Программное обеспечение позволяет задавать частоту выборки и сохранения результата. В итоге формируется таблица, отображающая изменения значений частоты сердечных сокращений в ходе измерений.

Непосредственный анализ полученных данных производится после экспортирования данных таблицы в стандартную программу статистической обработки, например, Exel или Origin.

Подводя итоги вышесказанному, следует отметить, что разработанный комплекс позволит выявить влияние освещения, создаваемого разноспектральными источниками света на состояние вегетативной нервной системы.

Литература

1. Овчинников, С. С. Оценка эффективности влияния световой среды на организм человека [Текст] / С. С. Овчинников, А. А. Серобаба // Светотехника и электроэнергетика. – 2008. - №4. - С. 4-10.
2. Мешков, В. В. Основы светотехники Ч. 2. [Текст]: учеб. / В. В. Мешков, А. Б. Матвеев. – М. : Энергоатомиздат, 1989. – 432 с.
3. Брейнард Г. К. Восприятие света как стимула незрительных реакций человека. [Текст] / Г. К. Брейнард, И. Провенсио //Светотехника. - 2008. - №1. - С.6-12.
4. Агаджанян Н. А. Основы физиологии человека. [Текст]: учеб. - М. : РУДН, 2001. - 408 с.

На основі аналізу атаки агента, що підслуховує, на три варіанти пінг–понг протоколу отримано оцінки витоку інформації залежно від імовірності виявлення атаки. Показано, що інформаційна місткість та безпека різних варіантів пінг–понг протоколу обернено пропорційні

Ключові слова: квантова криптографія, пінг–понг протокол, атака пасивного перехвату, асимптотична стійкість

На основе анализа атаки подслушивающего агента на три варианта пинг–понг протокола получены оценки утечки информации в зависимости от вероятности обнаружения атаки. Показано, что информационная емкость и безопасность различных вариантов пинг–понг протокола обратно пропорциональны

Ключевые слова: квантовая криптография, пинг–понг протокол, атака пассивного перехвата, асимптотическая стойкость

Based on the analysis of eavesdropping attacks on the three variants of the ping–pong protocol the estimations of information leakage depending on probability of attack detection are obtained. It is shown, that the information capacity and security of various variants of the ping–pong protocol are in the inverse proportion

Key words: quantum cryptography, ping–pong protocol, eavesdropping attack, asymptotic security

УДК 003.26:621.39+530.14

АНАЛІЗ СТІЙКОСТІ ТРЬОХ ВАРІАНТІВ ПІНГ–ПОНГ ПРОТОКОЛУ ДО АТАКИ ПАСИВНОГО ПЕРЕХОПЛЕННЯ

Є.В. Васіліу
Кандидат фізико-математичних наук, доцент
Кафедра «Інформатизації та управління»
Одеська національна академія зв'язку ім. О.С. Попова
вул. Ковальська, 1, м. Одеса, Україна, 65029
Контактний тел.: 067-302-99-49
E-mail: vasiliu@ua.fm

1. Вступ

Квантова криптографія є застосуванням квантової теорії інформації, що пропонує нові підходи до вирішення різних криптографічних завдань. Один з напрямків квантової криптографії – квантові протоколи прямого безпечного зв'язку, у яких секретні ключі взагалі не використовуються, а їхню роль грають

квантово-механічні ресурси, наприклад, переплутані квантові стани. Оскільки акт перехоплення руйнує переплутаність, це дозволяє виявити підслуховування у квантовому каналі зв'язку й, у цьому випадку, негайно припинити передачу повідомлення.

Квантовий протокол прямого безпечного зв'язку, що одержав назву пінг–понг протоколу й у якому використовуються пари переплутаних по поляризаційним ступеням свободи фотонів (стани Бела), запропонований в [1]. Для передачі біта використовується тільки один із фотонів пари, тому агент, що підслуховує (Єва), перехопивши фотон і вимірявши його поляризацію, не може одержати значення біта, не маючи доступу до другого фотона. Проте, використовуючи допоміжні квантові системи (проби) і виконуючи певні унітарні операції й наступні вимірювання над складеними (фотони – проби) квантовими системами, Єва має можливість перехопити деяку кількість інформації [1]. Відзначимо, що недавно цей варіант пінг–понг протоколу був реалізований на експериментальному встаткуванні [2]. При цьому швидкість передачі досягала 4250 біт/с, а рівень помилок склав 3,8%.

В оригінальному варіанті пінг–понг протоколу кожний передаваний фотон використовується для кодування одного класичного біта [1]. Таким чином, для реалізації протоколу використовують тільки два із чотирьох станів Бела. Використовуючи всі чотири стани, тобто використовуючи квантове надщільне кодування, можна передати два біти інформації, передаючи один фотон [3,4]. Подальше підвищення інформаційної місткості квантового каналу можливо шляхом використання замість переплутаних пар фотонів їхніх трійок, четвірок і т.д. При цьому квантове надщільне кодування дозволяє передавати каналом менше число фотонів, чим їх є в групі. Так, у пінг–понг протоколі із триплетами Грінбергера – Хорна – Цайлінгера (ГХЦ) для передачі трьох біт інформації досить передавати два фотони.

Пінг–понг протокол з белівськими парами й квантовим надщільним кодуванням запропонований в [4,5]. Проаналізовано атаку з використанням квантових проб на цей протокол [5]. Пінг–понг протокол з використанням ГХЦ–триплетів та надщільного кодування запропонований в [6], атака на цей протокол проаналізована в [7]. Показано, що ці два варіанти пінг–понг протоколу, як і оригінальний варіант [1], асимптотичне стійкі, тобто підслуховування Єви гарантовано буде виявлено, але до цього вона зможе одержати деяку частину повідомлення. Таким чином, всі варіанти пінг–понг протоколу потребують деяких додаткових процедур підсилення секретності, які не дозволять Єві одержати скільки-небудь значну інформацію на початковому етапі передачі повідомлення. Але, для розробки таких процедур підсилення секретності необхідна кількісна оцінка інформації, яку може одержати Єва. *Метою цієї роботи* є отримання таких кількісних оцінок і їхній порівняльний аналіз для трьох варіантів пінг–понг протоколу.

2. Кількість інформації Єви при атаці пасивного перехоплення на три варіанти пінг–понг протоколу

Детальний опис варіантів пінг–понг протоколу з белівськими парами й ГХЦ–триплетами дано в [1,5,6]. Тут відзначимо, що будь-який варіант передбачає два режими:

1. Режим передачі повідомлення, у якому відправник повідомлення (Аліса), одержавши спочатку один (або два) фотони з переплутаної групи від одержувача повідомлення (Боба), виконує кодувальні операції над цими фотонами з використанням квантових гейтів і відправляє фотони назад Бобові. Потім Боб виконує відповідне вимірювання над всією групою переплутаних фотонів і тим самим декодує послані Алісою біти.

2. Режим контролю підслуховування, у якому Аліса й Боб виконують певну послідовність квантових вимірювань в одному із двох взаємно незміщених базисів (B_z або B_x), кожний над своїми фотонами з переплутаної групи, а потім порівнюють результати з використанням звичайного відкритого (але аутентифікованого) каналу зв'язку. Якщо результати вимірювань не узгоджуються, то це приписується втручанню Єви й протокол переривається.

Імовірність того, що Єва не буде виявлена після n успішних атак і одержить інформацію $I = nI_0(d)$ визначається формулою [1]:

$$s(I,c,d) = \left(\frac{1-c}{1-c(1-d)}\right)^{I/I_0(d)}, \qquad (1)$$

де c – частота перемикання в режим контролю підслуховування (ця величина вибирається легітимними користувачами); d – імовірність виявлення атаки Єви за один раунд контролю підслуховування (цю величину Єва може вибрати, підбираючи параметри своїх квантових систем – проб, використовуваних для атаки); $I_0(d)$ – максимальна кількість інформації, яку може одержати Єва за одну атакуючу операцію при даному d.

Щоб обчислити повну ймовірність невиявлення атаки $s(I,c,d)$ (1) для різних варіантів пінг–понг протоколу, потрібно знати відповідні залежності $I_0(d)$ для цих варіантів протоколу. Такі залежності були отримані в [1,5,7]. Приведемо їх тут без виведення.

Кількість інформації Єви $I_0(d)$ для пінг–понг протоколу з белівськими парами й без квантового надщільного кодування [1]:

$$I_0(d) = -\lambda_1(d)\cdot\log_2\lambda_1(d) - \lambda_2(d)\cdot\log_2\lambda_2(d), \qquad (2)$$

де

$$\lambda_{1,2}(d) = \frac{1}{2} \pm \frac{1}{2}\sqrt{1-\left(4d-4d^2\right)\left(1-\left(p_1-p_2\right)^2\right)}; \qquad (3)$$

p_1 та p_2 – частоти «0» і «1» у повідомленні Аліси.

Для пінг–понг протоколу з белівськими парами й квантовим надщільним кодуванням $I_0(d)$ визначається виразом [5]:

$$I_0(d) = -\sum_{i=1}^{4}\lambda_i(d)\cdot\log_2\lambda_i(d), \qquad (4)$$

де

$$\lambda_{1,2}(d) = \frac{1}{2}\left(p_1+p_2\right) \pm \frac{1}{2}\sqrt{\left(p_1+p_2\right)^2 - 16p_1p_2\left(d-d^2\right)};$$

$$\lambda_{3,4}(d) = \frac{1}{2}\left(p_3+p_4\right) \pm \frac{1}{2}\sqrt{\left(p_3+p_4\right)^2 - 16p_3p_4\left(d-d^2\right)}; \qquad (5)$$

p_1, p_2, p_3 та p_4 – частоти біграмм «00», «01», «10» та «11» відповідно у повідомленні Аліси.

Для пінг–понг протоколу із ГХЦ–триплетами отримані наступні вирази [7]:

$$I_0(d) = -\sum_{i=1}^{8} \lambda_i(d) \cdot \log_2 \lambda_i(d), \qquad (6)$$

де

$$\lambda_{1,2}(d) = \frac{1}{2}(p_1 + p_2) \pm \frac{1}{2}\sqrt{(p_1 + p_2)^2 - 16p_1p_2 \cdot \frac{2}{3}d \cdot \left(1 - \frac{2}{3}d\right)};$$

$$\lambda_{3,4}(d) = \frac{1}{2}(p_3 + p_4) \pm \frac{1}{2}\sqrt{(p_3 + p_4)^2 - 16p_3p_4 \cdot \frac{2}{3}d \cdot \left(1 - \frac{2}{3}d\right)};$$

$$\lambda_{5,6}(d) = \frac{1}{2}(p_5 + p_6) \pm \frac{1}{2}\sqrt{(p_5 + p_6)^2 - 16p_5p_6 \cdot \frac{2}{3}d \cdot \left(1 - \frac{2}{3}d\right)};$$

$$\lambda_{7,8}(d) = \frac{1}{2}(p_7 + p_8) \pm \frac{1}{2}\sqrt{(p_7 + p_8)^2 - 16p_7p_8 \cdot \frac{2}{3}d \cdot \left(1 - \frac{2}{3}d\right)}; \qquad (7)$$

p_1, p_2, p_3, p_4, p_5, p_6, p_7 и p_8 – частоти триграм «000», «001», «010», «011», «100», «101», «110» и «111» відповідно у повідомленні Аліси.

3. Залежності повній імовірності невиявлення атаки від кількості інформації Єви

Розглянемо величину $s(I,c,d)$ (1) при однакових значеннях p_i в (3), (5), (7), що відповідає передаванню повністю випадкового бітового рядка. На рис. 1–3 наведені залежності $s(I,c,d)$ від кількості інформації I, що одержить Єва, при $p_1 = p_2 = 0.5$ в (3), $p_1 = p_2 = p_3 = p_4 = 0.25$ в (5) і $p_1 = p_2 = ... = p_8 = 0.125$ в (7).

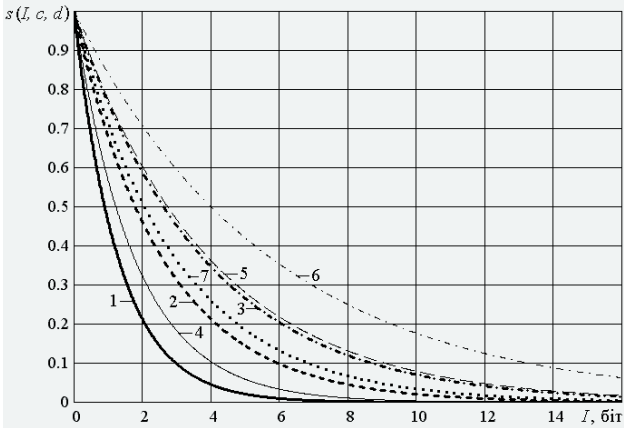

Рис. 1. Імовірність невиявлення атаки Єви при c = 0.7.
Протокол:
1 – з белівськими парами й без надщільного кодування, d = 0.5;
2 – з белівськими парами й надщільним кодуванням, d = 0.5;
3 – із ГХЦ–триплетами, d = 0.5;
4 – з белівськими парами й без надщільного кодування, d = 0.25;
5 – з белівськими парами й надщільним кодуванням, d = 0.25;
6 – із ГХЦ–триплетами, d = 0.25;
7 – із ГХЦ–триплетами, d = 0.75.

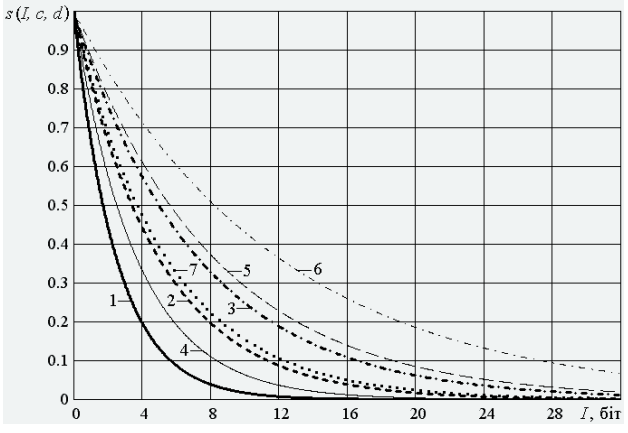

Рис. 2. Імовірність невиявлення атаки Єви при c = 0.5, позначення ті ж, що на рис. 1

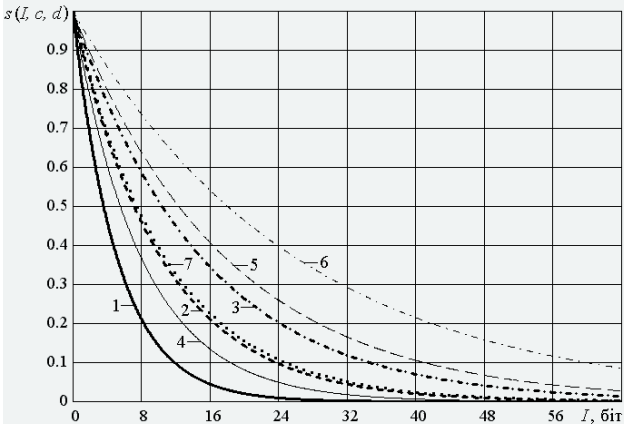

Рис. 3. Імовірність невиявлення атаки Єви при c = 0.3, позначення ті ж, що на рис. 1

Як видно з рис. 1 – 3, кількість інформації, що попадає до Єви (при фіксованій величині s), найменша для пінг–понг протоколу з белівськими парами й без надщільного кодування, дещо більше для такого ж протоколу із надщільним кодуванням і найбільша для протоколу із ГХЦ–триплетами. При цьому інформаційна місткість на один раунд протоколу становить 1 біт, 2 біти й 3 біти відповідно. Таким чином, інформаційна місткість і безпека різних варіантів пінг–понг протоколу обернено пропорційні. Що стосується залежності величини s від d, очевидно, що чим менше d, тим довше атака Єви не буде виявлена. Відзначимо, однак, що повну інформацію, тобто правильні значення переданих Алісою бітів, Єва одержить тільки при $d = 0.5$ в обох варіантах пінг–понг протоколу з белівськими парами [1,5] і при $d = 0.75$ в протоколі із ГХЦ–триплетами [7]. Відповідно при $d < 0.5$ для протоколів з белівськими парами й при $d < 0.75$ для протоколу із ГХЦ–триплетами, Єва визначить правильно тільки деякі біти повідомлення, причому вона не буде навіть точно знати, які саме біти визначені правильно.

Відзначимо ще один факт: криві $s(I,c,d)$ для протоколу з белівськими парами й надщільним кодуванням при $d = 0.5$ й для протоколу із ГХЦ–триплетами при $d = 0.75$ лежать дуже близько друг до друга (див. криві 2 і 7 на рис. 1 – 3). Це означає, що при виборі

Євою стратегії атаки, що дає їй повну інформацію, ці два варіанти протоколу мають майже однакову стійкість до такої атаки. При цьому інформаційна місткість протоколу із ГХЦ–триплетами в 1.5 рази вище. Таким чином, за критеріями найбільшої ефективності й стійкості пінг–понг протокол із ГХЦ–триплетами є переважнішим, ніж протокол з белівськими парами й надщільним кодуванням. Цей висновок, однак, справедливий для випадку, коли Єва хоче визначити правильно значення всіх переданих бітів за рахунок максимізації ймовірності виявлення підслуховування. Якщо ж Єва вибере більше обережну стратегію, що, однак, не дасть їй повної інформації, то стійкість протоколу із ГХЦ–триплетами виявляється нижче стійкості протоколу з белівськими парами й надщільним кодуванням (див. рис. 1 – 3). Що стосується варіанта протоколу з белівськими парами й без надщільного кодування, його стійкість найвища, але, інформаційна місткість цього варіанта протоколу найменша.

Відзначимо також, що навіть для протоколу із ГХЦ–триплетами при виборі легітимними користувачами малої частоти перемикання в режим контролю підслуховування $c = 0.3$ й виборі Євою досить обережної стратегії підслуховування $d = 0.25$, імовірність виявити атаку перевищує 90% при одержанні Євою усього 64 біт інформації (див. криву 6 на рис. 3). Таким чином, всі три варіанти пінг–понг протоколу мають досить високий рівень стійкості: агент, що підслуховує, може одержати не більше декількох десятків біт інформації на початковому етапі передавання повідомлення, перш, ніж він буде виявлений. У тих випадках, коли й такий витік інформації неприпустимий, всі варіанти пінг–понг протоколу потребують додаткових заходів з підсилення секретності.

4. Висновки

В роботі отримані оцінки кількості інформації, яка попадає до агента, що підслуховує, залежно від повної імовірності виявлення атаки для трьох варіантів пінг–понг протоколу квантового безпечного зв'язку. Показано, що інформаційна місткість і безпека різних варіантів пінг–понг протоколу обернено пропорційні, але всі розглянуті варіанти протоколу мають досить високий рівень асимптотичної стійкості. Показано також, що при виборі такої стратегії атаки, яка дає повну інформацію, протокол з белівськими парами й надщільним кодуванням і протокол із ГХЦ–триплетами мають майже однакову стійкість до такої атаки.

Література

1. Bostrom K., Felbinger T. Deterministic secure direct communication using entanglement // Physical Review Letters. – 2002. – V. 89, № 18. – 187902.
2. Ostermeyer M., Walenta N. On the implementation of a deterministic secure coding protocol using polarization entangled photons // Optics Communications. – 2008. – V. 281, № 17. – P. 4540 – 4544.
3. Deng F.-G., Long G.L., Liu X.-S. Two-step quantum direct communication protocol using the Einstein – Podolsky – Rosen pair block // Physical Review A. – 2003. – V. 68, № 4. – 042317.
4. Cai Q.-Y., Li B.-W. Improving the capacity of the Bostrom – Felbinger protocol // Physical Review A. – 2004. – V. 69, № 5. – 054301.
5. Василиу Е.В. Анализ безопасности пинг-понг протокола с квантовым плотным кодированием // Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 1. – С. 32 – 38.
6. Василиу Е.В., Василиу Л.Н. Пинг–понг протокол с трех– и четырехкубитными состояниями Гринбергера – Хорна – Цайлингера // Труды Одесского политехнического университета. – 2008. – Вып. 1(29). – С. 171 – 176.
7. Василиу Е.В. Анализ атаки на пинг–понг протокол с триплетами Гринбергера – Хорна – Цайлингера // Наукові праці ОНАЗ ім. О.С. Попова. – 2008. – № 1. – С. 15 – 24.