Optimal attacks on Quantum Key Recycling with qubits

Daan Leermakers and Boris Škorić
d.leermakers.1@.tue.nl, b.skoric@tue.nl

Quantum communication differs significantly from classical communication. On a classical channel it is trivial to read and copy all messages. On a quantum channel, on the other hand, any form of eavesdropping is detectable. This fact has been exploited by cryptographers since the 1980s, most notably by the introduction of Quantum Key Distribution (QKD). However, even before the invention of BB84 another concept was studied: information-theoretically secure re-use of encryption keys. If Bob detects no disturbance on the quantum channel, it may be safe to re-use the encryption key, in stark contrast to e.g. One Time Pad (OTP) encryption on a classical channel. Although the idea of Quantum Key Recycling (QKR) was already proposed in 1982, until recently it received very little attention. Only at the start of this century new QKR schemes were proposed. A drawback of these schemes is that they require a quantum computer to perform encryption and decryption. In 2016 Fehr and Salvail [1] and Škorić and de Vries [2] returned to qubit-based schemes that do not require a quantum computer. In the latter, a QKR scheme based on 8-state encoding (four bases) was proposed.
The long neglect of QKR is undeserved. In a QKD-equipped world, QKR has an important role to play. The process of repeatedly generating new QKD keys for every classical OTP encryption is very wasteful of bandwidth. One QKD instance followed by repeated QKR runs is more communication-efficient.

In this work we prove the security of QKR protocols based on qubits encoded in 4-, 6- and 8-states. We determine the optimal attacks against individual qubits which has been shown to be sufficient to prove the security of the entire scheme [3]. We rely upon the proof technique for qubit-based QKR introduced in [1], which can directly be applied to the scheme of [2] provided that correct values are known for the required amount of privacy amplification as a function of the noise parameter β.

The 8-state encoding consists of the states:

$$|\psi_{uwg}\rangle = (-1)^{gu}\left[(-\sqrt{i})^g \cos\tfrac{\alpha}{2}|g\oplus w\rangle + (-1)^u(\sqrt{i})^{1-g}\sin\tfrac{\alpha}{2}|\overline{g\oplus w}\rangle\right]. \quad (1)$$

Here $g\in\{0,1\}$ is the encoded bit values and u,$w\in\{0,1\}$ describe the four possible encoding bases (keys). These states are in fact the Quantum One Time Pad encryptions applied to the (1,1,1) and (-1,-1,-1) directions on the Bloch sphere. This results in 8 possible states which can be represented as the corners of a cube on the Bloch sphere. Due to this even distribution over the Bloch sphere, the entropy-loss of an encrypted bit is zero, given that Eve does not know the encryption key. In the 4- and 6-state Eve can, by choosing a smart measurement, learn a non-zero amount about the message bit without knowing the key.

The key recycling scheme makes use of a Secure Sketch $S:\{0,1\}^n\to\{0,1\}^a$, with $a > nh(\beta)$. (Asymptotically a approaches $nh(\beta)$ with h the binary entropy function). Furthermore the scheme uses an extractor $\texttt{Ext}:\{0,1\}^n\to\{0,1\}^\ell$ and a message-independent, key-private [1] MAC function that produces a tag of length λ. The message is $\mu\in\{0,1\}^\ell$. The key material shared between Alice and Bob consists of three parts: a basis sequence $b\in\{0,1,2,3\}^n$, a MAC key $K_{\rm M}$ and a classical OTP $K_{\rm SS}\in\{0,1\}^a$ for protecting the secure sketch.

Encryption: Alice performs the following steps. Generate random $g \in \{0,1\}^n$. Compute $s = K_{\mathrm{SS}} \oplus S(g)$ and $z = \mathtt{Ext}\, g$. Compute the ciphertext $c = \mu \oplus z$ and authentication tag $T = M(K_{\mathrm{M}}, g||c||s)$. Prepare the quantum state $|\Psi\rangle = \bigotimes_{i=1}^{n} |\psi_{b_i g_i}\rangle$. Send $|\Psi\rangle$, s, c, T.
Decryption: (Bob gets $|\Psi'\rangle$, s', c', T'). Bob performs the following steps. Measure $|\Psi'\rangle$ in the b-basis. This yields $g' \in \{0,1\}^n$. Recover $\hat{g}$ from g' and $K_{\mathrm{SS}} \oplus s'$ (by the syndrome decoding procedure of the Secure Sketch primitive). Compute $\hat{z} = \mathtt{Ext}\, \hat{g}$ and $\hat{\mu} = c' \oplus \hat{z}$. Accept the message $\hat{\mu}$ if the syndrome decoding succeeded and $T' = M(K_{\mathrm{M}}, \hat{g}||c'||s')$. Communicate Accept/Reject to Alice.
Key update: If Bob Accepts, replace K_{SS}. If Bob Rejects, replace K_{SS} and compute the updated key b' as a function of b and n fresh secret bits.
In case of Bob accepting the transmission, an ℓ-bit message has been communicated while only $a \approx nh(\beta)$ bits of key material have been spent.

Attacks

In a QKR recycling scheme one has to protect the key as well as the message. When attacking the message there are two relevant scenarios: i) Eve steals an entire transmission and does an optimal measurement. With overwhelming probability the attack will be detected, but detecting the attack alone is not enough. Eve should in no case be able to learn the message; ii) Eve can couple each individual qubit to an ancilla introducing as much noise as possible without being detected. Since the same key will be used to encode different messages, she can do this for many qubits before finally doing a measurement on her ancillas.

When attacking the key, Eve can not afford to be detected since in that case the same key won't be used again. Again there exist two relevant attacks: i) She can steal a fraction 3β of the qubits entirely (where β is the maximum bit error rate Alice and Bob allow) and perform a optimal measurement on them; ii) She can couple each qubit to an ancilla, again introducing exactly noise β and perform the optimal measurement on her ancillas. In the worst case scenario, Eve already knows the plaintext when attacking the key. To guarantee that the key is protected, we have to therefore assume Eve has knowledge of the plaintext.

Main result

We determine the optimal attack on the 4-, 6- and 8-state protocols in terms of min-entropy as well as in terms of Shannon-entropy. When the number of qubits is very large, the relevant quantity to look at is Shannon entropy, for a small number of qubits it is min-entropy. In intermediate cases it is something in between. In the case of ancilla attacks we make use of the fact that the security of the protocol can be proven by analysing an EPR version of the protocol [4]. In this protocol Alice prepares an EPR pair and sends half of it to Bob while keeping the other half. Eve is allowed to manipulate the entire two-qubit system after which Alice and Bob perform some permutations to prevent Eve from attacking in a asymmetrical manner. Security of this EPR-version of the protocol implies security of the original protocol.

In terms of Shannon-entropy, an attack on the message provides Eve with the most information for all possible β. For the 4- and 6-state encodings, stealing the entire transmission is most effective at small β. At larger β values, it is more effective for Eve to couple each qubit to an ancilla for multiple consecutive messages. She can then do a measurement on her ancillas knowing the messages are protected by the same key. For the 8-state encoding, the latter attack is always the best since Eve does not learn anything from stealing an entire transmission since the 8-state provides a true encryption. When Eve extracts information out of many qubits, many bits are protected with

the same key bit. In the asymptotic limit the single key bit offers essentially no protection. The security of the protocol then reduces to the well known security of QKD. In QKD, Eve's strongest attack also uses the coupling to an ancilla after which she waits until she learns the basis (key) to perform a measurement on her ancilla [4]. This asymptotic equality provides an upper bound on the strength of the attack.

In terms of min-entropy, the optimal attack on the the 4- and 6-states protocols are the same attacks on the message as described above. The only difference is the optimal measurement Eve has to perform to extract the most information from the entire transmission or her ancillas. For the 8-state, the optimal attack for all β values is an ancilla attack on the key assuming Eve knows the plaintext. Figure 1 shows the QKR capacity $1 - h(\beta) - leakage$. Where in the case of Shannon-entropy we define the leakage as the mutual information and in the min-entropy case we define it as the min-entropy loss. In computing the mutual information and the min-entropy loss, the strongest attacks are used.

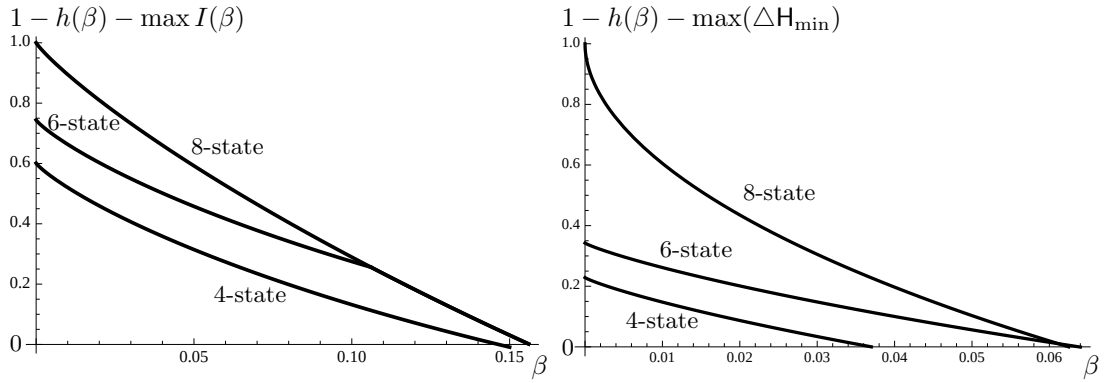

Figure 1: *QKR capacity as a function of the bit error rate β. Leakage is expressed as mutual information (left) and as min-entropy loss (right).*

We see that for low noise, the 8-state outperforms the 4- and 6-state encodings in terms of Shannon- as well as min-entropy. For larger values of β the 6- and 8-state encoding perform equally well in terms of Shannon-entropy. The 8-state always outperforms the 6-state in terms of min-entropy. The 6-state is always better than the 4-state. It is worth noting that since the security analysis in terms of Shannon-entropy reduces to the well known QKD analysis, the addition of artificial noise by Alice can further increase the capacity of the protocol.
Our results provide accurate bounds on the privacy amplification needed to do QKR in the case of noisy channels. The 8-state encoding is shown to provide the highest capacity. More details are provided in the full version [5].

References

[1] S. Fehr and L. Salvail. Quantum authentication and encryption with key recycling. In *Eurocrypt*, 2017. `https://arxiv.org/abs/1610.05614v1`.

[2] B. Škorić and M. de Vries. Quantum Key Recycling with eight-state encoding. (The Quantum One Time Pad is more interesting than we thought). *International Journal of Quantum Information*, 2017. `https://eprint.iacr.org/2016/1122`.

[3] R. Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3:645–649, 2007.

[4] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys.Rev.A*, 72:012332, 2005.

[5] D. Leermakers and B. Škorić. Optimal attacks on qubit-based quantum key recycling. 2017. `https://eprint.iacr.org/2017/331`.