Quantum key distribution with combined conjugate coding and information overloading

Boris Škorić
b.skoric@tue.nl

Abstract

Current quantum key distribution schemes depend either on a form of conjugate coding or on the principle of putting more information into a quantum state than can possibly be read out with a measurement. We construct a scheme that combines both these approaches. It has the advantage that it needs less privacy amplification and hence can be operated at higher noise levels.

1 Introduction

1.1 Quantum Key Distribution

Quantum Key Distribution (QKD) was the first application of quantum physics in cryptography and is still the best known. QKD allows Alice and Bob to generate an unconditionally secure key of arbitrary length, provided that they have an authenticated two-way classical communication channel and a one-way quantum channel.
There are two main 'flavours' of QKD. In BB84 [1], the first ever QKD scheme, Alice encodes a random data bit in one out of two qubit bases. This is called *conjugate coding* [2]. Bob measures in a random basis and then tells Alice which basis that was. If the bases do not match, they discard the result; if the bases do match, Alice and Bob have a shared secret bit. An eavesdropper (Eve) is hindered by the fact that she does not know in which basis Alice and Bob are working; any qubit manipulation by Eve is likely to be noticed by Alice and Bob. There is a whole family of schemes that use the same principle [3, 4] but with a different Hilbert space and/or a different set of bases. (Continuous-variable schemes based on non-commuting observables [5, 6, 7, 8] also belong to this family.)
Another approach is Differential Phase Shift (DPS) encoding [9, 10, 11]. Here the basis is known, but Alice puts more information into the quantum state than any measurement can possibly extract. Bob extracts only a small random subset of Alice's data. On the one hand, this suffices for generating a random key; on the other hand, Eve is seriously hindered by the fact that she can not access all the data embedded in the quantum state. (Into this category we can also place Bennett's nonorthogonal states approach [12], since it too prevents reliable extraction of all information.) We will refer to this approach as *information overloading*.

For an overview of quantum cryptography beyond QKD we refer to [13].

1.2 Noise tolerance of QKD schemes

In this paper we look at the noise tolerance of QKD schemes in abstracto, not taking into account the physics of noise in any way. There are many sources of noise, e.g. particle source inefficiencies, detector inefficiencies, thermal noise, channel noise, misalignment, particle loss etcetera, but we will ignore these distinctions. Instead we will treat noise in a general way, namely as a nonzero probability β that a data bit sent by Alice is received incorrectly by Bob. Here we do not care about the dimension of the Hilbert space, or the number of qubits used to convey one classical bit;

we are not interested in the noise per qubit but only in the bit error rate β in the communicated classical bit.
For the BB84-like schemes there is a well known theoretical bound on the maximum key generation rate when a protocol allows bit error rate β, namely $1 - h(\beta) - 2\beta$. Here h stands for the binary entropy function, $h(\beta) = -\beta \log_2 \beta - (1-\beta)\log_2(1-\beta)$. The bound can be understood as follows. The expression $1 - h(\beta)$ is the maximum rate at which Alice can send information to Bob over a channel with noise parameter β. If Alice does n bit transmissions over the channel, the actual information conveyed is at most $n[1 - h(\beta)]$ bits. Typically the noise is dealt with by applying a classical error-correcting code or cascade method [14].
Since Alice and Bob run a protocol that allows some errors, the worst case assumption they have to make is that *all bit errors are caused by Eve*. Consider the following attack ("**Attack A**"). In a fraction 2β of all qubit transmissions, Eve steals the quantum state and sends a random state to Bob. Later she learns what basis Alice and Bob used, which allows her to learn with 100% accuracy the data encoded in the quantum state. Meanwhile, Bob receives random data, and consequently the bit error rate is $\frac{1}{2} \cdot 2\beta = \beta$, just enough to be tolerated. The result of this attack is that Alice and Bob are not alarmed and that Eve knows a fraction 2β of the codeword. In the worst case this implies that Eve knows a fraction 2β of the transmitted information. Alice and Bob account for this partial knowledge by applying *privacy amplification* to their secret, which shortens their secret, ideally by no more than a fraction 2β. The bound $1 - h(\beta) - 2\beta$ implies that key generation is impossible at bit error rates β larger than approximately 0.17.
The same bound holds for DPS-like protocols.[1] The attack is slightly different ("**Attack B**"). Eve again steals a fraction 2β of quantum states, but she does not actually do anything with them.[2] She feeds Bob states that contain random data. Bob extracts a subset of this random data and publishes the subset (but not its content). Being random[3], Eve's data causes an overall bit error rate of $\frac{1}{2} \cdot 2\beta = \beta$; and since Eve created the data she knows exactly what Bob has measured.

1.3 Contributions

We note that the class of DPS-like protocols is in a certain sense complementary to the BB84-like class. In the former, an intervention by Eve gives her knowledge of Bob's data. In the latter it's Alice's data. This leads us to the following proposal. **Use both techniques: conjugate coding as well as information overloading**. The combination achieves the best of both worlds. It prevents Eve from learning enough from intercepted states and at the same time prevents her from feeding known data to Bob.

- We pick the best DPS scheme known to us, Round-Robin DPS (RRDPS) [10], and the best conjugate coding scheme known to us, Unclonable Encryption (UE) [15]. We construct a combined QKD protocol by running RRDPS in randomly chosen UE bases.

- We present a security analysis of our new scheme, in terms of min-entropy loss. We study first Attack B and then Attack A.

  It turns out that Attack B is by far the most powerful. Even so, our scheme reduces the min-entropy loss, and in theory can even entirely eliminate the min-entropy loss in the (impractical) limit of large Hilbert spaces. The result is that QKD becomes possible at $\beta > 0.17$, in theory up to $\beta < 0.5$. We have to warn the reader that the numbers presented in the analysis of Attack B are subject to a conjecture whose validity we verified only for small Hilbert spaces.
  Our analysis of Attack A applies not only to the combined scheme but also to the original RRDPS scheme. We are not aware of any previous security analysis of RRDPS in terms of min-entropy.

[1] Refs. [10, 11] underestimate the strength of Attack B and erroneously claim noise tolerance up to $\beta = 0.5$.

[2] Eve can gain some information by doing an uninformed measurement. This reduces the key rate. However, Eve's knowledge can be made arbitrarily small by going to larger Hilbert spaces, and hence we do not discuss this technicality here.

[3] Eve's partial knowledge of Alice's state gives her some advantage in feeding Bob correct data. Again, this advantage can be made small and hence we do not discuss it here.

In Section 2 we briefly review the RRDPS scheme and the conjugate coding employed in Unclonable Encryption. In Section 3 we describe the proposed scheme and in Section 4 we do the analysis. Section 5 concludes with a short discussion of protocol variants and implementation.

2 Preliminaries

2.1 Notation

Random Variables (RVs) are denoted with capital letters, and their realisations in lowercase. Sets are denoted in calligraphic font. 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 $\mathbb{E}_x f(x) = \sum_{x\in\mathcal{X}} \Pr[X = x]f(x)$. 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 '$\oplus$'. 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. The notation '$\otimes$' denotes the tensor (Kronecker) product of vectors. We write $\mathbb{1}_N$ for the $N \times N$ identity matrix. The fully mixed state is denoted as $\tau_N = \frac{1}{N}\mathbb{1}_N$. In a Hilbert space of dimension larger than 2 we use the notation $|\underline{k}\rangle$ for the k'th basis state in the standard basis. The notation 'tr' stands for trace. We will make use of the Positive Operator Valued Measure (POVM) formalism.

2.2 The Sasaki-Yamamoto-Koashi scheme

Alice generates a random bitstring $a \in \{0,1\}^N$. She prepares the state

$$|\mu(a)\rangle = N^{-1/2} \sum_{k=0}^{N-1} (-1)^{a_k} |\underline{k}\rangle \tag{1}$$

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

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

Here $k+r$ should be understood as $k+r$ mod N. The result of the measurement $M^{(r)}$ on $|\mu(a)\rangle$ is an random integer $k \in \{0, \ldots, N-1\}$ and a bit s that equals $a_k \oplus a_{k+r}$. Bob announces k and r. Alice and Bob now have a shared secret bit $a_k \oplus a_{k+r}$.
The physical implementation [10] is a *pulse train*: a photon is split into N coherent pieces which are released at different, equally spaced, points in time. The phase $(-1)^{a_k \oplus a_{k+r}}$ is the relative phase of the field oscillation in the $(k+r)$'th pulse relative to the k'th. The measurement $M^{(r)}$ is an interference measurement where one path is delayed by r time units.
The security properties are intuitively understood as follows. A measurement in an N-dimensional Hilbert space can extract at most $\log N$ bits of information. The state $|\mu(a)\rangle$, however, contains $N-1$ candidates for becoming Alice and Bob's shared secret, which is a lot more than $\log N$. Eve can learn only a small fraction of the phase information. This information is of limited use to her because she cannot force Bob to select precisely those phases that she knows. (i) She connot force Bob to choose a specific value of r. (ii) Even if she feeds Bob a state of the form $|\alpha\rangle = (|\underline{\ell}\rangle + (-1)^u |\underline{\ell+r}\rangle)/\sqrt{2}$ where r accidentally equals Bob's r, then there is a $\frac{1}{2}$ probability that Bob's measurement yields $k \neq \ell$ (with random s).
For large N, Attack B is far more powerful than Attack A. In [10] experiments were reported with $N = 128$.

2.3 Unclonable Encryption

Unclonable Encryption (UE) [16, 17, 15] is a technique by which Alice can send a classical ciphertext through a quantum channel in such a way that either Bob or Eve receives the cipherstate, but not both. We briefly discuss the four qubit bases introduced in [15]. Eight-state UE applies the Quantum One Time Pad (QOTP) [18, 19, 20] to a specially chosen qubit basis: the logical '0' is represented as the vector $(1,1,1)^{\mathrm{T}}/\sqrt{3}$ on the Bloch sphere, and the logical '1' as the opposite point $(-1,-1,-1)^{\mathrm{T}}/\sqrt{3}$. QOTP encryption of a qubit needs two bits of key material. Let the encryption key be denoted as $(u,w) \in \{0,1\}^2$. The encryption operator is $E_{uw} = \sigma_x^w \sigma_z^u$. On the Bloch sphere, acting with σ_x on a state flips the signs of the y and z coordinates; similarly, σ_z flips the x and y signs. The eight states obtained in this way are located at the corners of a cube. Let the encoded data bit be denoted as $g \in \{0,1\}$. Then the eight points on the Bloch sphere are $\boldsymbol{n}_{uwg} = (-1)^g((-1)^u,(-1)^{u+w},(-1)^w)^{\mathrm{T}}/\sqrt{3}$, which in the 2-dimensional Hilbert space corresponds to the following cipherstates,

$$|\psi_{uwg}\rangle = (-1)^{g\overline{u}}(\sqrt{i})^g \cos\tfrac{\alpha}{2}|g \oplus w\rangle + (-1)^{u\overline{g}}(\sqrt{i})^{\overline{g}} \sin\tfrac{\alpha}{2}|\overline{g \oplus w}\rangle, \tag{3}$$

where α is defined as $\cos\alpha = 1/\sqrt{3}$. The coefficients in (3) are given by $\cos\frac{\alpha}{2} = \sqrt{\frac{1}{2} + \frac{1}{2\sqrt{3}}} \approx 0.888$ and $\sin\frac{\alpha}{2} = \sqrt{\frac{1}{2} - \frac{1}{2\sqrt{3}}} \approx 0.460$. The inner products between the cipherstates are given by

$$\begin{aligned} |\langle\psi_{u'w'g'}|\psi_{uwg}\rangle|^2 &= \tfrac{1}{2} + \tfrac{1}{2}\boldsymbol{n}_{u'w'g'} \cdot \boldsymbol{n}_{uwg} \\ &= \delta_{uu'}\delta_{ww'}\delta_{gg'} + (1-\delta_{uu'}\delta_{ww'})\Big[\delta_{gg'}\frac{1}{3} + (1-\delta_{gg'})\frac{2}{3}\Big]. \end{aligned} \tag{4}$$

It is well know that the QOTP applied to any qubit state perfectly hides the state. Hence, if Eve has $|\psi_{uwg}\rangle$ with (u,w) unknown to her, she cannot derive any information about g.

3 The proposed scheme

We will consider a pulse train consisting of N pulses, with $N = 2^n$, so that the RRDPS Hilbert space is equivalent to n qubits. These qubits will be QOTP'ed independently. Each RRDPS basis state enumerator $k \in \{0,\ldots,N-1\}$ can be represented as a bitstring $(k_j)_{j=0}^{n-1}$, $k_j \in \{0,1\}$. For $u \in \{0,1\}^n$, $w \in \{0,1\}^n$, $k \in \{0,\ldots,N-1\}$ we define

$$|u,w,k\rangle \stackrel{\text{def}}{=} \bigotimes_{j=0}^{n-1} |\psi_{u_j w_j k_j}\rangle \tag{5}$$

where the single-qubit states in the right-hand-side are as defined by (3).

Protocol steps

1. Alice randomly selects $u \in \{0,1\}^n$, $w \in \{0,1\}^n$ and $a \in \{0,1\}^N$.
2. Alice sends to Bob the state
$$|\nu(u,w,a)\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} (-1)^{a_k} |u,w,k\rangle. \tag{6}$$
3. Bob acknowledges receipt. He stores the received quantum state.
4. After receiving Bob's acknowledgement Alice announces u and w.
5. Bob randomly selects $r \in \{1,\ldots,N-1\}$. He performs a POVM measurement described by the following set of $2N$ operators,
$$M_{ks}^{(r,u,w)} = \frac{1}{2} \frac{|u,w,k\rangle + (-1)^s|u,w,k+r\rangle}{\sqrt{2}} \frac{\langle u,w,k| + (-1)^s\langle u,w,k+r|}{\sqrt{2}}, \tag{7}$$

$k \in \{0, \ldots, N-1\}$, $s \in \{0,1\}$. Here $k+r$ stands for the arithmetic operation $k+r$ mod N. If the transmitted state was not altered, the result of the measurement is a random k and a bit s that equals $a_k \oplus a_{k+r}$.

6. Bob announces r and k.

Alice and Bob now have a shared secret bit $a_k \oplus a_{k+r}$. The above procedure is repeated many times. Then the standard steps of information reconciliation (error correction) and privacy amplification are performed.
However, the need for privacy amplification is reduced compared to existing schemes, as we will show in the next section.

4 Security analysis

We consider the following attack scenario. Eve steals Alice's state $|\nu(u,w,a)\rangle$ and stores it. She chooses a state φ and sends $|\varphi\rangle$ to Bob.[4] When Alice has announced u and w, Eve does a measurement on $|\nu(u,w,a)\rangle$ in order to obtain information about a. After Bob has announced r and k, Eve has partial knowledge of Bob's measurement outcome s.
We study two properties of the proposed scheme in this scenario: Eve's knowledge about Bob's measurement results (Attack B) and her knowledge of Alice's data a (Attack A).
Note that we do not consider scenarios in which Eve's φ depends on the intercepted quantum state. At the moment when Eve has to concoct φ, the quantum state she holds is still perfectly QOTP-encrypted and reveals no information about a whatsoever.

4.1 Eve's knowledge about Bob's outcome s (Attack B)

The most conservative approach is to determine the min-entropy of S given that Eve knows U, W, R, K and Φ. Note that Φ is a classical random variable. Also note that although Eve knows U, W, R, K, the Φ is *independent* of all these variables since Eve has to choose Φ before she knows any of them. The conditional min-entropy is written as

$$\begin{aligned}
\mathsf{H}_{\min}(S|\Phi UWRK) &= -\log \mathbb{E}_{\varphi uwrk} \max_{s\in\{0,1\}} \Pr[s|\varphi uwrk] \\
&= -\log \mathbb{E}_{\varphi uwrk} \max_{s\in\{0,1\}} \frac{\Pr[ks|\varphi uwr]}{\Pr[k|\varphi uwr]} \\
&= -\log \mathbb{E}_{\varphi uwr} \sum_{k=0}^{N-1} \max_{s\in\{0,1\}} \Pr[ks|\varphi uwr]. \qquad (8)
\end{aligned}$$

In the last step we used that $\Pr[k|\varphi uwr]$ does not depend on s, and that $\mathbb{E}_{\varphi uwrk}(\cdots) = \mathbb{E}_{\varphi uwr} \sum_k \Pr[k|\varphi uwr](\cdots)$. Next we write

$$\begin{aligned}
\max_{s\in\{0,1\}} \Pr[ks|\varphi uwr] &= \max_{s\in\{0,1\}} \langle\varphi| M_{ks}^{(r,u,w)} |\varphi\rangle \\
&= \max_{s\in\{0,1\}} \frac{1}{4} \left| \langle\varphi|u,w,k\rangle + (-1)^s \langle\varphi|u,w,k+r\rangle \right|^2 \\
&= \frac{1}{4} \left| \langle\varphi|u,w,k\rangle \right|^2 + \frac{1}{4} \left| \langle\varphi|u,w,k+r\rangle \right|^2 \\
&\quad + \frac{1}{4} \max_{s\in\{0,1\}} (-1)^s \langle\varphi| \Big(|u,w,k\rangle\langle u,w,k+r| + |u,w,k+r\rangle\langle u,w,k| \Big) |\varphi\rangle \\
&= \frac{1}{4} \left| \langle\varphi|u,w,k\rangle \right|^2 + \frac{1}{4} \left| \langle\varphi|u,w,k+r\rangle \right|^2 \\
&\quad + \frac{1}{4} \left| \langle\varphi| \Big(|u,w,k\rangle\langle u,w,k+r| + |u,w,k+r\rangle\langle u,w,k| \Big) |\varphi\rangle \right|. \qquad (9)
\end{aligned}$$

[4] We use notation that distinguishes between a physical state $|\varphi\rangle$ and its mathematical description φ.

In the last step we used that the operator $(\cdots)$ is Hermitian, which implies that it has real expectation values. We note that $\sum_k |\langle\varphi|u,w,k\rangle|^2 = 1$ and $\sum_k |\langle\varphi|u,w,k+r\rangle|^2 = 1$. This yields the following expression for the min-entropy loss,

$$\begin{aligned}&\mathsf{H}_{\min}(S) - \mathsf{H}_{\min}(S|\Phi UWRK) \\ &\qquad = \log\left(1 + \frac{1}{2}\mathbb{E}_{\varphi uwr}\sum_{k=0}^{N-1}\left|\langle\varphi|\left(|u,w,k\rangle\langle u,w,k+r| + |u,w,k+r\rangle\langle u,w,k|\right)|\varphi\rangle\right|\right). \quad (10)\end{aligned}$$

Now we have to determine which strategy for choosing φ maximizes the min-entropy loss (10). Numerics for $n = 2$ and $n = 3$ indicate that states of the form $|\varphi\rangle = |\underline{b}\rangle = \bigotimes_{j=0}^{n-1}|b_j\rangle$ achieve the maximum. This leads us to the following conjecture,

Conjecture 4.1 *Setting $|\varphi\rangle = |\underline{b}\rangle$ for any $b \in \{0,\ldots,2^n-1\}$ maximizes the min-entropy loss (10).*

There are some heuristic arguments in support of the conjecture. We expect the optimal attack state $|\varphi\rangle$ to exhibit a large amount of symmetry, given all the symmetries in the problem. Indeed, the qubit basis states $|0\rangle$, $|1\rangle$ have the special property that they are maximally removed from the eight cipherstates $|\psi_{uwg}\rangle$ (3).
We work with Conjecture 4.1 and set $|\varphi\rangle = |\underline{0}\rangle = |0\rangle^{\otimes n}$. We obtain an expression for the min-entropy loss, as specified in Theorem 4.3 below.

Lemma 4.2

$$\langle\underline{0}|u,w,k\rangle\langle u,w,\ell|\underline{0}\rangle = \prod_{j=0}^{n-1}\left[\delta_{w_j k_j}\delta_{\ell_j k_j}\cos^2\tfrac{\alpha}{2} + (-1)^{w_j}\delta_{\ell_j\overline{k_j}}\sin\tfrac{\alpha}{2}\cos\tfrac{\alpha}{2} + \delta_{w_j\overline{k_j}}\delta_{\ell_j k_j}\sin^2\tfrac{\alpha}{2}\right]. \quad (11)$$

Proof: See Appendix A. □

Theorem 4.3 *Consider the QKD protocol as described in Section 3. If Eve replaces Alice's state by $|\underline{0}\rangle$, then Eve's knowledge about Bob's measurement outcome S is given by*

$$\mathsf{H}_{\min}(S) - \mathsf{H}_{\min}^{|\varphi\rangle=|\underline{0}\rangle}(S|UWRK) = \log\left(1 + \frac{(1+\sin\alpha)^n - 1}{2^n - 1}\right) \quad (12)$$

where $\sin\alpha = \sqrt{2/3} \approx 0.816$.

Proof: See Appendix B. □
Fig. 1 shows the min-entropy loss (12) as a function of n. Already at small n the loss is well below 1. (Note that bare RRDPS can routinely handle pulse trains with $n = 7$.) In order to push the loss towards zero, unrealistically large n is required.

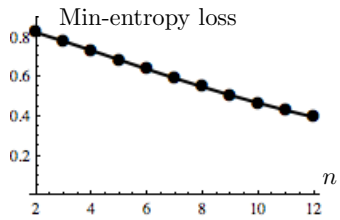

Figure 1: *Min-entropy loss as a function of n, the number of qubits. The length of the pulse train is $N = 2^n$.*

4.2 Eve's knowledge about Alice's secret bit (Attack A)

After Alice has revealed the QOTP key (u, w), Eve decrypts $|\nu(u, w, a)\rangle$ and obtains an ordinary RRDPS state in the $|\psi_{000}\rangle$, $|\psi_{001}\rangle$ qubit basis. From this point onward the analysis is the same as for RRDPS (Section 2.2) with $N = 2^n$. We switch to the standard basis for notational simplicity. We write $C = A_k \oplus A_{k+r}$. Eve knows k and r. Eve possesses the RRDPS state $|\mu(a)\rangle$,

$$|\mu(a)\rangle = \frac{1}{\sqrt{N}} \sum_{t=0}^{N-1} (-1)^{a_t} |\underline{t}\rangle \tag{13}$$

but she does not know a. We can define a mixed state $\rho^{(k,r)}$ for the classical random variable C and Eve's state as follows,

$$\rho^{(k,r)} = \sum_{c\in\{0,1\}} \tfrac{1}{2}|c\rangle\langle c| \otimes \rho_c^{(k,r)}, \quad \text{where} \quad \rho_c^{(k,r)} \stackrel{\text{def}}{=} \sum_{\substack{a\in\{0,1\}^N: \\ a_k\oplus a_{k+r}=c}} (\tfrac{1}{2})^{N-1} |\mu(a)\rangle\langle\mu(a)|. \tag{14}$$

There are 2^{N-1} strings a compatible with each possible c. The part of the quantum system held by Eve is denoted as ρ^{Eve}.

Lemma 4.4 *It holds that*

$$N\rho_0^{(k,r)} = \mathbb{1} + |\underline{k}\rangle\langle\underline{k+r}| + |\underline{k+r}\rangle\langle\underline{k}| \quad ; \quad N\rho_1^{(k,r)} = \mathbb{1} - |\underline{k}\rangle\langle\underline{k+r}| - |\underline{k+r}\rangle\langle\underline{k}|. \tag{15}$$

Proof: See Appendix C. □

From Lemma 4.4 it immediately follows that $\rho_0^{(k,r)} + \rho_1^{(k,r)} = 2\tau_N$ and $\operatorname{tr}\rho_c^{(k,r)} = 1$.

Corollary 4.5

$$\begin{aligned}
(N\rho_0^{(k,r)})^2 &= \mathbb{1} + 2|\underline{k}\rangle\langle\underline{k+r}| + 2|\underline{k+r}\rangle\langle\underline{k}| + |\underline{k}\rangle\langle\underline{k}| + |\underline{k+r}\rangle\langle\underline{k+r}| \\
(N\rho_1^{(k,r)})^2 &= \mathbb{1} - 2|\underline{k}\rangle\langle\underline{k+r}| - 2|\underline{k+r}\rangle\langle\underline{k}| + |\underline{k}\rangle\langle\underline{k}| + |\underline{k+r}\rangle\langle\underline{k+r}|.
\end{aligned} \tag{16}$$

Proof: Follows directly from Lemma 4.4. □

We follow the approach of [21] and express Eve's uncertainty about C, given the classical R, K and her mixed quantum state (ρ^{Eve}), as

$$\mathsf{H}_{\min}(C|RK\rho^{\text{Eve}}) = -\log \mathbb{E}_{rk} \max_{Q_0,Q_1} \mathbb{E}_c \operatorname{tr}\rho_c^{(k,r)} Q_c. \tag{17}$$

Here the operators Q_0, Q_1 form a POVM measurement set, satisfying the constraint $Q_0 + Q_1 = \mathbb{1}$. Furthermore Q_0 and Q_1 have to be positive semidefinite.

Theorem 4.6 *The entropy loss in C due to Eve's knowledge of R, K and her possession of the quantum state is*

$$\mathsf{H}_{\min}(C) - \mathsf{H}_{\min}(C|RK\rho^{\text{Eve}}) = \log(1 + \frac{2}{N}). \tag{18}$$

Proof: We omit the superscipts (k, r) for brevity. The maximisation in (17), using the Lagrange multiplier approach, yields the following system of equations [22],

$$\rho_0 Q_0 = \Lambda Q_0, \qquad \rho_1 Q_1 = \Lambda Q_1 \tag{19}$$

where Λ is the Lagrange multiplier for the constraint $Q_0 + Q_1 = \mathbb{1}$; it must be Hermitian and has to satisfy $\Lambda = \rho_0 Q_0 + \rho_1 Q_1$. Once the solution is found the min-entropy reduces to

$$\mathsf{H}_{\min}(C|RK\rho^{\text{Eve}}) = -\log \mathbb{E}_{rk} \tfrac{1}{2}\operatorname{tr}\Lambda = 1 - \log \mathbb{E}_{rk} \operatorname{tr}\Lambda. \tag{20}$$

It is readily verified that the solution is given by $Q_c = \frac{N}{2}\rho_c$ and

$$\Lambda = \frac{N}{2}(\rho_0^2 + \rho_1^2) = \frac{1}{N}\left(\mathbb{1} + |\underline{k}\rangle\langle\underline{k}| + |\underline{k+r}\rangle\langle\underline{k+r}|\right). \tag{21}$$

In the last line we made use of Corollary 4.5. We get $\operatorname{tr}\Lambda = \frac{N+2}{N}$. Substitution into (20) yields (18). □

Theorem 4.6 tells us that the RRDPS protocol is very good at hiding Alice's bits from Eve. The min-entropy loss per bit is only $\log(1 + \frac{2}{N}) < \frac{2}{N \ln 2}$.

5 Discussion

We have introduced a QKD scheme that combines conjugate coding with information overloading. The conjugate coding prevents Eve from reliably feeding Bob known data, while the information overloading prevents Eve from learning the data bits that Alice embeds into the quantum states. We have taken the eight-state encoding of qubits from Unclonable Encryption and combined it with the Round-Robin DPS scheme. The result is RRDPS run in a random UE basis which is afterward revealed to Bob.

From Theorems 4.3 and 4.6 we see that our scheme reduces the required amount of privacy amplification. (For small n we have verified Conjecture 4.1 numerically.) The main danger comes from Eve's (partial) ability to feed bits to Bob. The $\log(1+\frac{2}{N})$ is a small correction that has to be added to the min-entropy loss expression of Theorem 4.3. Let $\xi < 1$ denote the min-entropy loss per bit. Then the maximum key rate, which in other schemes equals $1-h(\beta)-2\beta$, is now given by

$$1-h(\beta)-2\beta\xi. \tag{22}$$

(In theory ξ can be made arbitrarily small by increasing n.) As a result, QKD can be operated at higher β than previously.

Many variations of our protocol can be thought of.

- If Bob is not able to store $|\nu(u,w,a)\rangle$ for very long (step 3), then there are at least two alternatives. (i) Alice does not wait for Bob's confirmation of receipt. She sends u,w after a fixed time interval. This variant requires that Bob knows exactly when to expect incoming quantum states and classical messages. He must store $|\nu(u,w,a)\rangle$ for a short time. (ii) The other alternative is that Bob immediately does the RRDPS measurement, but in a randomly chosen UE basis (u',w'). With probability $1/4^n$ he chooses the correct basis (u,w). All rounds with $(u',w') \neq (u,w)$ are discarded. This is very inefficient but possible. One could consider using a pseudorandom basis instead of fully random basis, in order to reduce the factor 4^n.
- A set of Mutually Unbiased Bases (MUBs) could yield a similar performance as the UE bases. Similarly, our choice of RRDPS as a building block may not be optimal; some other QKD scheme in the DPS class is perhaps better suited. This is left for future work.

We briefly comment on the physical implementation. We described quantum One Time Padding operations on qubits, whereas RRDPS works with a pulse train. The interpretation of the N-dimensional pulse train Hilbert space as a tensor product of n qubits is not very natural. It would be preferable to apply the QOTP in a way that is more compatible with the physics of pulse train handling. This is left for future work.

A Proof of Lemma 4.2

Let $u,w,k,\ell \in \{0,1\}$. From (3) we have $\langle 0|\psi_{uwk}\rangle = \delta_{wk}(-1)^{k\overline{u}}(\sqrt{i})^k \cos\frac{\alpha}{2} + \delta_{w\overline{k}}(-1)^{u\overline{k}}(\sqrt{i})^{\overline{k}}\sin\frac{\alpha}{2}$ and $\langle \psi_{uw\ell}|0\rangle = \delta_{w\ell}(-1)^{\ell\overline{u}}(\sqrt{-i})^{\ell}\cos\frac{\alpha}{2} + \delta_{w\overline{\ell}}(-1)^{u\overline{\ell}}(\sqrt{-i})^{\overline{\ell}}\sin\frac{\alpha}{2}$. The product $\langle 0|\psi_{uwk}\rangle\langle\psi_{uw\ell}|0\rangle$ is given by the following four terms which each represent a different 'case' concerning the (in)equalities between w, k and ℓ,

$$\begin{aligned} \delta_{wk}\delta_{w\ell}(-1)^{(k+\ell)\overline{u}}(\sqrt{i})^k(\sqrt{-i})^{\ell}\cos^2\tfrac{\alpha}{2} \quad &+ \quad \delta_{wk}\delta_{w\overline{\ell}}(-1)^{k\overline{u}+u\overline{\ell}}(\sqrt{i})^k(\sqrt{-i})^{\overline{\ell}}\cos\tfrac{\alpha}{2}\sin\tfrac{\alpha}{2} \\ +\delta_{w\overline{k}}\delta_{w\ell}(-1)^{u\overline{k}+\ell\overline{u}}(\sqrt{i})^{\overline{k}}(\sqrt{-i})^{\ell}\sin\tfrac{\alpha}{2}\cos\tfrac{\alpha}{2} \quad &+ \quad \delta_{w\overline{k}}\delta_{w\overline{\ell}}(-1)^{u(\overline{k}+\overline{\ell})}(\sqrt{i})^{\overline{k}}(\sqrt{-i})^{\overline{\ell}}\sin^2\tfrac{\alpha}{2}. \end{aligned} \tag{23}$$

In each term the Kronecker deltas conspire to make the powers of $\sqrt{i}$ and $\sqrt{-i}$ equal, which yields a power of $\sqrt{-i^2}=1$. Thus all the i's disappear and we are left with a real-valued expression. Furthermore, in the $\cos^2$ and $\sin^2$ terms the power of (-1) is even, which makes the sign equal to $+1$. In the $\cos\cdot\sin$ term we can write $k\overline{u}+u\overline{\ell}=w$, and in the $\sin\cdot\cos$ term we write $u\overline{k}+\ell\overline{u}=w$. Next we reorganise the Kronecker deltas as $\delta_{wk}\delta_{w\ell}=\delta_{wk}\delta_{\ell k}$ etc. The $\cos\cdot\sin$ and $\sin\cdot\cos$ terms

can then be combined using $\delta_{wk} + \delta_{w\overline{k}} = 1$. Finally, for $u, w \in \{0,1\}^n$, $k \in \{0, \ldots, 2^n - 1\}$ we use the factorisations $|u, w, k\rangle = \bigotimes_{j=0}^{n-1} |\psi_{u_j w_j k_j}\rangle$ and $|\underline{0}\rangle = |0\rangle^{\otimes n}$.

B Proof of Theorem 4.3

We have $\langle \underline{0}|u, w, k\rangle\langle u, w, \ell|\underline{0}\rangle = \langle \underline{0}|u, w, \ell\rangle\langle u, w, k|\underline{0}\rangle$. The addition in (10) yields a factor 2. Next, taking the absolute value of (11) is equivalent to taking the absolute value of each term individually, since the three terms correspond to mutually exclusive cases. Hence we have

$$|\langle \underline{0}|u, w, k\rangle\langle u, w, \ell|\underline{0}\rangle| = \prod_{j=0}^{n-1} \left[\delta_{w_j k_j}\delta_{\ell_j k_j} \cos^2 \tfrac{\alpha}{2} + \delta_{\ell_j \overline{k_j}} \sin \tfrac{\alpha}{2} \cos \tfrac{\alpha}{2} + \delta_{w_j \overline{k_j}}\delta_{\ell_j k_j} \sin^2 \tfrac{\alpha}{2}\right]. \tag{24}$$

Now we take the expectation $\mathbb{E}_w$ and use $\mathbb{E}_{w_j}\delta_{w_j k_j} = \frac{1}{2}$ and $\mathbb{E}_{w_j}\delta_{w_j \overline{k_j}} = \frac{1}{2}$. This yields

$$\mathbb{E}_w |\langle \underline{0}|u, w, k\rangle\langle u, w, \ell|\underline{0}\rangle| = 2^{-n} \prod_{j=0}^{n} [\delta_{\ell_j k_j} + \delta_{\ell_j \overline{k_j}} \sin \alpha]. \tag{25}$$

We put $\ell = k + r$ with $r \neq 0$. The operation $\mathbb{E}_r \sum_k (\cdots)$ is equivalent to $\frac{1}{2^n - 1} \sum_k \sum_{r=1}^{2^n - 1} (\cdots)$ $= \frac{1}{2^n - 1} [\sum_{k,\ell=0}^{2^n - 1} (\cdots) - \sum_{k,\ell=0}^{2^n - 1} \delta_{k\ell} (\cdots)]$. Applying this operation to (25) gives

$$\mathbb{E}_{rw} \sum_k |\langle \underline{0}|u, w, k\rangle\langle u, w, \ell|\underline{0}\rangle| = \frac{2^{-n}}{2^n - 1} \left[\prod_{j=0}^{n-1} (2 + 2\sin\alpha) - \prod_{j=0}^{n-1} 2\right] = \frac{(1 + \sin\alpha)^n - 1}{2^n - 1}. \tag{26}$$

C Proof of Lemma 4.4

From the definition of $|\mu(a)\rangle$ we get

$$\begin{aligned}
\rho_0^{(k,r)} &= (\tfrac{1}{2})^{N-1} \frac{1}{N} \sum_{t,z=0}^{N-1} |\underline{t}\rangle\langle \underline{z}| \sum_{\substack{a \in \{0,1\}^N : \\ a_k \oplus a_{k+r} = 0}} (-1)^{a_t + a_z} \\
&= (\tfrac{1}{2})^{N-1} \frac{1}{N} \sum_{t,z=0}^{N-1} |\underline{t}\rangle\langle \underline{z}| \left[\delta_{tz} 2^{N-1} + (\delta_{tk}\delta_{z,k+r} + \delta_{t,k+r}\delta_{zk}) 2^{N-1}\right] \qquad (27) \\
&= \frac{1}{N} \sum_{t=0}^{N-1} |\underline{t}\rangle\langle \underline{t}| + \frac{|\underline{k}\rangle\langle \underline{k+r}| + |\underline{k+r}\rangle\langle \underline{k}|}{N}. \qquad (28)
\end{aligned}$$

The derivation for ρ_1 is completely analogous.

References

[1] 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.

[2] S. Wiesner. Conjugate coding. *ACM SIGACT News - A special issue on cryptography*, 15:78–88, 1983.

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

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

[5] T.C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303, 1999.

[6] M. Hillery. Quantum cryptography with squeezed states. *Phys. Rev. A*, 61:022309, 2000.

[7] M.D. Reid. Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations. *Phys. Rev. A*, 62:062308, 2000.

[8] D. Gottesman and J. Preskill. Secure quantum key distribution using squeezed states. *Phys. Rev. A*, 63:022309, 2001.

[9] K. Inoue, E. Waks, and Y. Yamamoto. Differential phase shift quantum key distribution. *Phys. Rev. Lett.*, 89(3):037902,1–3, 2002.

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

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

[12] C.H. Bennett. Quantum cryptography using any two nonorthogonal states. *Pys. Rev. Lett.*, 68(21):3121–3124, 1992.

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

[14] G. Brassard and L. Salvail. Secret key reconciliation by public discussion. In *Eurocrypt*, pages 410–423, 1993.

[15] B. Škorić. Unclonable encryption revisited ($4 \times 2 = 8$). `https://eprint.iacr.org/2015/1221`, 2015.

[16] 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`.

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

[18] 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.

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

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

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

[22] A.S. Holevo. Statistical decision theory for quantum systems. *Journal of multivariate analysis*, 3:337–394, 1973.