2\sqrt{\left(\frac{2-3D}{\lambda} - 6D + 4\right)\left(1 - \frac{1-1{,}5D}{\lambda}\right)}\right], \qquad (10)$$

$$W_2(D,\lambda) = \frac{1}{9D}\left[\frac{3D-2}{\lambda} + 3D + 2 + 4\sqrt{\left(\frac{2-3D}{\lambda} + 3D - 2\right)\left(1 - \frac{1-1{,}5D}{\lambda}\right)}\right]. \qquad (11)$$

Відзначимо, що при $\lambda = 1$ вирази (10) та (11) істотно спрощуються:

$$W_1(D)=\frac{1}{9(1-D)}\left[3-\frac{3}{2}D+2\sqrt{9D-\frac{27}{2}D^2}\right],\qquad W_2(D)=\frac{2}{3}. \tag{12}$$

Підставляючи тепер $F\lambda$ з (2) в (5), а тоді отримані вирази в (4), одержимо остаточно:

$$\begin{aligned}I_{AE}(D,\lambda)=\log_2 3-(1-D)\log_2\frac{1-D}{3}-D\log_2\frac{D}{6}+(1-D)W_1(D,\lambda)\log_2\frac{(1-D)W_1(D,\lambda)}{3}+\\ +2(1-D)(1-W_1(D,\lambda))^2\log_2\frac{(1-D)(1-W_1(D,\lambda))^2}{3}+DW_2(D\,|\,\lambda)\log_2\frac{DW_2(D,\lambda)}{6}+\\ +2D(1-W_2(D,\lambda))^2\log_2\frac{D(1-W_2(D,\lambda))^2}{6},\end{aligned} \tag{13}$$

де $W_1(D,\lambda)$ і $W_2(D,\lambda)$ визначені в (10) та (11) відповідно.

Величина $I_{AE}(D,\lambda)$ залежить від λ не монотонно (рис. 3). Вертикальна штрихова лінія на цьому рисунку, як і на рисунку 2, відповідає $D=0{,}20257$.

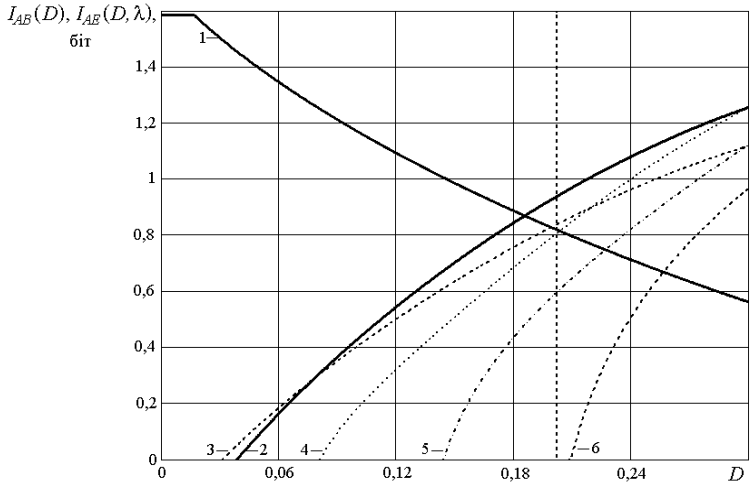

Рис. 3. Взаємна інформація $I_{AB}(D)$ (крива 1) та $I_{AE}(D,\lambda)$ для значень параметра λ: 0,9827 (крива 2), 1 (крива 3), 0,9 (крива 4), 0,8 (крива 5), 0,7 (крива 6)

Щоб знайти значення параметра λ, яке було б оптимальним для Єви, використаємо теорему Цізара і Кернера, згідно з якою Аліса і Боб можуть установити секретний ключ, якщо взаємна інформація між ними більше за взаємну інформацію між Алісою і Євою, тобто ключ може бути встановлено тільки в такому інтервалі помилок D, де $I_{AB}(D)>I_{AE}(D)$ [5]. Внаслідок цього факту в квантовій криптографії верхньою межею припустимого рівня помилок вважають значення $D_{\max}$, що одержують з рівняння $I_{AB}(D_{\max})=I_{AE}(D_{\max})$. Таким чином, для визначення $D_{\max}$ як функції від λ необхідно прирівняти праві частини (9) та (13). Рівняння, яке виходить при цьому, можна розв'язати тільки чисельно. Розв'язуючи це рівняння для різних значень λ, можна знайти таке, якому відповідає мінімальне значення $D_{\max}$. Саме це значення λ і буде оптимальним для Єви.

Чисельний розв'язок рівняння $I_{AB}(D)=I_{AE}(D,\lambda)$ відносно D при різних значеннях λ дає такий результат: мінімальне $D_{\max}$ дорівнює 0,186, чому відповідає $\lambda=0{,}9827$. Відповідна залежність взаємної інформації $I_{AE}(D,\lambda)$ при $\lambda=0{,}9827$ побудована на рисунку 3 (крива 2). Видно, що при цьому значенні λ Єва може отримати більше інформації, ніж при будь-якому іншому λ, в широкому інтервалі значень величини D.

Таким чином, знайдено оптимальну некогерентну атаку агента, що підслуховує, на протокол з передаванням кутритів. Для реалізації такої атаки необхідно готувати стани виду (1), вибираючи параметр проби λ таким, що дорівнює 0,9827. Тоді слід вибрати середній рівень помилок D, що буде створюватись при підслуховуванні, так, щоб він не сильно перевищував природний рівень перешкод в квантовому каналі. При цьому величина D не повинна перевищувати 0,20257, щоб легітимні користувачі системи квантового розподілення ключів упевнились в порушенні нерівностей Белла. Нарешті потрібно визначити параметр проби F з рівняння (2). Атака з таким вибором параметрів квантової проби буде оптимальною.

При оптимальній некогерентній атаці криві $I_{AB}(D)$ та $I_{AE}(D,\lambda)$ перетинаються в точці $D_{\max} = 0{,}186$. Якщо порівняти цю межу з відповідними межами для некогерентних атак на протокол BB84 — $D_{\max} = 0{,}146$, протокол з 6-ма станами — $D_{\max} = 0{,}156$ [6] та протокол Екерта — $D_{\max} = 0{,}146$ [7], то можна зробити висновок, що протокол з передаванням кутритів стійкіший до некогерентної атаки, ніж будь-який з перелічених протоколів.

Література

1. Gisin N. Quantum cryptography / Gisin N., Ribordy G., Tittel W., Zbinden H. // Reviews of Modern Physics. — 2002. — Vol. 74, № 1. — P. 145 — 195.
2. Баумейстер Д. Физика квантовой информации / Баумейстер Д., Экерт А., Цайлингер А. — М.: Постмаркет, 2002. — 376 с.
3. Ekert A. Quantum cryptography based on Bell's theorem // Physical Review Letters. — 1991. — Vol. 67, № 6. — P. 661 — 663.
4. Kaszlikowski D. Quantum Cryptography Based On Bell Inequalities for Three-Dimensional System / Kaszlikowski D., Chang K., Oi D.K.L. and others // Physical Review A. — 2003. — Vol. 67, № 1. — P. 012310 — 012313.
5. Csiszar I. Broadcast channels with confidential messages / Csiszar I., Korner J. // IEEE Trans. on Inform. Theory. — 1978. — Vol. IT-24, № 3. — P. 339 — 348.
6. Bruss D. Optimal Eavesdropping in Quantum Cryptography with Six States // Physical Review Letters.- 1998. — V. 81, № 14. — P. 3018 — 3021.
7. Inamori H. Security of EPR-based quantum cryptography against incoherent symmetric attacks / Inamori H., Rallan L., Vedral V. // J. of Physics A. — 2001. — Vol. 34, № 35. — P. 6913 — 6918.

Надійшла до редакції 21 грудня 2006 р.