IDentification for the Internet Of Things

ID_IOT

CHIST-ERA call 2015
project 651.002.003
Starting date February 2017

Boris Skoric (TU Eindhoven)
Teddy Furon (INRIA)
Slava Voloshynovskiy (Univ. Geneva)
+ three PhD students

TU/e Technische Universiteit Eindhoven University of Technology

Inria inventeurs du monde numérique

UNIVERSITÉ DE GENÈVE

Chist-era seminar, April 2018

Background

The IoT will contain a huge number of devices and objects that have very low or nonexistent processing and communication resources, coupled to a small number of high-power devices. The weakest devices, which are most ubiquitous, will not be able to authenticate themselves using cryptographic methods. Other important tasks in the IoT will be to verify if an object is **authentic**, or to **identify** an object. Furthermore, we foresee that back-end systems will not be able to provide security and privacy via crypto-graphic primitives due to the sheer number of IoT devices.

Project goals

Our plan is to address the low-power issues using Physical Unclonable Functions (PUFs). PUFs, and especially Quantum-Secure Authentication of **optical PUFs** (QSA), are ideally suited to the IoT setting because they allow for the authentication and identification of physical objects without requiring any crypto or storage of secret information.

We want to address the back-end load problems using **privacy-preserving database structures** and algorithms with good **scaling** behaviour.
Approximate Nearest Neighbour (ANN) search algorithms, which have remarkably good scaling behaviour, have recently become highly efficient, but do not yet have the right security properties and have not yet been applied to PUF data.

Summarised in a nutshell, the project aims to improve the theory and practice of technologies such as PUFs and ANN search in the context of generic IoT authentication and identification scenarios.

Project results so far

- Privacy preserving protocols with random projections with sparse vector representation and ambiguisation [1,2].
- Similarity search in high-dimensional spaces [3].
- Security analysis of QSA-related protocols [4,5].

Publications

[1] *Privacy Preserving Identification Using Sparse Approximation with Ambiguization*.
B. Razeghi, S. Voloshynovskiy, D. Kostadinov, O. Taran.
IEEE Workshop on Information Forensics and Security (WIFS) 2017. pp.1-6.

[2] *Privacy-preserving outsourced media search using secure sparse ternary codes*.
B. Razeghi, S. Voloshynovskiy.
International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2018.

[3] *Memory vectors for similarity search in high-dimensional spaces*.
A. Iscen, T. Furon, V. Gripon, M. Rabbat, H. Jégou.
IEEE Transactions on Big Data 4(1), pp. 65-77, 2018.

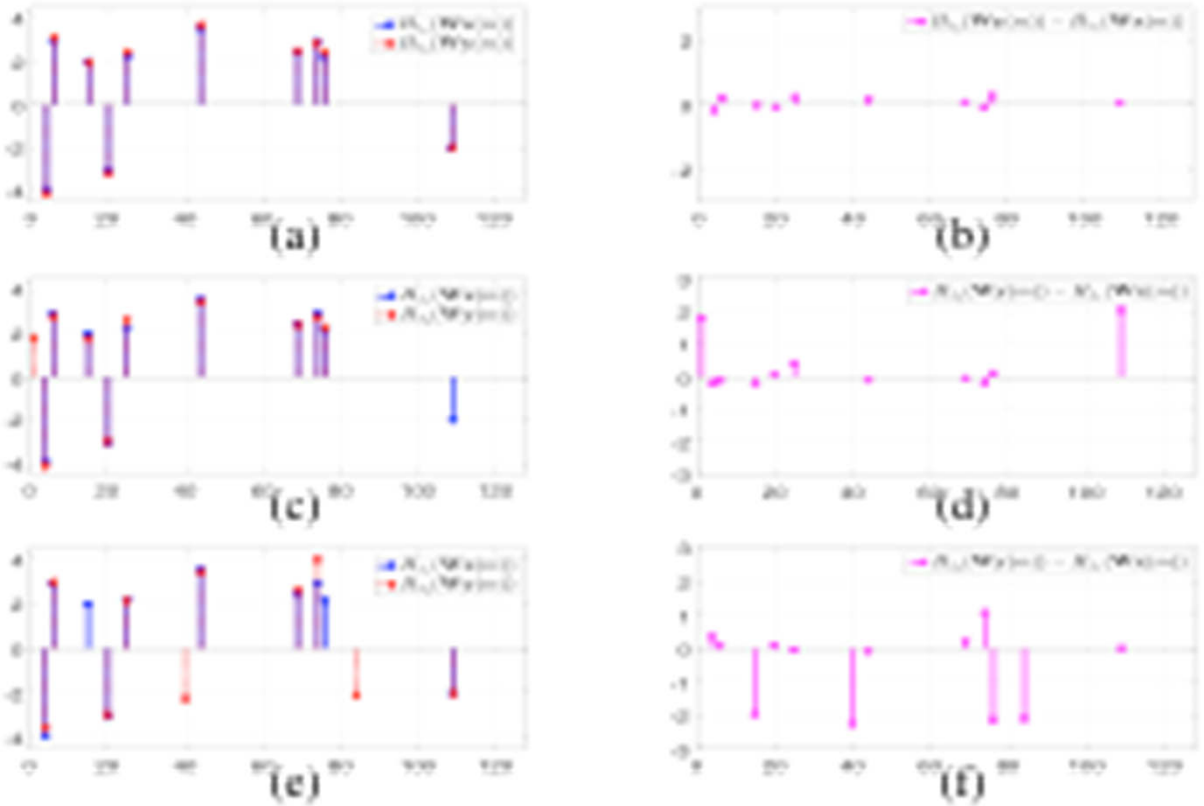
[4] *Optimal attacks on qubit-based Quantum Key Recycling*.
D. Leermakers, B. Škorić.
Quantum Information Processing 17(3), pp. 57, 2018.

[5] *Security proof for Round Robin Differential Phase Shift QKD*.
D. Leermakers, B. Škorić.
https://eprint.iacr.org/2017/830

Privacy-preserving identification

Random projections revisited

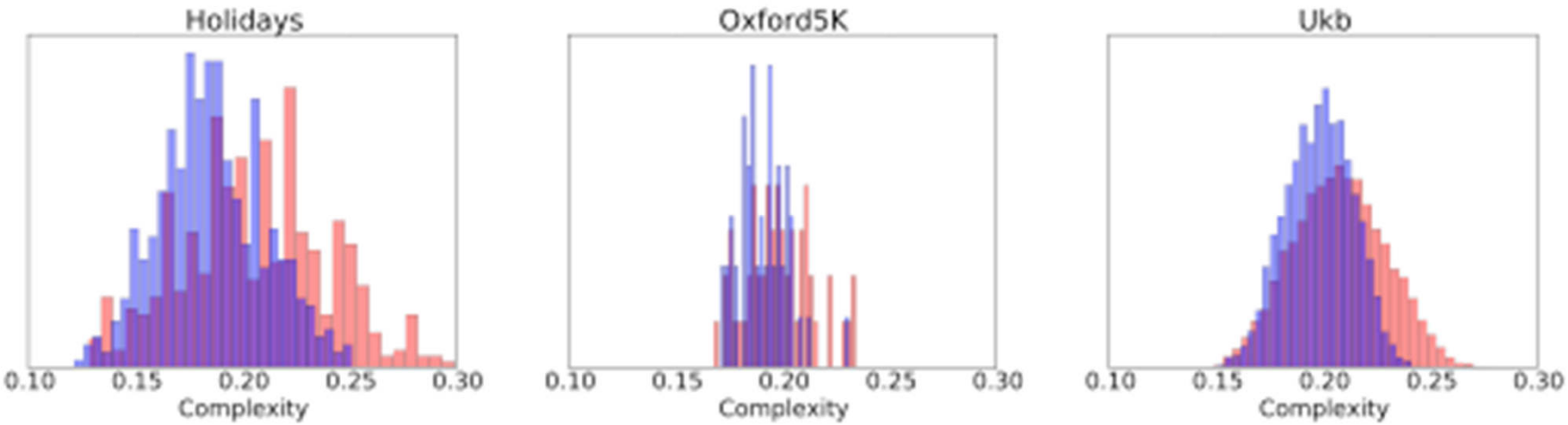
- Identifier is noisy vector $x \in R^k$.
- Multiply with random matrix M. $y=Mx$. $y \in R^n$, **n>k**.
- Random projections have polarising effect. Some compo-nents of y have very good SNR. Index set J together with sign(y_j) contains practically all information from x.
- Reveal M, and index set J with artificial perturbations. This data allows for identificaton protocols but preserves privacy of x.



Effect of noise in
sparse representations

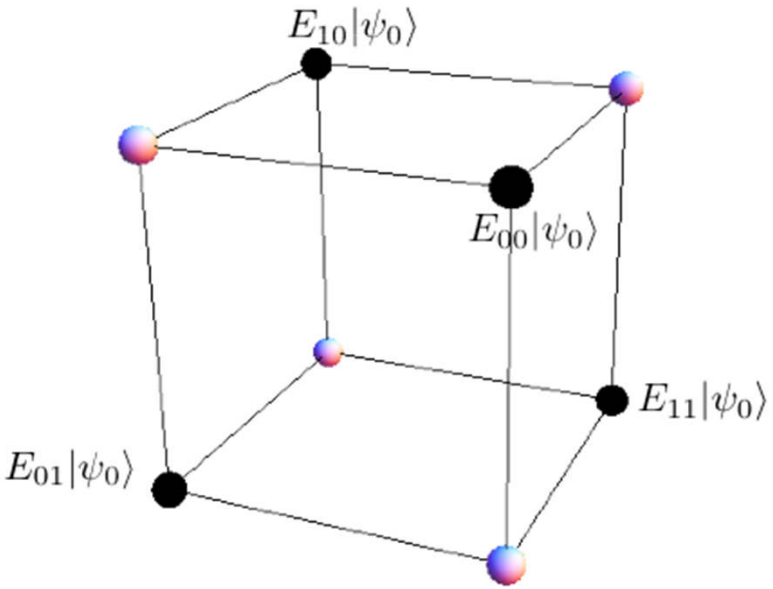
Similarity search

- Database of high-dimensional vectors, e.g. images
- Goal: efficient similarity search
- Compute a group representative for each group of vec-tors. Can be as simple as averaging. First compare to the representatives.
- Different ways to construct groups.

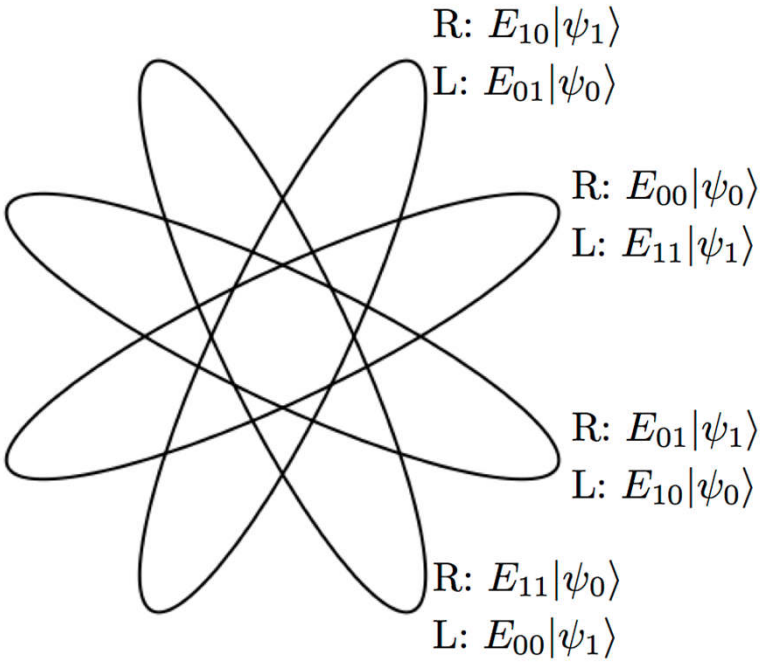


Quantum Key Recycling

- Using a quantum channel like QSA.
- Information-theoretic security with efficient use of keys.
- Old idea from 1982, revisited.
- More secure encoding of bits into qubits.



Cipherstates represented on the Bloch sphere



Cipherstates represented as elliptic polarisation

What Next

- Speckle challenge
- Apply tricks from multimedia signal processing to speckle
- Compression of PUF matrices
- Combine ANN with ternary sparse representation
- etc etc