Practical round-robin-differential-phase-shift quantum key distribution

arXiv:1702.01260 (2017)

Yunguang Han

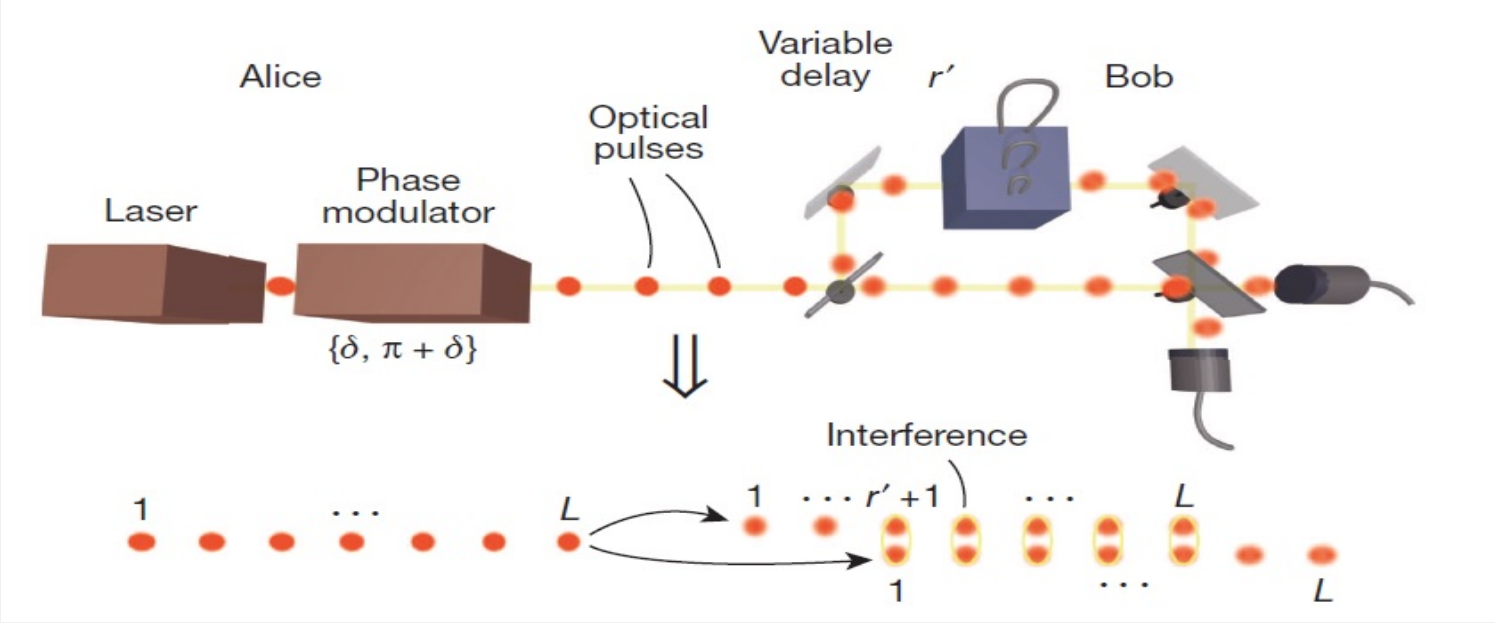
Collaborated with: Zhenqiang Yin, Shuang Wang, Wei Chen, Rong Wang, Zhenfu Han & Guangcan Guo
University of Science and Technology of China

AQIS 2017, Singapore

Outline

1. Introduction: RRDPS protocol
2. Security analysis of practical RRDPS
3. Experimental implementation

RRDPS QKD protocol



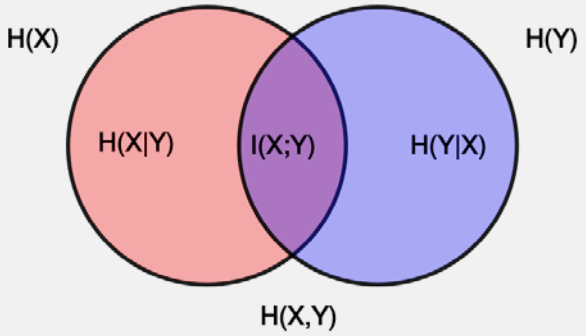
Practical quantum key distribution protocol without monitoring signal disturbance

T. Sasaki, Y. Yamamoto, and M. Koashi, Nature 509, 475 (2014)

Security analysis of QKD

- General secure key rate (Devetak –Winter formula)

$$R \geq I(A:B) - I(A:E)$$



Mutual information

- Understanding through post processing

$$R = 1 - H_{EC} - H_{PA}$$

H_{EC}: Difference between Alice and Bob,
shown as quantum error rate, EC-Error Correction

H_{PA}: Information leakage to the eavesdropper,
not directly observable, PA-Privacy Amplification

- Useful tool: Holevo bound

$$\chi(A:\rho_E) = S(\rho_E) - \sum_a p(a) S(\rho_E^a)$$

Security analysis of QKD

- BB84 QKD

$$H_{PA} = H_{EC} = h(e_{bit})$$

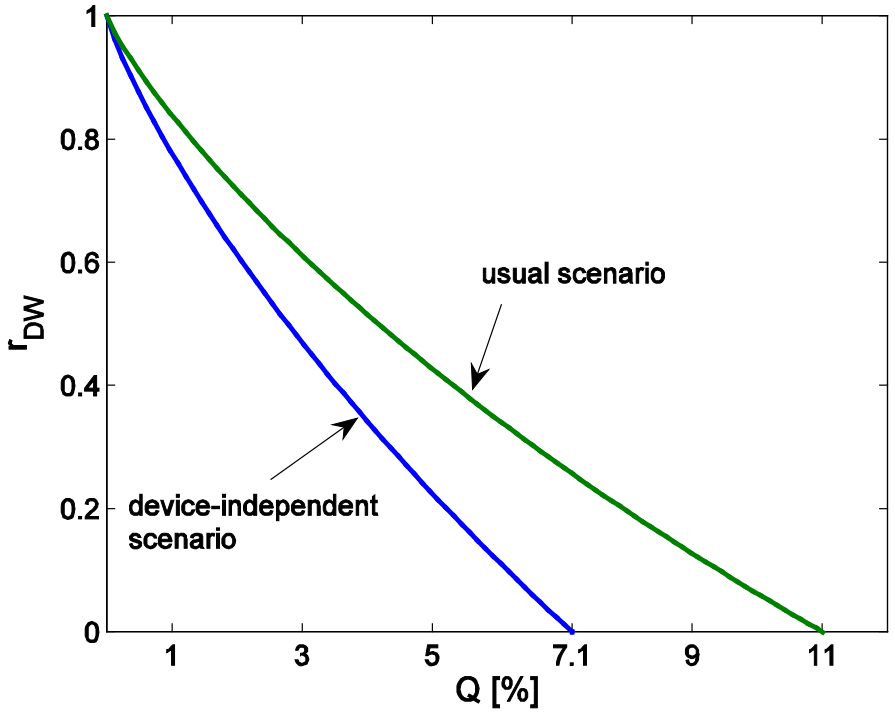
$$R \geq 1 - 2h(e_{bit})$$

- Device Independent(DI) QKD

$$\chi(B:E) \leq h\left(\frac{1+\sqrt{(S/2)^2-1}}{2}\right)$$

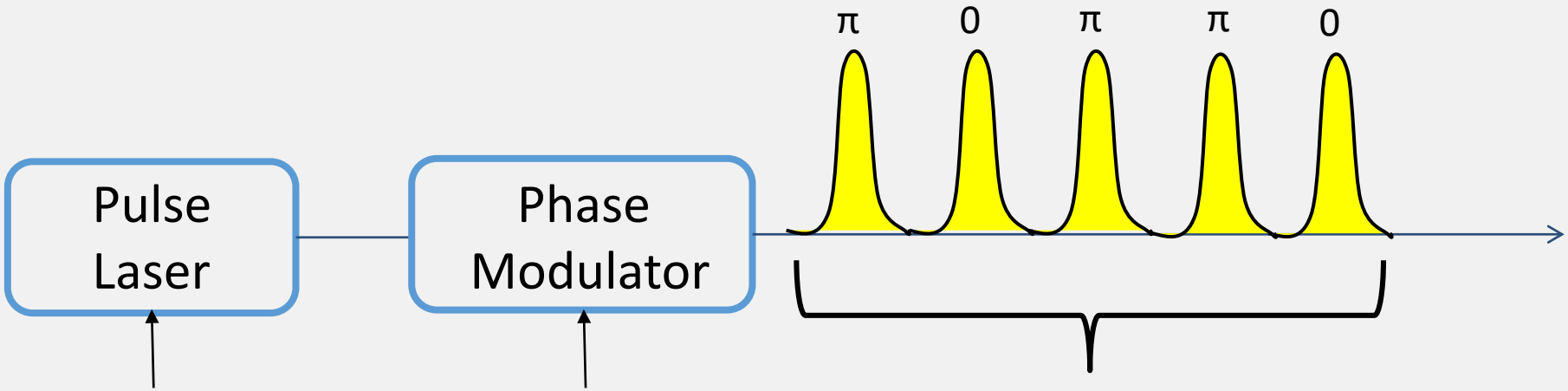
$$R \geq 1 - h(e) - h\left(\frac{1+\sqrt{(S/2)^2-1}}{2}\right)$$

$$S - CHSH\ value$$



In conventional QKD protocols, H_{PA} is a written as a function of the bit error rate or other outcome value. The signal disturbance should be monitored to estimate the leakage information.

RRDPS: sender



Low average photon number per pulse.
Total photon less than L.

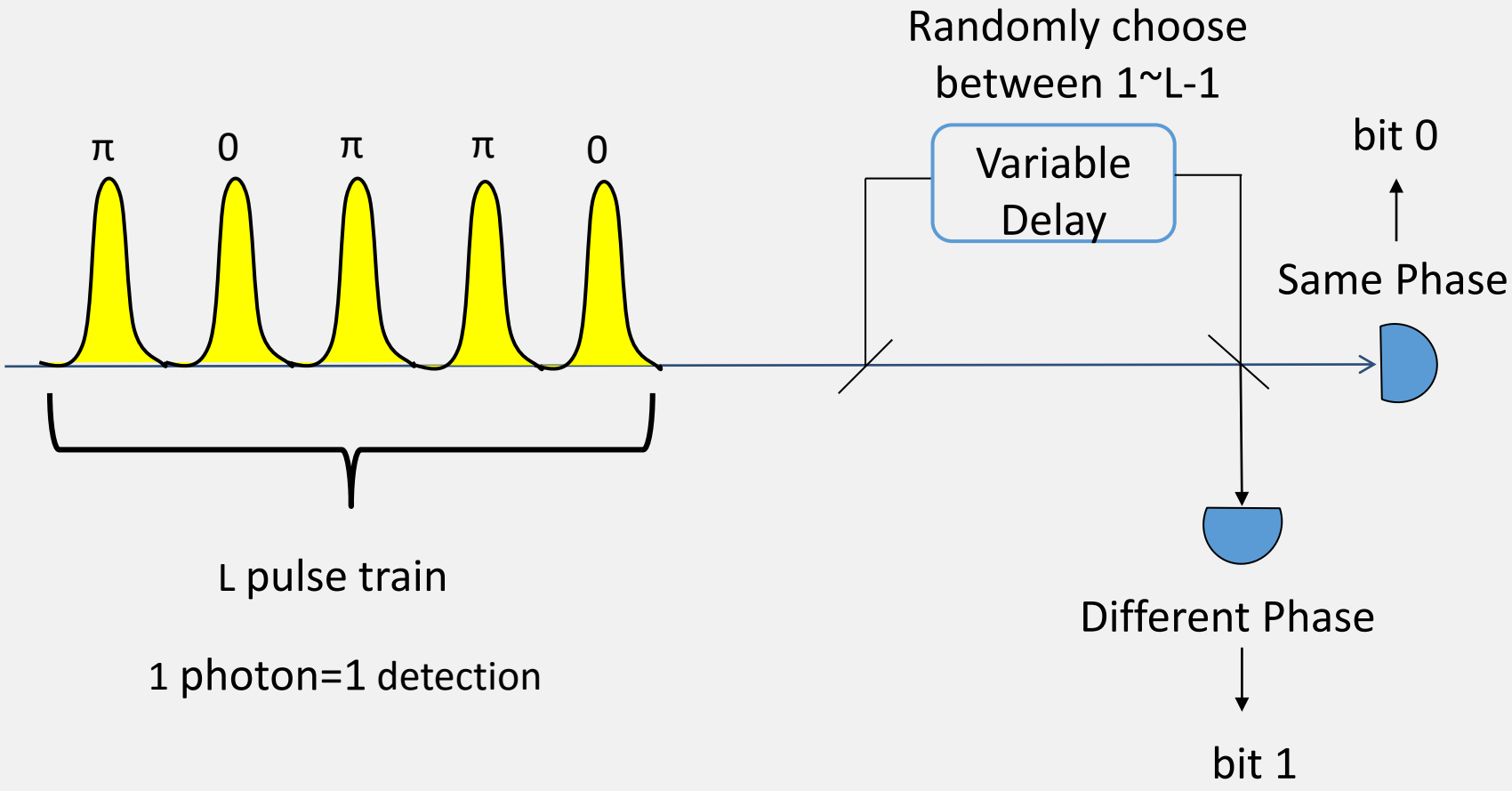
0 or π Phase shift

Encoded by L-bit random sequence $s_1 \dots s_L$

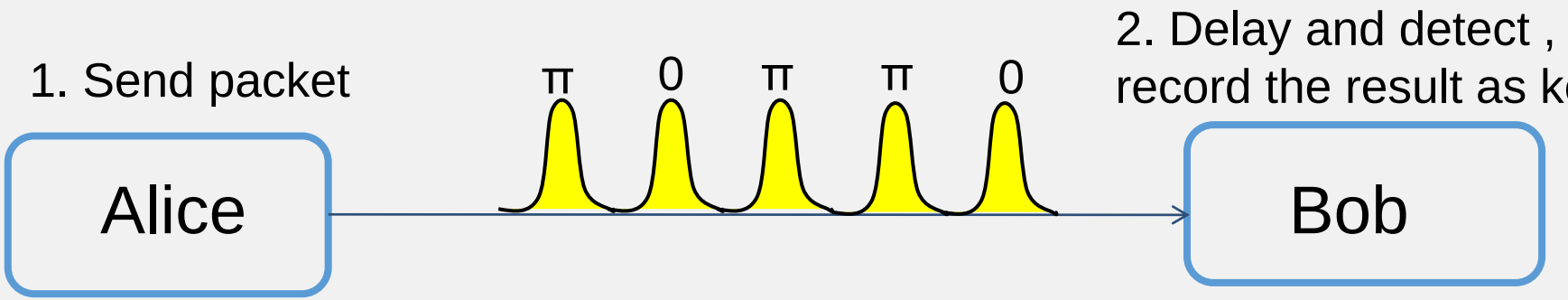
Packet = L pulse train

$$|\Psi_1\rangle := \frac{1}{\sqrt{L}} \sum_{k=1}^{L} (-1)^{s_k} |k\rangle$$

RRDPS：receiver



RRDPS protocol



Security:

- On Alice's side

Eve cannot deterministically read the phase difference of the pair that she wants to know.

- On Bob's side

Eve cannot fully control which pair Bob announces.

Key rate of RRDPS

1. Single photon case

$$I_{AE} = H_{PA} \leq h(1/(L-1))$$

$$R = 1 - h(e_{bit}) - h(1/(L-1))$$

2. Truncated at v_{th} photons

$$I_{AE} = H_{PA} \leq h(\frac{v_{th}}{L-1})$$

$$R = 1 - h(e_{bit}) - h(\frac{v_{th}}{L-1})$$

The leakage information is not related with error rate. Without monitoring the disturbance.

Advantages and Disadvantages

Advantages:

1. High tolerable error rate.

Setting a large enough L, tolerate up to 50% error rate.

2. Multi-photon event can be used to generate secure key.

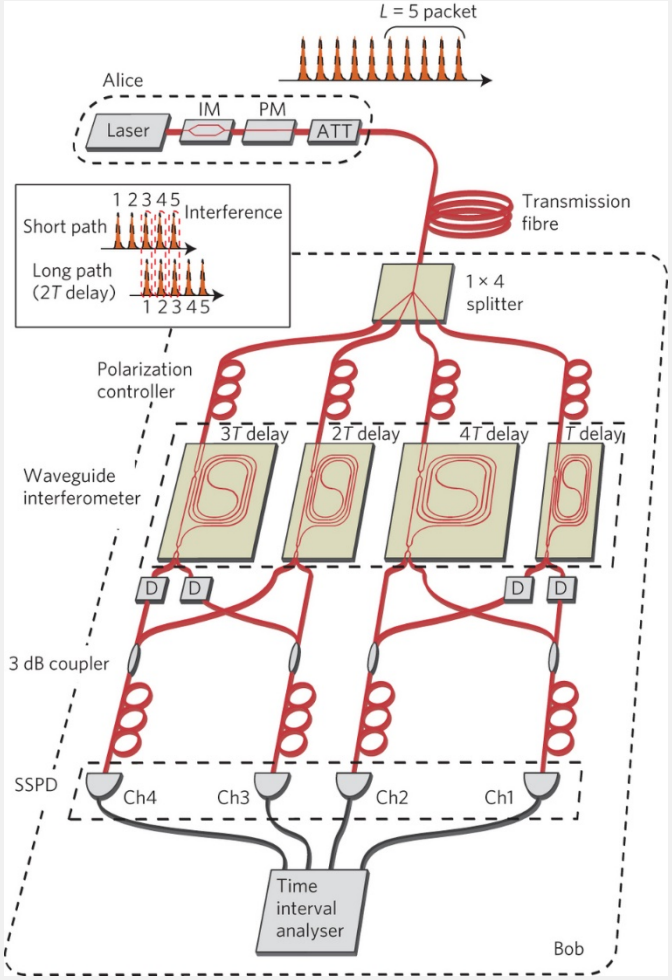
3. Less parameters when considering finite size effect.

Disadvantages:

1. Difficult to implement with large L, the key rate per packet also decreases.

2. The bound of leakage information is not tight.

Experimental progress

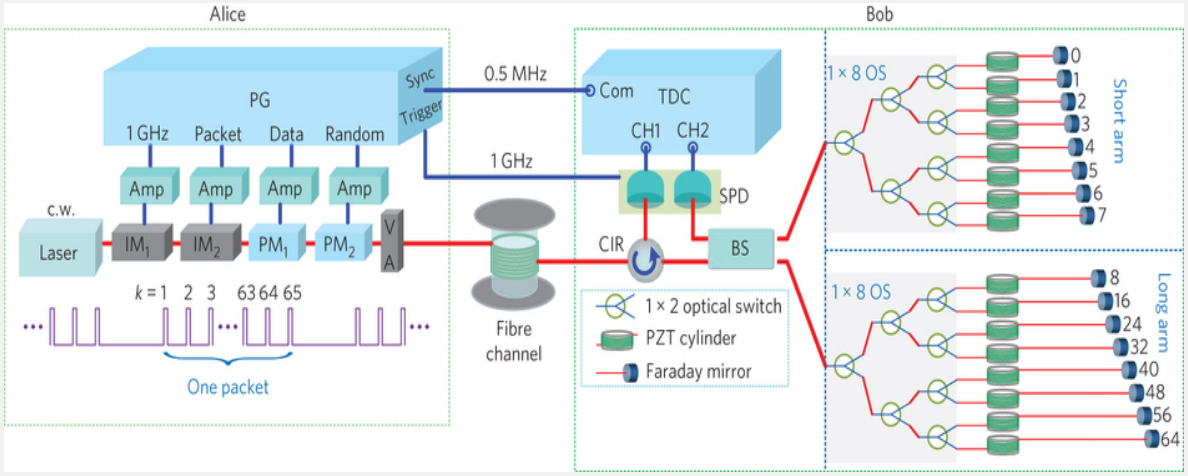


Exp1. Passive selection of delay, one detector on each route

L=5, distance 30km, key rate 10^-9, scaling problem

H. Takesue, et al. Nat Photon 9, 827–831 (2015)

Experimental progress



Exp2. Compact cascade Michelson interferometer, 8*8 choice
L=65, distance 90km, key rate 10^-6,
demanding phase control

S. Wang, et al. Nat Photon 9, 832–836 (2015)

New analysis method

Single photon case

- Alice prepares $|\psi\rangle = \sum_{i=1}^{L}(-1)^{k_i}|i\rangle$
- Eve's general collective attack

$$U_{Eve}|i\rangle|e_{00}\rangle = \sum_{j=1}^{L} c_{ij}|j\rangle|e_{ij}\rangle = \sum_{j=1}^{L} \widetilde{c_{ij}}|j\rangle$$

- Bob measures between $|a\rangle$ and $|b\rangle$, announce {a,b}

Project the incoming states into $(|a\rangle \pm |b\rangle)/\sqrt{2}$

- Density of Eve's ancilla

$$\rho_E = P\left\{\sum_{i=1}^{L}(-1)^{k_i}\widetilde{c_{ia}}\right\} + P\left\{\sum_{i=1}^{L}(-1)^{k_i}\widetilde{c_{ib}}\right\} \qquad P\{|x\rangle\} = |x\rangle\langle x|$$

Eve aims to guess $\mathrm{k_a} \oplus \mathrm{k_b}$ after Bob reveals the value {a,b}

Utilize phase randomization

- Phase randomization

$k_i (i \neq a, b)$ equals to 0,1 randomly, so we can randomize the relative phase between $|e_{aa}\rangle \; and \; |e_{ia}\rangle$ ($|e_{bb}\rangle \; and \; |e_{ib}\rangle$)

- Density of Eve's ancilla

$$\rho_E = P\{(-1)^{k_a}\widetilde{c_{aa}} + (-1)^{k_b}\widetilde{c_{ba}}\} + P\{(-1)^{k_a}\widetilde{c_{bb}} + (-1)^{k_b}\widetilde{c_{ab}}\}$$
$$+ \sum_{i \neq a,b} c_{ia}^2 P\{|e_{ia}\rangle\} + c_{ib}^2 P\{|e_{ib}\rangle\}$$

After phase randomization, the leakage information of the eavesdropper will be compressed.

Leakage information

$k_a \oplus k_b = 0$

$$\rho_0^{(a,b)} = P\{\tilde{c}_{aa} + \tilde{c}_{ba}\} + P\{\tilde{c}_{bb} + \tilde{c}_{ab}\} + \sum_{i \neq a,b} c_{ia}^2 P\{|e_{ia}\rangle\} + c_{ib}^2 P\{|e_{ib}\rangle\}.$$

$k_a \oplus k_b = 1$

$$\rho_1^{(a,b)} = P\{\tilde{c}_{aa} - \tilde{c}_{ba}\} + P\{\tilde{c}_{bb} - \tilde{c}_{ab}\} + \sum_{i \neq a,b} c_{ia}^2 P\{|e_{ia}\rangle\} + c_{ib}^2 P\{|e_{ib}\rangle\}.$$

Eve's Information for {a,b} (using Holevo bound)

$$\begin{aligned} Q^{(a,b)} I_{AE}^{(a,b)} &= (c_{aa}^2 + c_{ba}^2) S\left(\begin{bmatrix} \frac{c_{aa}^2}{c_{aa}^2 + c_{ba}^2} & 0 \\ 0 & \frac{c_{ba}^2}{c_{aa}^2 + c_{ba}^2} \end{bmatrix} \right) + (c_{bb}^2 + c_{ab}^2) S\left(\begin{bmatrix} \frac{c_{bb}^2}{c_{bb}^2 + c_{ab}^2} & 0 \\ 0 & \frac{c_{ab}^2}{c_{bb}^2 + c_{ab}^2} \end{bmatrix} \right) \\ &= \varphi(c_{ba}^2, c_{aa}^2) + \varphi(c_{ab}^2, c_{bb}^2), \end{aligned}$$

$$\varphi(x, y) = -x \log_2 x - y \log_2 y + (x + y) \log_2 (x + y)$$

Tighter bound

Total leakage information
(average weighted by the yield)

$$I_{AE} = \frac{\sum_{a<b} Q^{(a,b)} I_{AE}^{(a,b)}}{\sum_{a<b} Q^{(a,b)}} = \frac{\sum_{a<b} \varphi(c_{ba}^2, c_{aa}^2) + \varphi(c_{ab}^2, c_{bb}^2)}{(L-1)\sum_{i,j} c_{ij}^2}.$$

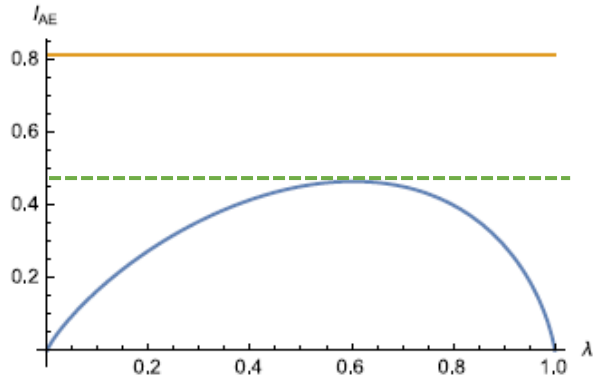
By convexity of function φ

$$I_{AE} \leqslant \frac{\varphi((L-1)x_1, x_2)}{(L-1)(x_1+x_2)}.$$

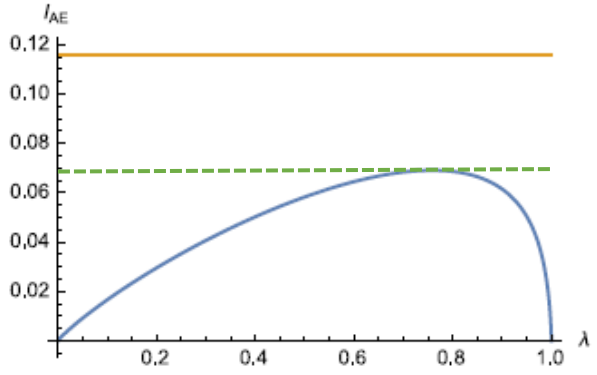
$x_1 = \sum_i c_{ii}^2$, $x_2 = \sum_{i \neq j} c_{ij}^2$, $x_1 + \mathrm{x}_2 = 1$,
Considering the worst case, get an upper bound of leakage information
Without monitoring error rate: x1 and x2 can be free variable;
Considering error rate: constraint on x1 and x2.

$$x_2/(x_1+x_2) \leqslant 2(L-1)E/(L-2).$$

Comparison



a. L=5



b. L=65

TABLE I. The maximum value of tolerant error rate of RRDPS with different methods.

L \ method	original RRDPS	without error rate	with error rate
3	–	0.0546	0.0811
5	0.0289	0.122	0.144
16	0.165	0.244	0.252
32	0.24	0.3	0.303
64	0.301	0.346	0.346

Tighter bound of the leakage information, especially for small L values, e.g. L=3 is acceptable.

Multi-photon case

Consider the odd and even photon number case respectively, get a recursive relation.
N-photon in L-pulse packet

$$I_{AE} \leqslant Max_{x_1,x_2,\ldots,x_{N+1}}\{\frac{\sum_{n=1}^{N}\varphi((L-n)x_n, nx_{n+1})}{L-1}\},$$

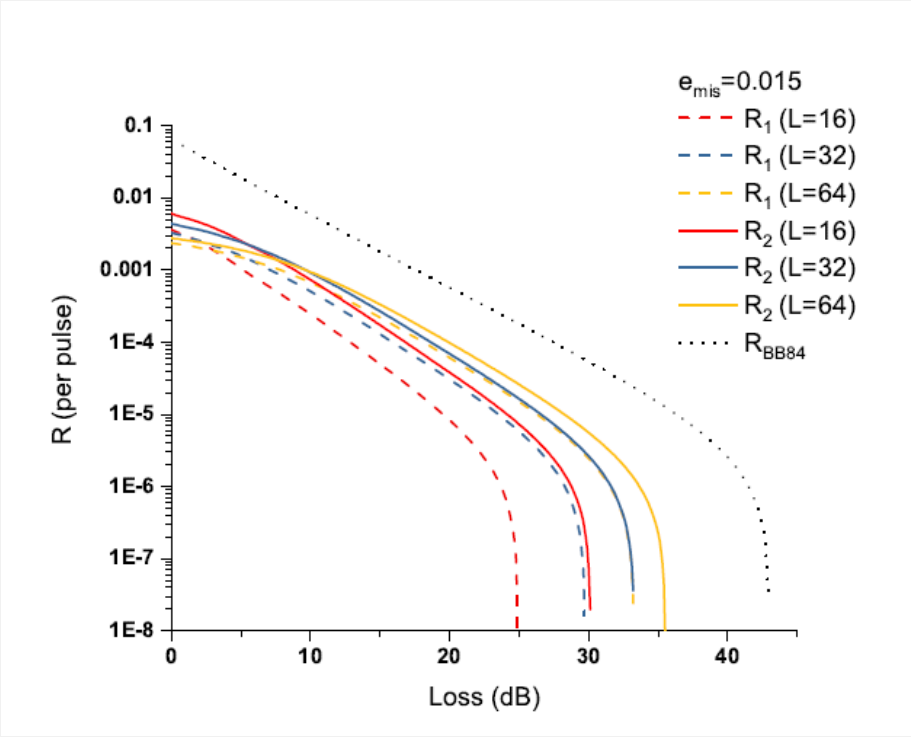
$$\sum_{i=1}^{N+1} x_i = 1$$

Consider the odd and even photon number case respectively, get a recursive relation.

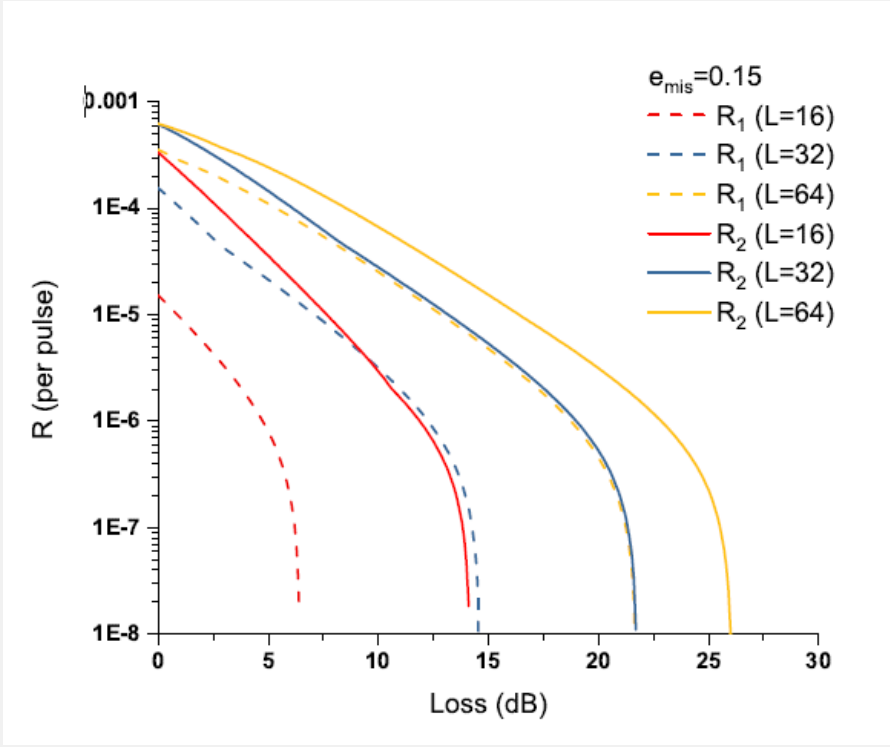
$$E \geqslant \frac{\sum_{n\geqslant 1}^{(N-1)/2}(\sqrt{(L-2n)x_{2n}} - \sqrt{2nx_{2n+1}})^2 + (L-N-1)x_{N+1}/2}{L-1} \text{ for odd } N,$$

$$E \geqslant \frac{\sum_{n\geqslant 1}^{N/2}(\sqrt{(L-2n+1)x_{2n-1}} - \sqrt{(2n-1)x_{2n}})^2 + (L-N-1)x_{N+1}/2}{L-1} \text{ for even } N.$$

Simulation



Error rate 0.015

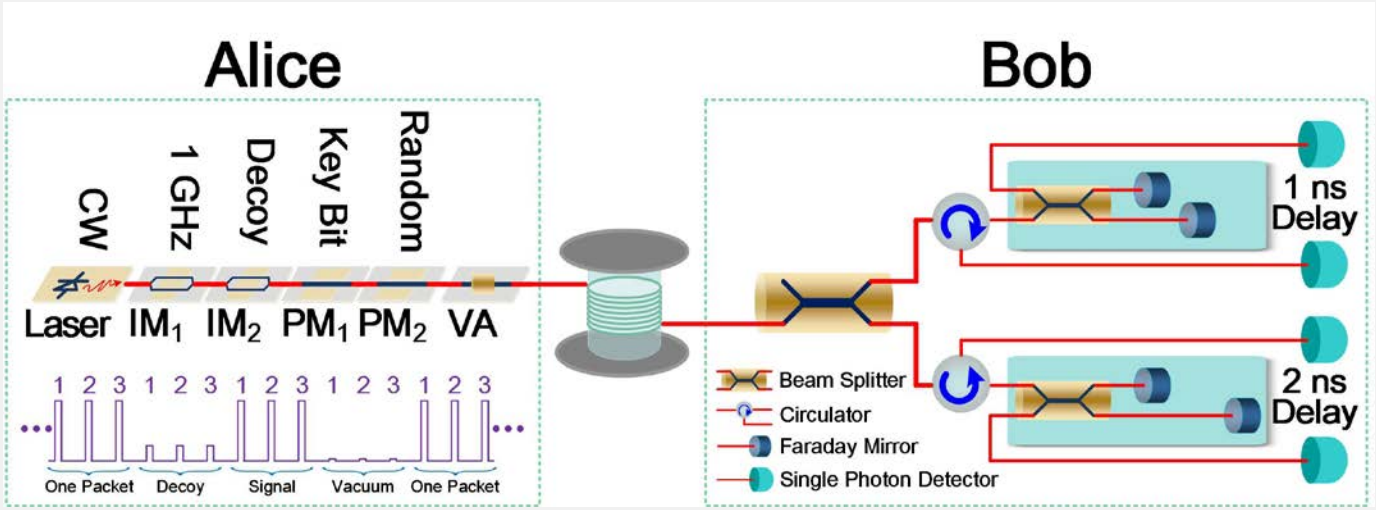


Error rate 0.15

Secret key rate R versus channel loss
R1-the original protocol
R2-the proposed protocol

Proof of principle experiment

Experiment setup



L=3, the simplest RRDPS realization

Experimental result

l(km)	Q_s	E_s	Q_d	E_d	Q_v	R_1	R_2
50	3.24×10^{-3}	1.76%	7.52×10^{-4}	1.95%	1.12×10^{-5}	8.14×10^{-5}	3.60×10^{-4}
100	3.28×10^{-4}	2.26%	7.86×10^{-5}	4.01%	4.50×10^{-6}	4.98×10^{-6}	3.15×10^{-5}
140	5.52×10^{-5}	4.99%	1.56×10^{-5}	13.31%	3.87×10^{-6}	–	1.45×10^{-6}

Conclusion & remarks

- Develop a new method to estimate the leakage information of RRDPS protocol, give a tighter bound.
- The main method is utilizing potential phase randomization.
- Demonstrate a proof of principle experiment with simplest setup L=3.

- ➢ Problem caused by phase coding inaccuracy and potential attack.
- ➢ Robustness of RRDPS protocol. Can it be measurement-device-independent?
- ➢ Connection with other redundant coding type protocols, e.g. quantum retrieval game, quantum hidden match problem.

THANK YOU!

Further readings related to this talk:

- T. Sasaki, Y. Yamamot, and M. Koashi, Nature 509, 475 (2014)
- S. Wang, et al. Nat Photon 9, 832–836 (2015)
- Z. Yin *et al.* arXiv:1702.01260 (2017)
- S. Wang, et al. arXiv:1707.00387 (2017)

Back up