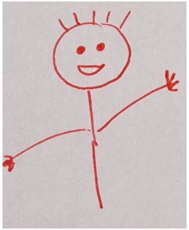
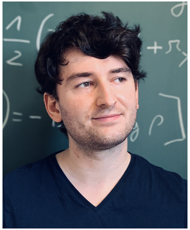
The Quantum No-Cloning Game

Pierre Botteron
(Toulouse, Wednesday January 24, 2024.)

Ongoing Work with...

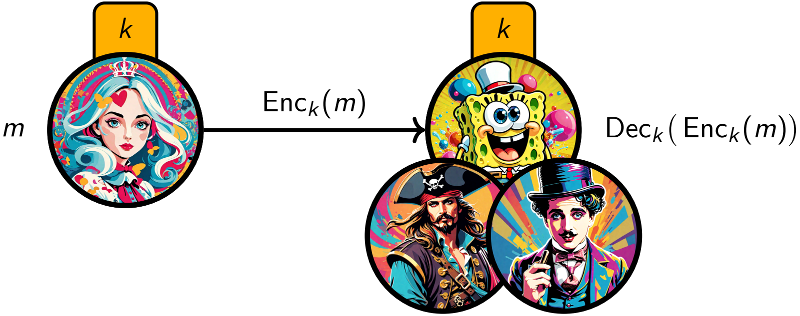
				
Anne Broadbent (Ottawa)	Eric Culf (Waterloo)	Ion Nechita (Toulouse)	Clément Pellegrini (Toulouse)	Denis Rochette (Ottawa)

Contents

— *Part* 1 —

The Scenario

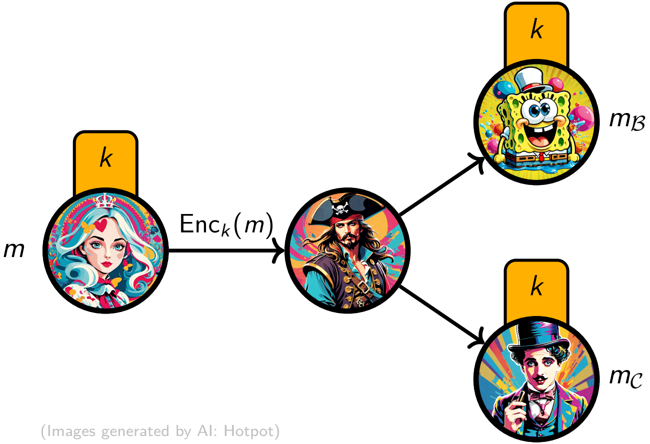
A Love Story...



Correctness: $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) \overset{a.s.}{=} m.$

(Images generated by AI: Hotpot)

The No-Cloning Game



(Images generated by AI: Hotpot)

- **Rule:** $\mathcal{P}, \mathcal{B}, \mathcal{C}$ win iff. $m = m_{\mathcal{B}} = m_{\mathcal{C}}$.
- If $\mathsf{Enc}_k(m)$ is classical, then $\mathbb{P}(\mathcal{P}, \mathcal{B}, \mathcal{C} \text{ win}) = 1$. So we are interested in $\mathsf{Enc}_k(m) \in \mathcal{D}(\mathbb{C}^d)$ quantum state.
- If $m \in \{0,1\}^n$ and $\mathcal{P}$ sends a uniformly random message $m_{\mathcal{B}} = m_{\mathcal{C}}$ to $\mathcal{B}, \mathcal{C}$, then $\mathbb{P}(\mathcal{P}, \mathcal{B}, \mathcal{C} \text{ win}) = 1/2^n = 0.5^n$.
- **Problem:** Find an encryption scheme for Alice that is “secure”.

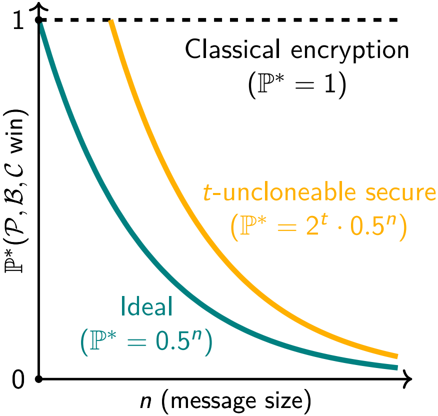
Uncloneable Security[1]

Definition. The encryption scheme Enc_k is said to be **$t(\lambda)$-uncloneable secure**, with $0 \leq t(\lambda) \leq n$, if the optimal winning probability is "almost" the random one:

$$\mathbb{P}^*(\mathcal{P}, \mathcal{B}, \mathcal{C} \text{ win}) \leq 2^{t(\lambda)} \cdot 0.5^n + \text{negl.}(\lambda)\,,$$

where $\lambda \in \mathbb{N}$ is the security parameter, and n is the size of the message m.

Remarks.
- $t = 0$ is ideal.
- $t = n$ is trivial.



[1] Broadbent and Lord. *Uncloneable Quantum Encryption via Oracles*. 2020.

— *Part* 2 —

Known Results

Open Question

- Gottesman[2] introduced a scheme that detects if an adversary could have had information about the plaintext when it was ecnrypted.

- **Open Question.** Is it possible to find an ecryption scheme that would prevent the splitting of a ciphertext?

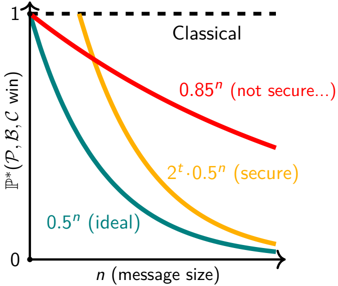
[2] Gottesman. "Uncloneable Encryption". In: *Quantum Info. Comput.* (2003).

Attempt Without Assumption

Encryption scheme: $\mathcal{A}$ encrypts her message $m \in \{0,1\}^n$ in a Wiesner state $|m^k\rangle := H^{k_1}|m_1\rangle \otimes \cdots \otimes H^{k_n}|m_n\rangle$, with a key $k \in \{0,1\}^n$:

$$\mathsf{Enc}_k(m) := |m^k\rangle\langle m^k| .$$

Decryption scheme: $\mathsf{Dec}_k(\rho) :=$ measurement of $H^k \rho H^k$ in the computational basis.



Theorem ([Tomamichel – Fehr – Kaniewski – Wehner][3])

Using this Enc_k, *no matter what* $\mathcal{P},\mathcal{B},\mathcal{C}$ *do, their winning probability is bounded by:*

$$\mathbb{P}^*(\mathcal{P},\mathcal{B},\mathcal{C}\ win) = \left(\cos^2(\pi/8)\right)^n \approx 0.85^n .$$

[3] Tomamichel et al. "A monogamy-of-entanglement game with applications to device-independent quantum cryptography". In: *New Journal of Physics* (2013).

Result in the Quantum Random Oracle Model

- **Definition.** "A **quantum-secure pseudorandom function (qPRF)** is a keyed function $f_\lambda : \{0,1\}^\lambda \times \{0,1\}^{\ell_{in}(\lambda)} \to \{0,1\}^{\ell_{out}(\lambda)}$, with $\lambda \in \mathbb{N}$, which appears random to an efficient quantum adversary who only sees its input/output behaviour and is ignorant of the particular key being used."

Encryption

Inputs: $m \in \{0,1\}^n$; $k = (s,\theta) \in \{0,1\}^{2\lambda}$

1. $x \in_R \{0,1\}^\lambda$;
2. $c := m \oplus f_\lambda(s,x)$;
3. $\rho := |c\rangle\langle c| \otimes |x^\theta\rangle\langle x^\theta|$.

Output: $\mathsf{Enc}_k(m) = \rho$

Decryption

Inputs: $\rho = |c\rangle\langle c| \otimes \sigma$; $k = (s,\theta) \in \{0,1\}^{2\lambda}$

1. $\sigma' := H^\theta \sigma H^\theta$;
2. $r :=$ measurement of σ';
3. $m' := c \oplus f_\lambda(s,r)$.

Output: m'

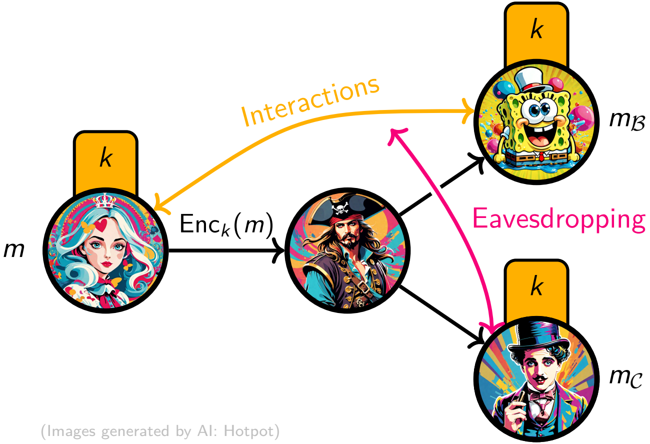
Theorem ([Broadbent – Lord][4])

If the qPRF is modeled by a q. oracle, this encryption is $\log_2(9)$*-unlconeable secure:*

$$\mathbb{P}(\mathcal{P},\mathcal{B},\mathcal{C} \text{ win}) \leq 9 \times 0.5^n \,.$$

[4] Broadbent and Lord. *Uncloneable Quantum Encryption via Oracles*. 2020.

Result with Interactions and Eavesdropping



(Images generated by AI: Hotpot)

- **Theorem ([Broadbent – Culf]):** For quantum encryption schemes of classical messages with interactive decryption, there is an equivalence between uncloneable and uncloneable-indistinguishable security.

(Broadbent and Culf. "Uncloneable Cryptographic Primitives with Interaction". In: (2023). arXiv: 2303.00048)

Results Under Other Assumptions

- Assumption of post-quantum one-way functions or post-quantum public key encryption.[5]
- Variant where $\mathcal{A}$ sends different keys to $\mathcal{B}$ and $\mathcal{C}$.[6]
- Assumption of post-quantum hardness of the learning with errors (LWE) problem.[7]
- Assumption of post-quantum indistinguishability obfuscation, one-way functions, and compute-and-compare obfuscation.[8]

---

[5] Ananth and Kaleoglu. "Unclonable Encryption, Revisited". In: 2021.
[6] Kundu and Tan. *Device-independent uncloneable encryption*. 2023. arXiv: 2210.01058.
[7] Gheorghiu, Metger, and Poremba. *Quantum cryptography with classical communication: parallel remote state preparation for copy-protection, verification, and more*. 2022. arXiv: 2201.13445.
[8] Chevalier, Hermouet, and Vu. *Unclonable Cryptography in the Plain Model*. 2023.

— *Part 3* —

Our Conjecture

(Hidden in the online version.)

Bibliography

- Ananth and Kaleoglu. "Unclonable Encryption, Revisited". In: 2021.
- Ananth et al. "On the Feasibility of Unclonable Encryption, and More". In: 2022.
- Broadbent and Culf. "Uncloneable Cryptographic Primitives with Interaction". In: (2023). arXiv: 2303.00048.
- Broadbent and Lord. *Uncloneable Quantum Encryption via Oracles*. 2020. DOI: 10.4230/LIPIcs.TQC.2020.4.
- Chevalier, Hermouet, and Vu. *Unclonable Cryptography in the Plain Model*. 2023.
- Gheorghiu, Metger, and Poremba. *Quantum cryptography with classical communication: parallel remote state preparation for copy-protection, verification, and more*. 2022. arXiv: 2201.13445.
- Gottesman. "Uncloneable Encryption". In: *Quantum Info. Comput.* (2003).
- Kundu and Tan. *Device-independent uncloneable encryption*. 2023. arXiv: 2210.01058.
- Tomamichel et al. "A monogamy-of-entanglement game with applications to device-independent quantum cryptography". In: *New Journal of Physics* (2013). DOI: 10.1088/1367-2630/15/10/103002.