Quantum Key Recycling with eight-state encoding

(The Quantum One Time Pad is more interesting than we thought)

Boris Škorić and Manon de Vries

b.skoric@tue.nl, m.d.vries@student.tue.nl

Abstract

Perfect encryption of quantum states using the Quantum One-Time Pad (QOTP) requires 2 classical key bits per qubit. Almost-perfect encryption, with information-theoretic security, requires only slightly more than 1. We improve the lower bound: we show that key length $n + 2\log\frac{1}{\varepsilon}$ suffices to encrypt n qubits in such a way that the cipherstate's L_1-distance from uniformity is upperbounded by ε.

We show how to QOTP-encrypt classical plaintext in a nontrivial way: if a plaintext bit is encoded on the Bloch sphere as $\pm(1,1,1)/\sqrt{3}$ then applying the Pauli encryption operators results in eight possible cipherstates which are equally spread out on the Bloch sphere. This encoding, especially when combined with the half-keylength option of QOTP, has advantages over 4-state and 6-state encoding in applications such as Quantum Key Recycling and Unclonable Encryption. We propose a key recycling scheme based on the 8-state encoding.

We derive bounds on the distance between pseudorandom-keyed QOTP cipherstates and the fully mixed state. We present numerics up to 9 qubits.

1 Introduction

1.1 Quantum encryption and key recycling

Quantum physics is markedly different from classical physics regarding information processing. For instance, performing a measurement on an unknown quantum state typically destroys state information. Furthermore, it is impossible to clone an unknown state by unitary evolution [1]. These two properties are very interesting for security applications, since they provide a certain amount of inherent confidentiality, unclonability and tampering detection. Quantum physics also has entanglement of subsystems, which allows for feats like teleportation [2, 3] that have no classical analogue. The laws of quantum physics have been exploited in numerous security schemes, such as Quantum Key Distribution [4, 5, 6], quantum anti-counterfeiting [7], quantum Oblivious Transfer [8, 9], authentication and encryption of quantum states [10, 11, 12], unclonable encryption [13], quantum authentication of PUFs [14, 15], and quantum-secured imaging [16], to name a few. A recent overview of quantum-cryptographic schemes is given in [17].

In this paper we focus on two features that distinguish quantum channels from classical channels:

(i) The possibility of achieving almost-perfect encryption of quantum states, with information-theoretic security guarantees, using a key length that is slightly more than half of the length required for perfect encryption. Hayden et al. [18] showed that a key of length $n + \log n + 2\log\frac{1}{\varepsilon}$ suffices to encrypt n qubits in such a way that the cipherstate's L_1-distance from uniformity is bounded by ε. In contrast, perfect encryption, e.g. using the Quantum One Time Pad (QOTP), requires a key of length $2n$.

(ii) The possibility of re-using encryption keys when a quantum channel is used to transmit classical messages. In Gottesman's unclonable encryption [13] half of the key material can be re-used if a transmission is successful. Damgård, Pedersen and Salvail [19, 20] introduced a scheme in which the *entire* key can be re-used. However, encryption and decryption require a quantum computer with circuit depth $\mathcal{O}(n^2)$ [21]. Fehr and Salvail [22] recently proposed a scheme which re-uses the entire key and which does not need a quantum computer.

1.2 Contributions and outline

We present a number of new results regarding the use of the QOTP.

- We introduce a new way of encoding a classical bit as a qubit state. The '0' is encoded as the vector $(1,1,1)^{\rm T}/\sqrt{3}$ on the Bloch sphere, and the '1' as the opposite vector $(-1,-1,-1)^{\rm T}/\sqrt{3}$. By acting with the four QOTP encryption operators on our two plaintext states we obtain eight cipherstates that are equally spread out on the Bloch sphere. We refer to this encoding as '8-state encoding'.
- We propose a key recycling scheme inspired by [22], but using 8-state encoding. Our scheme is more compact by virtue of the fact that 8-state encoding is a proper encryption, while 4-state and 6-state encoding are leaky.
- We study the use of the QOTP with a pseudorandom key, for *general* states. We model the pseudorandomness in the usual way, as the output of a random function. For n qubits and key length q, we construct a random table T of size $2^q \times n$, where the j'th row is the key corresponding to seed j. The adversary knows T but not the row index j.
  Using this model we improve upon Hayden et al.'s [18] key length $n + \log n + 2\log\frac{1}{\varepsilon}$. We show that key length $n + 2\log\frac{1}{\varepsilon}$ suffices to encrypt n qubits in such a way that the cipherstate's L1-distance from uniformity is upperbounded by ε.
- We study the pseudorandom-keyed QOTP in the case of 8-state encoding of classical plaintexts. We derive bounds on the statistical properties of the cipherstates; these bounds are sharper than for pseudorandom-keyed QOTP acting on arbitrary states.

The outline is as follows. In Section 2 we briefly review the QOTP and security definitions for quantum ciphers. In Section 3 we introduce 8-state encoding and examine its properties. A comparison is given with 4-state and 6-state encoding, regarding conditional entropies of plaintexts and keys. In Section 4 we present our Key Recycling scheme and discuss its security properties. We also briefly mention other possible applications of 8-state encoding, such as Unclonable Encryption with shorter keys and the three-pass keyless protocol.
The pseudorandom-keyed QOTP results for general states are given in Section 5. In Section 6 we restrict the states to 8-state encoding and investigate the statistics of the cipherstate eigenvalues.

2 Preliminaries

2.1 Notation and terminology

Classical Random Variables (RVs) are denoted with capital letters, and their realisations with lowercase letters. The probability that a RV X takes value x is written as $\Pr[X = x]$. The expectation with respect to RV X is denoted as $\mathbb{E}_x f(x) = \sum_{x\in\mathcal{X}} \Pr[X = x] f(x)$. Sets are denoted in calligraphic font. The notation 'log' stands for the logarithm with base 2. The min-entropy of $X \in \mathcal{X}$ is $\mathsf{H}_{\min}(X) = -\log\max_{x\in\mathcal{X}} \Pr[X = x]$, and the conditional min-entropy is $\mathsf{H}_{\min}(X|Y) = -\log\mathbb{E}_y \max_{x\in\mathcal{X}} \Pr[X = x|Y = y]$. The notation h stands for the binary entropy function $h(p) = p\log\frac{1}{p} + (1-p)\log\frac{1}{1-p}$. Bitwise XOR of binary strings is written as '$\oplus$'. The Kronecker delta is denoted as δ_{ab}. The inverse of a bit $b \in \{0,1\}$ is written as $\bar{b} = 1 - b$.
For quantum states we use Dirac notation, with the standard qubit basis states $|0\rangle$ and $|1\rangle$ represented as $\binom{1}{0}$ and $\binom{0}{1}$ respectively. The Pauli matrices are denoted as $\sigma_x, \sigma_y, \sigma_z$, and we write $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. The standard basis is the eigenbasis of σ_z, with $|0\rangle$ in the positive z-direction. We write $\mathbb{1}_d$ for the $d \times d$ identity matrix. The fully mixed state in d-dimensional Hilbert space is denoted as $\tau_d = \frac{1}{d}\mathbb{1}_d$, or simply τ if the dimension is clear from the context. The space of mixed state operators acting on Hilbert space $\mathcal{H}$ is written as $\mathcal{S}(\mathcal{H})$. The 1-norm of an operator L with eigenvalues λ_i is defined as $|L|_1 = \mathrm{tr}\,|L| = \sum_i |\lambda_i|$. The notation 'tr' stands for trace. The statistical distance (trace distance) between two mixed states is defined as $D(\rho, \rho') = \frac{1}{2}\mathrm{tr}\,|\rho - \rho'|$. The ∞-norm $|L|_\infty$ is $\max_i |\lambda_i|$.
We will use the Positive Operator Valued Measure (POVM) formalism. Consider a bipartite system 'AB' where the 'A' part is classical, i.e. the state is of the form $\rho^{\rm AB} = \mathbb{E}_{x\in\mathcal{X}} |x\rangle\langle x| \otimes \rho_x^{\rm B}$

with the $|x\rangle$ forming an orthonormal basis. The min-entropy of the classical RV X given part 'B' of the system is [23]

$$\mathsf{H}_{\min}(X|\rho_X^{\rm B}) = -\log \max_{\mathcal{M}} \mathbb{E}_{x\in\mathcal{X}} \operatorname{tr} M_x \rho_x^{\rm B}. \tag{1}$$

Here $\mathcal{M}$ denotes a POVM, i.e. $\mathcal{M} = (M_x)_{x\in\mathcal{X}}$ where the operators M_x are positive semidefinite and satisfy $\sum_{x\in\mathcal{X}} M_x = \mathbb{1}$. Let $\Lambda \stackrel{\text{def}}{=} \sum_x \rho_x^{\rm B} M_x$. The POVM which achieves the maximum in (1) satisfies the necessary and sufficient conditions $\Lambda^\dagger = \Lambda$ and $\forall_x :\ \Lambda - \rho_x^{\rm B} \geq 0$.

2.2 The Quantum One Time Pad

An arbitrary unknown qubit state can be perfectly encrypted using a classical two-bit key [12, 24, 25]. The simplest way of doing this is using the Quantum One-Time Pad (QOTP). Consider a pure state $|\psi\rangle$ and let the key be $(u, w) \in \{0,1\}^2$. The encrypted state is $|\psi_{uw}\rangle = E_{uw}|\psi\rangle$, with E_{uw} the unitary encryption operator, $E_{uw} = |w\rangle\langle 0| + (-1)^u |1 \oplus w\rangle\langle 1|$. In terms of Pauli spin matrices: $E_{00} = \mathbb{1}$, $E_{01} = \sigma_x$, $E_{10} = \sigma_z$, $E_{11} = \sigma_x\sigma_z$.

$$E_{uw} = \sigma_x^w \sigma_z^u. \tag{2}$$

For notational brevity we will often write the key as $b = 2u + w$, $b \in \{0,1,2,3\}$ and accordingly encryption operator E_b and cipherstate $|\psi_b\rangle = E_b|\psi\rangle$. From the point of view of an attacker Eve who does not know u, w, the qubit is in the fully mixed state: $\frac{1}{4}\sum_b |\psi_b\rangle\langle\psi_b| = \frac{1}{2}\mathbb{1}_2$. In other words, from Eve's point of view the cipherstate carries no information at all about ψ. For a mixed qubit state ρ the cipherstate is $E_b \rho E_b^\dagger$ and it holds that $\frac{1}{4}\sum_b E_b \rho E_b^\dagger = \frac{1}{2}\mathbb{1}_2$. Any Hilbert space $\mathcal{H}_d$ of dimension $d = 2^n$ can be interpreted as an n-qubit system. QOTP encryption on $\mathcal{H}_d$ works by encrypting every qubit individually. The key is $\boldsymbol{b} \in \{0,1,2,3\}^n$. The encryption operator factorises as $E_{\boldsymbol{b}} = \bigotimes_{i=1}^n E_{b_i}$. From Eve's point of view the encryption of a state $\rho \in \mathcal{S}(\mathcal{H}_d)$ is fully mixed,

$$\forall_{\rho\in\mathcal{S}(\mathcal{H}_{2^n})} \quad \frac{1}{4^n} \sum_{\boldsymbol{b}\in\{0,1,2,3\}^n} E_{\boldsymbol{b}} \rho E_{\boldsymbol{b}}^\dagger = (\tau_2)^{\otimes n} = \tau_{2^n}. \tag{3}$$

2.3 Security definitions for quantum ciphers

The performance of a quantum cipher can be quantified in several ways. We first consider encryption of generic mixed states.

Definition 2.1 (From [18]) *A completely positive, trace-preserving map $R : \mathcal{S}(\mathcal{H}_d) \to \mathcal{S}(\mathcal{H}_d)$ is called ε-randomising if*

$$\forall_{\varphi\in\mathcal{S}(\mathcal{H}_d)} : \qquad |R(\varphi) - \tau_d|_\infty \leq \frac{\varepsilon}{d}. \tag{4}$$

Next we consider quantum-encryption of classical data. Let $k \in \mathcal{K}$ be a key and $x \in \mathcal{X}$ a plaintext. Encryption of x using key k results in a (pure or mixed) state $\rho_{k,x}$ in a Hilbert space of dimension d. From Eve's point of view the total system, including the plaintext and the key, is a tripartite system in the state $\mathbb{E}_{k\in\mathcal{K}}\mathbb{E}_{x\in\mathcal{X}} |k\rangle\langle k| \otimes |x\rangle\langle x| \otimes \rho_{k,x}$. Eve has access only to the third part, and her main interest is in the second part. Tracing out the first subsystem gives the bipartite state

$$\rho = \mathbb{E}_{x\in\mathcal{X}} |x\rangle\langle x| \otimes \rho_x, \qquad \rho_x = \mathbb{E}_{k\in\mathcal{K}} \rho_{k,x}. \tag{5}$$

We introduce the notation

$$\xi \stackrel{\text{def}}{=} \mathbb{E}_{x\in\mathcal{X}} \rho_x. \tag{6}$$

Typically $\xi = \tau_d$. Eve's knowledge about the plaintext is related to the statistical distance between X and the uniform distribution, given the quantum state ρ_X for unknown X. This is written as

$$d(X|\rho_X) \stackrel{\text{def}}{=} D(\rho, \tau_{\mathcal{X}} \otimes \xi) = \mathbb{E}_{x\in\mathcal{X}} D(\rho_x, \xi). \tag{7}$$

If the encryption depends on some public randomness $Y \in \mathcal{Y}$, then we write $\rho_x(y)$, and (7) generalises to

$$d(X|Y, \rho_X(Y)) = \mathbb{E}_{x\in\mathcal{X}} \mathbb{E}_{y\in\mathcal{Y}} D(\rho_x(y), \xi). \tag{8}$$

Definition 2.2 *A symmetric quantum cipher is called "statistically ε-private" [19] or "a scheme with error ε" [13] if*

$$\forall_{x,x' \in \mathcal{X}}: \quad D(\rho_x, \rho_{x'}) < \varepsilon. \tag{9}$$

We introduce a security definition inspired by the conditional statistical distance (8).

Definition 2.3 *Let $R_y : \mathcal{S}(\mathcal{H}_d) \to \mathcal{S}(\mathcal{H}_d)$ be a completely positive trace-preserving map, with $y \in \mathcal{Y}$ public. The map is called "ε-uniform" if it satisfies*

$$\forall_{\varphi \in \mathcal{S}(\mathcal{H}_d)}: \quad \mathbb{E}_{y \in \mathcal{Y}} D(R_y(\varphi), \tau_d) \leq \varepsilon. \tag{10}$$

A symmetric quantum cipher for classical messages which makes use of public randomness $Y \in \mathcal{Y}$ is called "ε-uniform" if it satisfies

$$\forall_{x \in \mathcal{X}}: \quad \mathbb{E}_{y \in \mathcal{Y}} D(\rho_x(y), \xi) \leq \varepsilon. \tag{11}$$

We introduce Def. 2.3 because the properties (10,11) appear in the literature (without the conditioning on Y) but have not received a separate name. We will use this definition in Section 5.
Being ε-randomising (Def. 2.1) implies being $\frac{\varepsilon}{2}$-uniform (Def. 2.3 with deterministic y). Similarly, a cipher satisfying Def. 2.2 also satisfies Def. 2.3. Note that (11) implies $d(X|\rho_X) \leq \varepsilon$.
When the key is chosen completely at random, the QOTP has parameter $\varepsilon = 0$ in all the above definitions.
Other security definitions exist [26, 27, 28], more in line with entropies and cryptographic treatment of indistinguishability. We will use the definitions detailed above because (i) the related literature uses them, and (ii) they make it easy to reason about Universal Composability [29, 30, 31, 32].

3 Eight-state encoding

It has been remarked in the literature that applying the Quantum One Time Pad to classical data is not very exciting: Acting with any encryption operator E_{uw} on $|0\rangle$ or $|1\rangle$ yields either $|0\rangle$ or $|1\rangle$, and hence the QOTP does the same as the classical OTP except it needs twice the key material. Furthermore, the quantum encryption yields no protection against copying of the cipherstates. ***This is the case only when the basis for representing a classical bit is chosen badly.*** We propose a basis such that QOTP encryption of a classical bit is nontrivial, resulting in 8 different cipherstates which are equally spread out over the Bloch sphere. Although 8-state encoding is very simple and has interesting properties, we are not aware that it has ever been used.

3.1 Equally separated cipherstates

We define $\cos\alpha \stackrel{\text{def}}{=} 1/\sqrt{3}$, $\alpha \approx 0.96$.[1] We write $\sqrt{i} = e^{i\pi/4}$. We encode the classical '0' and '1' as qubit states ψ_0, ψ_1,

$$|\psi_0\rangle \stackrel{\text{def}}{=} \begin{pmatrix} \cos\frac{\alpha}{2} \\ \sqrt{i}\,\sin\frac{\alpha}{2} \end{pmatrix} \qquad |\psi_1\rangle \stackrel{\text{def}}{=} \begin{pmatrix} \sin\frac{\alpha}{2} \\ -\sqrt{i}\,\cos\frac{\alpha}{2} \end{pmatrix} \qquad \langle\psi_1|\psi_0\rangle = 0 \tag{12}$$

which on the Bloch sphere corresponds to the normal vectors $(1,1,1)^{\mathrm{T}}/\sqrt{3}$ and $(-1,-1,-1)^{\mathrm{T}}/\sqrt{3}$ respectively. In spherical coordinates (θ,φ) this corresponds to $(\theta,\varphi) = (\alpha, \frac{\pi}{4})$ and $(\theta,\varphi) = (\pi-\alpha, -\frac{3}{4}\pi)$. Compactly written in terms of the standard basis $|0\rangle$, $|1\rangle$,

$$|\psi_g\rangle = (-\sqrt{i})^g \cos\tfrac{\alpha}{2}|g\rangle + (\sqrt{i})^{1-g} \sin\tfrac{\alpha}{2}|1-g\rangle \qquad g \in \{0,1\}. \tag{13}$$

We act on these two states with the four encryption operators E_{uw} and obtain eight different cipherstates,

$$|\psi_{uwg}\rangle \stackrel{\text{def}}{=} E_{uw}|\psi_g\rangle = (-1)^{gu}\Big[(-\sqrt{i})^g \cos\tfrac{\alpha}{2}|g \oplus w\rangle + (-1)^u(\sqrt{i})^{1-g} \sin\tfrac{\alpha}{2}|\overline{g \oplus w}\rangle\Big]. \tag{14}$$

[1] $\sin\alpha = \sqrt{2/3}$; $\tan\alpha = \sqrt{2}$; $\cos\frac{\alpha}{2} = \sqrt{\frac{1}{2} + \frac{1}{2\sqrt{3}}}$; $\sin\frac{\alpha}{2} = \sqrt{\frac{1}{2} - \frac{1}{2\sqrt{3}}}$; $\tan\frac{\alpha}{2} = \frac{\sqrt{3}-1}{\sqrt{2}}$.

On the Bloch sphere these correspond to unit-length vectors $\boldsymbol{n}_{uwg}$ as follows (see Fig. 1),

$$\boldsymbol{n}_{uwg} = \frac{(-1)^g}{\sqrt{3}} \begin{pmatrix} (-1)^u \\ (-1)^{u+w} \\ (-1)^w \end{pmatrix}. \tag{15}$$

The relation between the Bloch sphere angles θ, φ and the elliptic polarisation parameters β (angle from the x-axis to the major axis) and $\tan\zeta$ (ratio minor/major, with $\zeta < 0$ left rotating) is given by

$$\begin{aligned} \cos\theta = \cos 2\zeta \cos 2\beta \quad &; \quad \sin\varphi = \sin 2\zeta / \sqrt{1 - (\cos 2\zeta \cos 2\beta)^2} \\ \tan 2\beta = \cos\varphi \tan\theta \quad &; \quad \sin 2\zeta = \sin\theta \sin\varphi. \end{aligned} \tag{16}$$

Our eight cipherstates have $\beta \in \{\pm\frac{\pi}{8}, \pm\frac{3\pi}{8}\}$, $\zeta = \pm(\frac{\pi}{4} - \frac{\alpha}{2}) \approx \pm 0.308$. We will often write $b = 2u + w$, $b \in \{0, 1, 2, 3\}$ as a basis index, with corresponding notation E_b, $|\psi_{bg}\rangle$, $\boldsymbol{n}_{bg}$.

u	w	g	x	y	z	θ	φ	β	ζ	cipherstate $\lvert\psi_{uwg}\rangle$
0	0	0	+	+	+	α	$\pi/4$	$\pi/8$	+	$\cos\frac{\alpha}{2}\lvert 0\rangle + \sqrt{i}\sin\frac{\alpha}{2}\lvert 1\rangle$
0	1	0	+	−	−	$\pi - \alpha$	$-\pi/4$	$3\pi/8$	−	$\cos\frac{\alpha}{2}\lvert 1\rangle + \sqrt{i}\sin\frac{\alpha}{2}\lvert 0\rangle$
1	0	0	−	−	+	α	$-3\pi/4$	$-\pi/8$	−	$\cos\frac{\alpha}{2}\lvert 0\rangle - \sqrt{i}\sin\frac{\alpha}{2}\lvert 1\rangle$
1	1	0	−	+	−	$\pi - \alpha$	$3\pi/4$	$-3\pi/8$	+	$\cos\frac{\alpha}{2}\lvert 1\rangle - \sqrt{i}\sin\frac{\alpha}{2}\lvert 0\rangle$
0	0	1	−	−	−	$\pi - \alpha$	$-3\pi/4$	$-3\pi/8$	−	$\sin\frac{\alpha}{2}\lvert 0\rangle - \sqrt{i}\cos\frac{\alpha}{2}\lvert 1\rangle$
0	1	1	−	+	+	α	$3\pi/4$	$-\pi/8$	+	$\sin\frac{\alpha}{2}\lvert 1\rangle - \sqrt{i}\cos\frac{\alpha}{2}\lvert 0\rangle$
1	0	1	+	+	−	$\pi - \alpha$	$\pi/4$	$3\pi/8$	+	$\sin\frac{\alpha}{2}\lvert 0\rangle + \sqrt{i}\cos\frac{\alpha}{2}\lvert 1\rangle$
1	1	1	+	−	+	α	$-\pi/4$	$\pi/8$	−	$\sin\frac{\alpha}{2}\lvert 1\rangle + \sqrt{i}\cos\frac{\alpha}{2}\lvert 0\rangle$

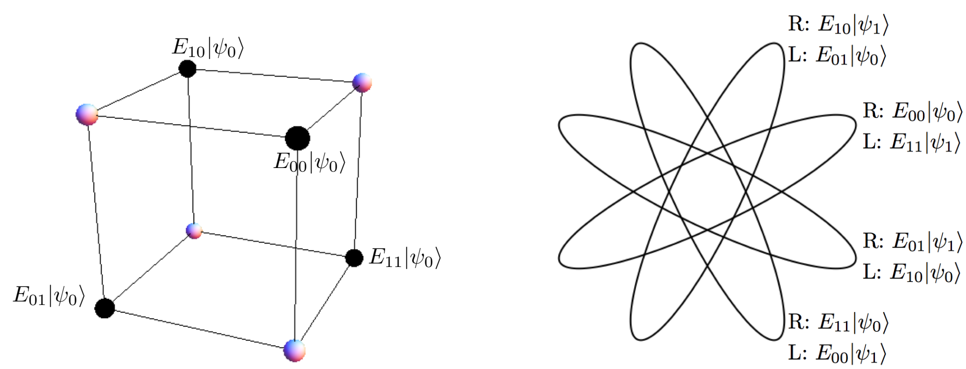

Figure 1: *The eight cipherstates $|\psi_{uwg}\rangle = E_{uw}|\psi_g\rangle$ shown (left) on the Bloch sphere, forming the corner points $(\pm 1, \pm 1, \pm 1)/\sqrt{3}$ of a cube; and (right) as elliptic polarisation states. 'R' stands for righthanded, 'L' for lefthanded.*

3.2 Some properties of eight-state encoding

It holds that $\langle\psi_{b0}|\psi_{b1}\rangle = 0$, i.e. opposite bit values encrypted with the same key lead to orthogonal cipherstates. This trivially follows from the unitarity of the encryption operators, $\langle\psi_{b0}|\psi_{b1}\rangle = \langle\psi_0|E_b^\dagger E_b|\psi_1\rangle = \langle\psi_0|\psi_1\rangle = 0$.
More generally, we can readily compute the inner products between all the various cipherstates from the general rule $|\langle\psi_{b'g'}|\psi_{bg}\rangle|^2 = \frac{1}{2} + \frac{1}{2}\boldsymbol{n}_{b'g'} \cdot \boldsymbol{n}_{bg}$,

$$|\langle\psi_{b'g'}|\psi_{bg}\rangle|^2 = \delta_{bb'} \cdot \delta_{gg'} + (1 - \delta_{bb'})\Big[\delta_{gg'}\frac{1}{3} + (1 - \delta_{gg'})\frac{2}{3}\Big]. \tag{17}$$

In words: When g gets encrypted with two different keys the two cipherstates have (squared) inner product 1/3; any encryption of g, g', $g' \neq g$, with unequal keys yields cipherstates that have (squared) inner product 2/3. The squared inner product determines the probability that one cipherstate gets projected onto another when a projective measurement is performed. Eq. (17) tells us that the nontrivial encryptions of $|\psi_{1-g}\rangle$ look more like $|\psi_g\rangle$ than the nontrivial encryptions of $|\psi_g\rangle$ itself.
The phases of the inner products $\langle\psi_{u'w'g'}|\psi_{uwg}\rangle$ are given by

$$\frac{\langle\psi_{u'w'g'}|\psi_{uwg}\rangle}{i^{(u'-u)(w'+w)}(-1)^{\delta_{3,u'+u+w'+w}}} = \delta_{gg'}\delta_{uu'}\delta_{ww'} + \delta_{gg'}(1-\delta_{uu'}\delta_{ww'})\frac{(-1)^g}{\sqrt{3}} + \delta_{\overline{g}g'}\sqrt{\frac{2}{3}}\left\{\delta_{ww'}\delta_{\overline{u}u'} - \delta_{\overline{w}w'}\exp\left[(g-g')(-1)^{u+u'}i\frac{\pi}{3}\right]\right\}. \quad (18)$$

Table 1: *Conditional Shannon entropies and min-entropies*

		4-state	**6-state**	**8-state**
H	$B\|E$	1	$\log 3 \approx 1.585$	2
	$G\|E$	$h(\cos^2\frac{\pi}{8}) \approx 0.601$	$h(\cos^2\frac{\alpha}{2}) \approx 0.744$	1
	$B\|GE$	$h(\cos^2\frac{\pi}{8}) \approx 0.601$	$H(\frac{1-2/\sqrt{6}}{3}, \frac{1+1/\sqrt{6}}{3}, \frac{1+1/\sqrt{6}}{3}) \approx 1.271$	$\log 3$
	$G\|BE$	0	0	0
	$BG\|E$	$\frac{3}{2}$	$\log 3 + \frac{2}{3} \approx 2.252$	$\frac{3}{2} + \frac{3}{4}\log 3 \approx 2.689$
$\mathsf{H}_{\min}$	$B\|E$	1	$\log 3$	2
	$G\|E$	$-\log\cos^2\frac{\pi}{8} \approx 0.228$	$-\log\cos^2\frac{\alpha}{2} \approx 0.342$	1
	$B\|GE$	$-\log\cos^2\frac{\pi}{8} \approx 0.228$	$-\log(\frac{1}{3} + \frac{2}{3\sqrt{6}}) \approx 0.724$	1
	$G\|BE$	0	0	0
	$BG\|E$	1	$\log 3$	2

Table 2: *Entropy losses*

	4-state	**6-state**	**8-state**
$\mathsf{H}(G) - \mathsf{H}(G\|E)$	0.399	0.256	0
$\mathsf{H}(B) - \mathsf{H}(B\|GE)$	0.399	0.314	0.415
$\mathsf{H}(BG) - \mathsf{H}(BG\|E)$	$\frac{1}{2}$	$\frac{1}{3}$	0.311
$\mathsf{H}_{\min}(G) - \mathsf{H}_{\min}(G\|E)$	0.772	0.658	0
$\mathsf{H}_{\min}(B) - \mathsf{H}_{\min}(B\|GE)$	0.772	0.861	1

Table 1 gives a comparison of four-, six-, and eight-state encoding regarding the entropy of the classical variables G and B given that an attacker Eve holds the qubit ('E'). Table 2 contains the same information but lists entropy *losses*.
The states in 4-state encoding are the eigenstates of σ_z and σ_x. In 6-state encoding one uses the eigenstates of σ_z, σ_x and σ_y. Let the random variable M denote the outcome of a measurement (possibly POVM) on the qubit E. In the 4-state case, the measurement that minimises $\mathsf{H}(G|M)$ and $\mathsf{H}_{\min}(G|M)$ is the projective measurement $\sigma_x + \sigma_z$; the $\mathsf{H}(B|GM)$ and $\mathsf{H}_{\min}(B|GM)$ are minimised by measuring $\sigma_x - \sigma_z$.
In the 6-state case, $\mathsf{H}(G|M)$ and $\mathsf{H}_{\min}(G|M)$ are minimised by measuring $\sigma_x + \sigma_y + \sigma_z$; the $\mathsf{H}(B|GM)$ by the POVM $\{M_b^{(g)}\}_{b=1}^{3}$, $M_b = \frac{1}{3}\mathbb{1} + \frac{1}{3}(-1)^g \boldsymbol{n}_b \cdot \boldsymbol{\sigma}$, $\boldsymbol{n}_1 = (-2,1,1)^{\mathrm{T}}/\sqrt{6}$, $\boldsymbol{n}_2 =$

$(1,-2,1)^{\mathrm{T}}/\sqrt{6}$, $\boldsymbol{n}_3=(1,1,-2)^{\mathrm{T}}/\sqrt{6}$; the $\mathsf{H}_{\min}(B|GM)$ is minimized by the POVM 'opposite' to the one above, i.e. with $\boldsymbol{n}_b\to-\boldsymbol{n}_b$.
In the 8-state case, the $\mathsf{H}(B|GM)$ is minimised by the POVM $M_b^{(g)}=\frac{1}{2}|\psi_{b\overline{g}}\rangle\langle\psi_{b\overline{g}}|$ and the $\mathsf{H}_{\min}(B|GM)$ by the 'opposite' POVM $M_b^{(g)}=\frac{1}{2}|\psi_{bg}\rangle\langle\psi_{bg}|$.
In all encodings (4,6,8) the $\mathsf{H}(BG|M)$ and $\mathsf{H}_{\min}(BG|M)$ are minimised by the POVM $\{M_{bg}\}_{bg}$ with $M_{bg}=\frac{1}{\#\text{bases}}|\varphi_{bg}\rangle\langle\varphi_{bg}|$, where $|\varphi_{bg}\rangle$ denotes the encoding of bit value g in basis b. In all encodings we find that $\mathsf{H}_{\min}(G|BE)=0$; $\mathsf{H}_{\min}(B|E)=\mathsf{H}_{\min}(B)$; $\mathsf{H}_{\min}(BG|E)=\mathsf{H}_{\min}(B)$.
Another important property is the *intercept-resend disturbance probability*. Let Alice send $|\varphi_{bg}\rangle$ for random b,g. Eve does a projective measurement in any basis and forwards the outcome $|\chi\rangle$ to Bob. Bob measures $|\chi\rangle$ in basis b. Averaged over b and g, Bob's probability of getting the wrong outcome ($\overline{g}$) is 1/4 in the case of 4-state encoding and 1/3 for 6-state and 8-state.
In Section 4.1 we will be interested in (i) hiding G and (ii) hiding B when the plaintext G is known. In Table 2 we see that 8-state encoding does a better job of ensuring these two things simultaneously than 4-state and 6-state.

4 Uses for the 8-state encoding

4.1 Key Recycling

When Alice and Bob have a (one-way) quantum channel at their disposal and an authenticated two-way classical channel, they can achieve unconditionally secure communication by using Quantum Key Distribution (QKD) and then applying a classical One Time Pad (OTP). This has been well known since the first work on quantum cryptography.
A less known advantage of quantum channels is the possibility of re-using key material [33] when Alice and Bob detect no eavesdropping: the fact that Bob receives an 'intact' message means that Eve has learned at most a negligible amount of information about the key(s). It is possible to construct Key Recycling schemes that have the same unconditional security as QKD+OTP but better efficiency, i.e. less data has to be communicated.

4.1.1 Requirements for Key Recycling; state of the art

Consider an m-bit message encoded in n qubits (with $n>m$), using a key k. A Quantum Key Recycling (QKR) scheme typically needs to refresh n bits of key material if Bob detects tampering ("reject"), and a much smaller amount t, $t\ll n$, possibly $t=0$, if Bob does not detect tampering ("accept"). Loosely speaking a QKR scheme has to satisfy the following requirements.

R1 If Eve steals the entire cipherstate, the message must remain secret.

R2 If Eve knows the entire plaintext and Bob accepts, Eve does not learn more than $t+\varepsilon$ bits of information about the key, where ε is negligible.

If Bob accepts, the key update mechanism computes a new key k' from the old key k and t bits of fresh key material unknown to Eve. This makes sure that Eve has negligible knowledge about the new key k'. If Bob rejects, the worst case assumption is that Eve has stolen the entire cipherstate and already knew the plaintext. Eve then could in principle learn up to n key bits. Hence Alice and Bob have to introduce n fresh key bits in the next encryption.
Damgård et al. [19, 20] introduced a QKR scheme with $t=0$, for a noiseless quantum channel. A classical authentication tag is first attached to the message; this is then classically on-time-padded; finally quantum encryption is performed by selecting a basis from a set of 2^n Mutually Unbiased Bases (MUBs). The scheme is elegant but has the drawback that it needs a quantum computer with circuit depth $\mathcal{O}(n^2)$ [21] for the encryption and decryption.
Fehr and Salvail [22] recently proposed a QKR scheme that works with individual BB84 qubits, without needing a quantum computer. It has $t=0$ and tolerates[2] a bit error rate β in the quantum channel up to $\beta\approx0.06$.

[2]Asymptotically the scheme is able to correct noise under the condition $1-3h(\beta)>0$.

4.1.2 Proposed QKR scheme

We propose a QKR scheme (with $t = 0$) inspired by [22] but using QOTP encryption. The message is $\mu \in \{0,1\}^\ell$. We make use of an error-correcting code $\mathcal{C}$ which encodes k-bit messages as n-bit codewords, $\ell < k < n$. The syndrome of a string $x \in \{0,1\}^n$ is denoted as $\texttt{Syn}\,x \in \{0,1\}^{n-k}$. Syndrome decoding is denoted as $\texttt{SynDec} : \{0,1\}^{n-k} \to \{0,1\}^n$. Asymptotically for large n it holds that $n - k \approx nh(\beta)$ where β is the bit error rate that can be corrected by the code.
Furthermore we need an extractor $\texttt{Ext} : \{0,1\}^n \to \{0,1\}^\ell$ and a MAC function M that produces an authentication tag of length λ. The security parameter of the MAC is λ.
The key material consists of three parts: K_{MAC}, for MAC-ing; K_{SS}, for encrypting a secure sketch; and $b \in \{0,1,2,3\}^n$ being QOTP bases.

Encryption

Generate random $x \in \{0,1\}^n$. Compute $s = K_{\text{SS}} \oplus \texttt{Syn}\,x$ and $z = \texttt{Ext}\,x$. Compute the ciphertext $c = \mu \oplus z$ and authentication tag $T = M(K_{\text{MAC}}, x||c||s)$. Prepare the quantum state $|\Psi\rangle = \bigotimes_{i=1}^n |\psi_{b_i x_i}\rangle$. Send $|\Psi\rangle$, s, c, T.

Decryption

(The recipient gets $|\Psi'\rangle$, s', c', T'.)
Measure $|\Psi'\rangle$ in the b-basis. This yields $x' \in \{0,1\}^n$. Compute the error vector $e = \texttt{SynDec}(K_{\text{SS}} \oplus s' \oplus \texttt{Syn}\,x')$ and the estimator $\hat{x} = x' \oplus e$. Compute $\hat{z} = \texttt{Ext}\,\hat{x}$ and $\hat{\mu} = c' \oplus \hat{z}$. Accept the message $\hat{\mu}$ if the syndrome decoding succeeded and $T' = M(K_{\text{MAC}}, \hat{x}||c'||s')$.

Key update

In case of Accept, re-use the entire key. In case of Reject, compute b' as a function of b and n fresh secret bits.

4.1.3 Analysis

We discuss the security using heuristic arguments. An actual security proof is left for future work.

- Requirement R1 holds if Eve has negligible information about b. This is evident from the fact that $|\Psi\rangle$ is a QOTP encryption.
- Regarding requirement R2. Let Eve know μ (known plaintext).
  - Eve knows $z = \mu \oplus c$. Eve's uncertainty about x (given z) is $n - \ell$ bits.
  - There are $n - k$ 'endangered' bits of the key K_{SS} which might leak from s if Eve were to guess $\texttt{Syn}\,x$.
  - From the worst case assumption that all noise is caused by Eve, it follows that Eve may hold $n_{\text{EVE}} = nf(\beta) + a \cdot \log \frac{1}{\lambda}$ qubits. Here a is a constant of order 1 which does not depend on n, and $f(\beta) \in [0,1]$ is a noise-dependent fraction, with $f(0) = 0$. From each of the n_{EVE} qubits she can potentially learn one bit of b.
  - The tag T can leak at most λ bits about K_{MAC}.

  Eve's ignorance $n - \ell$ must cover all three contributions $n - k$, n_{EVE} and λ. This yields the requirement $\ell \leq n[1 - h(\beta) - f(\beta)] - \lambda - a \cdot \log \frac{1}{\lambda}$. If this requirement is satisfied, Eve's knowledge about the three keys is negligible.

As a simple intercept-resend attack on an individual qubit has a $\frac{1}{3}$ probability of being noticed by Bob, we can bound[3] $f(\beta) \geq 3\beta$.
For large n the λ-dependent contributions are small compared to n and hence asymptotically of no importance. It follows that our QKR scheme works for noise parameter β satisfying $1 - h(\beta) - f(\beta) > 0$. If we use the optimistic estimate $f(\beta) = 3\beta$ this means $\beta < 0.14$. Unsurprisingly, this is similar to the noise tolerance of qubit-based QKD schemes (as opposed to higher-dimensional Hilbert spaces).

[3] More complicated attacks involving ancillas, such as [34], are possible and yield a larger $f(\beta)$. The analysis of such attacks is left for future work.

It is interesting to look at the asymptotics in the case $\beta = 0$, i.e. no noise. At $\beta = 0$ our scheme has $\ell \approx n$. In contrast, a scheme based on 4-state or 6-state conjugate coding would need n to be much larger than ℓ, because $|\Psi\rangle$ would leak a lot of information about x (see the 'G|E' entropy loss entries in Table 2); hence 8-state encoding has better communication efficiency by virtue of being an actual encryption.

4.2 Unclonable encryption

The concept of Unclonable Encryption (UE) was introduced by Gottesman in 2003 [13]. Alice sends a quantum-encrypted classical message to Bob. If Bob accepts then the message remains confidential *even if Eve learns the full encryption key afterward.* UE can be useful for primitives like revocable time-release encryption [35], for communication-efficient QKD, and in attacker models where the storage of keys suffers particular vulnerabilities.

Gottesman identified the chain of implications: quantum authentication $\implies$ UE $\implies$ QKD. He constructed an UE scheme using BB84 states. Replacing those BB84 states by 8-state encoding will improve the performance. However, we do not expect that the improvement will go far beyond what would be achieved with 6-state encoding. The security analysis of UE is almost exactly the same as for QKD (which also has the basis key revealed after the quantum transmission). For qubit-based QKD it is known [34] that 6-state encoding is essentially optimal; going to more bases does not improve noise tolerance.

An interesting option is to use 8-state encoding with a *pseudorandom key*, achieving almost-perfect security while using slightly more than one bit of key material per qubit (see Sections 5 and 6). This would result in a UE scheme using shorter keys than for 6-state encoding.

4.3 The three-pass 'key-less' protocol

If a bidirectional authenticated channel is available, and a commuting encryption scheme, then a peculiar protocol becomes possible [36, 37] which does not require Alice and Bob to share an encryption key.

Let E_K denote the operation 'encrypt with key K'. For a commuting encryption scheme it holds that $E_K E_Q x = E_Q E_K x$ for all x. The three-pass protocol, also known as key-less protocol, works as follows.

1. Alice has a plaintext message x. She chooses a random key A. She computes $c_1 = E_A x$ and sends c_1.
2. Bob chooses a random key B. He computes $c_2 = E_B c_1$ and sends c_2.
3. Alice computes $c_3 = E_A^{-1} c_2$ and sends c_3. Bob computes $x = E_B^{-1} c_3$.

The protocol is called key-less because the keys A and B never have to be known at the other side.

It has been noted [37] that QOTP encryption of general quantum states, which is (anti)commuting, is perfectly suited for this protocol. We observe that the special case of QOTP, 8-state encoding of classical data, allows us to apply the three-pass protocol to classical data.

It remains to be seen how useful the three-pass protocol is compared to QKD+OTP or QKD+QKR. An obvious drawback is the amount of communication. Sending an n-bit message requires communicating n qubits three times, versus n qubits plus n bits for QKD+OTP, versus n qubits for QKD+QKR under optimal conditions (indefinite re-use of keys). These numbers are approximate and do not take into account the error-correction overhead. The three-pass protocol might become an interesting alternative in the case of very noisy quantum channels, where qubit-based QKD and QKR do not work and the error-correction overheads for QKD [38] are large due to the increased dimension of the employed Hilbert space.

5 QOTP with a pseudorandom key; general states

The main result of this section is Theorem 5.3, in which we give a tighter bound on the required key length.
We model a pseudorandom key for QOTP of an n-qubit system as follows. The length of the seed is q bits. We introduce the notation $Q = 2^q$. (The seed is the actual key that is used.) We define a uniformly random table B of size $Q \times n$, with $B_{ji} \in \{0, 1, 2, 3\}$. All entries are independent RVs. The entry b_{ji} is the encryption key for qubit i given the j'th possible value of the seed. The table B is known to the adversary, but not j.
For given table $B = b$ and row index j, the encryption operator is given by

$$F_{bj} = \bigotimes_{i=1}^{n} E_{b_{ji}}. \tag{19}$$

The encryption of a state ρ, as seen by the adversary, is

$$\rho'(b) \stackrel{\text{def}}{=} \frac{1}{Q}\sum_{j=1}^{Q} F_{bj}\rho F_{bj}^\dagger. \tag{20}$$

Lemma 5.1 *Let $d = 2^n$. For any state $\rho \in \mathcal{S}(\mathcal{H}_d)$ it holds that*

$$\mathbb{E}_b \mathrm{tr}\,[\rho'(b)]^2 = \tfrac{1}{Q}(\mathrm{tr}\,\rho^2 - \tfrac{1}{d}) + \tfrac{1}{d} \qquad ; \qquad \mathbb{E}_b \mathrm{tr}\,[\rho'(b) - \tau]^2 = \tfrac{1}{Q}(\mathrm{tr}\,\rho^2 - \tfrac{1}{d}). \tag{21}$$

Proof: We write $\mathbb{E}_b \mathrm{tr}\,[\rho'(b)]^2 = \frac{1}{Q^2}\sum_{j,k=1}^{Q} \mathrm{tr}\,\mathbb{E}_b F_{bj}\rho F_{bj}^\dagger F_{bk}\rho F_{bk}^\dagger$. There are Q terms with $j = k$; here the $F^\dagger$ and F cancel each other and the summand reduces to $\mathrm{tr}\,\rho^2$. In the other $Q^2 - Q$ terms of the summation we have $j \neq k$ and the summand factorises to

$$\mathrm{tr}\,[\mathbb{E}_{b_j} F_{bj}\rho F_{bj}^\dagger][\mathbb{E}_{b_k} F_{bk}\rho F_{bk}^\dagger].$$

(Here b_j stands for the j'th row of b). The rows are mutually independent; hence the $\mathbb{E}_{b_j}$ does not act on the expression containing k. Now we use $\mathbb{E}_{b_j} F_{bj}\rho F_{bj}^\dagger = \tau$ due to the general QOTP property (3), yielding $\mathrm{tr}\,\tau^2 = \frac{1}{d}$. Adding the contributions gives $\frac{1}{Q^2}[Q\mathrm{tr}\,\rho^2 + (Q^2 - Q)\frac{1}{d}]$, which is the first part of (21). Next we write $\mathrm{tr}\,(\rho' - \tau)^2 = \mathrm{tr}\,(\rho')^2 + \mathrm{tr}\,\tau^2 - 2\mathrm{tr}\,\tau\rho' = \mathrm{tr}\,(\rho')^2 - \frac{1}{d}$, where we have used $\tau = \frac{1}{d}\mathbb{1}$ and $\mathrm{tr}\,\rho' = 1$. The second part of (21) follows. □

Theorem 5.2 *Let $d = 2^n$. For any state $\rho \in \mathcal{S}(\mathcal{H}_d)$ it holds that*

$$\mathbb{E}_b|\rho'(b) - \tau|_1 \leq \sqrt{\frac{2^n}{Q}(\mathrm{tr}\,\rho^2 - 2^{-n})}. \tag{22}$$

Proof: We denote the eigenvalues of $\rho'(b) - \tau$ as $(\lambda_a)_{a=1}^d$. We have $\mathbb{E}_b|\rho'(b) - \tau|_1 = \mathbb{E}_b\sum_a|\lambda_a| = d \cdot \mathbb{E}_b\frac{1}{d}\sum_a\sqrt{\lambda_a^2}$. Using Jensen's inequality we get $\mathbb{E}_b|\rho'(b) - \tau|_1 \leq d\sqrt{\mathbb{E}_b\frac{1}{d}\sum_a\lambda_a^2} = \sqrt{d\mathbb{E}_b\mathrm{tr}\,[\rho'(b) - \tau]^2}$. Finally we use Lemma 5.1. □

Theorem 5.3 *The Quantum One Time Pad operated with a pseudorandom key of length $q \geq n - 2 + 2\log\frac{1}{\varepsilon}$ is ε-uniform (see Def. 2.3).*

Proof: Follows directly from Theorem 5.2, using $\mathrm{tr}\,\rho^2 \leq 1$ and $q = \log Q$. The table B plays the role of the public randomness Y in Def. 2.3. □
Hence the key length can be taken slightly shorter[4] than Hayden et al.'s $n - 2 + \log n + 2\log\frac{1}{\varepsilon}$ [18].
Next we investigate powers of ρ'. We introduce the following notation. Let $\left\{ {t \atop k} \right\}$ be the Stirling number of the second kind, which counts in how many ways we can partition a set of t elements into k non-empty subsets. By convention $\left\{ {t \atop 0} \right\} = 0$ for $t \geq 1$ and $\left\{ {0 \atop 0} \right\} = 1$. The notation $(Q)_k$ stands for the falling factorial $\frac{Q!}{(Q-k)!}$.

[4]The term '-2' appears because the statistical distance D is half the L_1-norm.

Theorem 5.4 *Let $t \in \mathbb{N}$. For any pure state $\rho \in \mathcal{S}(\mathcal{H}_{2^n})$ it holds that*

$$\mathbb{E}_b \mathrm{tr}\,[\rho'(b)]^t \le \frac{1}{Q^t} \sum_{k=0}^{t} \left\{ \begin{array}{c} t \\ k \end{array} \right\} (Q)_k (\tfrac{1}{2})^{(k-1)n}. \tag{23}$$

For $t = 0, 1, 2, 3$ the equality holds.

Proof: See Appendix A.

Corollary 5.5 *For any pure state $\rho \in \mathcal{S}(\mathcal{H}_{2^n})$ it holds that*

$$\mathbb{E}_b \mathrm{tr}\,[\rho'(b) - \tau]^3 = \frac{1}{Q^2}(1 - \frac{1}{2^n})(1 - \frac{2}{2^n}) \tag{24}$$

$$\mathbb{E}_b \mathrm{tr}\,[\rho'(b) - \tau]^4 < \frac{1}{Q^3}[1 + \frac{3Q}{2^n}]. \tag{25}$$

Proof: $\mathrm{tr}\,(\rho' - \tau)^3 = \mathrm{tr}\,(\rho')^3 - 3\mathrm{tr}\,\tau(\rho')^2 + 3\mathrm{tr}\,\tau^2\rho' - \mathrm{tr}\,\tau^3 = \mathrm{tr}\,(\rho')^3 - 3(\frac{1}{2})^n \mathrm{tr}\,(\rho')^2 + 3(\frac{1}{2})^{2n} - (\frac{1}{2})^{2n}$. Using (21) and (23) we get (24).
Similarly, $\mathrm{tr}\,(\rho' - \tau)^4 = \mathrm{tr}\,(\rho')^4 - 4\mathrm{tr}\,\tau(\rho')^3 + 6\mathrm{tr}\,\tau^2(\rho')^2 - 4\mathrm{tr}\,\tau^3\rho' + \mathrm{tr}\,\tau^4 = \mathrm{tr}\,(\rho')^4 - 4(\frac{1}{2})^n \mathrm{tr}\,(\rho')^3 + 6(\frac{1}{2})^{2n}\mathrm{tr}\,(\rho')^2 - 4(\frac{1}{2})^{3n} + (\frac{1}{2})^{3n}$. Using (21) and (23) gives $\mathbb{E}_b \mathrm{tr}\,(\rho' - \tau)^4 \le \frac{1}{Q^3}[1 + \frac{3Q}{2^n}] - \frac{1}{2^n Q^3}[7 + 3\frac{Q-2}{2^n}(2 - 2^{-n})]$. □

6 Pseudorandom-keyed QOTP encryption of classical data

6.1 The cipherstate

We use the method described in Section 5 to model a pseudorandom QOTP key for encrypting an n-qubit state. The adversary knows the table B.
We consider a quantum system consisting of three parts: the classical random variable $J \in \{1, \dots, Q\}$ in the Hilbert space labeled 'K' ('key'), the classical random variable $G \in \{0,1\}^n$ in space 'D' ('data'), and Eve's quantum state in space 'E'. A cipherstate is prepared by choosing a message G at random and encrypting it with the J'th row of B, for random J. For given $B = b$ we have

$$\rho^{\mathrm{KDE}}(b) = \frac{1}{Q}\sum_{j=1}^{Q} \frac{1}{2^n} \sum_{g \in \{0,1\}^n} |j\rangle\langle j| \otimes |g\rangle\langle g| \otimes \rho^{\mathrm{E}}_{jg}(b) \tag{26}$$

$$\rho^{\mathrm{E}}_{jg}(b) = \bigotimes_{i=1}^{n} |\psi_{b_{ji}g_i}\rangle\langle\psi_{b_{ji}g_i}|. \tag{27}$$

We want to study Eve's knowledge about the data G given subsystem E. To this end we need only the D and E subspaces. Tracing out the K gives

$$\rho^{\mathrm{DE}}(b) = \frac{1}{2^n} \sum_{g \in \{0,1\}^n} |g\rangle\langle g| \otimes \rho^{\mathrm{E}}_g(b) \quad \text{with} \quad \rho^{\mathrm{E}}_g(b) = \frac{1}{Q}\sum_{j=1}^{Q} \bigotimes_{i=1}^{n} |\psi_{b_{ji}g_i}\rangle\langle\psi_{b_{ji}g_i}|. \tag{28}$$

Eve's object of study is $\rho^{\mathrm{E}}_g(b)$; from this state she wants to learn g. Theorem 5.2 already gives an upper bound on the distance between $\rho^{\mathrm{E}}_g(b)$ and τ, namely

$$\forall_{g \in \{0,1\}^n}: \quad \mathbb{E}_b |\rho^{\mathrm{E}}_g(b) - \tau|_1 < \sqrt{2^n/Q}. \tag{29}$$

Eq. (29) implies that pseudorandom-keyed QOTP is ε-uniform (Def. 2.3) with $\varepsilon = \frac{1}{2}\sqrt{2^n/Q}$. This is a useful statement, but we want to know more about 8-state encoding.

(i) Eq. (29) is merely a bound. We would like to know typical values of $|\rho_g^{\rm E}(b)-\tau|_1$ in practice. Such numbers give insight into the actual security. In Section 6.2 we present numerical results.
(ii) Definition 2.1, 'ε-randomising', is a stronger security notion than ε-uniformity. It involves the maximum eigenvalue ('$\lambda_{\max}$') of $\rho_g^{\rm E}-\tau$. In Section 6.2 we present a bound on the maximum eigenvalue of $\lambda_{\max}$, from which we derive conclusions about the ε-randomising property. We also present numerical data on $\lambda_{\max}$ and analytic results regarding the moments of $\rho_g^{\rm E}-\tau$.
(iii) Def. 2.2 defines 'statistically ε-private' as a property involving $\rho_g^{\rm E}-\rho_{g'}^{\rm E}$. In Section 6.5 we show that pseudorandom-keyed 8-state encoding is statistically ε-private with $\varepsilon=\sqrt{2^{n-1}/Q}$. Furthermore we analyse the moments of $\rho_g^{\rm E}-\rho_{g'}^{\rm E}$ and we present numerical results.
(iv) Apart from statistical security definitions we are also interested in information-theoretic measures. Below we give a simple bound on the min-entropy of one message bit given the cipherstate. Unfortunately this does not allow us to draw conclusions about the whole plaintext G.

Theorem 6.1 *Eve's knowledge about a single data bit g_i, $i\in\{1,\ldots,n\}$, can be bounded as*

$$\mathsf{H}_{\min}(G_i|B,\rho_{G_i}^{\rm E})\geq 1-\log(1+\frac{1}{\sqrt{Q}})>1-\frac{\log e}{\sqrt{Q}}. \tag{30}$$

Proof: See Appendix B.

6.2 The L_1-norm of $\rho_g^{\rm E}-\tau$

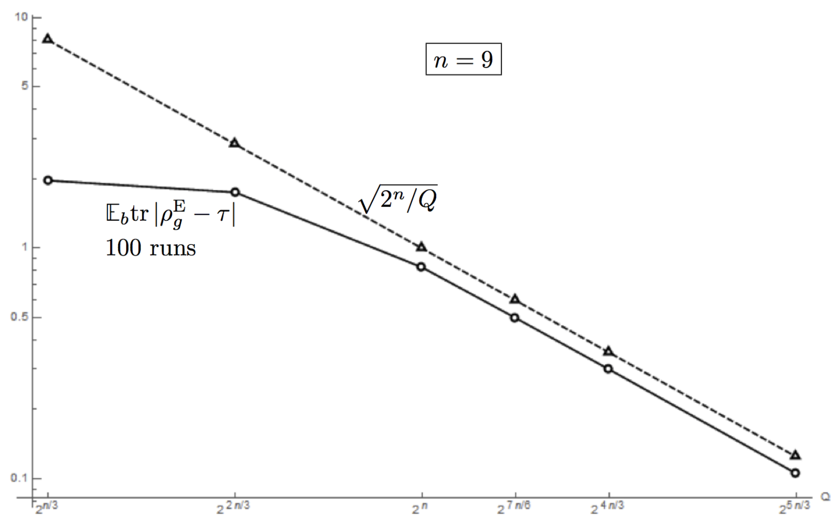

Figure 2: *Numerical results for $\mathbb{E}_b\mathrm{tr}\,|\rho_g^{\rm E}-\tau|$, at $n=9$ qubits, for various values of Q. The $\mathbb{E}_b$ was approximated by taking 100 random tables b.*

Fig. 2 shows the numerics for $\mathbb{E}_b\mathrm{tr}\,|\rho_g^{\rm E}-\tau|$ as a function of Q, for $n=9$, and the upper bound $\sqrt{2^n/Q}$. In Fig. 3 we have plotted results for $n=7,8,9$ together. In spite of the small number of qubits we tentatively identify some trends.
With increasing n the slope of $\mathbb{E}_b D(\rho_g^{\rm E},\tau)$ for $Q>2^n$ increases. This could indicate that for large n and $Q>2^n$ the trace distance decreases faster than the bound $\propto 1/\sqrt{Q}$. Furthermore, at $Q=2^n$ there seems to be a constant factor ≈ 0.83 between the bound and the empirical value. More work is needed to see if these trends persist at large n.

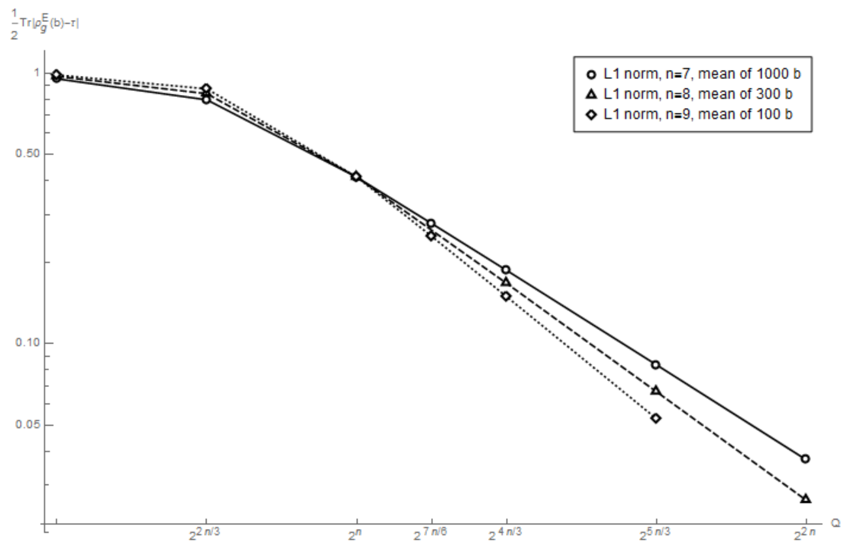

Figure 3: *Numerical results for* $\mathbb{E}_b D(\rho_g^{\mathrm{E}}, \tau)$*, at* $n = 7, 8, 9$ *qubits, for various values of* Q*. For larger* n *fewer random tables* b *were taken to estimate the* $\mathbb{E}_b$*.*

6.3 Eigenvalues of ρ_g^{E}

Fig. 4 shows eigenvalue histograms. We see a qualitative change as Q increases. At small Q, there are distinct bunches of large and small eigenvalues. At $Q = 2^n$ we see something resembling an exponential or power law distribution. At $Q \gg 2^n$ the distribution becomes more peaked around $\lambda = 2^{-n}$.

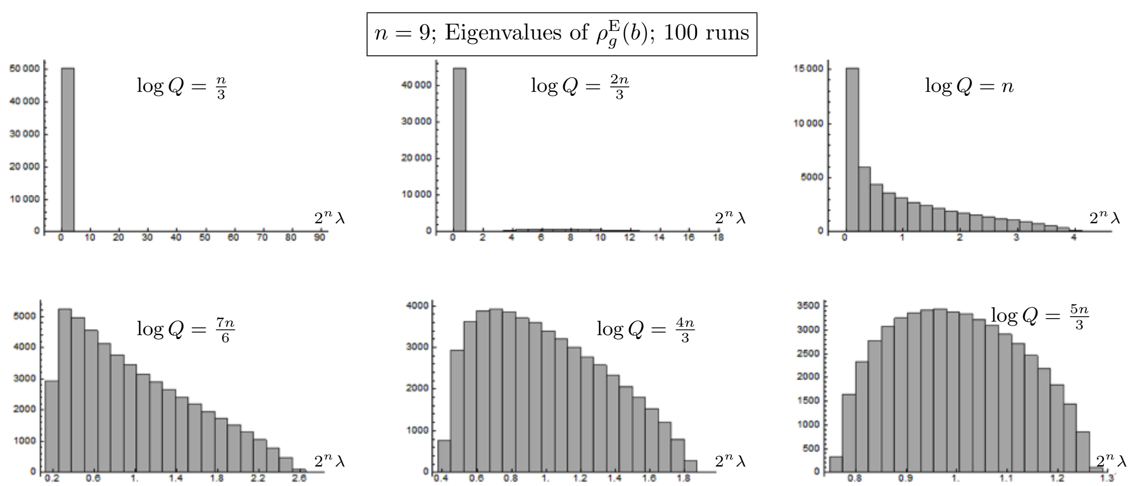

Figure 4: *Histogram of the eigenvalues of* $\rho_g^{\mathrm{E}}(b)$*, plotted for various values of* Q*. The eigenvalues from 100 runs are combined. The horizontal axis is scaled by a factor* 2^n *so that '1' corresponds to the eigenvalues of the fully mixed state* τ*.*

6.4 Maximum eigenvalue of $\rho_g^{\mathrm{E}} - \tau$

In order to make contact with Def. 2.1, which makes a statement about a maximum eigenvalue, we first use a concentration inequality (Theorem 6.3) to upper bound the probability mass in the right tail of the distribution of $\lambda_{\max}(\rho_g^{\rm E})$. This allows us to make a probabilistic statement about the 'ε-randomising' property of the encryption.

Lemma 6.2 (Matrix version of Bennett and Bernstein inequalities [39]) *Let $(X_j)_{j=1}^Q$ be a sequence of independent Hermitean random matrices with dimension d satisfying $\mathbb{E}X_j = 0$ and $\lambda_{\max}(X_j) \leq R$ for all j. Let $\sigma^2 \stackrel{\rm def}{=} \lambda_{\max}(\sum_j \mathbb{E}X_j^2)$. Let $A(u) \stackrel{\rm def}{=} (1+u)\ln(1+u) - u$. Then*

$$\Pr[\lambda_{\max}(\sum_j X_j) \geq t] \leq d \cdot \exp\left[-\frac{\sigma^2}{R^2}A(\frac{Rt}{\sigma^2})\right] \leq d \cdot \exp\left[\frac{-t^2/2}{\sigma^2 + Rt/3}\right]. \tag{31}$$

Theorem 6.3 *For any $g \in \{0,1\}^n$ the mixed state $\rho_g^{\rm E}$ satisfies the following Bennett inequality*

$$\Pr\left[\lambda_{\max}(\rho_g^{\rm E} - \tau) \geq z \cdot \frac{1}{2^n}\right] \leq 2^n \cdot \exp\left[-\frac{Q}{2^n - 1}A(z)\right] \tag{32}$$

and Bernstein inequality

$$\Pr\left[\lambda_{\max}(\rho_g^{\rm E} - \tau) \geq z \cdot \frac{1}{\sqrt{2^n Q}}\right] \leq 2^n \cdot \exp\left[\frac{-z^2/2}{(1-2^{-n})(1+\frac{1}{3}z\sqrt{2^n/Q})}\right]. \tag{33}$$

Here the probability '$\Pr$' is taken over the random table B.

<u>*Proof:*</u> In Lemma 6.2 we set $d = 2^n$ and $X_j = \frac{1}{Q}(P_j - \tau)$, with $P_j = \bigotimes_{i=1}^n |\psi_{b_{ji}g_i}\rangle\langle\psi_{b_{ji}g_i}|$ the projection operator constructed using the j'th row of the matrix b. This gives $\mathbb{E}_b X_j = 0$, $\sum_j X_j = \rho_g^{\rm E} - \tau$, $R = \frac{1}{Q}(1-1/d)$, and $\sigma^2 = \frac{1}{Qd}(1-1/d) = R/d$. We substitute these values into (31). Writing $t = z/d$ in the Bennett inequality yields (32); writing $t = z/\sqrt{Qd}$ in the Bernstein inequality yields (33). □

While (32) is tighter than (33), the latter makes it easy to derive analytic expressions for z.

Corollary 6.4 *Let $2^n \gg n$ and $Q \gg 2^n$. Let $\eta < 1$ be a constant. Pseudorandom-keyed 8-state encryption is ε-randomising, $\varepsilon = \sqrt{\frac{2^n}{Q}(2n\ln 2 + 2\ln\frac{1}{\eta})}$, except with probability $\approx 2\eta$.*

<u>*Proof:*</u> In (33) we set the left-hand side to η and we write $z = \varepsilon\sqrt{Q/2^n} = \sqrt{2n\ln 2 + 2\ln\frac{1}{\eta}}$. Using $2^n \gg n$ and $Q \gg 2^n$ we can approximate the 'exp' in (33) by $\exp(\cdots) \approx \exp(-z^2/2) = 2^{-n}\eta$. Thus the probability mass in the right tail is approximately η. Taking into account the left tail as well gives the factor 2 in 2η. □

Note that the ε in Corollary 6.4 becomes small for Q larger than $2^n n\cdot$constant; this is consistent with the $q > n + \log n$ result of Hayden et al [18]. Also note that Corollary 6.4 is only a probabilistic statement, with probability $\approx 2\eta$ that the statement does not hold.

Fig. 5 shows empirical data on $\max_i |\lambda_i(\rho_g^{\rm E} - \tau)| = |\rho_g^{\rm E} - \tau|_\infty$. The plots are rather noisy due to the limited number of runs. We observe that *the empirical $|\rho_g^{\rm E} - \tau|_\infty$ is orders of magnitude smaller than the Bennett bound*, for the values of n that we studied. In order to get a better theoretical understanding of the maximum eigenvalue it is necessary to have detailed knowledge of the eigenvalue distribution. Below we present a preliminary study of the moments of the eigenvalue distribution. As future work we plan to use distribution moments to derive a sharper bound on $|\rho_g^{\rm E} - \tau|_\infty$.

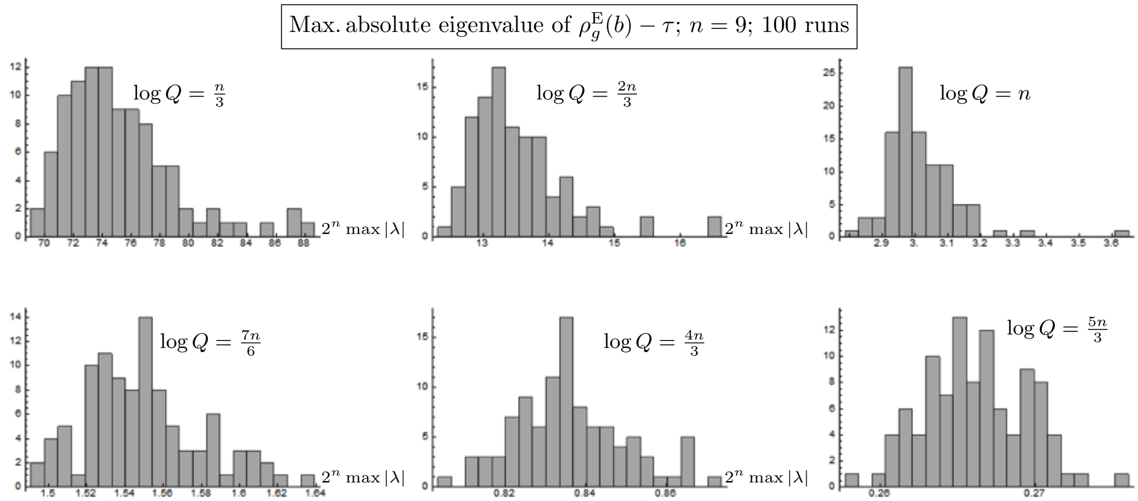

Figure 5: *Histogram of the maximum absolute eigenvalue of $\rho_g^{\rm E}(b)-\tau$, plotted for various values of Q. The horizontal axis is scaled by a factor 2^n.*

Table 3: *Moments of $\rho_g^{\rm E}(b)$*

t	$Q^t \cdot \mathbb{E}_b {\rm tr}\,(\rho_g^{\rm E}(b))^t$
2	$Q+\frac{(Q)_2}{2^n}$
3	$Q+3\frac{(Q)_2}{2^n}+\frac{(Q)_3}{2^{2n}}$
4	$Q+6\frac{(Q)_2}{2^n}+\frac{(Q)_2}{3^n}+6\frac{(Q)_3}{2^{2n}}+\frac{(Q)_4}{2^{3n}}$
5	$Q+10\frac{(Q)_2}{2^n}+5\frac{(Q)_2}{3^n}+20\frac{(Q)_3}{2^{2n}}+5\frac{(Q)_3}{2^n 3^n}+10\frac{(Q)_4}{2^{3n}}+\frac{(Q)_5}{2^{4n}}$
6	$Q+(Q)_2\left\{\frac{15}{2^n}+(\frac{5}{18})^n+\frac{15}{3^n 2^n}\right\}+(Q)_3\left\{\frac{50}{2^{2n}}+\frac{36}{3^n 2^n}+3(\frac{5}{36})^n+\frac{1}{9^n}\right\}$ $+(Q)_4\left\{\frac{50}{2^{3n}}+\frac{15}{3^n 2^{2n}}\right\}+15\frac{(Q)_5}{2^{4n}}+\frac{(Q)_6}{2^{5n}}$

Theorem 6.5 *The moments of $\rho_g^{\rm E}(b)$ and $\rho_g^{\rm E}(b)-\tau$, averaged over b, are as given in Tables 3 and 4 respectively.*

Proof: See Appendix C.
In Table 4 the contributions $\{\cdots\}$ are negligible (at large n and $Q \ll 3^n$) w.r.t. the preceding terms; hence the expressions can be simplified substantially if one wants to know upper bounds only. Furthermore, for $Q=\mathcal{O}(2^n)$ the terms of order $Q/3^n$, $Q/(\frac{18}{5})^n$ and $Q^2/(\frac{36}{5})^n$ are negligible as well.
It is interesting to look at the quantity $c_t \stackrel{\rm def}{=} \frac{1}{2^n}\mathbb{E}_b {\rm tr}\,(\rho_g^{\rm E}-\tau)^t$. In some sense it represents the t'th moment of the eigenvalues of $\rho_g^{\rm E}-\tau$. If one imagines that there is a probability density μ on $[-\frac{1}{2^n}, 1-\frac{1}{2^n}]$ governing the value of the i'th eigenvalue for random i,b,g, then c_t is the t'th moment of μ. At $Q\approx 2^n$ we have

$$c_1=0, \quad c_2\approx(\frac{1}{2^n})^2 \stackrel{\rm def}{=} \sigma^2, \quad c_3\approx\sigma^3, \quad c_4\approx 3\sigma^4, \quad c_5\approx 6\sigma^5, \quad c_6\approx 15\sigma^6. \tag{34}$$

Note that c_4 and c_6 are exactly as in a Gaussian distribution. The odd central moments are positive because the interval $[-\frac{1}{2^n}, 1-\frac{1}{2^n}]$ extends only a little distance into the negative side.

Table 4: *Moments of* $\rho_g^{\mathrm{E}}(b) - \tau$

t	$Q^{t-1} \cdot \mathbb{E}_b \mathrm{tr}\,(\rho_g^{\mathrm{E}}(b) - \tau)^t$
2	$1 - \frac{1}{2^n}$
3	$(1 - \frac{1}{2^n})(1 - \frac{2}{2^n})$
4	$1 + 2\frac{Q}{2^n} + \frac{Q-1}{3^n} - \left\{\frac{6}{2^n} + \frac{3(Q-2)}{2^{2n}}(2 - \frac{1}{2^n})\right\}$
5	$1 + 5\frac{Q}{2^n} + \frac{5(Q-1)}{3^n} - \left\{\frac{10}{2^n} + \frac{30Q-40}{2^{2n}} - \frac{50Q-60}{2^{3n}} + \frac{10(Q-1)}{2^n 3^n} + \frac{20Q-24}{2^{4n}}\right\}$
6	$1 + 9\frac{Q}{2^n} + 5\frac{Q^2}{2^{2n}} + \frac{3(Q-1)(2Q-19)}{2^n 3^n} + \frac{Q-1}{(18/5)^n} + \frac{3(Q-1)(Q-2)}{(36/5)^n}$ $- \left\{\frac{15}{2^n} + \frac{18Q-4}{2^{2n}} + 10\frac{3Q^2-31Q+3}{2^{3n}} - 15\frac{3Q^2-26Q+2}{2^{4n}} + 5\frac{3Q^2-26Q+2}{2^{5n}} - \frac{(Q-1)(Q-2)}{9^n} + \frac{15(Q-1)(Q-6)}{3^n 2^{2n}}\right\}$

6.5 Statistical properties of $\rho_g^{\mathrm{E}} - \rho_{g'}^{\mathrm{E}}$

For completeness we also present theoretical and empirical results on $\rho_g^{\mathrm{E}} - \rho_{g'}^{\mathrm{E}}$. This is motivated by Def. 2.2.

Theorem 6.6 *For any* $g, g' \in \{0,1\}^n$ *with* $g' \neq g$ *it holds that*

$$\mathbb{E}_b \mathrm{tr}\, \left(\rho_g^{\mathrm{E}}(b) - \rho_{g'}^{\mathrm{E}}(b)\right)^2 \;=\; \frac{2}{Q} \tag{35}$$

$$\mathbb{E}_b \mathrm{tr}\, \left(\rho_g^{\mathrm{E}}(b) - \rho_{g'}^{\mathrm{E}}(b)\right)^3 \;=\; 0 \tag{36}$$

$$Q^3 \mathbb{E}_b \mathrm{tr}\, \left(\rho_g^{\mathrm{E}}(b) - \rho_{g'}^{\mathrm{E}}(b)\right)^4 \;=\; 2 + 8\tfrac{Q}{2^n} + \tfrac{4Q}{3^n} + \tfrac{4(Q-1)}{3^n}(-\tfrac{1}{2})^{|g\oplus g'|} - \{\tfrac{8}{2^n} + \tfrac{4}{3^n}\}. \tag{37}$$

Here $|g \oplus g'|$ *stands for the Hamming weight of* $g \oplus g'$.

Proof: see Appendix D.
Furthermore we have $\mathbb{E}_{gg'} \mathrm{tr}\, \left(\rho_g^{\mathrm{E}}(b) - \rho_{g'}^{\mathrm{E}}(b)\right)^t = 0$ for odd t due to symmetry.

Corollary 6.7 *Pseudorandom-keyed QOTP encryption of classical data using the 8-state encoding is on average (w.r.t. b) statistically* ε*-private (Def. 2.2) with* $\varepsilon = \sqrt{2^{n-1}/Q}$.

Proof. We follow the same steps as in the proof of Theorem 5.2. Let $d = 2^n$ and let $\{\lambda_a\}_{a=1}^d$ be eigenvalues of $\rho_g^{\mathrm{E}} - \rho_{g'}^{\mathrm{E}}$. We have $\mathbb{E}_b D(\rho_g^{\mathrm{E}}, \rho_{g'}^{\mathrm{E}}) = \frac{1}{2} d \mathbb{E}_b \frac{1}{d} \sum_a \sqrt{\lambda_a^2} \leq \frac{1}{2} d \sqrt{\frac{1}{d} \mathbb{E}_b \mathrm{tr}\,(\rho_g^{\mathrm{E}} - \rho_{g'}^{\mathrm{E}})^2}$. In the last step we used Jensen's inequality. Substituting (35) gives $\mathbb{E}_b D(\rho_g^{\mathrm{E}}, \rho_{g'}^{\mathrm{E}}) \leq \sqrt{\frac{d}{2Q}}$. □

Fig. 6 shows eigenvalues of $\rho_g^{\mathrm{E}} - \rho_{g'}^{\mathrm{E}}$. As a function of Q the same trends are visible as in Fig. 4, but now with symmetry around zero. Fig. 7 shows empirical values of $|\rho_g^{\mathrm{E}} - \rho_{g'}^{\mathrm{E}}|_\infty$. Again there is a large gap between the actual numbers and the bound obtained from the matrix Bennett inequality (see below).

Theorem 6.8 *For any* $g, g' \in \{0,1\}^n$ *the mixed states* ρ_g^{E}, $\rho_{g'}^{\mathrm{E}}$ *satisfy the following (Bennett and Bernstein) inequalities*

$$\Pr\left[\lambda_{\max}(\rho_g^{\mathrm{E}} - \rho_{g'}^{\mathrm{E}}) \geq \frac{z}{2^n}\right] \;\leq\; 2^n \exp\left[-\frac{2Q}{2^n} A(\frac{z}{2})\right] \tag{38}$$

$$\Pr\left[\lambda_{\max}(\rho_g^{\mathrm{E}} - \rho_{g'}^{\mathrm{E}}) \geq z\frac{\sqrt{2}}{\sqrt{Q 2^n}}\right] \;\leq\; 2^n \exp\left[\frac{-z^2/2}{1 + \frac{1}{3\sqrt{2}} z \sqrt{2^n/Q}}\right]. \tag{39}$$

Proof: We proceed as in the proof of Theorem 6.3, but now with $X_j = \frac{1}{Q}(P_j - P'_j)$, where $P'_j = \bigotimes_{i=1}^n |\psi_{b_{ji} g'_i}\rangle\langle\psi_{b_{ji} g'_i}|$ We have $\mathbb{E}_b X_j = 0$ and $\sum_j X_j = \rho_g^{\mathrm{E}} - \rho_{g'}^{\mathrm{E}}$. Furthermore $R = \lambda_{\max}(X_j) = 1/Q$

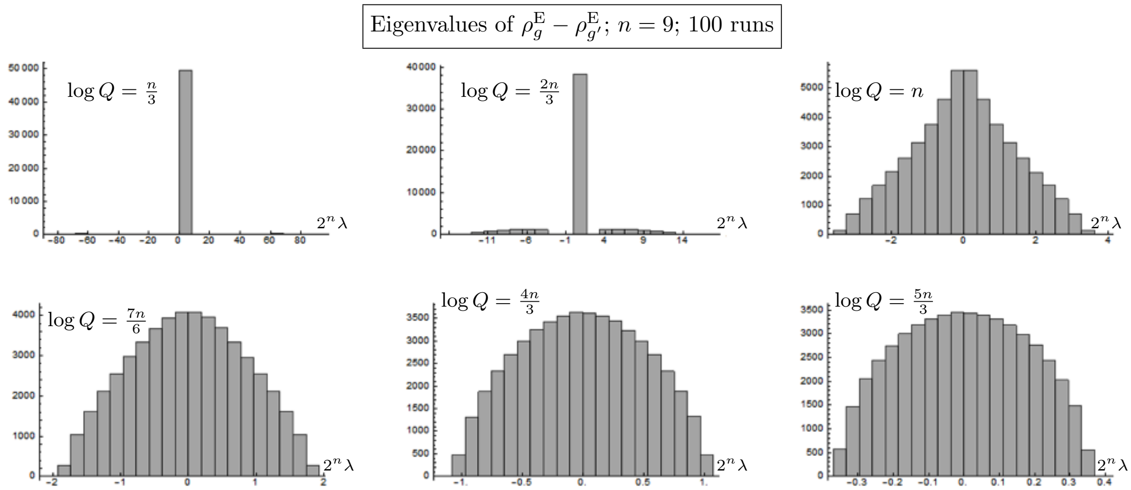

Figure 6: *Histogram of the eigenvalues of $\rho_g^{\mathrm{E}} - \rho_{g'}^{\mathrm{E}}$, plotted for various values of Q. The horizontal axis is scaled by a factor 2^n.*

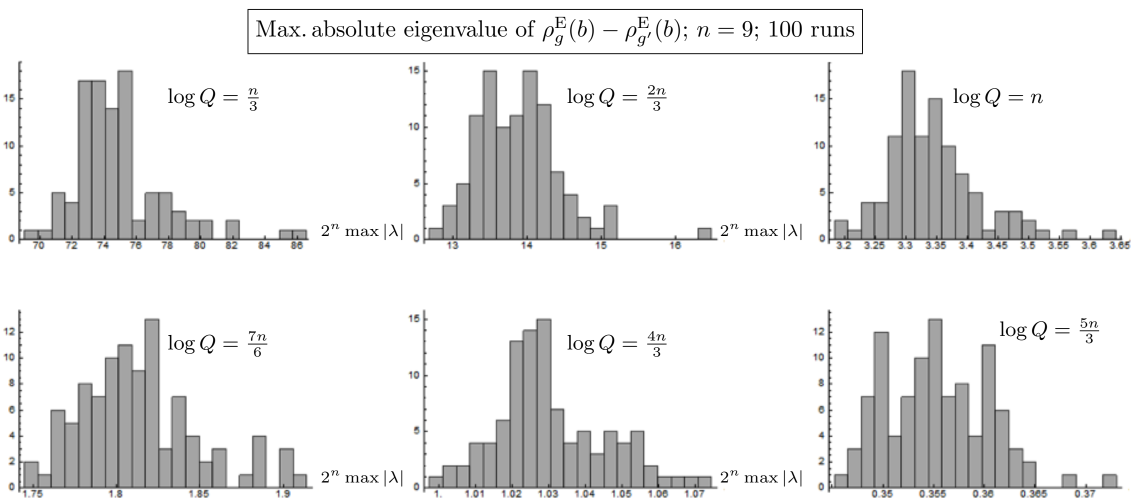

Figure 7: *Histogram of the maximum absolute eigenvalue of $\rho_g^{\mathrm{E}} - \rho_{g'}^{\mathrm{E}}$, plotted for various values of Q. The horizontal axis is scaled by a factor 2^n.*

and $\sigma^2 = \lambda_{\max}(\sum_j \mathbb{E}_b X_j^2) = \lambda_{\max}(\frac{2}{Q}\tau) = \frac{2}{Qd}$. Here we have used Theorem 6.6. Substitution into (31) and setting $t = z/d$ in the Bennett inequality, and $t = z\frac{\sqrt{2}}{\sqrt{Q2^n}}$ in the Bernstein inequality, yields the result. $\square$.

Again we investigate the moments of the eigenvalues in the case $Q \approx 2^n$. Theorem 6.6 gives $s^2 \stackrel{\text{def}}{=} \frac{1}{2^n}\mathbb{E}_b \mathrm{tr}\,(\rho_g^{\mathrm{E}} - \rho_{g'}^{\mathrm{E}})^2 \approx (\frac{\sqrt{2}}{2^n})^2$ and $\frac{1}{2^n}\mathbb{E}_b \mathrm{tr}\,(\rho_g^{\mathrm{E}} - \rho_{g'}^{\mathrm{E}})^4 \approx 10 \cdot 2^{-4n} \approx \frac{5}{2}s^4$. Note that the number $\frac{5}{2}$ is smaller than the '3' that would hold in the case of a Gaussian distribution. The implications of this fact for the distribution of $\lambda_{\max}$ are left for future work.

7 Discussion

We briefly discuss the physical implementation of 8-state encoding. The eight photon polarisation states as depicted in Fig. 1 are not necessarily the most practical implementation. Most single-photon sources produce linearly polarised states; hence elliptic polarisation may be more difficult to handle than linear. We note that it is possible to rotate the cube in Fig. 1 in such a way that four of the eight cipherstates lie in the xz-plane [40], corresponding to linear polarisation. Another physical implementation of qubits is to use pulse trains as in Differential Phase Shift QKD [38], but with different amplitudes and phases.
As topics for future work we mention (i) proving the security of the proposed key recycling scheme; (ii) using the moments listed in the tables, and higher moments, to derive sharper bounds on $|\rho_g - \tau|_1$, $|\rho_g - \rho_{g'}|_1$, $|\rho_g - \tau|_\infty$ and $|\rho_g - \rho_{g'}|_\infty$.

Acknowledgments

We thank Christian Schaffner, Serge Fehr and Andreas Hülsing for useful discussions.

A Proof of Theorem 5.4

We write $\rho = |\psi\rangle\langle\psi|$. We introduce short notation $P_j = F_{bj}|\psi\rangle\langle\psi|F_{bj}^\dagger$. The P_j is a projection operator satisfying $\mathbb{E}_{b_j} P_j = \tau$. We have

$$\mathbb{E}_b \mathrm{tr}\, [\rho'(b)]^t = \frac{1}{Q^t} \sum_{j_1=1}^{Q} \cdots \sum_{j_t=1}^{Q} \mathrm{tr}\, \mathbb{E}_b P_{j_1} \cdots P_{j_t}. \tag{40}$$

If for some $a \in \{1, \ldots, Q\}$ a projection P_a occurs only once in the product $P_{j_1} \cdots P_{j_t}$ then the $\mathbb{E}_b$ reduces it to τ. However, in the t-fold summation many different collisions can occur between the summation variables $j_1, j_2, \ldots, j_t$. In any of the Q^t terms we denote the number of *distinct* values as k, with $k \in \{1, \ldots, t\}$. There are $\left\{ {t \atop k} \right\} (Q)_k$ terms with a given value of k. At given k, there are k distinct projectors in the product $P_{j_1} \cdots P_{j_t}$; they occur multiple times spread out over the product. If the identical projections are direct neighbours then we can immediately use the reduction $P_a^m = P_a$ ($m \geq 1$). For $t \leq 3$ there are only direct neighbours. (This follows from the circular property of the trace, $\mathrm{tr}\, ABC = \mathrm{tr}\, CAB$). Then the expression $\mathrm{tr}\, \mathbb{E}_b P_{j_1} \cdots P_{j_t}$ reduces to $\mathrm{tr}\, \tau^k = (\frac{1}{2^n})^{k-1}$, which immediately yields (23). For $t \geq 4$, however, there are sub-expressions like $P_\alpha P_\beta P_\alpha P_\beta$, $P_\alpha P_\beta P_\gamma P_\beta P_\alpha P_\gamma$, etcetera.
We define an inner product on the space of $2^n \times 2^n$ complex matrices as $\langle M, N\rangle = \mathbb{E}_b \mathrm{tr}\, M^\dagger(b) N(b)$. We now use Cauchy-Schwartz, $|\langle M, N\rangle|^2 \leq \langle M, M\rangle\langle N, N\rangle$ to bound our product expressions for $t \geq 4$. For example, at $t = 4, k = 2$ we have $\mathbb{E}_b \mathrm{tr}\, P_\alpha P_\beta P_\alpha P_\beta = |\mathbb{E}_b \mathrm{tr}\, P_\alpha P_\beta P_\alpha P_\beta| = |\langle P_\beta P_\alpha, P_\alpha P_\beta\rangle|$ $\leq \sqrt{\langle P_\beta P_\alpha, P_\beta P_\alpha\rangle\langle P_\alpha P_\beta, P_\alpha P_\beta\rangle} = \sqrt{(\mathbb{E}_b \mathrm{tr}\, P_\alpha P_\beta)(\mathbb{E}_b \mathrm{tr}\, P_\beta P_\alpha)} = \mathrm{tr}\, \tau^2$. At $t = 6, k = 2$ we have $\mathbb{E}_b \mathrm{tr}\, (P_\alpha P_\beta)^3 = |\langle P_\alpha P_\beta P_\alpha, P_\beta P_\alpha P_\beta\rangle| \leq \sqrt{[\mathbb{E}_b \mathrm{tr}\, (P_\alpha P_\beta)^2][\mathbb{E}_b \mathrm{tr}\, (P_\beta P_\alpha)^2]} = \mathrm{tr}\, \tau^2$. At $t = 6, k = 3$ we have $\mathbb{E}_b \mathrm{tr}\, (P_\alpha P_\beta P_\gamma)^2 = |\langle P_\gamma P_\beta P_\alpha, P_\alpha P_\beta P_\gamma\rangle| \leq \sqrt{\langle P_\gamma P_\beta P_\alpha, P_\gamma P_\beta P_\alpha\rangle\langle P_\alpha P_\beta P_\gamma, P_\alpha P_\beta P_\gamma\rangle} = \sqrt{[\mathbb{E}_b \mathrm{tr}\, P_\alpha P_\beta P_\gamma P_\beta][\mathbb{E}_b \mathrm{tr}\, P_\gamma P_\beta P_\alpha P_\beta]} = \mathrm{tr}\, \tau^3$. With every use of Cauchy-Schwartz we remove duplications of projectors, until only single occurrences remain.

B Proof of Theorem 6.1

The D subsystem consists of n qubit systems $D_1, \ldots, D_n$. We take $i = n$ without loss of generality. Since we concentrate on g_n, only the subsystem D_n is of interest. Tracing out $D_1, \ldots, D_{n-1}$ gives

$$\rho^{\mathrm{D_n E}}(b) = \frac{1}{2} \sum_{g_n=0}^{1} |g_n\rangle\langle g_n| \otimes \rho^{\mathrm{E}}_{G_n=g_n}(b) \qquad \rho^{\mathrm{E}}_{G_n=g_n}(b) = \tau_2^{\otimes(n-1)} \otimes \frac{1}{Q} \sum_{j=1}^{Q} |\psi_{b_{jn} g_n}\rangle\langle\psi_{b_{jn} g_n}|. \tag{41}$$

Eve's first $n-1$ qubits give no information about g_i. We compute the min-entropy of G_n given Eve's subsystem E_n using (1).

$$\mathsf{H}_{\min}(G_n|B,\rho^{\mathrm{E}_n}_{G_n}(B)) = -\log \mathbb{E}_b \max_{M_0,M_1} \mathbb{E}_{g_n\in\{0,1\}} \mathrm{tr}\, M_{g_n} \rho^{\mathrm{E}_n}_{G_n=g_n}(b). \tag{42}$$

Here we have inserted the $\mathbb{E}_b$ in the logarithm because of the conditioning on the classical variable B. As the POVM has to satisfy $M_0 + M_1 = \mathbb{1}$ we eliminate M_1 as a degree of freedom and are left with

$$\begin{aligned}\mathsf{H}_{\min}(G_n|B,\rho^{\mathrm{E}_n}_{G_n}(B)) &= 1-\log\left[1+\mathbb{E}_b \max_{M_0} \mathrm{tr}\, M_0(\rho^{\mathrm{E}_n}_{G_n=0}-\rho^{\mathrm{E}_n}_{G_n=1})\right] \\ &= 1-\log[1+\mathbb{E}_b\, \lambda_{\max}(\rho^{\mathrm{E}_n}_{G_n=0}-\rho^{\mathrm{E}_n}_{G_n=1})]. \end{aligned} \tag{43}$$

Here we have used that the optimal M_0 is a projection operator in the direction of the positive eigenvector of $\rho^{\mathrm{E}_n}_{G_n=0}-\rho^{\mathrm{E}_n}_{G_n=1}$. The notation $\lambda_{\max}(A)$ stands for the maximum eigenvalue of A. We introduce tallies Q_β, $\beta\in\{0,1,2,3\}$, which count how many times key β occurs in the n'th column of b. The tallies are multinomial-distributed with parameters Q and $(\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4})$. We have

$$\begin{aligned}\rho^{\mathrm{E}_n}_{G_n=0}-\rho^{\mathrm{E}_n}_{G_n=1} &= \frac{1}{Q}\sum_{j=1}^{Q}\Big(|\psi_{b_{jn}0}\rangle\langle\psi_{b_{jn}0}| - |\psi_{b_{jn}1}\rangle\langle\psi_{b_{jn}1}|\Big) \\ &= \frac{1}{Q}\sum_{\beta=0}^{3} Q_\beta \Big(|\psi_{\beta 0}\rangle\langle\psi_{\beta 0}| - |\psi_{\beta 1}\rangle\langle\psi_{\beta 1}|\Big). \end{aligned} \tag{44}$$

We define $v_x = Q_0+Q_1-Q_2-Q_3$, $v_y = Q_0-Q_1-Q_2+Q_3$, $v_z = Q_0-Q_1+Q_2-Q_3$. Using $|\psi_{\beta 0}\rangle\langle\psi_{\beta 0}| - |\psi_{\beta 1}\rangle\langle\psi_{\beta 1}| = \boldsymbol{n}_{\beta 0}\cdot\boldsymbol{\sigma}$ we find, after some algebra,

$$\rho^{\mathrm{E}_n}_{G_n=0}-\rho^{\mathrm{E}_n}_{G_n=1} = \frac{v_x\sigma_x + v_y\sigma_y + v_z\sigma_z}{Q\sqrt{3}}. \tag{45}$$

This expression can be written as a spin operator in some direction times a scalar factor which is exactly $\lambda_{\max}$. We have

$$v^2 = v_x^2+v_y^2+v_z^2 = 3(Q_0^2+Q_1^2+Q_2^2+Q_3^2) - 2\sum_{\beta\neq\beta'} Q_\beta Q_{\beta'}. \tag{46}$$

Using the multinomial property $\mathbb{E}_b Q_\beta^2 = (\frac{Q}{4})^2 + Q\cdot\frac{1}{4}\cdot\frac{3}{4}$ for the four square terms and $\mathbb{E}_b Q_\beta Q_{\beta'} = (\frac{Q}{4})^2 - Q\cdot\frac{1}{4}\cdot\frac{1}{4}$ for the six crossterms we finally get $\mathbb{E}_b v^2 = 3Q$ and

$$\mathbb{E}_b \lambda_{\max} = \frac{\mathbb{E}_b\sqrt{v^2}}{Q\sqrt{3}} \le \frac{\sqrt{\mathbb{E}_b v^2}}{Q\sqrt{3}} = \frac{1}{\sqrt{Q}}. \tag{47}$$

C Proof of Theorem 6.5

The results for $t=2$ follow from Theorem 5.4. The results for $t=3$ are copied from Theorem 5.4 and Corollary 5.5.

For $t=4$ we closely follow the proof of Corollary 5.5. The only difference lies in one type of summation term in the computation of $\mathbb{E}_b \mathrm{tr}\,(\rho')^4$, namely $\mathrm{tr}\,\mathbb{E}_b P_j P_\ell P_j P_\ell$ with $j,\ell\in\{1,\ldots,Q\}$, $\ell\neq j$. In Corollary 5.5 this was upperbounded as $\mathrm{tr}\,\mathbb{E}_b P_j P_\ell P_j P_\ell \le \mathrm{tr}\,\mathbb{E}_b P_j P_\ell = \mathrm{tr}\,\tau^2 = 2^{-n}$. For states restricted to the 8-state system we can do the computation exactly. We have $P_j = \rho^{\mathrm{E}}_{jg}(b)$ as defined in (27) for some arbitrary $g\in\{0,1\}^n$, which gives

$$\mathrm{tr}\,\mathbb{E}_b P_j P_\ell P_j P_\ell = \prod_{i=1}^{n} \mathbb{E}_{b_{ji}} \mathbb{E}_{b_{\ell i}} \left|\langle\psi_{b_{ji}g_i}|\psi_{b_{\ell i}g_i}\rangle\right|^4 = \prod_{i=1}^{n}\frac{1}{3} = (\frac{1}{3})^n. \tag{48}$$

Here we have used that $b_{ji} \neq b_{\ell i}$ occurs with probability 3/4 (and yields $|\cdots|^4 = (\frac{1}{3})^2$) while $b_{ji} = b_{\ell i}$ occurs with probability 1/4 (and yields $|\cdots|^4 = 1$). The upshot is that a contribution $\frac{1}{Q^4}\frac{Q(Q-1)}{2^n}$ in the proof of Corollary 5.5 has to be replaced by $\frac{1}{Q^4}\frac{Q(Q-1)}{3^n}$.
For $t = 5$ we follow the same procedure. At $k = 2$ there are 5 terms of the form $P_j P_\ell P_j P_\ell P_j$ (or rotations thereof), which each yield a contribution (48).
For $t = 6$ the procedure is the same but with more complicated combinations. At $k = 2$ there is one term of the form $(P_j P_\ell)^3$ which yields[5] $(\frac{5}{18})^n$, and 15 terms that reduce to $(P_j P_\ell)^2$ by idempotency, yielding (48). At $k = 3$ there is one term $(P_j P_\ell P_m)^2$ yielding $(\frac{1}{9})^n$, three terms of the form $P_j P_\ell P_j P_m P_\ell P_m$ yielding $(\frac{5}{36})^n$, and 36 terms that reduce to $\tau(P_j P_\ell)^2$ yielding $\frac{1}{2^n 3^n}$. Careful bookkeeping results in the expressions listed in Table 3.
Table 4 follows by applying the binomial expansion $\mathbb{E}_b \mathrm{tr}\,(\rho - \tau)^t = \sum_{a=0}^{t} \binom{t}{a} \mathbb{E}_b \mathrm{tr}\,\rho^a (-\tau)^{t-a} = \sum_{a=0}^{t} \binom{t}{a} (-\frac{1}{2^n})^{t-a} \mathbb{E}_b \mathrm{tr}\,\rho^a$ and then using Table 3.

D Proof of Theorem 6.6

<u>2nd power</u>. Since $\mathbb{E}_b \mathrm{tr}\,\rho_g^2$ does not depend on g we can write $\mathbb{E}_b \mathrm{tr}\,(\rho_g - \rho_{g'})^2 = 2\mathbb{E}_b \mathrm{tr}\,\rho_g^2 - 2\mathbb{E}_b \mathrm{tr}\,\rho_g \rho_{g'}$. The first term follows from Lemma 5.1 using $\mathrm{tr}\,\rho^2 = 1$ (the plaintext is a pure state). We define P_j as in the proof of Theorem 5.4, and $R_\ell = \bigotimes_{i=1}^n |\psi_{b_{\ell i} g'_i}\rangle\langle\psi_{b_{\ell i} g'_i}|$, and $\rho_{g'} = \frac{1}{Q}\sum_{\ell=1}^{Q} R_\ell$. It holds that $\mathbb{E}_b R_\ell = \tau$ and $P_j R_j = 0$. We write $\mathbb{E}_b \mathrm{tr}\,\rho_g \rho_{g'} = \frac{1}{Q^2}\sum_{j=1}^{Q}\sum_{\ell:\ell\neq j} \mathrm{tr}\,\mathbb{E}_b P_j R_\ell = \frac{Q^2-Q}{Q^2}\mathrm{tr}\,\tau^2$.
<u>4th power</u>. We note that $\mathbb{E}_b \mathrm{tr}\,\rho_g^3 \rho_{g'}$ does not depend on g and g' as long as $g' \neq g$. This allows us to write $\mathbb{E}_b \mathrm{tr}\,(\rho_g - \rho_{g'})^4 = 2\mathbb{E}_b \mathrm{tr}\,\rho_g^4 - 8\mathbb{E}_b \mathrm{tr}\,\rho_g^3 \rho_{g'} + 2\mathbb{E}_b \mathrm{tr}\,(\rho_g \rho_{g'})^2 + 4\mathbb{E}_b \mathrm{tr}\,\rho_g^2 \rho_{g'}^2$. The first term is given in Table 3. We write $Q^4 \mathbb{E}_b \mathrm{tr}\,\rho_g^3 \rho_{g'} = \sum_{j\ell m}\sum_{s:s\neq j\ell m} \mathrm{tr}\,\mathbb{E}_b P_j P_\ell P_m R_s$. The R_s reduces to τ and we get $Q^4 \mathbb{E}_b \mathrm{tr}\,\rho_g^3 \rho_{g'} = \sum_{j\ell m}(\sum_{s:s\neq j\ell m})\mathrm{tr}\,\mathbb{E}_b P_j P_\ell P_m \tau = (Q)_2 \mathrm{tr}\,\tau^2 + 3(Q)_3 \mathrm{tr}\,\tau^3 + (Q)_4 \mathrm{tr}\,\tau^4$.
Next we have $Q^4 \mathbb{E}_b \mathrm{tr}\,(\rho_g \rho_{g'})^2 = \sum_{js}\sum_{\ell:\ell\neq js}\sum_{m:m\neq js} \mathrm{tr}\,\mathbb{E}_b P_j R_\ell P_s R_m$ As earlier we use the notation k for the number of different table rows present in a summation term. At $k = 1$ we get zero contribution since a P and R projector must collide. At $k = 2$ we have to set $j = s, \ell = m$ yielding a contribution $(Q)_2(\frac{1}{3})^n$. At $k = 3$ we have the combinations $P_j R_\ell P_j R_m$ and $P_j R_\ell P_m R_\ell$ which both yield $(Q)_3 \mathrm{tr}\,\tau^3$. At $k = 4$ there is the unsurprising contribution $(Q)_4 \mathrm{tr}\,\tau^4$. Together this yields $Q^4 \mathbb{E}_b \mathrm{tr}\,(\rho_g \rho_{g'})^2 = \frac{(Q)_2}{3^n} + 2\frac{(Q)_3}{2^{2n}} + \frac{(Q)_4}{2^{3n}}$.
Finally we have $Q^4 \mathbb{E}_b \mathrm{tr}\,\rho_g^2 \rho_{g'}^2 = \sum_{j\ell}\sum_{m:m\neq j}\sum_{s:s\neq \ell} \mathrm{tr}\,\mathbb{E}_b P_j P_\ell R_s R_m$. At $k = 1$ there is again zero contribution because of the collisions between P and R. At $k = 4$ we have the usual $(Q)_4 \mathrm{tr}\,\tau^4$. At $k = 3$ the only nonzero contributions come from the combinations $P_j^2 R_s R_m$ and $P_j P_\ell R_m^2$, which both yield $(Q)_3 \mathrm{tr}\,\tau^3$. The case $k = 2$ is the most complicated. The combination $P_j^2 R_m^2$ yields $(Q)_2 \mathrm{tr}\,\tau^2$. For the combination $P_j P_\ell R_j R_\ell$ we get a factorised expression $\prod_{i=1}^n \mathbb{E}_b \mathrm{tr}\,P_{ji} P_{\ell i} R_{ji} R_{\ell i}$, where $\mathbb{E}_b$ refers to the i'th column of b. It turns out that $\mathbb{E}_b \mathrm{tr}\,P_{ji} P_{\ell i} R_{ji} R_{\ell i}$ depends on $g_i \oplus g'_i$. For $g'_i = g_i$ we get $\frac{1}{3}$, while for $g'_i \neq g_i$ the outcome is $-\frac{1}{6} = \frac{1}{3}\cdot(-\frac{1}{2})$. The product over i yields $(\frac{1}{3})^n(-\frac{1}{2})^{|g\oplus g'|}$. Adding up the pieces gives $Q^4 \mathbb{E}_b \mathrm{tr}\,\rho_g^2 \rho_{g'}^2 = \frac{(Q)_2}{2^n} + \frac{(Q)_2}{3^n}(-\frac{1}{2})^{|g\oplus g'|} + 2\frac{(Q)_3}{2^{2n}} + \frac{(Q)_4}{2^{3n}}$.
Taking $\mathbb{E}_b \mathrm{tr}\,(\rho_g - \rho_{g'})^4 = 2\mathbb{E}_b \mathrm{tr}\,\rho_g^4 - 8\mathbb{E}_b \mathrm{tr}\,\rho_g^3 \rho_{g'} + 2\mathbb{E}_b \mathrm{tr}\,(\rho_g \rho_{g'})^2 + 4\mathbb{E}_b \mathrm{tr}\,\rho_g^2 \rho_{g'}^2$ yields the final result.

References

[1] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[2] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[5] With probability $\frac{3}{4}$ it occurs that $b_{ji} \neq b_{\ell i}$, yielding $|\langle\psi_{b_{ji} g_i}|\psi_{b_{\ell i} g_i}\rangle|^6 = (\frac{1}{3})^3$. With probability $\frac{1}{4}$ it occurs that $b_{ji} = b_{\ell i}$, yielding 1. The expectation is $\frac{3}{4}\cdot(\frac{1}{3})^3 + \frac{1}{4} = \frac{5}{18}$.

[3] D.N. Matsukevich and A. Kuzmich. Quantum state transfer between matter and light. *Science*, 306(5696):663–666, 2004.

[4] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[5] A.K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661 – 663, 1991.

[6] D. Gottesman and J. Preskill. *Quantum Information with Continuous Variables*, chapter Secure quantum key exchange using squeezed states, pages 317–356. Springer, 2003. arXiv:quant-ph/0008046v2.

[7] C.H. Bennett, G. Brassard, S. Breidbard, and S. Wiesner. Quantum cryptography, or unforgeable subway tokens. In *CRYPTO*, pages 267–275, 1982.

[8] I.B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In *IEEE Symposium on Foundations of Computer Science*, page 449, 2005.

[9] C. Schaffner. Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. *Phys. Rev. A*, 82:032308, 2010.

[10] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp. Authentication of quantum messages. In *IEEE Symposium on Foundations of Computer Science*, pages 449–458, 2002. Full version at `http://arxiv.org/abs/quant-ph/0205128`.

[11] P.O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. *Phys.Rev.A*, 67:042317, 2003.

[12] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *Annual Symposium on Foundations of Computer Science*, pages 547–553, 2000.

[13] D. Gottesman. Uncloneable encryption. *Quantum Information and Computation*, 3(6):581–602, 2003.

[14] B. Škorić. Quantum Readout of Physical Unclonable Functions. *International Journal of Quantum Information*, 10(1):1250001:1–31, 2012.

[15] S.A. Goorden, M. Horstmann, A.P. Mosk, B. Škorić, and P.W.H. Pinkse. Quantum-Secure Authentication of a physical unclonable key. *Optica*, 1(6):421–424, 2014.

[16] M. Malik, O.S. Magaña-Loaiza, and R.W. Boyd. Quantum-secured imaging. *Appl.Phys.Lett.*, 101:241103, 2012.

[17] A. Broadbent and C. Schaffner. Quantum cryptography beyond quantum key distribution. *Des. Codes Cryptogr.*, 78:351–382, 2016.

[18] P. Hayden, D. Leung, P.W. Shor, and A. Winter. Randomizing quantum states: constructions and applications. *Commun. Math. Phys.*, 250:371–391, 2004.

[19] I.B. Damgård, T.B. Pedersen, and L. Salvail. A quantum cipher with near optimal key-recycling. In *CRYPTO*, pages 494–510, 2005.

[20] I.B. Damgård, T.B. Pedersen, and L. Salvail. A quantum cipher with near optimal key-recycling. Technical Report rs RS-05-17, BRICS, Department of Computer Science, University of Aarhus, 2005.

[21] I.B. Damgård, T.B. Pedersen, and L. Salvail. On the key-uncertainty of quantum ciphers and the computational security of one-way quantum transmission. In *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 91–108, 2004.

[22] S. Fehr and L. Salvail. Quantum authentication and encryption with key recycling, 2016. `https://arxiv.org/abs/1610.05614v1`.

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

[24] D.W. Leung. Quantum Vernam cipher. *Quantum Information and Computation*, 2(1):14–34, 2002.

[25] P.O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. *Phys. Rev. A*, 67(4):042317, 2003.

[26] G. Alagic, A. Broadbent, B. Fefferman, T. Gagliardoni, C. Schaffner, and M. St.Jules. Computational security of quantum encryption, 2016. `https://arxiv.org/abs/1602.01441v1`.

[27] J. Oppenheim and M. Horodecki. How to reuse a one-time pad and other notes on authentication, encryption, and protection of quantum information. *Phys. Rev. A*, 72(4):042309, 2005.

[28] S.P. Desrosiers. Entropic security in quantum cryptography. *Quantum Information Processing*, 8(4):331–345, 2009.

[29] R. Canetti. Universally composable security: a new paradigm for cryptographic protocols. In *Symposium on Foundations of Computer Science*, pages 136–145. IEEE, 2001.

[30] 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.

[31] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography*, volume 3378 of *LNCS*, pages 407–425, 2005.

[32] D. Unruh. Universally composable quantum multi-party computation. In *Eurocrypt 2010*, volume 6110 of *LNCS*, pages 486–505. Springer, 2010.

[33] C.H. Bennett, G. Brassard, and S. Breidbart. Quantum Cryptography II: How to re-use a one-time pad safely even if P=NP. *Natural Computing*, 13:453–458, 2014. Original manuscript 1982.

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

[35] D. Unruh. Revocable quantum time-release encryption. In *Eurocrypt*, volume 8441 of *LNCS*, pages 129–146, 2014.

[36] J.L. Massey and J.K. Omura. Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission, 1982. US patent 4567600.

[37] Y. Kanamori and S.-M. Yoo. Quantum three-pass protocol: key distribution using quantum superposition states. *Int. J. of Network Security and its Applications*, 1(2):64–70, 2009.

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

[39] J.A. Tropp. User-friendly tail bounds for sums of random matrices. *Foundations of Computational Mathematics*, 12(4):389–434, 2012.

[40] M. de Vries. Master's thesis, Eindhoven University of Technology, the Netherlands, 2017. In preparation.