Thesis: Unclonable Secret Keys.

Abstract: We propose a novel concept of securing cryptographic keys which we call “Unclonable Secret Keys,” where any cryptographic object is modified so that its secret key is an unclonable quantum bit-string whereas all other parameters such as messages, public keys, ciphertexts, signatures, etc., remain classical. We study this model in the authentication and encryption setting giving a plethora of definitions and positive results as well as several applications that are impossible in a purely classical setting.

In the authentication setting, we define the notion of one-shot signatures, a fundamental element in building unclonable keys, where the signing key not only is unclonable, but also is restricted to signing only one message even in the paradoxical scenario where it is generated dishonestly. We propose a construction relative to a classical oracle and prove its unconditional security. Moreover, we provide numerous applications including a signature scheme where an adversary can sign as many messages as it wants and yet it cannot generate two signing keys for the same public key. We show that one-shot signatures are sufficient to build a proof-of-work-based decentralized cryptocurrency with several ideal properties: it does not make use of a blockchain, it allows sending money over insecure classical channels and it admits several smart contracts. Moreover, we demonstrate that a weaker version of one-shot signatures, namely privately verifiable tokens for signatures, are sufficient to reduce any classically queried stateful oracle to a stateless one. This effectively eliminates, in a provable manner, resetting attacks to hardware devices (modeled as oracles).

In the encryption setting, we study different forms of unclonable decryption keys. We give constructions that vary on their security guarantees and their flexibility. We start with the simplest setting of secret key encryption with honestly generated keys and show that it exists in the quantum random oracle model. We provide a range of extensions, such as public key encryption with dishonestly generated keys, predicate encryption, broadcast encryption and more.

Committee:

- Professor Nelly Fazio, Mentor, The City College Of New York
- Professor Rosario Gennaro, The City College Of New York
- Professor William E. Skeith Iii, The City College Of New York

Outside member:

- Professor Mark Zhandry, Princeton University