A short note on the security of Round-Robin Differential Phase-Shift QKD

Boris Škorić
b.skoric@tue.nl

Abstract

Round-Robin Differential Phase-Shift (RRDPS) is a Quantum Key Distribution (QKD) scheme proposed by Sasaki, Yamamoto and Koashi in 2014 [1]. It works with high-dimensional quantum digits (qudits). Its main advantage is that it tolerates more noise than qubit-based schemes while being easy to implement.
The security of RRDPS has been discussed in several papers [1, 2, 3]. However, these analyses do not have the mathematical rigor that is customary in cryptology. In this short note we prove a simple result regarding the min-entropy of the distributed key; this may serve as a step towards a full security proof.

1 Preliminaries

1.1 The RRDPS scheme

The dimension of the qudit space is d. The basis states are denoted as $|0\rangle, \ldots, |d-1\rangle$.[1] Alice generates a random bitstring $a \in \{0,1\}^d$. She prepares the state

$$|\mu(a)\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{d}} \sum_{t=0}^{d-1} (-1)^{a_t} |t\rangle \tag{1}$$

and sends it to Bob. Bob chooses a random integer $r \in \{1, \ldots, d-1\}$. Bob performs a POVM measurement $M^{(r)}$ described by a set of $2d$ operators $(M^{(r)}_{ks})_{k \in \{0,\ldots,d-1\}, s\in\{0,1\}}$,

$$M^{(r)}_{ks} = \frac{1}{2} \, \frac{|k\rangle + (-1)^s |k+r\rangle}{\sqrt{2}} \, \frac{\langle k| + (-1)^s \langle k+r|}{\sqrt{2}}. \tag{2}$$

Here $k+r$ should be understood as $k+r \bmod d$. The result of the measurement $M^{(r)}$ on $|\mu(a)\rangle$ is an random integer $k \in \{0,\ldots,d-1\}$ and a bit $s = a_k \oplus a_{k+r}$.[2] Bob announces k and r over a public but authenticated channel. Alice and Bob now have a shared secret bit s. This procedure is repeated multiple times, after which the standard procedures of information reconciliation and privacy amplification are carried out.
The security of RRDPS is intuitively understood as follows. A measurement in a d-dimensional Hilbert space can extract at most $\log d$ bits of information. The state $|\mu(a)\rangle$, however, contains $d-1$ candidate bits for becoming Alice and Bob's shared secret, which is a lot more

[1] The physical implementation [1] is a *pulse train*: a photon is split into d coherent pieces which are released at different, equally spaced, points in time.

[2] The phase $(-1)^{a_k \oplus a_{k+r}}$ is the phase of the field oscillation in the $(k+r)$'th pulse relative to the k'th. The measurement $M^{(r)}$ is an interference measurement where one path is delayed by r time units.

than $\log d$. Eve can learn (by measurement) only a small fraction of the phase information embedded in the qudit. Eve's information is of limited use to her because she cannot force Bob to select precisely those phases that she knows. (i) She cannot force Bob to choose a specific value of r. (ii) Even if she feeds Bob a state of the form $(|\ell\rangle+(-1)^u|\ell+r\rangle)/\sqrt{2}$ where r accidentally equals Bob's r, then there is a $\frac{1}{2}$ probability that Bob's measurement yields $k\neq\ell$ *with random* s.

1.2 Min-entropy of a classical variable given a quantum state

Consider a combined classical-quantum system, where the (mixed) quantum state depends on a uniformly distributed classical random variable $X\in\mathcal{X}$. Alice knows X and prepares state ρ_X, which is then given to Eve. The combined system can be written as

$$\rho^{\mathrm{AE}}=\frac{1}{|\mathcal{X}|}\sum_{x\in\mathcal{X}}|x\rangle\langle x|\otimes\rho_x, \tag{3}$$

where the states $|x\rangle$ form an orthonormal basis. In this situation, the min-entropy of X given Eve's quantum state ρ_X is [4]

$$\mathsf{H}_{\min}(X|\rho_X)=-\log\max_M\mathbb{E}_{x\in\mathcal{X}}\ \mathrm{tr}\,\rho_x M_x \tag{4}$$

where M is a POVM measurement described by positive semidefinite operators $(M_x)_{x\in\mathcal{X}}$ satisfying $\sum_{x\in\mathcal{X}}M_x=\mathbb{1}$.

2 Min-entropy of the secret bit S in RRDPS

Lemma 2.1 *Let ρ^{AE} be a combined classical-quantum system as in (3), with $\mathcal{X}=\{0,1\}$. Let $\lambda_j(\rho_0-\rho_1)$ denote the j'th eigenvalue of $\rho_0-\rho_1$. Let $\mathcal{P}=\{m\in\{1,\ldots,d\}|\lambda_m(\rho_0-\rho_1)>0\}$. Then (4) reduces to*

$$\mathsf{H}_{\min}(X|\rho_X)=1-\log[1+\sum_{j\in\mathcal{P}}\lambda_j(\rho_0-\rho_1)]. \tag{5}$$

Proof: In (4) we write $\mathbb{E}_x=\frac{1}{2}\sum_x$ and pull the factor $\frac{1}{2}$ out of the logarithm. We write $M_1=\mathbb{1}-M_0$. This gives $\mathsf{H}_{\min}(X|\rho_X)=1-\log\max_{M_0}[\mathrm{tr}\,\rho_0M_0+\mathrm{tr}\,\rho_1(\mathbb{1}-M_0)]=1-\log[1+\max_{M_0}\mathrm{tr}\,(\rho_0-\rho_1)M_0]$. The M_0 that maximises this expression is a projection onto the subspace spanned by the those eigenvectors of $\rho_0-\rho_1$ that have positive eigenvalue. □

Lemma 2.2 *Let Alice and Bob carry out the RRDPS steps as described in Section 1.1. Let Eve intercept the state $|\mu(a)\rangle$ and send an arbitrary unrelated state to Bob. After Bob has announced r and k, Alice's secret bit $s=a_k\oplus a_{k+r}$ and Eve's intercepted state together form a classical-quantum system of the form (3),*

$$\rho^{\mathrm{AE}}(k,r)=\frac{1}{2}\sum_{s\in\{0,1\}}|s\rangle\langle s|\otimes\rho_s^{(k,r)} \tag{6}$$

with

$$\rho_s^{(k,r)}=\frac{\mathbb{1}}{d}+(-1)^s\frac{|k\rangle\langle k+r|+|k+r\rangle\langle k|}{d}. \tag{7}$$

Proof: Using the definition of $|\mu(a)\rangle$ we get

$$\rho_0^{(k,r)} = (\tfrac{1}{2})^{d-1} \sum_{\substack{a\in\{0,1\}^d:\\ a_k\oplus a_{k+r}=0}} |\mu(a)\rangle\langle\mu(a)| = (\tfrac{1}{2})^{d-1}\frac{1}{d}\sum_{t,z=0}^{d-1} |t\rangle\langle z| \sum_{\substack{a\in\{0,1\}^d:\\ a_k\oplus a_{k+r}=0}} (-1)^{a_t+a_z}. \tag{8}$$

The $\sum_a$ summation yields zero unless $t=z$ or $t-z=\pm r$. We have

$$\begin{aligned} \rho_0^{(k,r)} &= (\tfrac{1}{2})^{d-1}\frac{1}{d}\sum_{t,z=0}^{d-1} |t\rangle\langle z| \Big[\delta_{tz}2^{d-1} + (\delta_{tk}\delta_{z,k+r} + \delta_{t,k+r}\delta_{zk})2^{d-1}\Big] \\ &= \frac{1}{d}\sum_{t=0}^{d-1} |t\rangle\langle t| + \frac{|k\rangle\langle k+r| + |k+r\rangle\langle k|}{d}. \end{aligned} \tag{9}$$

The derivation for $\rho_1^{(k,r)}$ is completely analogous. □

Theorem 2.3 (Main result) *Let Alice and Bob carry out the RRDPS steps as described in Section 1.1. Let Eve intercept the state $|\mu(a)\rangle$ and send an arbitrary unrelated state to Bob. After Bob has announced k and r, Eve's uncertainty about Alice's secret S, given the intercepted quantum state, is given by*

$$\mathsf{H}_{\min}(S|K,R,\rho_S^{(K,R)}) = 1 - \log(1+\frac{2}{d}). \tag{10}$$

Proof: The conditioning on the classical K,R modifies [5] expression (4) to $\mathsf{H}_{\min}(S|K,R,\rho_S^{(K,R)}) = -\log \mathbb{E}_{kr}\max_M \mathbb{E}_s \mathrm{tr}\, \rho_s^{(k,r)} M_s$, which following Lemma 2.1 reduces to

$$\mathsf{H}_{\min}(S|K,R,\rho_S^{(K,R)}) = 1 - \log[1 + \mathbb{E}_{kr}\sum_{j\in\mathcal{P}^{(k,r)}} \lambda_j(\rho_0^{(k,r)} - \rho_1^{(k,r)})]. \tag{11}$$

From Lemma 2.2 it follows that $\rho_0^{(k,r)} - \rho_1^{(k,r)} = 2\frac{|k\rangle\langle k+r|+|k+r\rangle\langle k|}{d}$. The eigenvalues of this matrix are 0 ($d-2$ times), $+\frac{2}{d}$ and $-\frac{2}{d}$, independent of k and r. We substitute the positive eigenvalue into (11). □

With this attack Eve learns only $\log(1+2/d)$ bits of information, as compared to 1 bit in the case of qubit-based QKD schemes such as BB84 and its many variants.

3 Discussion

The attack analysed above is not the most general attack possible; hence the analysis does not constitute a proof of security. However, we have learned something useful. Let Alice and Bob accept bit error rate (BER) β on the quantum channel. It is prudent to assume that actually the channel is noiseless and all the noise is caused by Eve. In BB84 and similar schemes such as 6-state QKD, the most powerful attack on individual qubits [6] is to couple an ancilla to the qubit, perform a unitary on the total system, pass the qubit on to Bob, wait until Bob has announced the basis, and then perform a projective measurement on the ancilla. The unitary should be such that the BER does not exceed β. Let Alice send n qubits. Eve learns $nf(\beta)$ bits of information, where f is an increasing function [6] satisfying $f(0)=0$ and $f(\frac{1}{2})=1$. Now for RRDPS we have some as yet unknown increasing function g instead of f, with $g(0)=0$ and $g(\frac{1}{2}) = \log(1+2/d) < \frac{2\log e}{d}$. Even if the function $g(\beta)$ behaves very differently from $f(\beta)$, it holds that $g(\frac{1}{2}) \ll f(\frac{1}{2})$ if $d\gg 1$. In the strong noise regime RRDPS has far less leakage than qubit-based QKD, and hence requires far less privacy amplification.

References

[1] T. Sasaki, Y. Yamamoto, and M. Koashi. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature*, 509:475–478, May 2014.

[2] K. Inoue. Differential Phase-Shift Quantum Key Distribution Systems. *IEEE J. of selected topics in quantum electronics*, 21(3):6600207, 2015.

[3] Z. Zhang, X. Yuan, Z. Cao, and X. Ma. Round-robin differential-phase-shift quantum key distribution. `http://arxiv.org/abs/1505.02481v1`, 2015.

[4] R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Trans.Inf.Th.*, 55(9):4337–4347, 2009.

[5] S. Fehr and S. Berens. On the conditional Rényi entropy. *IEEE Transactions on Information Theory*, 60:6801–6810, 2014.

[6] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81(14):3018–3021, 1998.