

Quantum-safe entity authentication with physical-unclonable keys

Georgios M. Nikolopoulos^{1,2}

¹ Institute of Electronic Structure & Laser, FORTH, P.O. Box 1385, GR-70013 Heraklion, Greece

² Institut für Angewandte Physik, Technische Universität Darmstadt, D-64289 Darmstadt, Germany

Abstract

We report on a new entity authentication protocol for physical keys that are materialized by optical multiple-scattering media. The protocol exploits standard wavefront-shaping techniques, and homodyne detection, while a key is accepted or rejected based on its response when probed by randomly selected coherent states of light. We discuss the security of the protocol against cloning as well as against quantum adversaries and emulation attacks.

Entity authentication (sometimes also referred to as identification) is an important cryptographic task, in which one party (the verifier) obtains assurance that the identity of another party (the claimant) is as declared, thereby preventing impersonation. Typically, entity authentication relies on one of the following techniques: (i) something that the claimant knows (e.g., a secret password or numerical key); (ii) something that the claimant possesses (e.g., a physical token or card); (iii) something inherent (e.g., biometrics). Most of the entity authentication protocols (EAPs) used in everyday tasks (e.g., transactions in automatic teller machines, purchases, etc), rely on dynamic challenge-response mechanisms which combine techniques (i) and (ii). In such mechanisms, after the user types in the correct numerical key (PIN), the smart card is challenged with random numerical challenges, and the verifier checks if the responses of the card are valid.

Conventional EAPs are not totally immune to card-cloning, while they are susceptible to emulation attacks, in which an adversary knows the challenge-response properties of the smart card (e.g., by hacking the database of challenge-response pairs), and his task is to intercept each numerical challenge during the verification stage, and send to the verifier the expected response. Currently, optical physical unclonable keys (PUKs) are considered to be the most promising candidates for the development of highly secure EAPs. Such PUKs are materialized by an optical multiple-scattering disordered medium, and they are considered to be unclonable, in the sense that their cloning requires the exact positioning (on a nanometre scale) of millions of scatterers with the exact size and shape, which is considered to be a formidable challenge not only for current, but for future technologies as well. Typically, a PUK-based EAP relies on a challenge-response mechanism, in which the PUK is interrogated by light pulses (probes) with randomly chosen parameters, and acceptance or rejection of the PUK is decided upon whether the recorded responses agree with the expected ones. Although, in general, PUK-based EAPs are more robust against cloning than conventional EAPs, they are still vulnerable to emulation attacks when challenges pertain to classical light, and the verification set-up is not tamper-resistant.

We report on a quantum-optical EAP in which a PUK is interrogated by random coherent quantum states of light, and the quadratures of the scattered light are analyzed by means of a coarse-grained homodyne detection. The response of the PUK to a quantum state (challenge) is sensitive to the internal disorder of the PUK, which makes our protocol collision resistant, and robust against cloning. Moreover, the security of our protocol against an emulation attack relies on the laws of quantum physics, which do not allow unambiguous discrimination between non-orthogonal quantum states, while information gain cannot be obtained without disturbing the quantum state under interrogation. Implementation of the protocol relies on standard wavefront-shaping and homodyne-detection techniques, and it is within reach of current technology.

- [1] G. M. Nikolopoulos and E. Diamanti, *Continuous-variable quantum authentication of physical unclonable keys*, Scientific Reports **7**, 46047 (2017).
- [2] G. M. Nikolopoulos, *Continuous-variable quantum authentication of physical unclonable keys: Security against an emulation attack*, Physical Review A **97**, 012324 (2018).