property. This result explains the phenomenon of the so-called curious approximation.
Keywords: Riemann zeta function, remainder of a number series, asymptotic expansion, enveloping series, curious approximation, Apery constant.

УДК 519.248.3

ВЕРХНИЕ ОЦЕНКИ СТОЙКОСТИ КВАНТОВОЙ КРИПТОГРАФИИ ПРИ ИСПОЛЬЗОВАНИИ ГЕОМЕТРИЧЕСКИ ОДНОРОДНЫХ КОГЕРЕНТНЫХ СОСТОЯНИЙ

Д.А. Кронберг[1]

1 *dmitry.kronberg@gmail.com*; Математический институт им.В.А.Стеклова РАН

В работе исследуется стойкость квантовой криптографии на геометрически однородных когерентных состояниях. Технология использования большого количества симметричных состояний позволяет бороться с атакой безошибочным различением состояний (USD-атакой), но в то же время стойкость против данной атаки не гарантирует стойкости против любых других атак. Рассматриваются атаки, которые в условиях затухания могут быть эффективными против данной системы квантового распределения ключей.

Ключевые слова: квантовая криптография, когерентные состояния, квантовая теория информации.

Когерентное квантовое состояние $|\alpha\rangle$ имеет вид

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{+\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle,$$

где $|n\rangle$ — базис Фока. Можно рассмотреть конфигурацию N симметричных когерентных состояний. Они записываются как [1]

$$|\alpha_j\rangle = |\alpha e^{\frac{2\pi i j}{N}}\rangle, \quad j = 0, \ldots, N-1,$$

то есть их интенсивности равны $\mu = |\alpha|^2$, а фаза принимает значения $\{\frac{2\pi j}{N}\}_{j=0}^{N-1}$ из набора с равным промежутком. N — четное число, и состояния делятся на $M = N/2$ базисов. Фазовый сдвиг θ внутри каждого базиса совпадает, поэтому состояния одного базиса b, соответствующие отправке 0 и 1, имеют вид

$$|\alpha_b^0\rangle = |\alpha e^{i\frac{2\pi k(b)}{N}}\rangle, \; |\alpha_b^1\rangle = |\alpha e^{i(\frac{2\pi k(b)}{N} + \theta)}\rangle, \tag{1}$$

где исходное значение $k(b)$ для каждого базиса определяется конфигурацией состояний.

Важным результатом для симметричных когерентных квантовых состояний является верхняя оценка вероятности безошибочного различения [1]. Такое измерение может быть полезно перехватчику, так как при нем он получает всю информацию о передаваемых состояниях, и может приготовить более яркие состояния в случае успеха, на чем и основана USD-атака [2].

В то же время в условиях квантового распределения ключей перехватчик в общем случае не стоит перед такой сложной задачей, так как ему требуется получить информацию о состояниях одного базиса в условиях, когда базис становится известен впоследствии.

Простым примером атаки, которая в ряде случаев более эффективна, чем различение всех состояний, является атака разделением по числу фотонов, при которой перехватчик отводит один из фотонов сигнального импульса в свою квантовую память, а затем, когда легитимные пользователи раскрывают базисы, измеряет фотон должным образом. В случае, когда импульс содержит несколько фотонов, можно провести безошибочное различение в каждом базисе, используя разные фотоны для разных базисов, что позволяет получить всю информацию о передаваемых посылках, когда легитимные пользователи используют произвольный фазовый сдвиг между состояниями внутри базиса.

Другим примером атаки может быть проведение общего унитарного преобразования над системой и анциллой [3], результатом чего является классический сигнал об успехе или неудаче, а также набор состояний для приемной стороны и для перехватчика. Важно, что можно подобрать состояния таким образом, что в случае успеха состояния оказываются более различимы, и для них уже не действует оценка информации перехватчика через величину Холево исходных состояний.

Работа выполнена при финансовой поддержке государства в лице Минобрнауки России (соглашение № 075-15-2020-788).

Литература

1. Chefles A., Barnett S. M. *Optimum unambiguous discrimination between linearly independent symmetric states* //Physics letters A. - 1998. - Т. 250. - №. 4-6. - С. 223-229.

2. Dusek M., Jahma M., Lutkenhaus N. *Unambiguous state discrimination in quantum cryptography with weak coherent states* //Physical Review A. - 2000. - Т. 62. - №. 2. - С. 022306.

3. Kronberg D. A. Generalized discrimination between symmetric coherent states for eavesdropping in quantum cryptography //Lobachevskii Journal of Mathematics. - 2020. - Т. 41. - №. 12. - С. 2332-2337.

UPPER BOUNDS FOR THE SECURITY OF QUANTUM CRYPTOGRAPHY ON GEOMETRICALLY UNIFORM COHERENT STATES

D.A. Kronberg

This paper investigates the security of quantum cryptography on geometrically uniform coherent states. Using large number of coherent states is a contermeasure against unambiguous state discrimination (USD) attack, but security against this attack does not imply security against any other attack. We consider other possible attack which can be effective for lossy communication line.

Keywords: quantum cryptography, coherent states, quantum information theory.