## Supplementary Information

In this Supplementary Information, we clarify how the security proof by Lim *et al.* [S1] can be plugged into the argument given in Methods to determine a secure key length under the presence of the pattern effect. We also modify the key length formula by Lim *et al.* [S1] to accommodate fluctuations in the pulse intensities. We note that, as pointed out in Ref. [S2], the key rate formula given in Ref. [S1] is not strictly secure for the protocol assumed in Ref. [S1]. Here we assume a different protocol in which the quantum communication ends after a predetermined number of pulses have been sent from Alice to Bob, and until then the basis choices $\boldsymbol{x}_A$ and $\boldsymbol{x}_B$ are kept secret. In this protocol, the valid data sizes such as the sifted key length become variables instead of predetermined values. For this type of protocols, the key rate formula given in Ref. [S1] is secure. Security arguments for protocols with a predetermined sifted key length were given in Refs. [S2, S3], which lead to different key rate formulas.

### Application of the security proof in Ref. [S1]

In addition to the notations used in Methods, we define three sequences included in $\mathbf{\Lambda}$ as follows.

- $\mathbf{d}$: a sequence whose element $d_i \in \{0,1\}$ is 1 when the $i$-th pulse is detected by Bob.
- $\mathbf{b}_B$: a sequence whose element $b_{B,i} \in \{0,1\}$ represents Bob's bit value when $d_i = 1$.
- $\mathbf{e}$: a sequence whose element $e_i \in \{0,1\}$ represents a bit error $b_{A,i} \oplus b_{B,i}$ between Alice and Bob when $d_i = 1$.

For $x = Y, Z$ and $a = S, D, V$, define

$$\begin{aligned}
N_{x,a,n}(\mathbf{a},\mathbf{n},\mathbf{\Lambda}) &:= |\{i \mid a_i = a,\ n_i = n,\ x_i = x_{B,i} = x,\ d_i = 1\}| && (1)\\
M_{x,a,n}(\mathbf{a},\mathbf{n},\mathbf{\Lambda}) &:= |\{i \mid a_i = a,\ n_i = n,\ x_i = x_{B,i} = x,\ d_i = 1,\ e_i = 1\}| && (2)\\
N_{x,a}(\mathbf{a},\mathbf{\Lambda}) &:= \sum_n N_{x,a,n}(\mathbf{a},\mathbf{n},\mathbf{\Lambda}),\ \ N_x(\mathbf{\Lambda}) := \sum_{n,a} N_{x,a,n}(\mathbf{a},\mathbf{n},\mathbf{\Lambda}), && (3)\\
M_{x,a}(\mathbf{a},\mathbf{\Lambda}) &:= \sum_n M_{x,a,n}(\mathbf{a},\mathbf{n},\mathbf{\Lambda}),\ \ M_x(\mathbf{\Lambda}) := \sum_{n,a} M_{x,a,n}(\mathbf{a},\mathbf{n},\mathbf{\Lambda}), && (4)\\
s_{x,n}(\mathbf{n},\mathbf{\Lambda}) &:= \sum_a N_{x,a,n}(\mathbf{a},\mathbf{n},\mathbf{\Lambda}) && (5)\\
v_{x,n}(\mathbf{n},\mathbf{\Lambda}) &:= \sum_a M_{x,a,n}(\mathbf{a},\mathbf{n},\mathbf{\Lambda}) && (6)
\end{aligned}$$

Let $f(a,n) = p_a \exp(-\mu_a)\mu_a^n/n!$, $f(n) = \sum_a f(a,n)$, and $f(a|n) = f(a,n)/f(n)$. Let $E(\cdot)$ be the expectation over $\mathbf{a}$ according to the conditional distribution $\Pr(\boldsymbol{a}|\boldsymbol{n},\mathbf{\Lambda})$. Then we have

$$E(N_{x,a,n}) = f(a|n)s_{x,n}(\mathbf{n},\mathbf{\Lambda}), \quad E(M_{x,a,n}) = f(a|n)v_{x,n}(\mathbf{n},\mathbf{\Lambda}). \tag{7}$$

Lim *et al.* used Hoeffding's inequality

$$\Pr(M_{Y,D} \geq E(M_{Y,D}) - \Delta|\boldsymbol{n},\mathbf{\Lambda}) \geq 1 - \exp(-2\Delta^2/M_Y), \tag{8}$$

which implies that the inequality

$$E(M_{Y,D}) \leq M_{Y,D}^{+} := M_{Y,D} + \delta(M_Y, \epsilon_2) \tag{9}$$

holds with a probability no smaller than $1 - \epsilon_2$, where

$$\delta(M,\epsilon) := \sqrt{(M/2)\ln(1/\epsilon)}. \tag{10}$$

They introduced eleven other inequalities,

$$\begin{aligned}
E(M_{Y,V}) &\geq M_{Y,V}^{-} := M_{Y,V} - \delta(M_Y, \epsilon_2) && (11)\\
E(N_{x,a}) &\leq N_{x,a}^{+} := N_{x,a} + \delta(N_x, \epsilon_1)\ \ (x = Y, Z; a = S, D, V) && (12)\\
E(N_{x,a}) &\geq N_{x,a}^{-} := N_{x,a} - \delta(N_x, \epsilon_1)\ \ (x = Y, Z; a = D, V). && (13)
\end{aligned}$$

As pointed out in Refs. [S4, S5], one may also use a Chernoff bound for a sum of independent variables instead of Eq. (8), leading to tighter inequalities. Based on the asymmetric decoy-state analysis proposed in [S6], they combined the 12 inequalities with Eq. (7) to derive the bounds on $v_{Y,1}$, $s_{x,0}$, and $s_{x,1}$ as

$$\begin{aligned} v_{Y,1} &\leq v^U_{Y,1}(M^+_{Y,D}, M^-_{Y,V}) && (14)\\ s_{x,0} &\geq s^L_{x,0}(N^+_{x,D}, N^-_{x,V}) \ \ (x = Y, Z) && (15)\\ s_{x,1} &\geq s^L_{x,1}(N^+_{x,S}, N^+_{x,D}, N^-_{x,D}, N^+_{x,V}, N^-_{x,V}) \ \ (x = Y, Z), && (16)\end{aligned}$$

where the explicit forms of the functions on the right-hand sides are given in [S1]. Inequalities (14) - (16) can be regarded as a set of conditions on $(\mathbf{a}, \mathbf{n}, \mathbf{\Lambda})$, and hence we can write them as $(\mathbf{a}, \mathbf{n}, \mathbf{\Lambda}) \in \Gamma$. From the union bound, $\Pr((\mathbf{a}, \mathbf{n}, \mathbf{\Lambda}) \in \Gamma) \geq 1 - \epsilon_a$ with $\epsilon_a = 10\epsilon_1 + 2\epsilon_2$. This corresponds to the statement (a) in Methods.

Lim *et al.* then proved the statement (b) with $\epsilon_{\rm b} = 9\epsilon + \epsilon_{\rm cor}$ with a final key length

$$l(\mathbf{a}, \mathbf{\Lambda}) = \lfloor s^L_{Z,0} + s^L_{Z,1} - s^L_{Z,1} h(\phi^U_Z) - \lambda_{\rm EC} - \log_2 \frac{2}{\epsilon_{\rm cor}\epsilon^6} \rfloor, \tag{17}$$

where $\lambda_{\rm EC}$ is the cost of the error correction, and $\phi^U_Z$ is defined as

$$\phi^U_Z := \frac{v^U_{Y,1}}{s^L_{Y,1}} + \gamma\left(\epsilon, \frac{v^U_{Y,1}}{s^L_{Y,1}}, s^L_{Y,1}, s^L_{Z,1}\right), \tag{18}$$

$$\gamma(a, b, c, d) = \sqrt{\frac{(c+d)(1-b)b}{cd \ln 2} \log_2\left(\frac{c+d}{cd(1-b)b}\frac{1}{a^2}\right)}. \tag{19}$$

Applying the argument in Methods, it follows that the protocol with PS and AKD under the pattern effect is $2(\epsilon_a + \epsilon_b)$-secure with a final key length

$$\sum_{\pi \in \{\text{even, odd}\}} l(\mathbf{a}^{\pi,\rm PS}, \mathbf{\Lambda}^{\pi,\rm PS}). \tag{20}$$

**Key length formula under intensity fluctuations**

Here we consider the case where the mean photon number $\mu_a$ of each pulse is not precisely known and may be varied from pulse to pulse. We assume that we know the upper and lower bounds on $\mu_a$, namely,

$$\mu^L_a \leq \mu_a \leq \mu^U_a \ \ (a = S, D, V). \tag{21}$$

An argument to cover such a situation was given in Ref. [S7], but our analysis here is different and tighter.

In the following, we assume that $1 \geq \mu^U_S$, $\mu^L_S \geq \mu^U_D + \mu^L_V$, $\mu^L_D \geq \mu^U_V$,

$$\kappa^U_2 := \frac{(\mu^U_D)^2 - (\mu^L_V)^2}{(\mu^L_S)^2} \leq \frac{e^{\mu^L_S}}{e^{\mu^U_S}}, \tag{22}$$

and further,

$$\kappa^U_2 \leq \frac{\mu^L_D - \mu^U_V}{\mu^U_S}. \tag{23}$$

These assumptions are usually met if the fluctuations are small. The values of $f(a, n)$ are bounded as

$$f^L(a, n) \leq f(a, n) \leq f^U(a, n) \tag{24}$$

$$f^L(a, 0) = p_a \exp(-\mu^U_a), \ \ f^U(a, 0) = p_a \exp(-\mu^L_a) \tag{25}$$

$$f^L(a, n) = p_a \exp(-\mu^L_a)(\mu^L_a)^n/n!, \ \ f^U(a, n) = p_a \exp(-\mu^U_a)(\mu^U_a)^n/n! \ \ (n \geq 1). \tag{26}$$

The difference from the ideal case lies in Eq. (7), which must be replaced by inequalities involving the known values $f^L(a,n)$ and $f^U(a,n)$. Then we can derive modified formulas for $v^U_{Y,1}$, $s^L_{x,0}$, and $s^L_{x,1}$ appearing in Eqs. (14)-(16).

We first determine $v^U_{Y,1}(M^+_{Y,D}, M^-_{Y,V})$. We have, for all $n$,

$$\frac{f(D|n)}{f^L(D,0)} - \frac{f(V|n)}{f^U(V,0)} = \frac{1}{n!f(n)}\left(\frac{f(D,0)}{f^L(D,0)}\mu_D^n - \frac{f(V,0)}{f^U(V,0)}\mu_V^n\right) \geq 0. \tag{27}$$

This leads to

$$\frac{E(M_{Y,D,n})}{f^L(D,0)} - \frac{E(M_{Y,V,n})}{f^U(V,0)} \geq 0. \tag{28}$$

In general, for $\xi_j^U \geq \xi_j \geq \xi_j^L \geq 0$, $a_j \geq 0$, and $a_1\xi_1^L - a_2\xi_2^U - a_3\xi_3^U \geq 0$, we have bounds

$$\frac{a_1\xi_1^L - a_2\xi_2^U - a_3\xi_3^U}{\xi_1^L + \xi_2^U + \xi_3^U} \leq \frac{a_1\xi_1 - a_2\xi_2 - a_3\xi_3}{\xi_1 + \xi_2 + \xi_3} \leq \frac{a_1\xi_1^U - a_2\xi_2^L - a_3\xi_3^L}{\xi_1^U + \xi_2^L + \xi_3^L}. \tag{29}$$

Since $f^L(D,1)/f^L(D,0) - f^U(V,1)/f^U(V,0) \geq \mu_D^L - \mu_V^U \geq 0$, we have

$$\frac{f(D|1)}{f^L(D,0)} - \frac{f(V|1)}{f^U(V,0)} \geq \left(\frac{f^L(D,1)}{f^L(D,0)} - \frac{f^U(V,1)}{f^U(V,0)}\right)\frac{1}{\tau_1^{ULU}} \tag{30}$$

holds with

$$\tau_1^{ULU} := f^U(S,1) + f^L(D,1) + f^U(V,1) \tag{31}$$

Hence,

$$\frac{E(M_{Y,D})}{f^L(D,0)} - \frac{E(M_{Y,V})}{f^U(V,0)} \geq \frac{E(M_{Y,D,1})}{f^L(D,0)} - \frac{E(M_{Y,V,1})}{f^U(V,0)} \geq \left(\frac{f^L(D,1)}{f^L(D,0)} - \frac{f^U(V,1)}{f^U(V,0)}\right)\frac{v_{Y,1}}{\tau_1^{ULU}} \tag{32}$$

and

$$v_{Y,1} \leq v^U_{Y,1} := \tau_1^{ULU}\left(\mu_D^L\frac{e^{\mu_D^U}}{e^{\mu_D^L}} - \mu_V^U\frac{e^{\mu_V^L}}{e^{\mu_V^U}}\right)^{-1}\left(\frac{e^{\mu_D^U}M^+_{Y,D}}{p_D} - \frac{e^{\mu_V^L}M^-_{Y,V}}{p_V}\right). \tag{33}$$

In a similar way we can determine $s^L_{x,0}(N^+_{x,D}, N^-_{x,V})$. For $n \geq 1$, we have

$$\frac{f(D|n)}{f^L(D,1)} - \frac{f(V|n)}{f^U(V,1)} = \frac{1}{n!f(n)}\left(\frac{f(D,1)}{f^L(D,1)}\mu_D^{n-1} - \frac{f(V,1)}{f^U(V,1)}\mu_V^{n-1}\right) \geq 0. \tag{34}$$

Since $f^L(V,0)/f^U(V,1) - f^U(D,0)/f^L(D,1) \geq 0$, we have

$$\frac{E(N_{x,V})}{f^U(V,1)} - \frac{E(N_{x,D})}{f^L(D,1)} \leq \frac{E(N_{x,V,0})}{f^U(V,1)} - \frac{E(N_{x,D,0})}{f^L(D,1)} \leq \left(\frac{f^U(V,0)}{f^U(V,1)} - \frac{f^L(D,0)}{f^L(D,1)}\right)\frac{s_{x,0}}{\tau_0^{LLU}} \tag{35}$$

holds with $\tau_0^{LLU} := f^L(S,0) + f^L(D,0) + f^U(V,0)$, and

$$s_{x,0} \geq s^L_{x,0} := \tau_0^{LLU}\left(\mu_D^L\frac{e^{\mu_V^U}}{e^{\mu_V^L}} - \mu_V^U\frac{e^{\mu_D^L}}{e^{\mu_D^U}}\right)^{-1}\left(\frac{\mu_D^L e^{\mu_V^U}N^-_{x,V}}{p_V} - \frac{\mu_V^U e^{\mu_D^L}N^+_{x,D}}{p_D}\right). \tag{36}$$

Finally, we determine $s^L_{x,1}(N^+_{x,S}, N^+_{x,D}, N^-_{x,D}, N^+_{x,V}, N^-_{x,V})$. Define

$$\kappa_n := \frac{\mu_D^n - \mu_V^n}{\mu_S^n} \tag{37}$$

where $\kappa_2^U \geq \kappa_2 \geq 0$. Since $\alpha^{n-1} - \beta^{n-1} \geq (\alpha^{n-1} - \beta^{n-1})(\alpha + \beta) = \alpha^n - \beta^n + \alpha\beta(\alpha^{n-2} - \beta^{n-2}) \geq \alpha^n - \beta^n$ for $\alpha \geq \beta \geq 0$ and $\alpha + \beta \leq 1$, we have $\kappa_{n-1} \geq \kappa_n$ $(n \geq 2)$. We then obtain, for $n \geq 2$,

$$\kappa_2^U\frac{f(S|n)}{f^L(S,0)} - \frac{f(D|n)}{f^U(D,0)} + \frac{f(V|n)}{f^L(V,0)} \geq \frac{\kappa_2\mu_S^n - \mu_D^n + \mu_V^n}{n!f(n)} = \frac{\mu_S^n}{n!f(n)}(\kappa_2 - \kappa_n) \geq 0. \tag{38}$$

For $\alpha, \beta, \gamma > 0$ that satisfy $\alpha f^U(S,0) \le \beta f^U(D,0)$ and $\beta f^U(D,0) \ge \gamma f^L(V,0)$,

$$\begin{aligned}\alpha f(S|0) - \beta f(D|0) + \gamma f(V|0) &= \frac{\alpha f(S,0) - \beta f(D,0) + \gamma f(V,0)}{f(S,0) + f(D,0) + f(V,0)} \ge \frac{\alpha f(S,0) - \beta f^U(D,0) + \gamma f(V,0)}{f(S,0) + f^U(D,0) + f(V,0)} \\ &\ge \frac{\alpha f(S,0) - \beta f^U(D,0) + \gamma f^L(V,0)}{f(S,0) + f^U(D,0) + f^L(V,0)} \ge \frac{\alpha f^L(S,0) - \beta f^U(D,0) + \gamma f^L(V,0)}{f^L(S,0) + f^U(D,0) + f^L(V,0)}. \end{aligned} \tag{39}$$

Hence, combined with Eq. (22), we have

$$\kappa_2^U \frac{f(S|0)}{f^L(S,0)} - \frac{f(D|0)}{f^U(D,0)} + \frac{f(V|0)}{f^L(V,0)} \ge \frac{\kappa_2^U}{\tau_0^{LUL}}. \tag{40}$$

Since $f^L(D,1)/f^U(D,0) - \kappa_2^U f^U(S,1)/f^L(S,0) - f^U(V,1)/f^L(V,0) \ge 0$ from Eq. (23), it holds that

$$-\kappa_2^U \frac{f(S|1)}{f^L(S,0)} + \frac{f(D|1)}{f^U(D,0)} - \frac{f(V|1)}{f^L(V,0)} \le \left( -\kappa_2^U \frac{f^L(S,1)}{f^L(S,0)} + \frac{f^U(D,1)}{f^U(D,0)} - \frac{f^L(V,1)}{f^L(V,0)} \right) \frac{1}{\tau_1^{LUL}}, \tag{41}$$

and

$$-\kappa_2^U \frac{E(N_{x,S})}{f^L(S,0)} + \frac{E(N_{x,D})}{f^U(D,0)} - \frac{E(N_{x,V})}{f^L(V,0)} \le \left( -\kappa_2^U \frac{f^L(S,1)}{f^L(S,0)} + \frac{f^U(D,1)}{f^U(D,0)} - \frac{f^L(V,1)}{f^L(V,0)} \right) \frac{s_{x,1}}{\tau_1^{LUL}} - \frac{\kappa_2^U s_{x,0}}{\tau_0^{LUL}}. \tag{42}$$

We thus obtain

$$s_{x,1} \ge s_{x.1}^L := \tau_1^{LUL} \left( -\kappa_2^U \mu_S^L \frac{e^{\mu_S^U}}{e^{\mu_S^L}} + \mu_D^U \frac{e^{\mu_D^L}}{e^{\mu_D^U}} - \mu_V^L \frac{e^{\mu_V^U}}{e^{\mu_V^L}} \right)^{-1} \left[ \kappa_2^U \left( \frac{s_{x,0}^L}{\tau_0^{LUL}} - \frac{e^{\mu_S^U} N_{x,S}^+}{p_S} \right) + \frac{e^{\mu_D^L} N_{x,D}^-}{p_D} - \frac{e^{\mu_V^U} N_{x,V}^+}{p_V} \right]. \tag{43}$$

The final secure key length is still given by Eqs. (17)–(19) as in the nonfluctuating case, except that the parameters $s_{Z,0}^L$, $s_{Z,1}^L$, $v_{Y,1}^U$, and $s_{Y,1}^L$ are defined by Eqs. (33), (36), and (43). The numerical calculation for Figure 3 in the main text was done by choosing $\epsilon = \epsilon_1 = \epsilon_2 = 10^{-11}/21$ and $\epsilon_{\rm cor} = 2^{-128}$, which ensures that the final concatenated key after AKD of length (20) is $2 \times (10^{-11} + 2^{-128})$-secure. We chose the observed sifted key length to be $N_Z = 1 \times 10^8$, and chose the other lengths proportionally as

$$N_{x,a} = \frac{N_Z p_a \tilde{D}_{ax}}{p_S \tilde{D}_{SZ} + p_D \tilde{D}_{DZ} + p_V \tilde{D}_{VZ}} \tag{44}$$

and $M_{x,a} = N_{x,a} e_{ax}$.

## References

[S1] C. C. W. Lim, et al., Phys. Rev. A **89**, 022307 (2014).

[S2] C. Pfister, N. Lütkenhaus, S. Wehner, and P. J. Coles, New Journal of Physics **18**, 053001 (2016).

[S3] K. Tamaki, H. -K. Lo, A. Mizutani, G. Kato, C. C. W. Lim, K. Azuma, and M. Curty, Quantum Science and Technology **3**, 014002 (2017).

[S4] Y. Wang, W. -S. Bao, C. Zhou, M. -S. Jiang, and H. -W. Li, Phys. Rev. A **94**, 032335 (2016).

[S5] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, Phys. Rev. A **95**, 012333 (2017).

[S6] X. Ma, B. Qi, Y. Zhao, and H. -K. Lo, Phys. Rev. A **72**, 012326 (2005).

[S7] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto and K. Tamaki, New J. Phys. **17**, 093011 (2015).