1. Introduction: A Hierarchy of Uncloneability

The no-cloning theorem tells us that it is impossible to create perfect copies of arbitrary quantum states. One can use this fact to construct a hierarchy of uncloneable cryptographic primitives. At the base of this hierarchy, we have primitives which achieve a notion of authenticity that is uncloneable. This includes quantum money schemes. One level up, we have schemes to make information uncloneable, such as uncloneable encryption and tamper-evident evidence.

There has been recent interest in achieving uncloneable functionalities, the next level in this hierarchy. These are instantiated either as copy-protection schemes [Aar09] or as secure software leasing schemes [ALP21].

2. What is Secure Software Leasing (SSL)?

An SSL scheme is a set of procedures to encode a circuit $C$, taken from a suitable family $\mathcal{C}$, as a quantum state $\rho_C$ which can then be used to evaluate $C$ on an input $x$. Formally, we have $\rho_C = \text{Lease}(C)$ and $C(x) = \text{Eval}(\rho_C, x)$. (1) An SSL scheme also includes a procedure which allows the original creator of a program state to verify the return of a program state: $\text{Accept}/\text{Reject} \leftarrow \text{Verify}(\sigma, C)$. (2)

An SSL scheme should also satisfy a security guarantee which essentially states that a user can no longer evaluate $C$ once they have returned $\rho_C$ to the vendor.

3. The Secure Software Leasing Security Game

Let $(\text{Auth}_k, \text{Verf}_k)_k$ be a total authentication scheme and $|\psi\rangle$ a fixed state.

\[
\text{Lease} : \text{Input: A circuit } C \text{ for the function } f \Rightarrow \rho_C = \text{Lease}(C).
\]

\[
\text{Eval} : \text{Input: A state } \sigma \text{ and a string } x \Rightarrow \text{Output } \sigma, f(x)(\psi|x\rangle).
\]

The Verify procedure checks if $\text{Eval}(\sigma, x) = C(x)$ for a suitably sampled $x$.

4. Point Functions and Total Authentication

For any $p \in \{0, 1\}^n$, the point function $f_p : \{0, 1\}^n \rightarrow \{0, 1\}$ is defined by $f_p(q) = 1 \iff p = q$. (3)

A total authentication scheme $\{\text{Auth}_k, \text{Verf}_k\}_k$ is a pair of keyed procedures such that

\[
\text{Verf}_k, \text{Auth}_k(\rho) = \rho \otimes |\text{Accept}\rangle_1|\text{Accept}\rangle_2.
\] (4)

Note that the Verf$_k$ procedure could also produce a $|\text{Reject}\rangle$ state.

The security guarantee is that, conditioned on acceptance, any eavesdropper between Auth$_k$ and Verf$_k$ essentially did not interact with the encoded state.

5. From Copy-Protection to Secure Software Leasing

A copy protection scheme is essentially an SSL scheme with a different security guarantee. There is no Verify procedure. Instead, we guarantee that no pirate given a single program state can create two states which can be used to evaluate the underlying circuit. This is tested by challenging two evaluators to compute the circuit on given inputs.

We consider a variation called honest-malicious copy-protection where one of the evaluators must use the honest evaluation procedure.

Theorem. Under mild conditions, any honest-malicious copy-protection scheme yields a secure software leasing scheme.

Theorem. Our construction offers honest-malicious copy protection.

Acknowledgements

We thank Christian Majenz and Martti Karvonen for related discussions. This material is based upon work supported by the Air Force Office of Scientific Research under award number FA9550-17-1-0081; Canada’s NFRF and NSERC; an Ontario ERA; and the University of Ottawa’s Research Chairs program. SJ is a CIFAR Fellow in the Quantum Information Science program.