SCIENCE CHINA
Information Sciences

• **Supplementary File** •

supplementary material

Jia-Wei Ying[1], Shi-Pu Gu[1], Xing-Fu Wang[3], Lan Zhou[2,3] & Yu-Bo Sheng[1,2*]

[1] *College of Electronic and Optical Engineering and College of Flexible Electronics (Future Technology), Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu 210023, China*
[2] *School of Physics, Hangzhou Normal University, Hangzhou, Zhejiang 311121, China*
[3] *College of Science, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu 210023, China*

Appendix A The Kato's inequality

Let $\xi_1, ..., \xi_N$ be a sequence of Bernoulli random variables and let $\mathcal{F}_1 \subseteq \mathcal{F}_2 \subseteq ... \subseteq \mathcal{F}_N$ be an increasing chain of $\sigma-$algebras. Let $\Lambda_l = \sum_{u=0}^{l} \xi_u$. The Kato's inequality [1] is shown as:

$$Pr[\sum_{u=1}^{N} Pr(\xi_u = 1|\mathcal{F}_{u-1}) - \Lambda_N] \geqslant [b + a(\frac{2\Lambda_N}{N} - 1)]\sqrt{N}] \leqslant \exp[\frac{-2(b^2 - a^2)}{(1 + \frac{4a}{3\sqrt{N}})^2}]. \tag{A1}$$

Replacing $\xi_l \to 1 - \xi_l$, and $a \to -a$ in Eq. (A1), we can derive:

$$Pr[\Lambda_N - \sum_{u=1}^{N} Pr(\xi_u = 1|\mathcal{F}_{u-1})] \geqslant [b + a(\frac{2\Lambda_N}{N} - 1)]\sqrt{N}] \leqslant \exp[\frac{-2(b^2 - a^2)}{(1 - \frac{4a}{3\sqrt{N}})^2}]. \tag{A2}$$

Among them, Λ_N represents the statistical value, and $\sum_{u=1}^{N} Pr(\xi_u = 1|\mathcal{F}_{u-1})$ represents the theoretical value. These two formulas describe the upper and lower bounds of the statistical value and the theoretical value within a certain precision. Both the precision and the upper and lower bounds are related to the parameters a and b. When the precision is fixed, we hope that the fluctuation of the upper and lower bounds is as small as possible. That is, we need to solve:

$$\begin{aligned} &\min_{a,b}[b + a(\frac{2\Lambda_N}{N} - 1)]\sqrt{N}, \\ &s.t. \exp[\frac{-2(b^2 - a^2)}{(1 + \frac{4a}{3\sqrt{N}})^2}] = \epsilon, b \geqslant |a|, \end{aligned} \tag{A3}$$

and

$$\begin{aligned} &\min_{a,b}[b + a(\frac{2\Lambda_N}{N} - 1)]\sqrt{N}, \\ &s.t. \exp[\frac{-2(b^2 - a^2)}{(1 - \frac{4a}{3\sqrt{N}})^2}] = \epsilon, b \geqslant |a|, \end{aligned} \tag{A4}$$

The solution of Eq. (A3) is [2,3]

$$\begin{aligned} a &= \frac{3\{9\sqrt{2}N(N - 2\Lambda_N)\sqrt{-\ln\epsilon[9\Lambda_N(N - \Lambda_N) - 2N\ln\epsilon]} + 16N^{3/2}\ln^2\epsilon - 72\Lambda_N\sqrt{N}(N - \Lambda_N)\ln\epsilon\}}{4(9N - 8\ln\epsilon)[9\Lambda_N(N - \Lambda_N) - 2N\ln\epsilon]}, \\ b &= \frac{\sqrt{18Na^2 - (16a^2 - 24\sqrt{N}a + 9N)\ln\epsilon}}{3\sqrt{2}N}, \end{aligned} \tag{A5}$$

and

$$\begin{aligned} &\sum_{u=1}^{N} Pr(\xi_u = 1|\mathcal{F}_{u-1}) \overset{\epsilon}{>} K^L_{N,\epsilon}(\Lambda_N), \\ &K^L_{N,\epsilon}(\Lambda_N) = \Lambda_N - (b + a(2\Lambda_N/N - 1))\sqrt{N}. \end{aligned} \tag{A6}$$

* Corresponding author (email: shengyb@njupt.edu.cn)

For the convenience of distinction, we set the solutions of Eq. (A4) as $c = a_{opt}$ and $d = b_{opt}$. The solution is [2, 3]

$$c = \frac{3\{9\sqrt{2}N(N-2\Lambda_N)\sqrt{-\ln\epsilon[9\Lambda_N(N-\Lambda_N)-2N\ln\epsilon]} - 16N^{3/2}\ln^2\epsilon + 72\Lambda_N\sqrt{N}(N-\Lambda_N)\ln\epsilon\}}{4(9N-8\ln\epsilon)[9\Lambda_N(N-\Lambda_N)-2N\ln\epsilon]},$$

$$d = \frac{\sqrt{18Nc^2 - (16c^2 + 24\sqrt{N}c + 9N)\ln\epsilon}}{3\sqrt{2}N}, \tag{A7}$$

and

$$\sum_{u=1}^{N} Pr(\xi_u = 1|\mathcal{F}_{u-1}) \overset{\epsilon}{<} K^U_{N,\epsilon}(\Lambda_N), \tag{A8}$$
$$K^U_{N,\epsilon}(\Lambda_N) = \Lambda_N - (d + c(2\Lambda_N/N - 1))\sqrt{N}.$$

At this stage, the upper and lower bounds of the theoretical value $\sum_{u=1}^{N} Pr(\xi_u = 1|\mathcal{F}_{u-1})$ are determinable based on the statistical value Λ_N.

At this point, through reverse solving, we can also estimate the upper and lower bounds of the statistical value from the theoretical value. Let $\sum_{u=1}^{N} Pr(\xi_u = 1|\mathcal{F}_{u-1}) = S_N$, and

$$\bar{K}^L_{N,\epsilon}(S_N) \overset{\epsilon}{\leqslant} \Lambda_N \overset{\epsilon}{\leqslant} K^U_{N,\epsilon}(S_N), \tag{A9}$$

$$\bar{K}^L_{N,\epsilon}(S_N) = (\sqrt{N}S_N + N(e-f))/(2e+\sqrt{N}), \tag{A10}$$

$$\bar{K}^U_{N,\epsilon}(S_N) = (\sqrt{N}S_N + N(g-h))/(\sqrt{N}-2g), \tag{A11}$$

where $e = a_{opt}$ and $f = b_{opt}$ are the solution of:

$$\max_{a,b} \frac{\sqrt{N}S_N + N(a-b)}{2a+\sqrt{N}}, \tag{A12}$$
$$s.t. \exp\left[\frac{-2(b^2-a^2)}{(1+\frac{4a}{3\sqrt{N}})^2}\right] = \epsilon, b \geqslant |a|,$$

and [2, 3]

$$e = \frac{3\sqrt{N}\{9(N-2S_N)\sqrt{N\ln\epsilon[N\ln\epsilon - 18S_N(N-S_N)]} - 4N\ln^2\epsilon - 9\ln\epsilon(8S_N^2 - 8NS_N + 3N^2)\}}{4\{4N\ln^2\epsilon + 36\ln\epsilon(2S_N^2 - 2NS_N + N^2) + 81NS_N(N-S_N)\}},$$

$$f = \frac{1}{3}\sqrt{9e^2 - \frac{(4e+3\sqrt{N})^2\ln\epsilon}{2N}}. \tag{A13}$$

$g = a_{opt}$ and $h = b_{opt}$ are the solution of:

$$\min_{a,b} \frac{\sqrt{N}S_N - N(a-b)}{\sqrt{N}-2a}, \tag{A14}$$
$$s.t. \exp\left[\frac{-2(b^2-a^2)}{(1-\frac{4a}{3\sqrt{N}})^2}\right] = \epsilon, b \geqslant |a|,$$

and [2, 3]

$$g = \frac{3\sqrt{N}\{9(N-2S_N)\sqrt{N\ln\epsilon[N\ln\epsilon - 18S_N(N-S_N)]} + 4N\ln^2\epsilon + 9\ln\epsilon(8S_N^2 - 8NS_N + 3N^2)\}}{4\{4N\ln^2\epsilon + 36\ln\epsilon(2S_N^2 - 2NS_N + N^2) + 81NS_N(N-S_N)\}},$$

$$h = \frac{\sqrt{18Ng^2 - (16g^2 - 24\sqrt{N}g + 9N)\ln\epsilon}}{3\sqrt{2}N}. \tag{A15}$$

Appendix B The parameter optimization process

In numerical simulations, we conducted parameter optimization for the secure key transmission rate of the protocol, and this process was mainly implemented using Python. First, we set $\triangle\theta_Z = \triangle\theta_{X/Y} = \triangle\theta$, and $\triangle\phi_{X/Y} = \triangle\phi$, simplifying the secure key transmission rate into a function mainly related to parameters I, $\triangle\theta$, and $\triangle\phi$ to carry out three-parameter optimization.

The optimization algorithm we adopted is the Nelder-Mead algorithm, a derivative-free nonlinear optimization algorithm suitable for solving optimization problems with complex objective functions. In an n-dimensional optimization problem, the algorithm uses n+1 points of the function to construct a polyhedron. Through multiple rounds of iteration, the range of the polyhedron is gradually reduced. Finally, the optimal solution of the function is obtained.

In our optimization problem, the function space is three-dimensional, with the three coordinate axes corresponding to parameters I, $\triangle\theta$, and $\triangle\phi$, respectively. We first randomly selected four sets of parameter values for I, $\triangle\theta$, and $\triangle\phi$ in this space to construct a tetrahedron, and then initiated the iteration process. The iteration process mainly includes four steps:

Step 1. Reflection. Calculate the function values corresponding to the parameters of the four vertices of the tetrahedron, and select point a with the smallest function value. Then calculate the parameter value corresponding to centroid b of the triangle formed by the other three vertices, and further obtain the reflected point a_1 of point a with respect to centroid b. If the function value of a_1 is greater than that of a, proceed to Step 2; otherwise, proceed to Step 3.

Step 2. Expansion: If the function value of the reflected point is larger, it indicates that the reflection direction is correct. Expand along this direction to obtain the expanded point a_2. If the function value of a_2 is better than that of a_1, replace the original vertex a with a_2; otherwise, replace a with a_1.

Step 3. Contraction: If the function value of the reflected point is poor, contract the point a toward the centroid b to obtain the contracted point b_1. If the function value of b_1 is greater than that of a, replace a with b_1; otherwise, proceed to Step 4.

Step 4. Shrinkage: If contraction is ineffective, contract the other vertices of the tetrahedron toward the current optimal vertex, reduce the search range, and then enter the next round of iteration.

When the volume of the tetrahedron is sufficiently small, the corresponding optimal vertex parameters are the optimal solution of the function.

References

1 Kato G. Concentration Inequality Using Unconfirmed Knowledge. arXiv:2002.04357, 2020
2 Zapatero V, and Curty M. Finite-Key Security of Passive Quantum Key Distribution. Phys Rev Appl, 2024, 21:01401
3 Lorenzo G C, Navarrete Á, Pereira M, and Tamaki K. Finite-Key Analysis of Loss-Tolerant Quantum Key Distribution Based on Random Sampling Theory. Phys Rev A, 2021, 104:012406