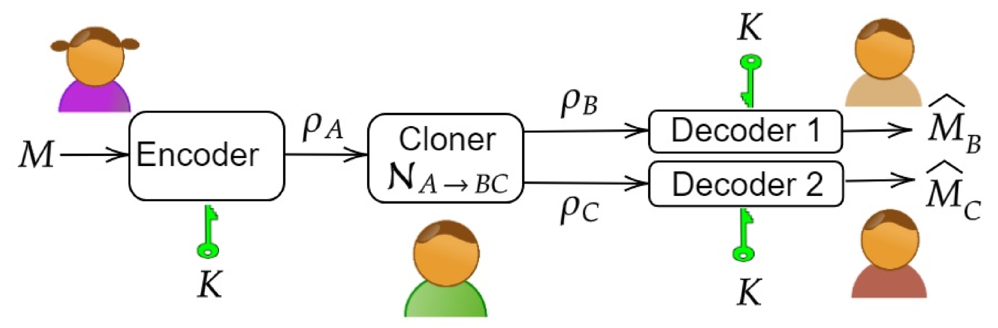
Limitations on Uncloneable Encryption and Simultaneous One-Way-to-Hiding

Christian Majenz, Christian Schaffner, Mehrdad Tahmasbi
QuSoft, Amsterdam, Netherlands

QuSoft
Research Center for Quantum Software

1. Uncloneable Encryption: Introduction

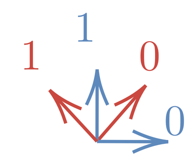
Goal: Devise symmetric-key encryption/decryption algorithms such that an adversary cannot create two copies of the ciphertext from which the message can be decoded using key
Quantum encryption of classical messages (QECM): Alice encrypts classical message m into *quantum* ciphertext $\mathsf{Enc}_k(m)$ using classical key k
Cloning attack: 1) Eve clones ciphertext using quantum channel $\mathcal{N}_{A\to BC}$. 2) Eve provides each part to two separated parties, Bob and Charlie, who receive the key k. 3) Bob and Charlie a attempt to guess the message m
The adversaries win if and only if Bob and Charlie both correctly decrypt the message.



2. Two Constructions

Two uncloneable encryption schemes are studied in [2]

- **Construction 1**: Alice encodes n bits using n bits of key, which specify the BB84 bases in which the message bits are encoded. The optimal probability of winning for the adversaries is $\left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)^n$



- **Construction 2**: Let $m \in \{0,1\}^n$ be the message.Alice, Bob, and Charlie have quantum access to a random oracle $H : \{0,1\}^\lambda \to \{0,1\}^n$. Alice encodes a random string x of λ bits similar to Construction 1 and transmits it together with $H(x) \oplus m$. The optimal probability of winning is upper-bounded by $\frac{9}{M} + \mathrm{negl}(\lambda)$

3. Uncloneable-Indistinguishable Security

Uncloneable-Indistinguishable attack: Message chosen uniformly to be either an adversarially chosen message or a default one

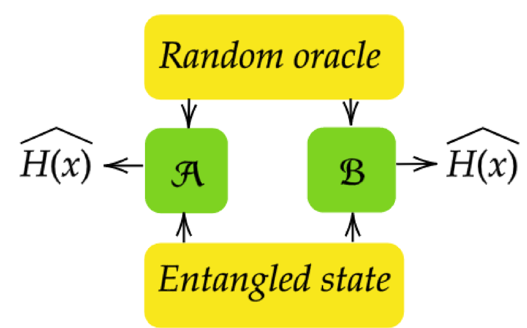
Theorem 1 *For any correct QECM scheme, and arbitrary default message m_0, there exists an uncloneable-indistinguishable attack for which the adversary wins with probability at least*

$$\frac{1}{2} + \frac{\max_{m\in\mathcal{M}} \mathbb{E}_{k\sim P_K}(\|\mathsf{Enc}_k(m))\|)}{16} \tag{1}$$

- When probability of success for all attacks is $\frac{1}{2} + \mathrm{negl}(\lambda)$ (as desired in [2, Definition 11]), $\max_{m\in\mathcal{M}} \mathbb{E}_{k\sim P_K}(\|\mathsf{Enc}_k(m))\|)$ should be negligible
- We use the "cloning operation" $V_{A\to BC} : |\phi\rangle \mapsto \frac{1}{\sqrt{2}}(|\bot\rangle_B \otimes |\phi\rangle_C + |\phi\rangle_B \otimes |\bot\rangle_C)$ where $|\bot\rangle$ is a unit vector orthogonal to A, which intuitively speaking distributes the input state in A to B and C "in superposition."

4. Simultanuous O2H Lemma

Simultanuous O2H Lemma We run quantum algorithms $\mathcal{A}$ and $\mathcal{B}$ with quantum oracle access to random function $H : \mathcal{X} \to \{0,1\}^n$ and access to shared entanglement.
The probability that both algorithms correctly output $H(x)$ for a fixed x is upper-bounded by $9 \times 2^{-n} + \mathrm{poly}(q_\mathcal{A}, q_\mathcal{B})\sqrt{p}$
$q_\mathcal{A}$ and $q_\mathcal{B}$: number of queries made by $\mathcal{A}$ and $\mathcal{B}$, respectively,
p: probability that measuring the input registers of both algorithms at two independently chosen queries returns x on both sides.
Question: is the factor 9 an artifact of the proof technique used in [2], or whether a probability of success of $2^{-n} + \mathrm{poly}(q_\mathcal{A}, q_\mathcal{B})\sqrt{p}$ is possible?



Theorem 2 *There exists an example with $p = 0$ (so simultaneous query-based extraction never succeeds), $\mathcal{X} = \{0,1\}$ and $n = 1$ but $\mathcal{A}$ and $\mathcal{B}$ both output $H(0)$ with probability 9/16, which is strictly larger than the trivial $\frac{1}{2}$.*

5. Optimal Scheme

Question: for a uniformly distributed message over a fixed set and a fixed ciphertext space A, which QECM scheme minimizes the optimal probability of winning?

Theorem 3 *The optimal QECM scheme is as follows.*

1. *Alice independently samples $T = (t_1, \cdots, t_M)$ which is a permutation-invariant random vector such that $\sum_m t_m = d$ and random unitary U distributed according to Haar measure.*
2. *For encryption of message m, Alice chooses a fixed subspace of dimension t_m, prepares the maximally mixed state on that subspace, and then applies the unitary operation U.*

We conjecture that a deterministic $T = (d/M, \cdots, d/M)$ that splits the space evenly is optimal.

6. Uniformly Distributed Message

When the message is uniformly distributed over all messages, we prove the following lower-bound on the optimal winning probability for the adversaries.

Theorem 4 *Consider a correct QECM scheme satisfying the following conditions:*

1. *The key is uniformly distributed over a finite set.*
2. *All ciphertexts are maximally mixed states over sub-spaces of fixed size.*

Then the adversaries can win the cloning game with probability at least $\Omega\left(\sqrt{\frac{\log|\mathcal{M}|}{|\mathcal{M}||A|}}\right)$.

7. Open Questions

- Does exist a sequence of QECMs $\{\mathcal{E}_\lambda\}_{\lambda\in\mathbb{N}}$ such that

$$\lim_{\lambda\to\infty} \mathrm{p}^*_{\text{win-ind}}(\mathcal{E}_\lambda) = \frac{1}{2} \text{ or } \lim_{\lambda\to\infty} |\mathcal{M}_\lambda|\, \mathrm{p}^*_{\text{win-unif}}(\mathcal{E}_\lambda) = 1. \tag{2}$$

- Does our conjecture for the optimal scheme hold?
- What is the optimal constant infront of 2^{-n} in the simultaneous O2H lemma?

8. References

[1] Christian Majenz, Christian Schaffner, and Mehrdad Tahmasbi. Limitations on uncloneable encryption and simultaneous one-way-to-hiding, 2021.

[2] Anne Broadbent and Sébastien Lord. Uncloneable Quantum Encryption via Oracles. In *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020).*