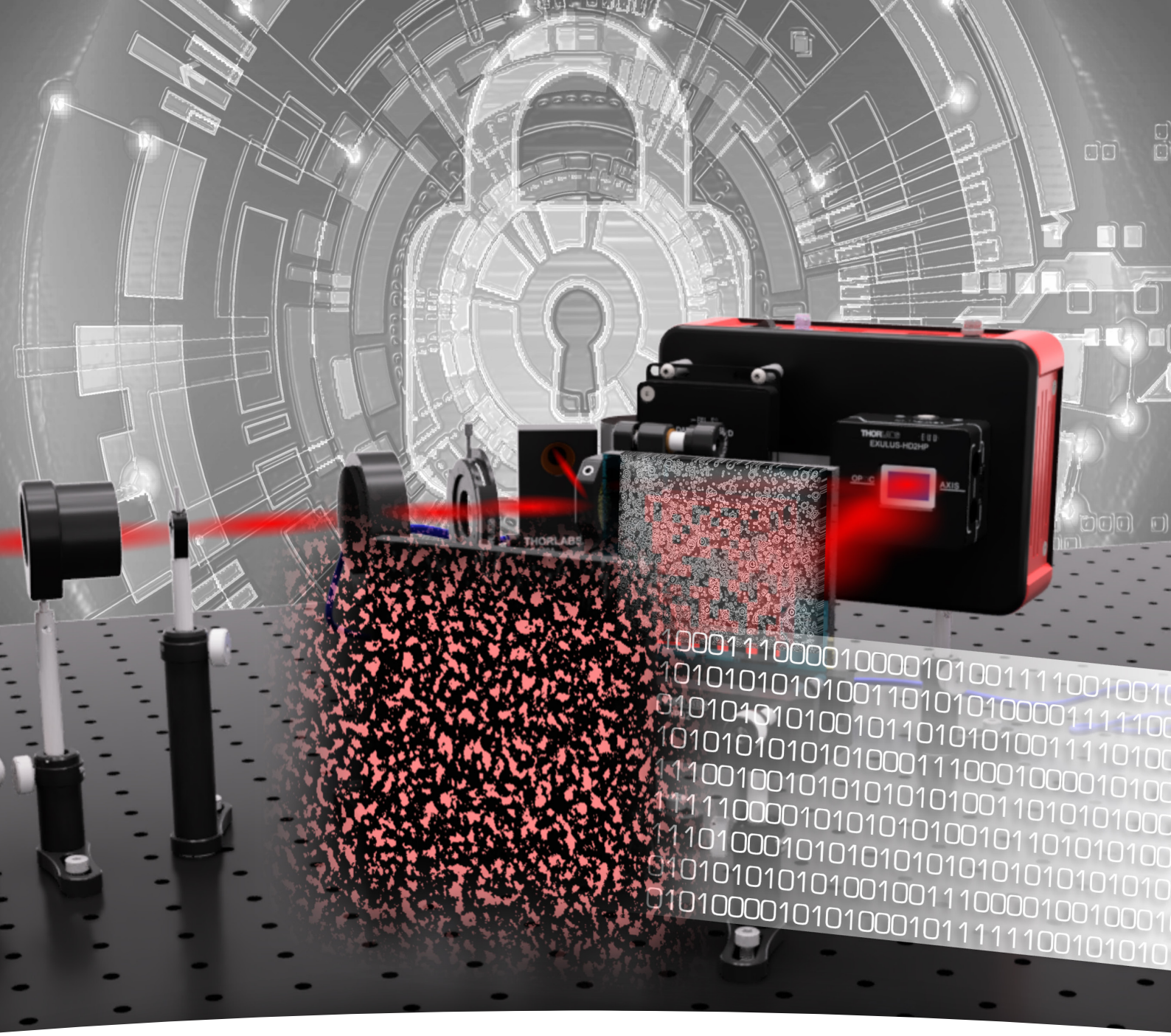

Chiavi fisiche non clonabili per la sicurezza informatica

Physical unlclonable keys for the cyber security

Sistemi fotonici complessi per la generazione di milioni di chiavi crittografiche ad alto contenuto entropico sicure contro diversi tipi di attacchi informatici e con maggior resilienza contro attacchi di apprendimento automatico

Complex photonic systems for the generation of millions of cryptographic keys with a large entropic content, secure against different type of cyber attacks and with higher resilience against machine learning attacks.

Contatti | *Contacts:* riboli@lens.unifi.it
nocentini@lens.unifi.it

CON IL CONTRIBUTO DI:

Value Proposition

Offriamo generatori di chiavi crittografiche sicure contro diversi tipi di attacco informatico e con una maggior resilienza contro attacchi di apprendimento automatico. A differenza delle memorie non volatili in cui vengono registrate le chiavi tradizionali, le funzioni fisiche non clonabili codificano un vasto numero di chiavi ad alto contenuto informativo nella complessità strutturale del materiale a livello microscopico.

We offer physical generators of cryptographic keys secure against different types of cyber attacks and with higher resilience against machine learning attacks.
Unlike nonvolatile memories in which traditional keys are recorded, physical unclonable functions encode a large number of cryptographic keys in the structural complexity of the material at the microscopic level.

Key technologies

- Funzioni fisiche non clonabili realizzati in materiali con diverso indice di rifrazione e con proprietà riconfigurabili
- Apparato ottico sperimentale di generazione e raccolta di milioni di chiavi crittografiche. Setup composto da laser, digital micromirror device, CMOS camera e ottiche.
- Algoritmi di post processing e analisi di chiavi crittografiche
- Metodi e modelli di valutazione del contenuto entropico (bits) delle chiavi generate

- *Physical unclonable functions made by materials with different refractive indeces and reconfigurability properties*
- *Set-up for the generation and characterization of million of cryptographic keys. Set-up: Laser, Digital Micromirror device, CMOS camera and optical components.*
- *Post-processing Algorithms for the analysis of the cryptographyc keys*
- *Methods and models for the estimation of the entropic content (bits) of the generated keys*

Applications

- Etichette anticontraffazione per identificazione univoca con diversi livelli di riconoscimento
- Autenticazione di utenti e servizi tramite chiavi crittografiche ad alta complessità
- Autenticazione di diversi utenti tramite un singolo token con funzionamento multi-livello

- *Anticounterfeiting labels for good identification (also with multi-factor identification)*
- *Autentication of services and users via cryptographic keys with large complexity*
- *Authentication of different users with a single token with multi-level operation*

Background

- Progetto FOTCOM “Sistemi fotonici complessi per le tecnologie dell’informazione e della comunicazione” Fondazione Cassa di Risparmio Firenze
- Progetto AFOSR (Air force Office of Scientific Research)/RTA2 «Highly secure nonlinear physical unclonable functions».

- *Funded project Ente cassa di Risparmio FOTCOM “Sistemi fotonici complessi per le tecnologie dell’informazione e della comunicazione”*
- *Funded project AFOSR /RTA2 «Highly secure nonlinear physical unclonable functions».*