Unclonable encryption revisited

$(4 \times 2 = 8)$

Boris Škorić

b.skoric@tue.nl

Abstract

Unclonable Encryption is a technique similar to Quantum Key Distribution and authentication of quantum states; it quantum-protects classical ciphertext so that it cannot be copied by eavesdroppers. We propose an improved variant which has higher efficiency and better error tolerance. Our variant uses four cipherstate bases that are equally spaced on the Bloch sphere, instead of the usual + and × basis.

1 Introduction

1.1 Quantum physics in cryptography and security

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 (cryptographic) schemes, such as Quantum Key Distribution (QKD) [4, 5, 6], quantum anti-counterfeiting [7], quantum Oblivious Transfer [8, 9], authentication and encryption of quantum states [10, 11, 12], quantum authentication of PUFs [13, 14], and quantum-secured imaging [15], to name a few.

1.2 Unclonable ciphertext

A less known achievement is *Unclonable Encryption* introduced by Daniel Gottesman in 2003 [16].[1] The context here is that there is a quantum channel from Alice to Bob, but, in contrast to QKD, no channel from Bob to Alice. This scenario is relevant for instance when a message is sent into the future, or in the case of significant time lags in long-distance communication, or if multiple-round protocols are too costly. The aim of Unclonable Encryption is to send a classical ciphertext to Bob, quantum-protected in such a way that one of the following two outcomes occurs: Either (i) Bob successfully recovers the plaintext and verifies its authenticity. Eve learns nothing about the ciphertext. Or (ii) Eve learns some of the ciphertext. Bob is not able to recover&verify the plaintext, i.e. the attack has been noticed.

Gottesman listed a number of use cases for Unclonable Encryption,

1. Alice and Bob use a classical One Time Pad (OTP). When an OTP has not yet been used, it needs to be strictly protected. After it has been used, it must be completely erased from memory. With today's computer infrastructure both data protection and data erasure are nontrivial tasks. Eve copies the classical ciphertext and she may later obtain information about the OTP. Unclonable Encryption thwarts this attack by denying Eve the ability to copy the ciphertext.

[1] That work was presaged by an unpublished manuscript by Bennett, Brassard and Breidbart in 1982 [17].

2. Similar to use case 1, but with cryptography based on computational assumptions. Instead of an OTP, Alice and Bob repeatedly use the same short key to encrypt large plaintexts. Now, even if she cannot get hold of the encryption key, Eve's ability to make a copy of each ciphertext allows her to launch brute force attacks. Again, Unclonable Encryption thwarts the attack.

3. Quantum Key Distribution with less interaction than standard schemes, and fewer bits spent for eavesdropping detection.

Gottesman's scheme protects the classical ciphertext by encoding each ciphertext bit in a qubit state, either in the standard basis ("+") or in the Hadamard basis ("×"). The sequence of bases is a secret known only by Alice and Bob. Any attempt by Eve, who does not know the sequence, to measure a qubit state will cause a disturbance at Bob's side with substantial probability.

The scheme does not need any entanglement (which is difficult to create and preserve) or complicated unitary transformations, and can be implemented using purely "prepare and measure" techniques such as in BB84.

One interesting aspect of the scheme is that, as long as no disturbance is noticed, Alice and Bob can keep re-using their secret bases sequence.[2] Remarkably, this holds even if the sequence is generated pseudorandomly from a short secret: Eve must break the pseudo-randomness before Bob receives the qubits.

1.3 Contributions and outline

We propose an improvement of Gottesman's Unclonable Encryption scheme. We use the well known two-bit encryption of qubit states, and encode a classical ciphertext bit into one of eight states which are maximally spread apart on the Bloch sphere. We refer to this as the *eight-state system*. Making use of the full Bloch sphere, instead of just the one circle containing the "+" and "×" basis, brings a number of advantages. Eve's knowledge about the classical ciphertext is drastically reduced, even to zero in case of a fully random sequence of bases. Furthermore, the probability of detecting eavesdroppers increases. These advantages reduce the amount of privacy amplification (compression) needed in the scheme and thereby reduce the number of qubits needed to send a message and improve the noise tolerance. Our improved unclonable encryption may lead to improvements of low-interaction QKD variants.

The outline of this paper is as follows. In Section 2 we briefly review Gottesman's scheme and encryption of quantum states. Section 3 discusses the privacy amplification in Gottesman's scheme. In Section 4 we introduce our 8-state system and the improved unclonable encryption. In Section 5 we analyse the privacy amplification needs of the improved scheme, and in Section 6 we provide some heuristic arguments to estimate the amount of key leakage in cases where keys are generated pseudorandomly.

2 Preliminaries

2.1 Notation and terminology

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 denoted as $\mathsf{H}_{\min}(X) = -\log \max_{x\in\mathcal{X}} \Pr[X = x]$, and the conditional min-entropy as $\mathsf{H}_{\min}(X|Y) = -\log \mathbb{E}_y \max_{x\in\mathcal{X}} \Pr[X = x|Y = y]$. The notation h stands for the entropy function $h(p) = p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}$. Bitwise XOR is written as '$\oplus$'. In the treatment of error-correcting codes we write messages, codewords and syndromes as *column* vectors.

[2] The aim of [17] was to re-use the classical OTP.

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 written as $\sigma_x, \sigma_y, \sigma_z$. The standard basis is the eigenbasis of σ_z, with $|0\rangle$ in the positive z-direction.

2.2 Gottesman's Unclonable Encryption scheme

We briefly describe Gottesman's scheme, in particular the second variant presented in [16], and its main properties.

Preparation phase

Alice and Bob share three classical secrets: an authentication key $a \in \{0,1\}^s$, a OTP $e \in \{0,1\}^N$ and a basis sequence $b \in \{0,1\}^N$. Alice and Bob agree on a message length n and on a Message Authentication Code (MAC) that uses the key a and produces a string of length s. They agree on an error-correcting code C with message length k ($k > n+s$) and codeword length N, as well as an error-correcting code D with message length $k' = (n+s)+N-k$ ($k' < k$) and codeword length N, satisfying[3] $D^\perp \subset C$. The parity check matrix of C is contained in the parity check matrix of $D^\perp$. (See Fig. 1). The purpose of code C is to correct noise on the quantum channel, while D is used for privacy amplification. For D it is not necessary to have an efficient decoding algorithm.

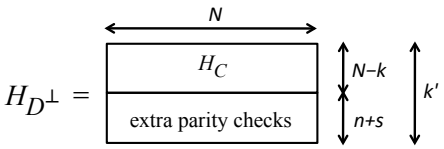

Figure 1: *Relation between the codes C and $D^\perp \subset C$.*

Encryption

Alice performs the following steps.

A1. Take the plaintext $x \in \{0,1\}^n$ and compute a MAC $\mu \in \{0,1\}^s$ using the key a. Concatenate x and μ into $y = x\mu \in \{0,1\}^{n+s}$.

A2. Find any vector $z_y \in \{0,1\}^N$ that satisfies

$$H_{D^\perp}\, z_y = \begin{pmatrix} 0^{N-k} \\ y \end{pmatrix} \in \{0,1\}^{k'}, \tag{1}$$

i.e. z_y is a codeword of C and has additional syndrome bits y w.r.t. $D^\perp$. Pick a random codeword $r \in D^\perp$ ($N-k'$ random bits) and compute $z = z_y \oplus r$.

A3. Apply the One-Time Pad: $g = z \oplus e \in \{0,1\}^N$.

A4. For $i \in \{1,\ldots,N\}$ encode ciphertext bit g_i in the basis "+" if $b_i = 0$ and in the basis "×" if $b_i = 1$. The resulting state is denoted as $|\psi\rangle_i$. Send $|\psi\rangle_i$ to Bob.

Decryption

Bob performs the following steps.

B1. For $i \in \{1,\ldots,N\}$ receive qubit states $|\psi'\rangle_i$. If $b_i = 0$ measure the qubit in the "+" basis, otherwise in the "×" basis. The result is $g'_i \in \{0,1\}$.

B2. Apply the One-Time Pad: $z' = g' \oplus e \in \{0,1\}^N$.

B3. Apply error correction on z' using code C. The result is denoted as $\hat{z} \in C$.

B4. Compute $y' = (H_{D^\perp}\hat{z})_{\text{last } n+s \text{ bits}}$.

B5. Parse y' as the concatenation $x'\mu'$ with $x' \in \{0,1\}^n$. Using the key a, verify if μ' is a correct MAC on x'.

[3]The notation $D^\perp$ stands for the dual code, i.e. all vectors in $D^\perp$ are orthogonal to all vectors in D. The notation $D^\perp \subset C$ means that each codeword of $D^\perp$ is also a codeword of C.

If the verification in step B5 fails, then either Eve tampered with the transmitted qubits or there was too much noise on the quantum channel. Step B3 corrects transmission errors. Step B4 achieves privacy amplification, which is necessary since the noise that is tolerated by the protocol could be due to Eve's snooping, from which she obtains some information about the ciphertext g. (See Section 3).

Re-usability

As long as the OTP is fully random in each message and Bob detects no disturbance, the keys a and b can be safely re-used. Consequently, for asymptotic number of undisturbed messages the number of key bits required to encrypt a message is practically the same as for a classical OTP, and the unclonability has been obtained 'for free'.

If Alice and Bob are re-using b and Eve at some point in time learns b, then (i) Eve can copy future ciphertexts g but not decrypt them because of the fresh OTPs; and (ii) she can not learn anything about the ciphertext g of past messages.

If Eve learns the OTP e for a message before/during transmission, then the unclonability prevents her from learning g (and hence the plaintext). However, she can obtain information about b, which endangers the unclonability of future transmissions if Alice and Bob re-use b.

Pseudorandom basis sequence

Unclonability still holds if b is generated pseudorandomly. Eve has to break the pseudorandomness *before* message transmission, otherwise she cannot clone the qubits.

2.3 Perfect encryption of arbitrary qubit states

An arbitrary unknown qubit state can be perfectly encrypted using a classical two-bit key. Let the state be 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, $E_{uw} = i^{uw}(|w\rangle\langle 0| + (-1)^u|1 \oplus w\rangle\langle 1|)$. In terms of Pauli spin matrices: $E_{00} = \mathbf{1}$, $E_{01} = \sigma_x$, $E_{10} = \sigma_z$, $E_{11} = \sigma_y$. From the point of view of an attacker Eve who does not know u, w, the state is a mixed state $\frac{1}{4}\sum_{u,w} |\psi_{uw}\rangle\langle\psi_{uw}| = \frac{1}{2}\mathbf{1}$. In other words, from Eve's point of view the result of the encryption carries no information at all about ψ.

3 Privacy amplification parameters in Gottesman's scheme

The code C is capable of correcting up to $N\delta$ errors, where δ depends on the noise level of the quantum channel. In [16] it is specified that D must be able to correct $N(\delta + \eta)$ errors, where for large N the η is allowed to go to zero. The requirement on D is a consequence of the particular way in which Gottesman derived his scheme from a quantum authentication protocol.

Below we present heuristic arguments about the privacy amplification requirements. These arguments give some intuition on the parameter choices.

If $N\delta$ errors are tolerated, then in the worst case all these errors are due to Eve's eavesdropping as opposed to random noise. When Eve does a projective measurement on a qubit $|\psi\rangle_i$, she causes a disturbance $g_i' \neq g_i$ at Bob's side with probability $\frac{1}{4}$. (The $\frac{1}{4}$ probability holds for all measurement bases of the form $\cos\varphi|0\rangle + \sin\varphi|1\rangle$ that Eve could choose; it is a property of the "$+\times$" bases system used by Alice and Bob.) Hence, when $N\delta$ errors occur it is prudent to assume that Eve has performed a measurement on approximately $4N\delta$ qubits. It is well known that Eve learns most if she applies the '$\frac{\pi}{8}$-attack', i.e. measuring polarisation at an angle $\varphi = \pi/8$ which lies exactly halfway between the "$+$" and "$\times$" basis. In this way she achieves $\mathsf{H}_{\min}(G_i|\text{Eve's observation}) = -\log_2(\cos\frac{\pi}{8})^2 \approx 0.228$. Thus, in terms of min-entropy, we can say that Eve has learned $N_E \approx 4N\delta \cdot 0.772 = 3.09N\delta$ bits of information about the RV $G \in \{0, 1\}^N$ without being detected.

Consider the case where Alice and Bob keep re-using the basis sequence b. Eve collects $2N\delta$ qubits from each transmission (e.g. the first $2N\delta$ qubits) without being noticed. (Now the probability of causing a bit flip is $\frac{1}{2}$). After a large number of transmissions, she applies a measurement on all qubits with the same index i; since they are encrypted with the same key b_i, Eve learns practically everything about the ciphertext bits. She does this for each of the $2N\delta$ positions. Her knowledge N_E about each transmitted ciphertext is almost $2N\delta$.

The privacy amplification step has to turn Eve's N_E bits of knowledge about g into practically zero knowledge about the $n+s$ last bits of the $D^\perp$-syndrome of g. After the error correction, a string in $\{0,1\}^N$ is obtained with k degrees of freedom. Then the privacy amplification maps this to a syndrome of size $n+s$. The number of bits 'ignored' by the syndrome is $k-(n+s)=N-k'$, which is precisely the redundancy of the code D. This should exceed Eve's knowledge N_E. Indeed, [16] suggests a construction with redundancy $N-k'=Nh(2\delta+2\eta)>4N(\delta+\eta)>N_E$. The paper also states that setting the redundancy of the code C to $N-k=Nh(2\delta)$ is achievable (though closer to the Shannon bound $Nh(\delta)$ is of course desirable). According to these somewhat pessimistic parameter choices, the number of qubits used to send a message of length $n+s$ would be $N=(n+s)/[1-h(2\delta)-h(2\delta+2\eta)]$.

The 'overhead' from the privacy amplification, without counting the error correction, is a factor $\frac{N}{(n+s)/[1-h(2\delta)]}=\frac{1-h(2\delta)}{1-h(2\delta)-h(2\delta+2\eta)}=1+\frac{h(2\delta+2\eta)}{1-h(2\delta)-h(2\delta+2\eta)}$. Even for $\eta\to 0$ the overhead factor is considerable and explodes to infinity around $\delta=0.055$. This would imply that the scheme does not work at noise levels higher than approximately 5.5%. The numbers improve if we move closer to the Shannon bound. In the most optimistic case, we set $\eta=0$, $N-k=Nh(\delta)$ and $N-k'=N_E$ resulting in an overhead factor $1+\frac{N_E/N}{1-h(\delta)-N_E/N}$. Now the overhead explodes only at $\delta\approx 0.137$; however, the overhead is still considerable, e.g. a factor 2 at $\delta\approx 0.09$.

4 Eight-state Unclonable Encryption

Intuitively, it should be possible to obtain an Unclonable Encryption scheme better than [16] from the perfect encryption scheme of Section 2.3. However, we observe that it makes no sense to apply the perfect encryption scheme to a classical bit *if that bit is encoded in the standard basis* $|0\rangle,|1\rangle$.[4] All the eight encrypted states are proportional either to $|0\rangle$ or to $|1\rangle$. While the plaintext value is perfectly hidden, Eve can learn the encrypted state with 100% accuracy, completely breaking the unclonability property that we are aiming for. What has in fact been achieved is a wasteful two-bit masking of a single classical bit.

We propose a system in which a classical bit is *nontrivially* quantum-encrypted using the 2-bit key; this results in 8 entirely different states which are maximally spread out over the Bloch sphere. Although our 8-state set is very simple and has interesting properties, we are not aware that it has ever been used.

4.1 Maximally separated cipherstates

We define $\cos\alpha \stackrel{\text{def}}{=} 1/\sqrt{3}$, $\alpha\approx 0.96$.[5] We write $\sqrt{i}=e^{i\pi/4}$. We encode the classical '0' and '1' as qubit states ψ_0,ψ_1,

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

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 $|0\rangle$, $|1\rangle$,

$$|\psi_g\rangle=(-\sqrt{i})^g\cos\tfrac{\alpha}{2}|g\rangle+(\sqrt{i})^{1-g}\sin\tfrac{\alpha}{2}|1-g\rangle \qquad g\in\{0,1\}. \tag{3}$$

We act on these qubit states with the four encryption operators E_{uw} defined in Section 2.3 and thus obtain eight different states which we call the *cipherstates*,

$$|\psi_{uwg}\rangle \stackrel{\text{def}}{=} E_{uw}|\psi_g\rangle = i^{uw}(-1)^{gu}\Big[(-\sqrt{i})^g\cos\tfrac{\alpha}{2}|g\oplus w\rangle+(-1)^u(\sqrt{i})^{1-g}\sin\tfrac{\alpha}{2}|1-g\oplus w\rangle\Big]. \tag{4}$$

[4] Which is in fact what happens in Appendix B of [16].

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

On the Bloch sphere these correspond to unit-length vectors $\boldsymbol{n}_{uwg}$ as follows,

$$\boldsymbol{n}_{uwg} = \frac{(-1)^g}{\sqrt{3}} \begin{pmatrix} (-1)^u \\ (-1)^{u+w} \\ (-1)^w \end{pmatrix}. \tag{5}$$

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 $\cos\theta = \cos 2\zeta \cos 2\beta$, $\sin\varphi = \sin 2\zeta / \sqrt{1-(\cos 2\zeta \cos 2\beta)^2}$, $\tan 2\beta = \cos\varphi \tan\theta$, $\sin 2\zeta = \sin\theta \sin\varphi$. Our eight cipherstates have $\beta \in \{\pm\frac{\pi}{8}, \pm\frac{3\pi}{8}\}$, $\zeta = \pm(\frac{\pi}{4} - \frac{\alpha}{2}) \approx \pm 0.308$.

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

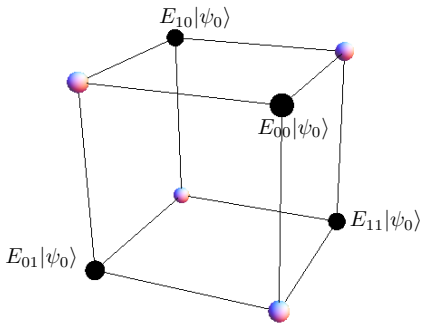

Figure 2: *The eight cipherstates $|\psi_{uwg}\rangle = E_{uw}|\psi_g\rangle$ on the Bloch sphere, forming the corner points $(\pm 1, \pm 1, \pm 1)/\sqrt{3}$ of a cube.*

We will often write $b = 2u + w$, $b \in \{0, 1, 2, 3\}$ as a basis index, with corresponding notation ψ_{bg} and $\boldsymbol{n}_{bg}$.

4.2 Properties of the eight-state system

It holds that $\langle\psi_{uw0}|\psi_{uw1}\rangle = 0$, i.e. opposite bit values encrypted with the same key lead to orthogonal cipherstates. This trivially follows from the unitarity of the encryption operators, $\langle\psi_{uw0}|\psi_{uw1}\rangle = \langle\psi_0|E_{uw}^\dagger E_{uw}|\psi_1\rangle = \langle\psi_0|\psi_1\rangle = 0$.

More generally, we can readily compute the inner products between all the various cipherstates from the general rule $|\langle\psi_{u'w'g'}|\psi_{uwg}\rangle|^2 = \frac{1}{2} + \frac{1}{2}\boldsymbol{n}_{u'w'g'} \cdot \boldsymbol{n}_{uwg}$,

$$|\langle\psi_{u'w'g'}|\psi_{uwg}\rangle|^2 = \delta_{uu'}\delta_{ww'} \cdot \delta_{gg'} + (1 - \delta_{uu'}\delta_{ww'})\Big[\delta_{gg'}\frac{1}{3} + (1-\delta_{gg'})\frac{2}{3}\Big]. \tag{6}$$

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 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. (6) 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.

4.3 Eight-state unclonable ciphertext scheme

We finally get to the main contribution, namely the improved Unclonable Encryption scheme. It closely follows the steps of Gottesman's scheme, with two differences: we use the eight-state system instead of the $+\times$ bases, and our code parameters are different. We first present the protocol steps; then we analyze the security.

Preparation phase

Same as Section 2.2, but now $b \in \{0,1,2,3\}^N$ and we introduce $u, w \in \{0,1\}^N$ such that $b_i = 2u_i + w_i$.

Encryption

A1. Take the plaintext $x \in \{0,1\}^n$ and compute a MAC $\mu \in \{0,1\}^s$ using the key a. Concatenate x and μ into $y = x\mu \in \{0,1\}^{n+s}$.

A2. Find any vector $z_y \in \{0,1\}^N$ that satisfies $H_{D^\perp}\, z_y = \begin{pmatrix} 0^{N-k} \\ y \end{pmatrix} \in \{0,1\}^{k'}$. Pick a random codeword $r \in D^\perp$ ($N-k'$ random bits) and compute $z = z_y \oplus r$.

A3. Apply the One-Time Pad: $g = z \oplus e \in \{0,1\}^N$.

A4. For $i \in \{1,\ldots,N\}$ prepare state $|\chi\rangle_i = |\psi_{u_i w_i g_i}\rangle$ according to (4). Send $|\chi\rangle_i$.

Decryption

B1. For $i \in \{1,\ldots,N\}$ receive qubit states $|\chi'\rangle_i$. Measure $|\chi'\rangle_i$ in the basis $|\psi_{u_i w_i 0}\rangle, |\psi_{u_i w_i 1}\rangle$. The result is $g'_i \in \{0,1\}$.

B2. Apply the One-Time Pad: $z' = g' \oplus e \in \{0,1\}^N$.

B3. Apply error correction on z' using code C. The result is denoted as $\hat{z} \in C$.

B4. Compute $y' = (H_{D^\perp}\hat{z})_{\text{last } n+s \text{ bits}}$.

B5. Parse y' as the concatenation $x'\mu'$ with $x' \in \{0,1\}^n$. Using the key a, verify if μ' is a correct MAC on x'.

5 Privacy amplification requirements

If Alice and Bob use a new random sequence B for each message, then it is impossible for Eve to get any information about G. No privacy amplification is required, and the code C_1 suffices. This implies a significant reduction of the number of qubits N and an improvement of the noise tolerance to any noise level that can be error-corrected by a classical code.

If Alice and Bob keep re-using B, then Eve may collect a small number of qubits from each message and postpone her measurements, as described in Section 3. When she replaces a qubit by a random state, she causes a bit flip with probability $\frac{1}{2}$. Thus she may learn up to $2N\delta$ bits of information about G while avoiding detection. The privacy amplification must discard $2N\delta$ bits.

In all other use cases we need to know how much disturbance Eve is causing when she does intercept-and-resend attacks on qubits. Below we show that a measurement causes a bit flip $g'_i \neq g_i$ at Bob's side with probability $\frac{1}{3}$. This is better than the $\frac{1}{4}$ of the original scheme.

Theorem 1 *Let Eve know g and receive a qubit state $|\psi_{uwg}\rangle$ randomly drawn from the four possible cipherstates. Let her choose an arbitrary direction $|\gamma\rangle$ without knowing u, w and perform a projective measurement in this direction, resulting in a final state $|\gamma_j\rangle$ with $j \in \{-1,+1\}$. Next, when a measurement in the $|\psi_{uwg}\rangle, |\psi_{uw,1-g}\rangle$ basis is done, the probability of projecting back onto $|\psi_{uwg}\rangle$, averaged over u, w, j, is $\frac{2}{3}$.*

Proof:

We write $|\gamma\rangle = (\cos\frac{\theta}{2}, e^{i\varphi}\sin\frac{\theta}{2})^{\mathrm{T}}$ which on the Bloch sphere corresponds to $\boldsymbol{n}_{\theta\varphi} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)^{\mathrm{T}}$. We use $|\langle\gamma|\psi_{uwg}\rangle|^2 = \frac{1}{2} + \frac{1}{2}\boldsymbol{n}_{\theta\varphi}\cdot\boldsymbol{n}_{uwg}$ with $\boldsymbol{n}_{uwg}$ as specified by (5),

$$\boldsymbol{n}_{\theta\varphi}\cdot\boldsymbol{n}_{uwg} = \frac{(-1)^g}{\sqrt{3}}\Big[(-1)^u\sin\theta\cos\varphi + (-1)^{u+w}\sin\theta\sin\varphi + (-1)^w\cos\theta\Big]. \tag{7}$$

The probability of projecting back-and-forth, averaged over Eve's outcome j, is $|\langle\gamma|\psi_{uwg}\rangle|^4 + (1 - |\langle\gamma|\psi_{uwg}\rangle|^2)^2 = (\frac{1}{2} + \frac{1}{2}\boldsymbol{n}_{\theta\varphi} \cdot \boldsymbol{n}_{uwg})^2 + (\frac{1}{2} - \frac{1}{2}\boldsymbol{n}_{\theta\varphi} \cdot \boldsymbol{n}_{uwg})^2 = \frac{1}{2} + \frac{1}{2}(\boldsymbol{n}_{\theta\varphi} \cdot \boldsymbol{n}_{uwg})^2 = \frac{1}{2} + \frac{1}{6}[1 + 2(-1)^w \sin^2\theta \sin\varphi\cos\varphi + 2(-1)^{u+w}\sin\theta\cos\theta\cos\varphi + (-1)^u \sin\theta\cos\theta\sin\varphi]$. After averaging over u, w all terms that depend on θ, φ disappear, leaving us with $\frac{1}{2} + \frac{1}{6} = \frac{2}{3}$. □

Note that Theorem 1 is formulated very generally, with Eve actually having complete knowledge of g_i. As long as B is truly random, the bit flip probability is $\frac{1}{3}$ no matter how much Eve knows about g_i.

Interesting use cases could be e.g. having pseudorandom B and/or pseudorandom OTP E. Here it is important to keep in mind that B provides unclonability of G, while the randomness of G protects the confidentiality of B.

- If B is pseudorandom, Eve has a small advantage in guessing the keys b_i which she may exploit to choose a measurement basis in which she obtains (partial) information about g_i *and* has a probability slightly lower than $\frac{1}{3}$ of causing a bit flip. Both these effects have to be taken into account for setting the parameter k' of the code D.
- Similarly, if G is pseudorandom (caused by pseudorandom E), then Eve can obtain some information about B, which limits the re-usability of B. If Alice and Bob decide to re-use B nonetheless, they have to take into account that Eve's accumulated knowledge about B allows her to obtain information about G, necessitating a certain amount of privacy amplification.
- If both B and G are pseudorandom, both the above mentioned effects play a role and in fact amplify each other.

In Section 6 we try to quantify some of these statements, without providing full security proofs.

6 Security heuristics

We do a partial security analysis for use cases where G or B is pseudorandom. We consider only attacks that act on individual qubits, and that do not depend on the outcomes of measurements, i.e. non-adaptive local attacks. Eve performs a measurement in a basis of her choice and forwards the resulting state to Bob. We look at three properties: the probability of causing a disturbance, the amount of information obtained about the ciphertext G, and the amount of information obtained about the basis sequence B.

6.1 Modelling pseudorandomness

We model a pseudorandom basis sequence as follows. Let q be a constant, and $Q = 4^q \in \mathbb{N}$, with $Q \ll 4^N$. Let T be a fully random $Q \times N$ publicly known table with elements $T_{ji} \in \{0, 1, 2, 3\}$. For each message, uniformly draw a random $J \in \{1, \ldots, Q\}$. Then the pseudorandom sequence B is the J'th row of t, i.e. $B_i = t_{Ji}$.[6] We can think of q as the length of the seed that is fed into an idealized pseudorandom number generator.

We model pseudorandomness of the pad e in a similar way. We introduce a security parameter ℓ and $L = 2^\ell \in \mathbb{N}$, $L \ll 2^N$. Let Γ be a fully random publicly known $L \times N$ binary table. For each message, uniformly draw a row index $V \in \{1, \ldots, L\}$. The ciphertext G_i is given by γ_{Vi}. Of course this is not how ciphertext is created in reality (there is not even a plaintext in this model), but our model captures the pseudorandomness of a classical pad $e \in \{0, 1\}^N$ masking a plaintext in such a way that the ciphertext has min-entropy $\ell < N$.

6.2 Random G, pseudorandom B

We investigate a number of simple attacks: (i) Eve measures in the standard basis or, equivalently, in the eigenbasis of σ_x or σ_y; (ii) she measures in a random u, w basis; (iii) at position i she picks

[6] Note that the case $q \to N$ is not entirely equivalent to a fully random B. Perfect randomness would correspond to a *structured* table of size $4^N \times N$, e.g. with row j given by the base-4 representation of the integer j.

the u, w basis that is most frequent in the i'th column of T. The results are presented in the theorems below.

Lemma 1 *Let the RV $G_i \in \{0,1\}$ be uniform, independent of B_i. Let Eve perform a measurement on the qubit, in a basis independent of the table T, with result $R_i \in \{-1,+1\}$. Then*

$$\Pr[G_i = g | B_i = b, R_i = r] = \Pr[R_i = r | G_i = g, B_i = b]. \tag{8}$$

Proof: We have (in abbreviated notation) $\Pr[g|br] = \frac{\Pr[gbr]}{\Pr[br]} = \frac{\Pr[b]\Pr[g|b]\Pr[r|gb]}{\Pr[b]\Pr[r|b]} = \frac{\Pr[g|b]\Pr[r|gb]}{\Pr[r|b]}$. Since G_i is independent of B_i and uniform, we have $\Pr[g|b] = \frac{1}{2}$. Eve measures in some direction θ, φ. We have $\Pr[r|b] = \mathbb{E}_g \Pr[r|gb] = \mathbb{E}_g[\frac{1}{2} + \frac{r}{2}\boldsymbol{n}_{\theta\varphi} \cdot \boldsymbol{n}_{bg}]$ where $\boldsymbol{n}_{\theta\varphi} \cdot \boldsymbol{n}_{bg}$ is given by (7). Finally, $\mathbb{E}_g[\boldsymbol{n}_{\theta\varphi} \cdot \boldsymbol{n}_{bg}] = 0$ yields $\Pr[r|b] = \frac{1}{2}$. □

Theorem 2 (Standard basis attack) *Let Alice and Bob use fully random G. Let $B \in \{0,1,2,3\}^N$ be a pseudorandom basis sequence as described above. Let Eve measure each individual qubit in the standard basis, yielding a sequence $R \in \{-1,+1\}^N$ of measurement results. Then Eve's knowledge about G can be summarized as*

$$\mathsf{H}_{\min}(G) - \mathsf{H}_{\min}(G|TR) = N \log \left[1 + \frac{2}{\sqrt{3}} \cdot \frac{1}{2^Q} \binom{Q-1}{\lfloor Q/2 \rfloor}\right] \approx N \log \left[1 + \frac{1}{\sqrt{6\pi}} \cdot \frac{1}{2^{q-1}}\right]. \tag{9}$$

For each individual qubit the probability of causing $g_i' \neq g_i$ is $\frac{1}{3}$.

Proof: see Appendix A.

Theorem 3 (Random basis attack) *Let Alice and Bob use fully random G. Let $B \in \{0,1,2,3\}^N$ be a pseudorandom basis sequence as described above. Let Eve measure each individual qubit $|\chi\rangle_i$ in a random basis $\lambda_i \in \{0,1,2,3\}$ which is one of the four possible bases used by Alice and Bob, yielding a sequence R of measurement results. Then Eve's knowledge about G can be bounded as*

$$\mathsf{H}_{\min}(G) - \mathsf{H}_{\min}(G|TR\Lambda) < N \log \left[1 + \frac{1}{\sqrt{3}} \cdot \frac{1}{2^q}\right]. \tag{10}$$

For each individual qubit the probability of causing $g_i' \neq g_i$ is $\frac{1}{3}$.

Proof: see Appendix B

Theorem 4 (Most-frequent-basis attack) *Let Alice and Bob use fully random G. Let $B \in \{0,1,2,3\}^N$ be a pseudorandom basis sequence as described above. Let Eve measure each individual qubit $|\chi\rangle_i$ in a basis $\beta_i \in \{0,1,2,3\}$ which is equal to the most frequently occurring basis in the i'th column of t, yielding a sequence R of measurement results. Then Eve's knowledge about G can be bounded as*

$$\mathsf{H}_{\min}(G) - \mathsf{H}_{\min}(G|TR) < N \log \left(1 + \frac{1}{2^{q-1}} \left\{\frac{2}{3} + \frac{\sqrt{2}}{3}\sqrt{q \ln 2 + \ln 3}\right\}\right). \tag{11}$$

For each individual qubit the probability of causing a disturbance is lower bounded as

$$\Pr[G_i \neq g_i] > \frac{1}{3} - \frac{1}{9 \cdot 2^{q-2}} \left(1 + \frac{1}{\sqrt{2}}\sqrt{\ln 3 + q \ln 2}\right). \tag{12}$$

Proof: see Appendix C.

The inequality (11) is not tight, but it shows the order $\mathcal{O}(\sqrt{q}/2^q)$ of the attacker's knowledge, i.e. exponentially small in q.

We see that all the investigated attacks perform more or less the same. The min-entropy reduction due to the attack is of order $3\delta N/2^q$ if Eve subjects $3\delta N$ qubits to measurement. This means that already with $q = \mathcal{O}(\log N)$ the need for privacy amplification can be reduced to practically zero.

Theorem 5 *Let Alice and Bob use fully random G. Let $B \in \{0,1,2,3\}^N$ be a pseudorandom basis sequence as described above. Let Eve perform an arbitrary measurement on each qubit individually. Then she obtains no knowledge about B that she did not already have.*

Proof: Given the table T, knowledge about B is equivalent to knowledge about the row index J. Before the attack, Eve's ignorance is given by $\mathsf{H}_{\min}(J) = q$. The attack reduces it to $\mathsf{H}_{\min}(J|TR)$ where $R \in \{-1,+1\}^N$ is the sequence of measurement outcomes. We write θ_i, φ_i for the measurement parameters in position i. We have $\Pr[jtr] = \Pr[j]\Pr[t]\mathbb{E}_g\Pr[r|jtg]$, with $\mathbb{E}_g\Pr[r|jtg] = \prod_i \mathbb{E}_{g_i}\Pr[r_i|t_{ji}g_i] = \prod_i \mathbb{E}_{g_i}(\frac{1}{2} + \frac{r_i}{2} n_{\theta_i\varphi_i} \cdot n_{t_{ji}g_i}) = \prod_i(\frac{1}{2}+0) = 2^{-N}$. Hence $\Pr[jtr]$ is a constant, and $\Pr[j|tr] = \Pr[jtr]/\sum_j \Pr[jtr] = 1/Q$, yielding $\mathsf{H}_{\min}[J|TR] = q$. □

6.3 Pseudorandom G, random B

Theorem 6 *Let B be fully random and let G be pseudorandom as described in Section 6.1. Let Eve measure each individual qubit in one of the four u, w bases of her own choice, yielding a sequence R. Then Eve's knowledge about B can be upper bounded as*

$$\mathsf{H}_{\min}(B) - \mathsf{H}_{\min}(B|R\,\Gamma) \leq N \log\left(1 + \frac{1}{3 \cdot 2^{\ell/2-1}}\right) \tag{13}$$

and for each individual qubit the probability of causing $g_i' \neq g_i$ is $\frac{1}{3}$.

Proof: see Appendix D.

If Eve measures $3\delta N$ qubits, she learns $\approx 2\delta N 2^{-\ell/2}$ bits of information about B, i.e. exponentially small in the security parameter ℓ. Already with $\ell = \mathcal{O}(\log N)$ it is possible to reduce the leakage to such an extent that B can be re-used multiple times.

7 Discussion

We have modified Gottesman's unclonable encryption scheme by introducing the $|\psi_{000}\rangle$ and $|\psi_{001}\rangle$ states as the logical '0' and '1' state to be quantum-encrypted. This leads to the 8-state system as described in Section 4.1, with eight cipherstates that are maximally spread out over the Bloch sphere. The immediate result is that the perfect quantum-encryption prevents Eve from learning anything about the classical ciphertext, in contrast to the situation with the $+\times$ bases. At the same time the probability that eavesdropping causes a disturbance increases from $\frac{1}{4}$ to $\frac{1}{3}$. Due to the reduction of Eve's knowledge, the scheme's need for privacy amplification is reduced (even to zero in the case of non-reused random B) which in turn allows for more error correction.

Gottesman identified the implications *quantum authentication* $\Longrightarrow$ *unclonable encryption* $\Longrightarrow$ *QKD* [16]. Our improvement makes unclonable encryption much more practical; perhaps this has implications for QKD variants with reduced interaction.

In Section 6 we have analysed a number of non-adaptive qubit-by-qubit intercept-resend attacks on the 8-state scheme in the case of *pseudo*random G or B. While these analyses give insight into the rate of key leakage, they are of course not security proofs. More formal analysis is left for future work.

Acknowledgments

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

A Proof of Theorem 2

In abbreviated notation we write $\Pr[g|tr] = \mathbb{E}_j\Pr[g|tjr]$ where j is the random row index in the table t. Knowledge of t and j implies knowledge of b; we use Lemma 1 and obtain $\Pr[g|tr] = \mathbb{E}_j\Pr[r|gtj]$. Next we make use of $\Pr[r_i|g_ib_i] = \frac{1}{2} + \frac{r_i}{2}\boldsymbol{n}_{b_ig_i} \cdot \boldsymbol{n}_{\theta\varphi}$ and (7) with $\theta = 0$, which gives

$\Pr[g|tr] = \mathbb{E}_j \prod_{i=1}^{N} (\frac{1}{2} + \frac{1}{2\sqrt{3}}(-1)^{g_i + r_i + w_{ji}})$. Here the notation $w_{ji} \in \{0,1\}$ stands for the w-part of the basis t_{ji}, i.e. $w_{ji} = t_{ji} \mod 2$. Now we define $\boldsymbol{w}_i \in \{0,1\}^Q$ as the i'th column of w, and $\nu(\boldsymbol{w}_i) \in \{0,1\}$ as the most frequent symbol in $\boldsymbol{w}_i$. Then the sequence g^* that maximizes $\Pr[g|tr]$ is given by $g_i^* = r_i \oplus \nu(\boldsymbol{w}_i)$ and we obtain

$$\max_g \Pr[g|tr] = \mathbb{E}_j \prod_{i=1}^{N} [\tfrac{1}{2} + \tfrac{1}{2\sqrt{3}}(-1)^{\nu(\boldsymbol{w}_i) + w_{ji}}]. \tag{14}$$

The dependence on r has vanished. Averaging over t and r is now equivalent to averaging over w. Since all the elements of w are generated independently, everything factorizes and we get

$$\mathbb{E}_{tr} \max_g \Pr[g|tr] = \mathbb{E}_j \prod_{i=1}^{N} [\tfrac{1}{2} + \tfrac{1}{2\sqrt{3}} \mathbb{E}_{\boldsymbol{w}_i} (-1)^{\nu(\boldsymbol{w}_i) + w_{ji}}]. \tag{15}$$

We write $\mathbb{E}_{\boldsymbol{w}_i} \to \mathbb{E}_{w_{ji}} \mathbb{E}_{\nu(\boldsymbol{w}_i)|w_{ji}}$ where w_{ji} is uniform. The $\nu(\boldsymbol{w}_i)$ conditioned on w_{ji} has a cumulative binomial distribution: $\Pr[\nu(\boldsymbol{W}_i) = 0 | W_{ji} = w_{ji}] = \sum_{a=0}^{\lfloor Q/2 \rfloor - w_{ji}} \binom{Q-1}{a} (\frac{1}{2})^{Q-1}$. We get

$$\begin{aligned}
\mathbb{E}_{w_{ji}} \mathbb{E}_{\nu(\boldsymbol{w}_i)|w_{ji}} (-1)^{\nu(\boldsymbol{w}_i) + w_{ji}} &= \tfrac{1}{2} \left(\Pr[\nu(\boldsymbol{W}_i) = 0 | W_{ji} = 0] - \Pr[\nu(\boldsymbol{W}_i) = 1 | W_{ji} = 0] \right) \\
&\quad - \tfrac{1}{2} \left(\Pr[\nu(\boldsymbol{W}_i) = 0 | W_{ji} = 1] - \Pr[\nu(\boldsymbol{W}_i) = 1 | W_{ji} = 1] \right) \\
&= \Pr[\nu(\boldsymbol{W}_i) = 0 | W_{ji} = 0] - \Pr[\nu(\boldsymbol{W}_i) = 0 | W_{ji} = 1] \\
&= \binom{Q-1}{\lfloor Q/2 \rfloor} (\tfrac{1}{2})^{Q-1}.
\end{aligned} \tag{16}$$

The final expression follows by using Stirling's approximation $n! \approx \sqrt{2\pi n}(n/e)^n$ and $Q = 2^{2q}$.
Disturbance probability. Each of the eight states has projection probabilities $\frac{1}{2} \pm \frac{1}{2\sqrt{3}}$ onto the $\pm z$ state. Then $\Pr[G_i' = g_i] = (\frac{1}{2} + \frac{1}{2\sqrt{3}})^2 + (\frac{1}{2} - \frac{1}{2\sqrt{3}})^2 = 2(\frac{1}{4} + \frac{1}{12}) = \frac{2}{3}$. □

B Proof of Theorem 3

We write $R \in \{0,1\}^N$. From Lemma 1 and (6) we get $\Pr[g_i|tjr_i\lambda_i] = \delta_{\lambda_i t_{ji}} \delta_{r_i g_i} + (1 - \delta_{\lambda_i t_{ji}})(\frac{1}{3}\delta_{r_i g_i} + \frac{2}{3}[1 - \delta_{r_i g_i}])$. We introduce tally variables $\tau_{ia} = \sum_{j=1}^{Q} \delta_{t_{ji} a}$ and write $\Pr[g_i|tr_i\lambda_i] = \mathbb{E}_j \Pr[g_i|tjr_i\lambda_i]$ $= (\tau_{i\lambda_i}/Q)\delta_{r_i g_i} + (1 - \tau_{i\lambda_i}/Q)(\frac{1}{3}\delta_{r_i g_i} + \frac{2}{3}[1 - \delta_{r_i g_i}])$. From this expression we see, after some reshuffling, that $\max_{g_i} \Pr[g_i|tr_i\lambda_i] = \frac{1}{2} + \frac{2}{3}|\tau_{i\lambda_i}/Q - \frac{1}{4}|$, which yields $\max_g \Pr[g|tr\lambda] = \prod_i (\frac{1}{2} + \frac{2}{3}|\tau_{i\lambda_i}/Q - \frac{1}{4}|)$. The dependence on r has vanished. Taking the expectation over t reduces to taking the expectation over $\tau_{i\lambda_i}$ for each column of t independently, $\mathbb{E}_{tr\lambda} \max_g \Pr[g|tr\lambda] = \mathbb{E}_\lambda \prod_i (\frac{1}{2} + \frac{2}{3}\mathbb{E}|\tau_{i\lambda_i}/Q - \frac{1}{4}|) \le \mathbb{E}_\lambda \prod_i (\frac{1}{2} + \frac{2}{3}\sqrt{\mathbb{E}|\tau_{i\lambda_i}/Q - \frac{1}{4}|^2}) = \mathbb{E}_\lambda \prod_i (\frac{1}{2} + \frac{2}{3}\sqrt{\frac{1}{4} \cdot \frac{3}{4}}/\sqrt{Q}) = (\frac{1}{2} + \frac{1}{2\sqrt{3}}/\sqrt{Q})^N$. Here we have made use of Jensen's inequality and of the fact that the tallies are binomial-distributed. Note that the result also holds for fixed λ independent of T.
Disturbance probability. With probability $\frac{1}{4}$ the correct basis is chosen, which results in 100% probability of having $g_i' = g_i$. With probability $\frac{3}{4}$ the wrong basis is chosen, resulting in a probability distribution $(\frac{1}{3}, \frac{2}{3})$ for Eve's measurement, and $\Pr[G_i' = g_i] = (\frac{1}{3})^2 + (\frac{2}{3})^2 = \frac{5}{9}$. Overall $\Pr[G_i' = g_i] = \frac{1}{4} \cdot 1 + \frac{3}{4} \cdot \frac{5}{9} = \frac{2}{3}$. □

C Proof of Theorem 4

We write $R \in \{0,1\}^N$. From Lemma 1 and (6) we get $\Pr[g_i|tjr_i] = \delta_{\beta_i t_{ji}} \delta_{r_i g_i} + (1 - \delta_{\beta_i t_{ji}})(\frac{1}{3}\delta_{r_i g_i} + \frac{2}{3}[1 - \delta_{r_i g_i}])$. We introduce the notation $\lambda_i = \sum_{j=1}^{Q} \delta_{\beta_i t_{ji}}$ for the number of entries in the i'th column of t that equal β_i, the most frequent value. This allows us to write $\Pr[g_i|tr_i] = \mathbb{E}_j \Pr[g_i|tjr_i] = \frac{\lambda_i}{Q}\delta_{r_i g_i} + \frac{Q - \lambda_i}{Q}(\frac{1}{3}\delta_{r_i g_i} + \frac{2}{3}[1 - \delta_{r_i g_i}]) = \delta_{r_i g_i}(\frac{1}{3} + \frac{2}{3} \cdot \frac{\lambda_i}{Q}) + (1 - \delta_{r_i g_i})\frac{2}{3}(1 - \frac{\lambda_i}{Q})$. Since $\lambda_i \ge Q/4$ by definition, the first term satisfies $\frac{1}{3} + \frac{2}{3} \cdot \frac{\lambda_i}{Q} \ge \frac{1}{2}$ and we have $\max_{g_i} \Pr[g_i|tr_i] = \frac{1}{3} + \frac{2}{3} \cdot \frac{\lambda_i}{Q}$

and $\max_g \Pr[g|tr] = \prod_{i=1}^{N}(\frac{1}{3} + \frac{2}{3} \cdot \frac{\lambda_i}{Q})$ which is independent of r. Taking the expectation over r and t is then equivalent to N independent expectations over λ_i, yielding $\mathbb{E}_{tr} \max_g \Pr[g|tr] = \prod_{i=1}^{N}(\frac{1}{3} + \frac{2}{3Q}\mathbb{E}\lambda_i) = (\frac{1}{3} + \frac{2}{3Q}\mathbb{E}\lambda_i)^N$. In the last step we used that all the entries of t are drawn independently. The index i in the last expression is arbitrary. We can now write $\mathsf{H}_{\min}(G|TR) = -\log \mathbb{E}_{tr} \max_g \Pr[g|tr] = -N \log(\frac{1}{3} + \frac{2}{3Q}\mathbb{E}\lambda_i)$.

Finally we have to bound $\mathbb{E}\lambda_i$. We write $\Pr[\lambda_i > \frac{Q}{4} + \kappa\sqrt{Q}] \leq 4\Pr[\text{binomial}(Q, \frac{1}{4}) > \frac{Q}{4} + \kappa\sqrt{Q}] \leq 4\exp(-2\kappa^2)$, where in the last step we used Hoeffding's inequality. We introduce the notation $P_\lambda = \Pr[\lambda_i = \lambda]$, $\lambda \in \{\frac{Q}{4}, \ldots, Q\}$ and $\lambda_* = \frac{Q}{4} + \kappa\sqrt{Q}$ We have

$$\begin{aligned}
\mathbb{E}\lambda_i &= \sum_{\lambda=Q/4}^{Q} \lambda P_\lambda = \sum_{\lambda=Q/4}^{\lambda_*} \lambda P_\lambda + \sum_{\lambda=\lambda_*+1}^{Q} \lambda P_\lambda \\
&< \lambda_* \sum_{\lambda=Q/4}^{\lambda_*} P_\lambda + Q \sum_{\lambda=\lambda_*+1}^{Q} P_\lambda = \lambda_* + (Q - \lambda_*)\Pr[\lambda_i > \lambda_*] \\
&\leq \lambda_* + (Q - \lambda_*)4e^{-2\kappa^2} = \tfrac{Q}{4} + \kappa\sqrt{Q} + (3Q - 4\kappa\sqrt{Q})e^{-2\kappa^2} \\
&< \tfrac{Q}{4} + \kappa\sqrt{Q} + 3Qe^{-2\kappa^2}. \qquad (17)
\end{aligned}$$

We set $\kappa^2 = \frac{1}{2}\ln(3\sqrt{Q})$ yielding $\mathbb{E}\lambda_i < \frac{Q}{4} + \sqrt{Q}\{1 + \sqrt{\frac{1}{2}\ln(3\sqrt{Q})}\}$.

Disturbance probability. As in the random-basis attack, we have $\Pr[G'_i = g_i|tj] = \delta_{\beta_i t_{ji}} + (1 - \delta_{\beta_i t_{ji}})\frac{5}{9}$. This yields $\Pr[G'_i = g_i|t] = \mathbb{E}_j \Pr[G'_i = g_i|tj] = \lambda_i/Q + (1 - \lambda_i/Q)\frac{5}{9}$ and $\Pr[G'_i = g_i] = \mathbb{E}_t \Pr[G'_i = g_i|t] = \frac{5}{9} + \frac{4}{9Q}\mathbb{E}\lambda_i$. We use the above given bound on $\mathbb{E}\lambda_i$. □

D Proof of Theorem 6

We write $R \in \{0,1\}^N$. We have $\mathsf{H}_{\min}(B|R\Gamma) = -\log \mathbb{E}_{r\gamma} \max_b \Pr[b|r\gamma] = -\log \mathbb{E}_{r\gamma} \max_b \frac{\Pr[b]\Pr[\gamma]\Pr[r|\gamma b]}{\Pr[r\gamma]}$ $= -\log(\frac{1}{4})^N \mathbb{E}_\gamma \sum_r \max_b \Pr[r|\gamma b] = \mathsf{H}_{\min}(B) - \log \mathbb{E}_\gamma \sum_r \max_b \Pr[r|\gamma b]$, with $\max_b \Pr[r|\gamma b] = \max_b \mathbb{E}_v \prod_i \Pr[r_i|\gamma_{vi} b_i]$. The v is a row index that applies to all columns of γ at the same time. If we were allowed to choose a separate row index v_i in each column, then we would have more freedom to select large numbers. Hence $\max_b \mathbb{E}_v \prod_i \Pr[r_i|\gamma_{vi} b_i] \leq \max_b \prod_i \mathbb{E}_{v_i} \Pr[r_i|\gamma_{v_i i} b_i]$. This inequality yields $\mathsf{H}_{\min}(B) - \mathsf{H}_{\min}(B|R\Gamma) \leq \log \prod_i \mathbb{E}_{\gamma_i} \sum_{r_i} \max_{b_i} \mathbb{E}_{v_i} \Pr[r_i|\gamma_{v_i i} b_i]$. We introduce the notation μ_i for the number of '1' symbols in the i'th column of γ. We have $\mathbb{E}_{v_i} \Pr[r_i|\gamma_{v_i i} b_i] = \frac{\mu_i}{L}\Pr[r_i|1 b_i] + (1 - \frac{\mu_i}{L})\Pr[r_i|0 b_i]$. Depending on b being equal to Eve's basis or not, this expression takes either of the two following values: $\frac{\mu_i}{L}\delta_{r_i 1} + (1 - \frac{\mu_i}{L})\delta_{r_i 0}$ or $\frac{\mu_i}{L}(\delta_{r_i 1}\frac{1}{3} + \delta_{r_i 0}\frac{2}{3}) + (1 - \frac{\mu_i}{L})(\delta_{r_i 0}\frac{1}{3} + \delta_{r_i 1}\frac{2}{3})$ respectively. After some algebra this yields $\sum_{r_i} \max_{b_i} \mathbb{E}_{v_i} \Pr[r_i|\gamma_{v_i i} b_i] = 1 + \frac{4}{3L}|\mu_i - L/2|$. The expectation over γ_i reduces to an expectation over the binomial-distributed μ_i. We use Jensen's inequality to write $\mathbb{E}_{\mu_i}|\mu_i - L/2| \leq \sqrt{\mathbb{E}_{\mu_i}|\mu_i - L/2|^2} = \sqrt{L \cdot 1/4}$.

Disturbance probability. Since B is random, the probability of projecting from $\boldsymbol{n}_{b_i g_i}$ to either of Eve's basis states and back to $\boldsymbol{n}_{b_i g_i}$ is given by: $0^2 + 1^2 = 1$ if Eve chose the correct basis; $(\frac{1}{3})^2 + (\frac{2}{3})^2 = \frac{5}{9}$ if Eve chose the wrong basis. The overall probability of not causing a bit flip is $\frac{1}{4} \cdot 1 + \frac{3}{4} \cdot \frac{5}{9} = \frac{2}{3}$. □

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.

[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 (FOCS)*, 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 *IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 547–553, 2000.

[13] B. Škorić. Quantum Readout of Physical Unclonable Functions. *International Journal of Quantum Information*, 10(1):1250001–1 – 125001–31, 2012.

[14] 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, Dec. 2014.

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

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

[17] C.H. Bennett, G. Brassard, and S. Breidbart. Quantum Cryptography II: How to re-use a one-time pad safely even if P=NP, 1982. Unpublished manuscript. `arxiv.org/abs/1407.0451`.