Quantum Information and Computation, Vol. 23, No. 11&12 (2023) 0949–0960

A SIMPLER SECURITY PROOF FOR 6-STATE QUANTUM KEY DISTRIBUTION

KAAN AKYUZ
Faculty of engineering, Middle East Technical University
06800 Çankaya Ankara, Turkey

BORIS ŠKORIĆ
Department of mathematics and computer science, Eindhoven University of Technology
5600MB Eindhoven, the Netherlands

Received June 29, 2023
Revised August 3, 2023

Six-state Quantum Key Distribution (QKD) achieves the highest key rate in the class of qubit-based QKD schemes. The standard security proof, which has been developed since 2005, invokes complicated theorems involving smooth Rényi entropies. In this paper we present a simpler security proof for 6-state QKD that entirely avoids Rényi entropies. This is achieved by applying state smoothing directly in the Bell basis. We obtain the well known asymptotic rate, but with slightly more favorable finite-size terms. We furthermore show that the same proof technique can be used for 6-state quantum key recycling.

Keywords: Quantum Key Distribution, quantum cryptography

1 Introduction

Early security proofs for quantum key distribution [1, 2, 3, 4, 5, 6] were not formulated in the universal composability framework. The universal composability approach has been followed for QKD since 2005 [7, 8, 9, 10, 11]. This has led to security proofs in which the Leftover Hash Lemma (LHL) against quantum adversaries plays a central role. The LHL provides an upper bound on the distinguishability between the generated QKD key and a completely random string, given all classical and quantum information held by the adversary. All the various versions of the LHL work with smooth Rényi entropies [12, 13] and invoke theorems about their properties. Hence, reading a QKD security proof requires an understanding of rather advanced concepts and a heavy theoretical toolbox.

In this paper we provide a more 'schoolbook' security proof for 6-state QKD that entirely avoids Rényi entropies. We rely on postselection [14] to lift security against collective attacks to security against general attacks. We follow a number of steps familiar from the LHL, but at the point where one would usually rewrite expressions in terms of Rényi entropies we work with expressions that are diagonalized in the Bell basis, so that square roots of operators can be explicitly computed. We apply smoothing (cutting off probability tails) in the Bell basis, in a way that resembles smoothing of classical probability distributions. This yields a finite-size result for the key rate, with $\mathcal{O}(1/\sqrt{n})$ finite-size contributions, which is the same order that the standard security proof gives.

We focus on 6-state QKD for several reasons: (i) Among qubit-based QKD schemes it stands out as the one with the highest key rate as a function of the quantum bit error rate (QBER). (ii) For BB84 very powerful proofs exist that immediately yield general security without needing to go via collective attacks and postselection. These do not work for the high rate of 6-state QKD. (iii) The level of simplification that our proof provides is more compelling for 6-state than for BB84.

The outline of the paper is as follows. In the preliminaries (Section 2) we briefly review the standard security proof for 6-state QKD, and we list a number of lemmas that we will use. We present our simplified proof in Section 3, and we plot key rates as a function of QBER for various finite sizes, showing convergence to the asymptotic rate. In Section 5 we discuss possible improvements. In the Appendix we show that the proof technique can also be applied to 6-state quantum key recycling.

2 Preliminaries

2.1 Notation

Classical Random Variables are denoted with capital letters, and their realisations with lowercase letters. Sets are denoted in calligraphic font. The probability that X takes value x is written as Pr[X = x]. The expectation with respect to X is denoted as $\mathbb{E}_x f(x) = \sum_{x\in\mathcal{X}} \Pr[X = x] f(x)$. The notation 'log' stands for the logarithm with base 2. We write the binary entropy function as $h(p) = p\log\frac{1}{p} + (1-p)\log\frac{1}{1-p}$, and more generally $h(p_1,\ldots,p_N) = \sum_{i=1}^N p_i \log\frac{1}{p_i}$. The inverse of a bit $b \in \{0,1\}$ is $\bar{b} = 1-b$. The Hamming weight of a string x is written as $w(x) = |\{i : w_i \neq 0\}|$. We write $\mathbb{1}$ for the identity matrix. The notation tr stands for trace. The Hermitian conjugate of an operator A is written as $A^\dagger$. Let A have eigenvalues λ_i. The 1-norm of A is written as $\|A\|_1 = \mathrm{tr}\sqrt{A^\dagger A} = \sum_i |\lambda_i|$. $\mathcal{S}(\mathcal{H})$ denotes the space of positive semidefinite operators on the Hilbert space $\mathcal{H}$. The trace distance between operators ρ,σ is $\|\rho-\sigma\|_{\mathrm{tr}} = \frac{1}{2}\|\rho-\sigma\|_1$. The Bell states are denoted as $|\Psi^\pm\rangle = \frac{|01\rangle\pm|10\rangle}{\sqrt{2}}$ and $|\Phi^\pm\rangle = \frac{|00\rangle\pm|11\rangle}{\sqrt{2}}$, where $|0\rangle, |1\rangle$ is the standard (z) basis.

2.2 'Standard' security proof for 6-state QKD

We briefly review the security analysis for 6-state QKD with a single-photon source, with one-way classical postprocessing and without artificial preprocessing noise. We focus on the proof technique developed by Renner et al. [7, 9, 10, 11, 14], which yields the highest key rate while satisfying universal composability [8, 11]. An important ingredient is the use of *post-selection* [14], which makes it possible to upgrade a security proof in case of collective attacks to a security proof in case of general attacks.[a] The cost of this upgrade is a modest reduction of the key length, by $30\log(n+1)$ bits. A second main ingredient is *symmetrisation* [7, 10]. Alice and Bob share n noisy EPR pairs. The security of the protocol does not change if they both apply the same Pauli operations on their own qubits, chosen at random independently for each EPR pair. The joint effect of postselection and symmetrisation is that it suffices to consider states of the form $(\sigma^{AB})^{\otimes n}$, where σ^{AB} is a two-qubit density matrix that is diagonal in the Bell basis and depends only on the QBER. For states $(\sigma^{AB})^{\otimes n}$ that successfully pass

[a] More recent techniques based on entropic uncertainty relations [15, 16] do not need such a step and immediately yield finite-size results for any attack. However, they do not work for the high rates of 6-state QKD.

the parameter estimation step of the QKD protocol, we may write

$$\sigma^{AB} = (1-\tfrac{3}{2}\gamma)|\Psi^-\rangle\langle\Psi^-| + \tfrac{\gamma}{2}|\Phi^-\rangle\langle\Phi^-| + \tfrac{\gamma}{2}|\Psi^+\rangle\langle\Psi^+| + \tfrac{\gamma}{2}|\Phi^+\rangle\langle\Phi^+| \tag{1}$$

where γ is the maximum allowed QBER. (Here we have taken the EPR pairs to be singlet states.) As a worst-case assumption it is considered that Eve holds the purification of the AB system. Using notation similar to [17] one can write the purification as

$$|\Psi^{ABE}\rangle = \sqrt{1-\tfrac{3}{2}\gamma}|\Psi^-\rangle|0\rangle + \sqrt{\tfrac{\gamma}{2}}\Big(-|\Phi^-\rangle|1\rangle + i|\Psi^+\rangle|2\rangle + |\Phi^+\rangle|3\rangle\Big) \tag{2}$$

which leads to a simple form for Eve's post-measurement state. Alice and Bob do a measurement in a basis that is characterised by spin direction j on the Bloch sphere, where $j \in \{1,2,3\}$ stands for the x, y, z-axis respectively. Alice's outcome is $x \in \{0,1\}$ and Bob's outcome is $y \in \{0,1\}$. Eve's post-measurement state, conditioned on outcomes x, y, is $\sigma^j_{xy} = |E^j_{xy}\rangle\langle E^j_{xy}|$ with

$$|E^j_{x\bar{x}}\rangle = \frac{1}{\sqrt{1-\gamma}}\Big[\sqrt{1-\tfrac{3}{2}\gamma}|0\rangle + (-1)^x\sqrt{\tfrac{\gamma}{2}}|j\rangle\Big] \tag{3}$$

$$|E^j_{xx}\rangle \propto \frac{1}{\sqrt{2}}\Big[|j+1\rangle + i(-1)^{x+1}|j+2\rangle\Big] \tag{4}$$

where the indices $j+1$, $j+2$ are understood to cycle back into $\{1,2,3\}$. (This state of Eve is also obtained from optimal attacks analysis [18].) The full post-measurement state is

$$\rho^{JXYE} = \sum_{j\in\{1,2,3\}^n} \Pr[J=j] \sum_{x,y\in\{0,1\}^n} p_{xy}|j,x,y\rangle\langle j,x,y| \otimes \rho^E_{jxy} \tag{5}$$

$$p_{xy} = 2^{-n}\gamma^{w(\bar{x}\oplus y)}(1-\gamma)^{n-w(\bar{x}\oplus y)} \tag{6}$$

$$\rho^E_{jxy} = \bigotimes_{i=1}^n \sigma^{j_i}_{x_i y_i}. \tag{7}$$

Alice sends the syndrome of x to Bob, one-time-pad encrypted. This allows Bob to reconstruct x from y and the syndrome. (If the reconstruction fails then Alice and Bob abort.) The QKD key $z \in \mathcal{Z}$ is derived from x as $z = \Phi(u, x)$, where Φ is a universal hash function and $u \in \mathcal{U}$ is a public seed. The security proof amounts to upper bounding the statistical distance (trace distance) between on the one hand Z given all of Eve's information and on the other hand a uniform variable on $\mathcal{Z}$. The encrypted syndrome does not enter into this analysis since the one-time pad key is entirely independent; the sending of this ciphertext ends up only as a penalty term in the QKD key rate due to the expenditure of key material. The quantity to be upper bounded is

$$D = \|\rho^{ZUJE} - \mu^Z \otimes \rho^{UJE}\|_{\rm tr}. \tag{8}$$

It can be written as $D = \frac{1}{2}{\rm tr}\sum_j \Pr[J=j]\sum_{z,u}\frac{1}{|\mathcal{U}|}\sqrt{(p_{z|u}\rho^E_{jzu} - \frac{1}{|\mathcal{Z}|}\rho^E_{ju})^2}$. The first step is to pull the sums $\sum_{zu}$ into the square root with a Jensen inequality (see Lemma 1), and make use of the universal hash properties to evaluate these sums. The result is $D \leq \frac{1}{2}\sum_j \Pr[J = j]{\rm tr}\sqrt{|\mathcal{Z}|\sum_x p^2_x(\rho^E_{jx})^2}$. However, Jensen's inequality is so un-tight that it pays off to take a different starting point before applying the inequality. A *smoothed* state $\bar{\rho}$ is considered, which lies close to ρ. It holds that

$$D \leq 2\|\rho^{ZUJE} - \bar{\rho}^{ZUJE}\|_{\rm tr} + \bar{D} \tag{9}$$

$$\bar{D} \stackrel{\rm def}{=} \|\bar{\rho}^{ZUJE} - \mu^Z \otimes \bar{\rho}^{UJE}\|_{\rm tr} \leq \tfrac{1}{2}\sum_j \Pr[J=j]{\rm tr}\sqrt{|\mathcal{Z}|\sum_x p_x^2(\bar{\rho}_{jx}^E)^2}. \tag{10}$$

Next the trace too is pulled into the square root with Jensen, which yields an extra factor support(ρ_j^E) inside the square root. Then it is noted that the expression $\log\sum_x p_x^2(\bar{\rho}_{jx}^E)^2$ is a Rényi 2-entropy, whereas $\log({\rm support}(\bar{\rho}_j^E))$ is a Rényi 0-entropy. Finally a number of 'sledgehammer' theorems are invoked to bound entropies of $\bar{\rho}$ by smooth entropies of ρ [11, 7] and finally to bound the smooth Rényi entropies by von Neumann entropies [7], in particular the von Neumann entropy of the averaged state $\rho^E = \sum_{jxy} p_j p_{xy}\rho_{jxy}^E$ which is identical in form to σ^{AB} (1). The end result is that asymptotically $\bar{D} \leq \frac{1}{2}\mathbb{E}_j\sqrt{|\mathcal{Z}|2^{-n}2^{S(E|j)-S(E|Xj)}}$ $= \frac{1}{2}\sqrt{2^{\ell-n}2^{nh(1-\frac{3}{2}\gamma,\frac{\gamma}{2},\frac{\gamma}{2},\frac{\gamma}{2})-nh(\gamma)}}$. (Here S stands for von Neumann entropy, and we have written $|\mathcal{Z}| = 2^\ell$.) Hence the QKD key length ℓ can be set to slightly below $n - nh(1-\frac{3}{2}\gamma,\frac{\gamma}{2},\frac{\gamma}{2},\frac{\gamma}{2}) + nh(\gamma)$. Taking into account the key material spent on sending the syndrome, which asymptotically has size $nh(\gamma)$, the asymptotic key rate is given by $\frac{1}{n}[\ell - nh(\gamma)]$,

$$\text{6-state QKD asymptotic key rate} = 1 - h(1-\tfrac{3}{2}\gamma,\tfrac{\gamma}{2},\tfrac{\gamma}{2},\tfrac{\gamma}{2}). \tag{11}$$

2.3 Useful Lemmas

Lemma 1 (Special case of Jensen's operator inequality) *Let f be an operator-concave function. Let $A_1,\ldots,A_n$ be hermitian operators and let $p_1,\ldots,p_n \geq 0$ be probabilities satisfying $\sum_{i=1}^n p_i = 1$. Then*

$$\sum_{i=1}^n p_i f(A_i) \leq f\Big(\sum_i p_i A_i\Big). \tag{12}$$

Lemma 2 (Lemma A.2.8 in [7]) *Let $\rho,\bar{\rho} \in \mathcal{P}(\mathcal{H})$ with $\bar{\rho} = P\rho P$ for some projector P on $\mathcal{H}$. Then*

$$\|\rho - \bar{\rho}\|_1 \leq 2\sqrt{{\rm tr}\,\rho\,{\rm tr}\,(\rho-\bar{\rho})}. \tag{13}$$

Lemma 3 (Bretagnolle-Huber-Carol inequality) *(Proposition 2 in [19].) Let $(Z_1,\ldots,Z_t)$ be a multinomial-distributed vector with parameters $(\pi_1,\ldots,\pi_t)$, satisfying $\sum_{s=1}^t Z_s = n$. Then*

$$\Pr\left[\sum_{s=1}^t |Z_s - n\pi_s| \geq \alpha\sqrt{n}\right] \leq 2^t e^{-\frac{1}{2}\alpha^2}. \tag{14}$$

3 Simplified security proof for 6-state QKD

3.1 Diagonal form in the Bell basis

We present a relatively simple security proof for 6-state QKD that uses smoothing but avoids Rényi entropies altogether. We take advantage of postselection and symmetrisation just like the proof discussed in Section 2.2. The point where we start to depart from the standard approach is (9,10). We note that the expression $A_j \stackrel{\rm def}{=} \sum_x p_x^2(\rho_{jx}^E)^2$ is diagonal in the Bell basis. We apply a smoothing procedure that acts as a projection $P_\mathcal{S}$ onto a subspace of Eve's

Hilbert space $\mathcal{H}_E^{\otimes n}$. We choose this subspace such that $P_\mathcal{S} A_j P_\mathcal{S}$ is still diagonal. We define the set $\mathcal{G} = \{0,1,2,3\}^n$. For $g \in \mathcal{G}$ we define the state $|g\rangle \in \mathcal{H}_E^{\otimes n}$ as

$$|g\rangle = \bigotimes_{i=1}^{n} |g_i\rangle. \tag{15}$$

Lemma 4 *Let $j \in \{0,1,2,3\}$ and $r \in \{0,1\}$.*

$$\frac{1}{2} \sum_{x \in \{0,1\}} \sigma^j_{x,\bar{x}\oplus r} = \begin{cases} r=0: & \frac{1-\frac{3}{2}\gamma}{1-\gamma}|0\rangle\langle 0| + \frac{\gamma/2}{1-\gamma}|j\rangle\langle j| \\ r=1: & \frac{1}{2}|j+1\rangle\langle j+1| + \frac{1}{2}|j+2\rangle\langle j+2| \end{cases} \tag{16}$$

Proof: Follows directly from $\sigma^j_{xy} = |E^j_{xy}\rangle\langle E^j_{xy}|$ with $|E^j_{xy}\rangle$ as given in (3),(4). $\square$

Lemma 5 *Let $j \in \{1,2,3\}^n$ and $g \in \mathcal{G}$. Let $t_0(g) = |\{i : g_i = 0\}|$ be the tally of zeroes in g. Let $t_{\rm eq}(g,j) = |\{i : g_i = j_i\}|$ be the tally of places where t and j coincide. Similarly, let $t_{+1}(g,j) = |\{i : g_i = j_i + 1\}|$ and $t_{+2}(g,j) = |\{i : g_i = j_i + 2\}|$ where it is understood that $j+1$ and $j+2$ cycle back into the set $\{1,2,3\}$. Then it holds that*

$$\sum_x p_x^2 (\rho^E_{jx})^2 = \sum_{g \in \mathcal{G}} \lambda_g(j) |g\rangle\langle g| \tag{17}$$

$$\lambda_g(j) = 2^{-n} \Big[(1-\gamma)(1-\tfrac{3}{2}\gamma)\Big]^{t_0(g)} \Big[\tfrac{\gamma}{2}(1-\gamma)\Big]^{t_{\rm eq}(g,j)} \Big[\tfrac{1}{2}\gamma^2\Big]^{t_{+1}(g,j)+t_{+2}(g,j)}. \tag{18}$$

Proof: We have $\rho^E_{jx} = \bigotimes_{i=1}^n [(1-\gamma)\sigma^{j_i}_{x_i \overline{x_i}} + \gamma \sigma^{j_i}_{x_i x_i}]$. Using the fact that the sigma matrices with $x = y$ are orthogonal to those with $x \neq y$ we get $(\rho^E_{jx})^2 = \bigotimes_{i=1}^n [(1-\gamma)^2 \sigma^{j_i}_{x_i\overline{x_i}} + \gamma^2 \sigma^{j_i}_{x_i x_i}]$. Next we use $p_x = 2^{-n}$ to obtain $A_j = \sum_x p_x^2 (\rho^E_{jx})^2 = 2^{-n} \bigotimes_{i=1}^n [(1-\gamma)^2 \frac{\sigma^{j_i}_{01} + \sigma^{j_i}_{10}}{2} + \gamma^2 \frac{\sigma^{j_i}_{00} + \sigma^{j_i}_{11}}{2}]$. Lemma 4 tells us that this expression is diagonal in the Bell basis. The eigenvectors are of the form (15). We find the eigenvalues by computing $A|g\rangle$. We see that every occurrence of $g_i = 0$ generates a factor $(1-\gamma)^2 \frac{1-\frac{3}{2}\gamma}{1-\gamma} = (1-\gamma)(1-\frac{3}{2}\gamma)$. Similarly, each occurrence $g_i = j_i$ yields a factor $(1-\gamma)^2 \frac{\gamma/2}{1-\gamma} = \frac{\gamma}{2}(1-\gamma)$. Finally, $g_i \notin \{0, j_i\}$ leads to a factor $\gamma^2 \cdot \frac{1}{2}$. Counting how often each factor occurs yields (18). $\square$

If no smoothing is applied at all, Lemma 5 directly yields a bound on the trace distance D (8).

Lemma 6 (Without smooting) *The distance $D = \|\rho^{ZUJE} - \mu^Z \otimes \rho^{UJE}\|_{\rm tr}$ for the state $\rho^E_{jx} = \bigotimes_{i=1}^n [(1-\gamma)\sigma^{j_i}_{x_i\overline{x_i}} + \gamma\sigma^{j_i}_{x_i x_i}]$ can be bounded as*

$$D \leq \frac{1}{2}\sqrt{2^{\ell-n}} \Big[\sqrt{(1-\gamma)(1-\tfrac{3}{2}\gamma)} + \sqrt{\tfrac{\gamma}{2}(1-\gamma)} + 2\sqrt{\gamma^2/2}\Big]^n. \tag{19}$$

Proof: We substitute (17) into (10) without smoothing. The resulting expression contains ${\rm tr}\sqrt{\sum_x p_x^2 (\rho^E_{jx})^2} = \sum_{g \in \mathcal{G}} \sqrt{\lambda_g(j)}$. Substituting (18) yields a summand that depends only on tallies. The sum $\sum_{g \in \mathcal{G}}$ then simplifies to the form $\sum_{\rm tallies} \binom{n}{\rm tallies}$ which is evaluated using the multinomial sum rule. $\square$

Lemma 6 yields a rate that is decidedly worse than the standard result (11).

3.2 Explicit recipe for smoothing

We pick a subset $\mathcal{T} \subset \{(a,b,c,d) \in \mathbb{N}^4 | a+b+c+d = n\}$. This will represent the set of tallies that remain after smoothing. We define sets

$$\mathcal{S}_j \stackrel{\text{def}}{=} \{g \in \mathcal{G} | \Big(t_0(g), t_{\text{eq}}(g,j), t_{+1}(g,j), t_{+2}(g,j) \Big) \in \mathcal{T}\}. \tag{20}$$

We introduce projection operators

$$P^j \stackrel{\text{def}}{=} \sum_{g \in \mathcal{S}_j} |g\rangle\langle g|. \tag{21}$$

For each combination of classical variables (j,x,y) with $j \in \{1,2,3\}^n$ and $x,y \in \{0,1\}^n$ we apply smoothing as follows

$$\bar{\rho}^E_{jxy} = P^j \rho^E_{jxy} P^j. \tag{22}$$

Lemma 7 *It holds that*

$$\|\rho^{ZUJE} - \bar{\rho}^{ZUJE}\|_{\text{tr}} \leq \sqrt{\sum_{(\tau_0,\tau_1,\tau_2,\tau_3) \notin \mathcal{T}} \binom{n}{\tau_0, \tau_1, \tau_2, \tau_3} (1 - \tfrac{3}{2}\gamma)^{\tau_0} (\tfrac{\gamma}{2})^{\tau_1+\tau_2+\tau_3}}. \tag{23}$$

<u>*Proof:*</u> The state ρ^{ZUJE} (9) is given by

$$\rho^{ZUJE} = \sum_{zuj} p_j \frac{1}{|\mathcal{U}|} |z,u,j\rangle\langle z,u,j| \otimes \sum_{xy} p_{xy} p_{z|ux} \rho^E_{jxy} \tag{24}$$

and hence the smoothed version is

$$\bar{\rho}^{ZUJE} = \sum_{zuj} p_j \frac{1}{|\mathcal{U}|} |z,u,j\rangle\langle z,u,j| \otimes \sum_{xy} p_{xy} p_{z|ux} \bar{\rho}^E_{jxy}. \tag{25}$$

This is a sub-normalised state, with trace

$$\begin{aligned}
\text{tr}\, \bar{\rho}^{ZUJE} &= \text{tr}_E \sum_j p_j \sum_{xy} p_{xy} P^j \rho^E_{jxy} P^j && (26)\\
&= \sum_j p_j \text{tr}_E P^j \rho^E_j P^j && (27)\\
&= \sum_j p_j \text{tr}_E P^j \Big\{ (1 - \frac{3}{2}\gamma)|0\rangle\langle 0| + \frac{\gamma}{2} \sum_{k=1}^{3} |k\rangle\langle k| \Big\}^{\otimes n} P^j && (28)\\
&= \sum_j p_j \sum_{g \in \mathcal{S}_j} (\tfrac{\gamma}{2})^{w(g)} (1 - \tfrac{3}{2}\gamma)^{n-w(g)} && (29)\\
&= \sum_{(\tau_0,\tau_1,\tau_2,\tau_3) \in \mathcal{T}} \binom{n}{\tau_0, \tau_1, \tau_2, \tau_3} \cdot (1 - \tfrac{3}{2}\gamma)^{\tau_0} (\tfrac{\gamma}{2})^{\tau_1+\tau_2+\tau_3} && (30)
\end{aligned}$$

Finally we use Lemma 2 to get $\|\rho^{ZUJE} - \bar{\rho}^{ZUJE}\|_{\text{tr}} \leq \sqrt{1 \cdot (1 - \text{tr}\bar{\rho}^{ZUJE})}$. □

Theorem 1

$$\bar{D} \leq \tfrac{1}{2}\sqrt{2^{\ell-n}} \sum_{(\tau_0,\tau_1,\tau_2,\tau_3)\in\mathcal{T}} \binom{n}{\tau_0,\tau_1,\tau_2,\tau_3} \left[\sqrt{(1-\gamma)(1-\tfrac{3}{2}\gamma)}\right]^{\tau_0} \left[\sqrt{\tfrac{\gamma}{2}(1-\gamma)}\right]^{\tau_1} \left[\sqrt{\tfrac{1}{2}\gamma^2}\right]^{\tau_2+\tau_3}. \tag{31}$$

Proof: We use $P^j(\rho^E_{jx})^2P^j - P^j\rho^E_{jx}P^j\rho^E_{jx}P^j = P^j\rho^E_{jx}(\mathbb{1}-P^j)\rho^E_{jx}P^j = (P_{\mathcal{S}}\rho^E_{jx}[\mathbb{1}-P^j])(P_{\mathcal{S}}\rho^E_{jx}[\mathbb{1}-P^j])^\dagger \geq 0$ to conclude that $(\bar{\rho}^E_{jx})^2 \leq P^j(\rho^E_{jx})^2P^j$. ¿From Lemma 5 we then get $\sum_x p_x^2(\bar{\rho}^E_{jx})^2 \leq \sum_{g\in\mathcal{S}_j}\lambda_g(j)|g\rangle\langle g|$. Substitution into (10) yields

$$\bar{D} \quad \leq \quad \tfrac{1}{2}\sqrt{2^\ell}\sum_j p_j \sum_{g\in\mathcal{S}_j}\sqrt{\lambda_g(j)} \tag{32}$$

with the eigenvalues $\lambda_g(j)$ as defined in (18). Since these eigenvalues depend only on the tallies, the sum over strings $g\in\mathcal{S}_j$ reduces to a sum over tallies in $\mathcal{T}$ with multiplicity factor $\binom{n}{t_0,t_{\rm eq},t_{+1},t_{+2}}$. Then, since the set $\mathcal{T}$ has no dependence on j, the $\sum_j p_j$ reduces to 1. □

Note that (31) can also be suggestively written as

$$\bar{D} \leq \tfrac{1}{2}\sqrt{2^{\ell-n}} \sum_{(\tau_0,\tau_1,\tau_2,\tau_3)\in\mathcal{T}} \binom{n}{\tau_0,\tau_1,\tau_2,\tau_3}\sqrt{(1-\tfrac{3}{2}\gamma)^{\tau_0}(\tfrac{\gamma}{2})^{\tau_1+\tau_2+\tau_3}\cdot(1-\gamma)^{\tau_0+\tau_1}\gamma^{n-\tau_0-\tau_1}} \tag{33}$$

$$= \tfrac{1}{2}\sqrt{2^{\ell-n}} \sum_{(\tau_0,\tau_1,\tau_2,\tau_3)\in\mathcal{T}} \binom{n}{\tau_0,\tau_1,\tau_2,\tau_3}(1-\tfrac{3}{2}\gamma)^{\tau_0}(\tfrac{\gamma}{2})^{\tau_1+\tau_2+\tau_3}\sqrt{\frac{(1-\gamma)^{\tau_0+\tau_1}\gamma^{n-\tau_0-\tau_1}}{(1-\tfrac{3}{2}\gamma)^{\tau_0}(\tfrac{\gamma}{2})^{\tau_1+\tau_2+\tau_3}}}. \tag{34}$$

The last line resembles an expectation of the square root expression, with a multinomial probability distribution.

Theorem 2 *Let* $m = (m_0,m_1,m_2,m_3) \stackrel{\rm def}{=} (n[1-\tfrac{3}{2}\gamma], n\tfrac{\gamma}{2}, n\tfrac{\gamma}{2}, n\tfrac{\gamma}{2})$. *Let* $\mathcal{T}$ *be the set of tallies in an* α*-neighborhood of* m*, defined as*

$$\mathcal{T} = \{(\tau_0,\tau_1,\tau_2,\tau_3)\mid \tau_0+\tau_1+\tau_2+\tau_3 = n \;\wedge\; \sum_{a=0}^{3}|\tau_a - m_a| < \alpha\sqrt{n}\}. \tag{35}$$

Then

$$\sum_{(\tau_0,\tau_1,\tau_2,\tau_3)\in\mathcal{T}} \binom{n}{\tau_0,\tau_1,\tau_2,\tau_3}(1-\tfrac{3}{2}\gamma)^{\tau_0}(\tfrac{\gamma}{2})^{\tau_1+\tau_2+\tau_3} > 1-16e^{-\frac{1}{2}\alpha^2}, \tag{36}$$

$$\|\rho^{ZUJE} - \bar{\rho}^{ZUJE}\|_{\rm tr} \leq 4e^{-\frac{1}{4}\alpha^2}, \tag{37}$$

$$\bar{D} < \tfrac{1}{2}\sqrt{2^{\ell-n}}\sqrt{2^{nh(1-\frac{3}{2}\gamma,\frac{\gamma}{2},\frac{\gamma}{2},\frac{\gamma}{2})-nh(\gamma)}2^{\alpha\sqrt{n}\frac{1}{2}\log[\frac{2}{\gamma}(1-\frac{3}{2}\gamma)]}}. \tag{38}$$

Proof: The summation in (23) is a partial sum over a multinomial distribution which exactly matches the probability in Lemma 3. That proves (36). The upper bound (37) immediately follows. Next, the summation in (34) can be interpreted (up to a factor $1-16e^{-\frac{1}{2}\alpha^2} < 1$) as an expectation of the square root expression, for a multinomial distribution restricted to the set $\mathcal{T}$. We upper bound the expectation by the maximum attainable value on the set $\mathcal{T}$,

$$\bar{D} < \tfrac{1}{2}\sqrt{2^{\ell-n}}\max_{(\tau_0,\tau_1,\tau_2,\tau_3)\in\mathcal{T}}\sqrt{\frac{(1-\gamma)^{\tau_0+\tau_1}\gamma^{n-\tau_0-\tau_1}}{(1-\tfrac{3}{2}\gamma)^{\tau_0}(\tfrac{\gamma}{2})^{\tau_1+\tau_2+\tau_3}}}. \tag{39}$$

The fraction under the square root equals $[\frac{1-\gamma}{1-\frac{3}{2}\gamma}]^{\tau_0}[\frac{2}{\gamma}(1-\gamma)]^{\tau_1}2^{\tau_2+\tau_3}$. This is maximized by increasing τ_1 as much as possible, at the cost of τ_0, i.e. $\tau_0 = m_0 - \frac{1}{2}\alpha\sqrt{n}$, $\tau_1 = m_1 + \frac{1}{2}\alpha\sqrt{n}$, $\tau_2 = m_2$, $\tau_3 = m_3$. Substitution into (39) yields (38). □

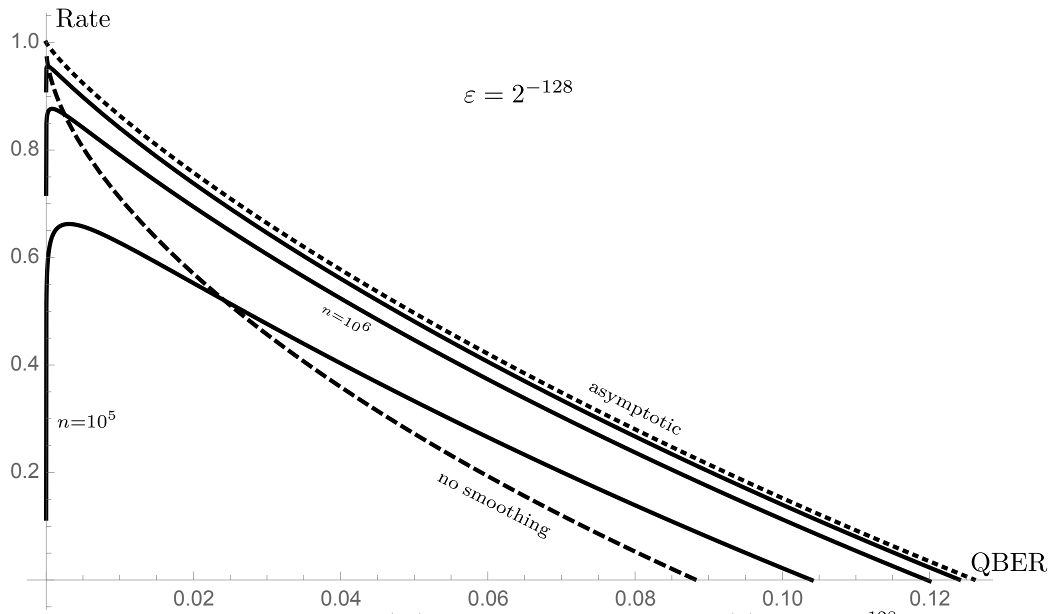

Fig. 1. *Solid curves: The rate (41) as a function of the QBER (γ) at $\varepsilon = 2^{-128}$, plotted for $n = 10^5$, $n = 10^6$ and $n = 10^7$. The dotted curve is the asymptotic rate (11). The dashed curve is the rate obtained from the without-smoothing bound (19) at $n = 10^5$.*

4 Key rate

We discuss the key rate that follows from Theorem 2. Say that we want both $\bar{D}$ and the expression $\|\rho^{ZUJE} - \bar{\rho}^{ZUJE}\|_{\rm tr}$ to be upper bounded by a constant ε. Then according to (37) we need to set $\alpha = 2\sqrt{\ln(4/\varepsilon)}$. Substituting α into (38) we find that ℓ must be set to

$$\ell(\varepsilon) = n + 2 - nh(1-\tfrac{3}{2}\gamma, \tfrac{\gamma}{2}, \tfrac{\gamma}{2}, \tfrac{\gamma}{2}) + nh(\gamma) - \sqrt{n\ln\tfrac{4}{\varepsilon}} \cdot \log[\frac{2}{\gamma}(1-\tfrac{3}{2}\gamma)] - 2\log\frac{1}{\varepsilon}. \tag{40}$$

The rate is obtained by subtracting from ℓ the size of the syndrome and the postselection penalty $30\log(n+1)$, and then normalising by a factor n. We assume the existence of an almost-perfect error correcting code,[b] such that the size of the syndrome is close to $nh(\gamma)$.

$$\text{Rate} \approx 1 - h(1-\tfrac{3}{2}\gamma, \tfrac{\gamma}{2}, \tfrac{\gamma}{2}, \tfrac{\gamma}{2}) - \frac{1}{\sqrt{n}}\sqrt{\ln\tfrac{4}{\varepsilon}} \cdot \log[\frac{2}{\gamma}(1-\tfrac{3}{2}\gamma)] - \frac{30\log n}{n} - \frac{2}{n}\log\frac{1}{\varepsilon}. \tag{41}$$

Note that (a) for $n \to \infty$ the asymptotic rate (11) is recovered; (b) leading-order finite size corrections of order $\sqrt{\frac{1}{n}\ln\frac{1}{\varepsilon}}$ occur in the standard proof technique too. In fact, for γ larger

[b] Finite-size results can be found in e.g. [20]. If a decoding error $\varepsilon_{\rm EC}$ is tolerated, then a syndrome size $nh(\gamma) + \sqrt{n}\Phi^{\rm inv}(\varepsilon_{\rm EC})\sqrt{\gamma(1-\gamma)}\log\frac{1-\gamma}{\gamma}$ is sufficient. Here Φ is defined as the right tail integral of the normal distribution, $\Phi(x) = \int_x^\infty {\rm d}z\ (2\pi)^{-1/2}e^{-z^2/2}$.

than approximately 0.006, our finite-size term $\frac{1}{\sqrt{n}}\sqrt{\ln\frac{4}{\varepsilon}}\cdot\log[\frac{2}{\gamma}(1-\frac{3}{2}\gamma)]$ is more favorable than the $7\sqrt{\frac{1}{n}\log\frac{2}{\varepsilon}}$ listed in [21].

In Fig. 1 we show how the obtained rate tends to the asymptotic result as n increases. The rate is close to the asymptotic value at realistic n.

Note that at QBER close to zero the rates go to zero. This is an artefact of the proof technique. We suspect that it is caused by upperbounding an average by a maximum in the proof of Theorem 2. At low QBER one can simply avoid the artefact by using the bound (19), which is obtained without smoothing, to obtain a rate close to 1 (dashed curve in Fig. 1).

5 Discussion

The standard approach to smoothing departs from the Bell-diagonal structure of $\sum_x p_x^2(\rho_{jx}^E)^2$. We have shown that it is possible to get a good finite-size result by retaining this structure. It is interesting to note that our smoothing procedure is a simple restriction from full summation over $\mathcal{G}=\{0,1,2,3\}^n$ to the typical set $\mathcal{S}_j\subset\mathcal{G}$. In contrast, the smoothing in [11] requires two different operations, one to reduce a Rényi-0 entropy and one to increase a Rényi-2 entropy.

We suggest a number of topics for future work. (i) We did not try to get the sharpest possible bounds. We expect that the constant in the $\mathcal{O}(1/\sqrt{n})$ finite-size contribution, which is already small, can be reduced further. In particular, the rate dip at small QBER may be avoided. At low QBER one can just switch to the result without smoothing, but that is not very elegant. (ii) The proof method may be applied to other qubit-based schemes.

Acknowledgements

Part of this work was supported by NGF Quantum Delta NL KAT-2.

References

1. D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In *CRYPTO 1996*, pages 343–357. Springer Berlin, 1996. Lecture Notes in Computer Science, Vol. 1109.
2. E. Biham, M. Boyer, P.O. Boykin, T. Mor, and V. Roychowdhury. A proof of the security of Quantum Key Distribution. In *Symposium on the Theory of Computing*, pages 715–724. ACM, 2000.
3. H.-K. Lo. Proof of unconditional security of six-state quantum key distribution scheme. *Quantum Information and Computation*, 1(2):81–94, 2001.
4. D. Gottesman and H.-K. Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans. Inf. Theory*, 49:457, 2003.
5. H. Inamori. Security of EPR-based Quantum Key Distribution using three bases, 2000. `https://arxiv.org/abs/quant-ph/0008076`.
6. P. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys.Rev.Lett.*, 85:441, 2000.
7. R. Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.
8. M. Ben-Or, M. Horodecki, D.W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In *Theory of Cryptography*, volume 3378 of *LNCS*, pages 386–406, 2005.
9. B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret key rate for quantum key distribution protocols using one-way classical communication. *Phys.Rev.Lett.*, 95:080501, 2005.

10. R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys.Rev.A*, 72:012332, 2005.
11. R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography*, volume 3378 of *LNCS*, pages 407–425, 2005.
12. R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Trans. on Information Theory*, 55(9):4337, 2009.
13. M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel. On quantum Rényi entropies: a new generalization and some properties . *J. Math. Phys.*, 54:122203, 2013.
14. M. Christandl, R. König, and R. Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, Jan 2009.
15. M. Tomamichel, C.C.W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3, 2012. article number 634.
16. M. Tomamichel and A. Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, 2017.
17. D. Leermakers and B. Škorić. Optimal attacks on qubit-based Quantum Key Recycling. *Quantum Information Processing*, 17(3):57, 2018.
18. Z. Shadman, H. Kampermann, T. Meyer, and D. Bruß. Optimal eavesdropping on noisy states in quantum key distribution. *Int. J. of Quantum Information*, 07(01):297, 2009.
19. J. Bretagnolle and C. Huber. Lois empiriques et distance de Prokhorov. In P.A. Meyer C. Oellacherie and M. Weil, editors, *Séminaire de Probabilités XII*, pages 332–341, 1978. Lecture notes in mathematics 649.
20. D. Baron, M.A. Khojastepour, and R.G. Baraniuk. How quickly can we approach channel capacity? In *Asilomar Conference on Signals, Systems and Computers*, pages 1096–1100. IEEE, 2004.
21. D. Bunandar, L.C.G. Govia, H. Krovi, and D. Englund. Numerical finite-key analysis of quantum key distribution. *NPJ Quantum Information*, 6(104), 2020.
22. C.H. Bennett, G. Brassard, and S. Breidbart. Quantum Cryptography II: How to re-use a one-time pad safely even if P=NP. Unpublished manuscript, 1983.
23. I. Damgård, T. B. Pedersen, and L. Salvail. A quantum cipher with near optimal key-recycling. In *Advances in Cryptology - CRYPTO 2013*, pages 494–511. Springer, Berlin, Heidelberg, 2013.
24. S. Fehr and L. Salvail. Quantum authentication and encryption with key recycling. In *Advances in Cryptology - ASIACRYPT 2017*, pages 611–641. Springer, Cham, 2017.
25. B. Škorić and M. de Vries. Quantum Key Recycling with 8-state encoding (The Quantum One-Time Pad is more interesting than we thought). *International Journal of Quantum Information*, 15(3):1750016, 2017.
26. D. Leermakers and B. Škorić. Security proof for quantum key recycling with noise. *Quantum Information and Computation*, 19(11-12):913–934, 2019.

Appendix A: Key recycling

6-state Quantum Key Recycling

In Quantum Key Recycling (QKR) [22, 23, 24, 25, 26] the measurement bases are known beforehand, as part of a secret key shared by Alice and Bob. In case of an *accept*, it is safe to re-use this secret. Not having to discuss the measurement bases can eliminate one round of communication between Alice and Bob. Furthermore, there are no basis mismatches and hence no qubits have to be discarded.

A 6-state QKR scheme was studied in [26]. It encrypts an ℓ-bit plaintext into a ciphertext that consists of n qubits and some classical data, including a one-time padded syndrome. Part of the ℓ-bit plaintext is reserved to carry the one-time pad for the next round. The security analysis is very close to QKD. A quantity $\bar{D}_{\rm qkr}$ similar to the trace distance $\bar{D}$ (10) needs to be made small. It was shown that $\bar{D}_{\rm qkr} \leq \frac{1}{2}\sqrt{2^{\ell-n}}{\rm tr}\sqrt{\mathbb{E}_{jx}(\bar{\rho}^E_{jx})^2}$, where j is uniform. Further analysis yields exactly the same Rényi entropies as for QKD and the same asymptotic rate (11). (The QKR rate is defined as the length of the actual message divided by the number of qubits).

It was noted in [26] that the expression $\mathbb{E}_{jx}(\rho^E_{jx})^2$, i.e. without smoothing, is diagonal in the Bell basis. This was exploited to obtain, without smoothing, a finite-size result for the QKR rate. However, this rate is significantly lower than (11).

Double smoothing

The explicit-smoothing analysis for QKR is a bit more involved than for QKD. The additional average over the basis choices $j \in \{1,2,3\}^n$ washes away the distinction between three of the tallies, and allows for multiple values of the noise $r = \bar{x} \oplus y \in \{0,1\}^n$ to fit a string $g \in \mathcal{G}$, whereas in QKD the r is entirely fixed by g. Hence the eigenvalues of $\mathbb{E}_j \sum_x p_x^2 (\rho^E_{jx})^2$ involve an additional summation over r, whose domain we need to restrict separately in order to get a good result for the rate. This leads to a two-step smoothing procedure that resembles the approach in [11]. First we restrict summations over r to a subset of Hamming weights $\mathcal{W} \subset \{0,\ldots,n\}$. We write the truncated version of ρ^E_{jx} as φ^E_{jx},

$$\varphi^E_{jx} = \sum_{r:w(r)\in\mathcal{W}} \mu_r \bigotimes_{i=1}^n \sigma^{j_i}_{x_i,\bar{x}_i\oplus r_i} \text{ with } \mu_r = (1-\gamma)^{n-w(r)}\gamma^{w(r)}. \tag{A.1}$$

Next we apply a projection $P_\mathcal{S}$ that restricts $\mathcal{G}$ to a subset $\mathcal{S} \subset \mathcal{G}$, but now not dependent on j. We get $\bar{\rho}^E_{jx} = P_\mathcal{S}\varphi^E_{jx}P_\mathcal{S}$. Next we bound $(\bar{\rho}^E_{jx})^2 \leq P_\mathcal{S}(\varphi^E_{jx})^2 P_\mathcal{S}$, analogous to the QKD case, to obtain $\mathbb{E}_j\sum_x p_x^2(\bar{\rho}^E_{jx})^2 \leq P_\mathcal{S}\mathbb{E}_j\sum_x p_x^2(\varphi^E_{jx})^2 P_\mathcal{S}$. We write $(\varphi^E_{jx})^2 = \sum_{r:w(r)\in\mathcal{W}} \mu_r^2 \bigotimes_{i=1}^n \sigma^{j_i}_{x_i,\bar{x}_i\oplus r_i}$. The averaged version of Lemma 4 is

$$\mathbb{E}_{jx}\sigma^j_{x,\bar{x}\oplus r} = \begin{cases} r=0: & \frac{1-\frac{3}{2}\gamma}{1-\gamma}|0\rangle\langle 0| + \frac{\gamma/6}{1-\gamma}\sum_{j=1}^3 |j\rangle\langle j| \\ r=1: & \frac{1}{3}\sum_{j=1}^3 |j\rangle\langle j| \end{cases} \tag{A.2}$$

This leads to a version of Lemma 5 with different constants and different tallies,

$$P_\mathcal{S}\mathbb{E}_j\sum_x p_x^2(\varphi^E_{jx})^2 P_\mathcal{S} = \sum_{g\in\mathcal{S}} \Lambda_g |g\rangle\langle g| \tag{A.3}$$

with

$$\Lambda_g = 2^{-n} \sum_{\substack{r:w(r)\in\mathcal{W} \\ g_i=0\Rightarrow r_i=0}} \mu_r^2 \left(\frac{1-\frac{3}{2}\gamma}{1-\gamma}\right)^{t_0(g)} \left(\frac{1}{3}\right)^{w(r)} \left(\frac{\gamma/6}{1-\gamma}\right)^{n-t_0(g)-w(r)} \tag{A.4}$$

$$= 2^{-n}(1-\gamma)^{t_0(g)}(1-\tfrac{3}{2}\gamma)^{t_0(g)}\left(\frac{\gamma}{6}\right)^{n-t_0(g)} \sum_{w\in\mathcal{W}} \binom{n-t_0(g)}{w} (2\gamma)^w (1-\gamma)^{n-t_0(g)-w}. \tag{A.5}$$

The r-summation in (A.4) is restricted to those strings $r \in \{0,1\}^n$ that have $r_i = 0$ in all locations i where $g_i = 0$. This leads to the combinatorial factor $\binom{n-t_0}{w}$. Note that taking the full summation $\sum_{w=0}^{n-t_0}$ would reproduce the unsmoothed eigenvalues from [26]. Compared to the QKD proof, we need extra inequalities to bound the w-summation. Let $w_{\min}$ be the lowest value in $\mathcal{W}$. We bound Λ_g as

$$\Lambda_g < 2^{-n}(1-\tfrac{3}{2}\gamma)^{t_0}(\tfrac{\gamma}{2})^{n-t_0}(\tfrac{1}{3})^{n-t_0}|\mathcal{W}|\binom{n-t_0}{w_{\min}}(2\gamma)^{w_{\min}}(1-\gamma)^{n-w_{\min}}. \tag{A.6}$$

Using Stirling's approximation $\sqrt{2\pi n}(\frac{n}{e})^n e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi n}(\frac{n}{e})^n e^{\frac{1}{12n}}$ for the binomial we get

$$\begin{aligned}\Lambda_g \quad < \quad & 2^{-n}(1-\tfrac{3}{2}\gamma)^{t_0}(\tfrac{\gamma}{2})^{n-t_0}\gamma^{w_{\min}}(1-\gamma)^{n-w_{\min}} \\ & \cdot\frac{|\mathcal{W}|}{\sqrt{2\pi w_{\min}}}\cdot\frac{2^{w_{\min}}(\frac{1}{3})^{n-t_0}(1-\frac{t_0}{n})^{n-t_0+\frac{1}{2}}}{(\frac{w_{\min}}{n})^{w_{\min}}(1-\frac{t_0}{n}-\frac{w_{\min}}{n})^{n-t_0-w_{\min}+\frac{1}{2}}}.\end{aligned} \tag{A.7}$$

Note that for $(t_0 \approx n - n\frac{3}{2}\gamma, w_{\min} \approx n\gamma)$ and $|\mathcal{W}| \propto \sqrt{n\gamma(1-\gamma)}$ both fractions in (A.7) are almost constants. Analogous to (34) we can obtain a bound

$$\begin{aligned}\bar{D}_{\text{qkr}} \quad < \quad & \tfrac{1}{2}\sqrt{2^{\ell-n}}\sum_{(\tau_0\cdots\tau_3)\in\mathcal{T}}\binom{n}{\tau_0,\tau_1,\tau_2,\tau_3}(1-\tfrac{3}{2}\gamma)^{\tau_0}(\tfrac{\gamma}{2})^{\tau_1+\tau_2+\tau_3}\sqrt{\frac{\gamma^{w_{\min}}(1-\gamma)^{n-w_{\min}}}{(1-\frac{3}{2}\gamma)^{\tau_0}(\frac{\gamma}{2})^{\tau_1+\tau_2+\tau_3}}} \\ & \cdot\sqrt{\frac{|\mathcal{W}|}{\sqrt{2\pi w_{\min}}}\cdot\frac{2^{w_{\min}}(\frac{1}{3})^{n-\tau_0}(1-\frac{\tau_0}{n})^{n-\tau_0+\frac{1}{2}}}{(\frac{w_{\min}}{n})^{w_{\min}}(1-\frac{\tau_0}{n}-\frac{w_{\min}}{n})^{n-\tau_0-w_{\min}+\frac{1}{2}}}}\end{aligned} \tag{A.8}$$

which has the form of an incomplete multinomial expectation of the square root expression. We can set $\mathcal{T}$ as in Theorem 2 and similarly upper bound the mean by the maximum; the maximum is again attained by setting $\tau_0 = \tau_0^* \stackrel{\text{def}}{=} n(1-\frac{3}{2}\gamma) - \frac{1}{2}\alpha\sqrt{n}$. Thus the obtained bound is

$$\begin{aligned}\bar{D}_{\text{qkr}} \quad < \quad & \tfrac{1}{2}\sqrt{2^{\ell-n}}\sqrt{2^{nh(1-\frac{3}{2}\gamma,\frac{\gamma}{2},\frac{\gamma}{2},\frac{\gamma}{2})}\gamma^{w_{\min}}(1-\gamma)^{n-w_{\min}}(\frac{\gamma/2}{1-\frac{3}{2}\gamma})^{-\frac{1}{2}\alpha\sqrt{n}}} \\ & \cdot\sqrt{\frac{|\mathcal{W}|}{\sqrt{2\pi w_{\min}}}\cdot\frac{2^{w_{\min}}(\frac{1}{3})^{n-\tau_0^*}(1-\frac{\tau_0^*}{n})^{n-\tau_0^*+\frac{1}{2}}}{(\frac{w_{\min}}{n})^{w_{\min}}(1-\frac{\tau_0^*}{n}-\frac{w_{\min}}{n})^{n-\tau_0^*-w_{\min}+\frac{1}{2}}}}.\end{aligned} \tag{A.9}$$

The asymptotic rate is the same as for 6-state QKD.