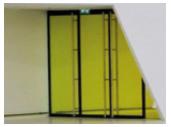
Identification for the Internet of Things

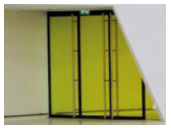
Boris Škorić
TU Eindhoven

TU/e



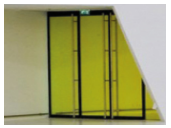
IDentification for the Internet Of Things

- European project, CHIST-ERA call 2015
  - Started Feb 2017
  - Three partners
    - TU Eindhoven: Boris Škorić
    - INRIA (France): Teddy Furon
    - University of Geneva: Slava Voloshynovskiy
  - Three PhD students



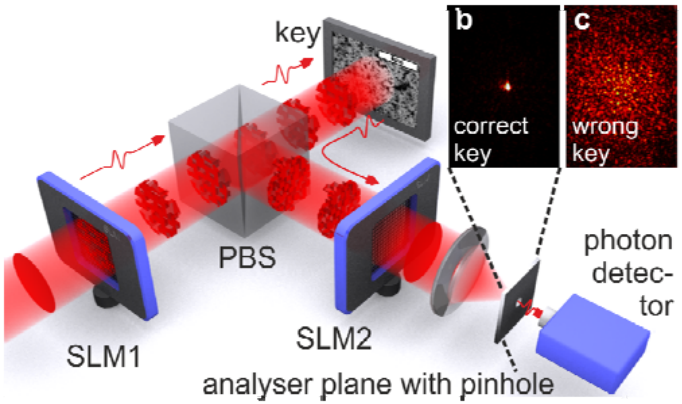
The Internet Of Things (whatever that may be)

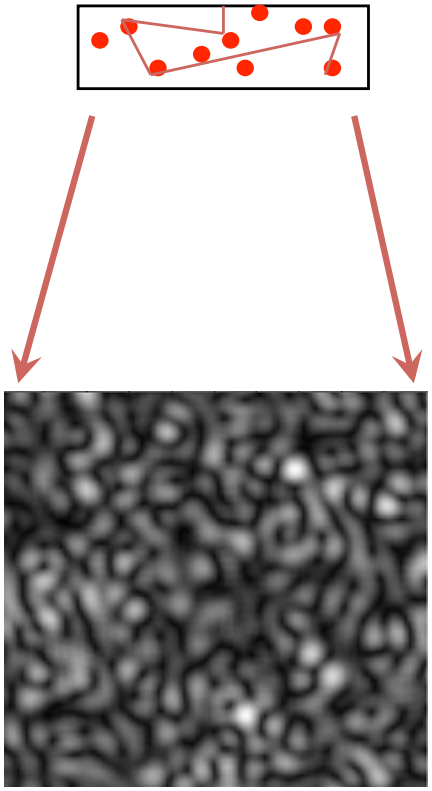
- Many IoT devices are either dead or low-resource
  - they cannot do crypto
- Verifier device is more powerful.
  Communicates with database.
- Security issues
  - identification / authentication of physical objects
  - searching in noisy databases
  - privacy w.r.t. database holder

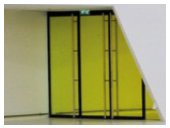


Topic 1: Identification of physical objects

- Physical Unclonable Functions
- Quantum Readout of PUFs
- speckle patterns
  - fuzzy extractors
  - compact representations



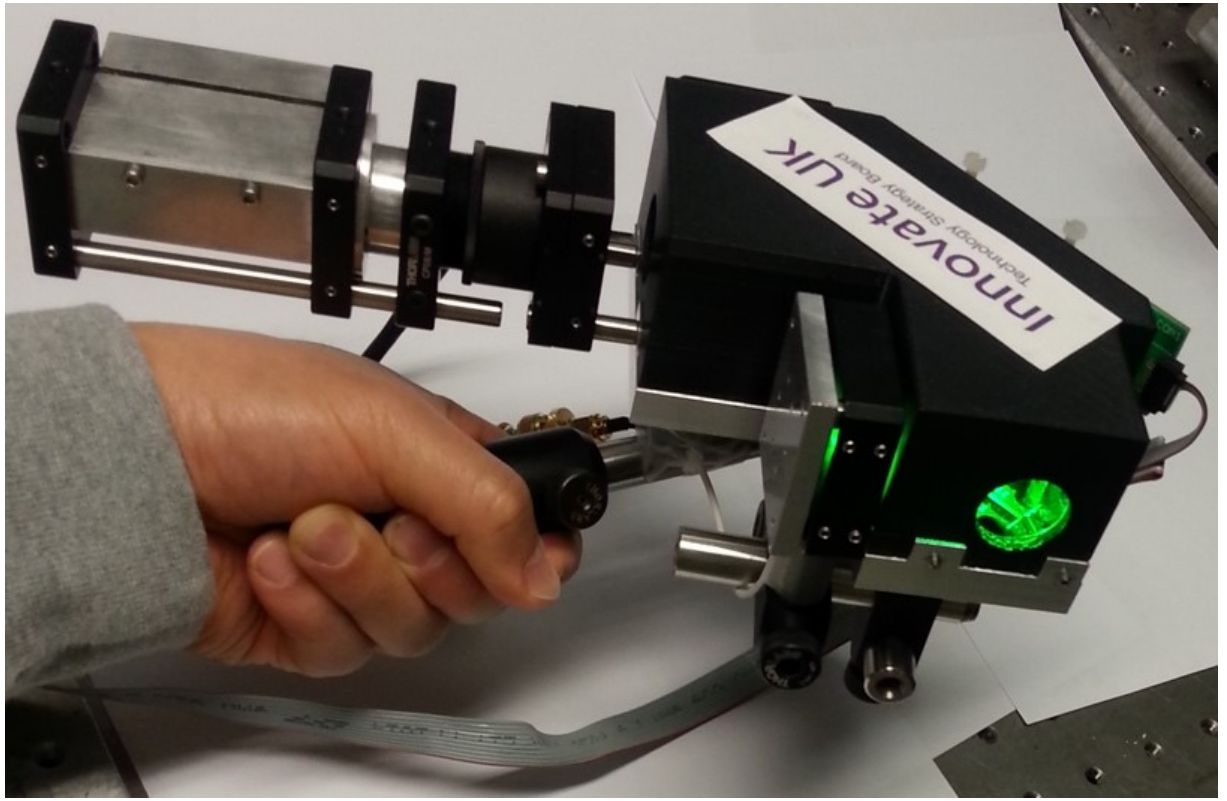




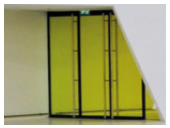
Quantum PUFs, is this science fiction?

Can this be made small and cheap??

Hardware components similar to Quantum Key Distribution.

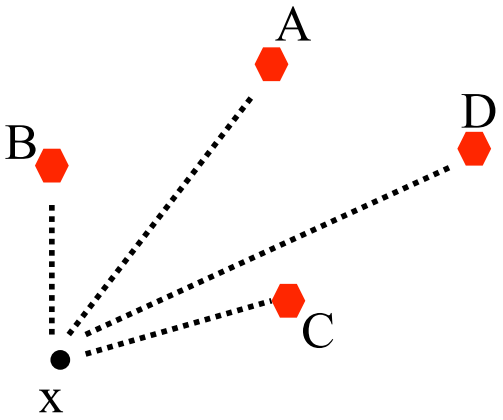


[H. Chun et al 2017]
Handheld free space quantum key distribution with dynamic motion compensation



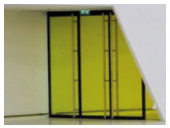
Topic 2: Searching in noisy databases

- noisy measurements
- privacy
- nearest neighbour search in high-dimensional space
  - scaling behaviour
  - e.g. "beacons" and buckets



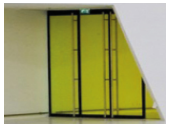
	dist to A	dist to B	dist to C	dist to D
$0\text{--}r_1$	...	...	...	...
$r_1\text{--}r_2$	...	...	...	...

data items binned according to distance



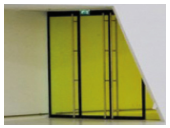
Topic 3: Privacy-preserving identification

- Database owner should not learn too much
- light-weight crypto; preferably no crypto at all
  - scaling
- proof of group membership
- connections with fuzzy extractors and noisy search



Progress after 8 months

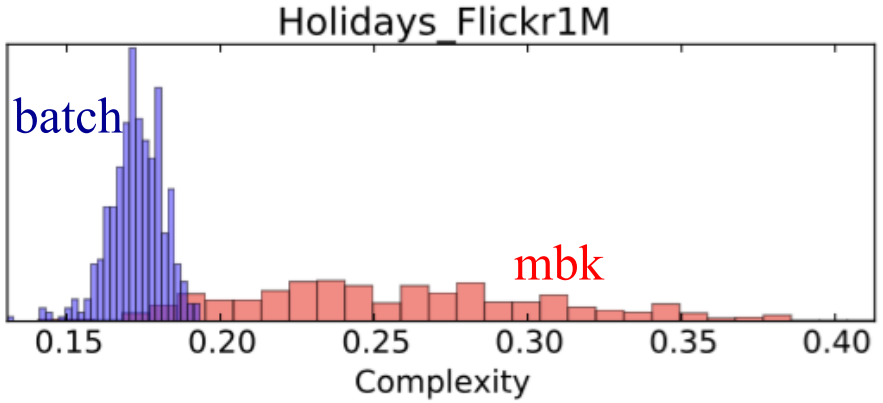
- PhD students starting in Feb, March, Nov 2017
- Submitted papers
  - 2 on quantum crypto 
  - 1 on noisy search
  - 1 on sparse representations of noisy data
- Organising a special session at WIFS 2017:
  - "Object identification and authentication"

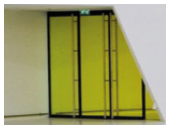


Memory vectors for similarity search in high-dimensional spaces

Ahmet Iscen, Teddy Furon, Vincent Gripon, Michael Rabbat, and Hervé Jégou

- Data points are noisy high-dimensional vectors.
- Goal: test for **group membership**.
- Enroll a group by storing the vector average.
  - fast test
  - application: image indexing

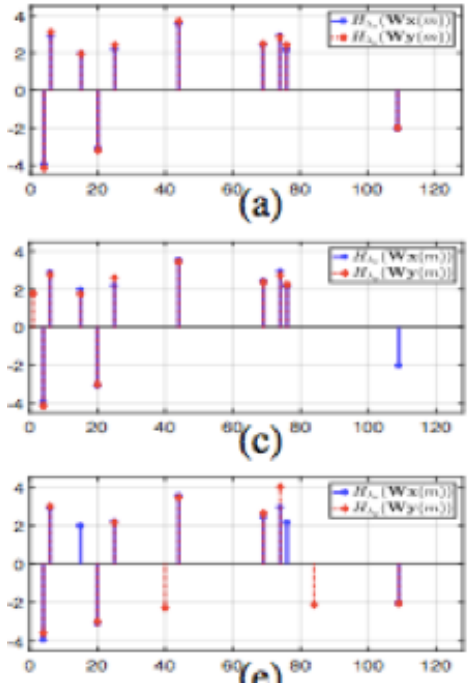


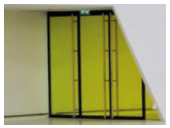


Privacy Preserving Identification Using Sparse Approximation with Ambiguization

Behrooz Razeghi, Slava Voloshynovskiy, Dimche Kostadinov and Olga Taran

- High-dimensional data points.
- Projection onto random vectors
  - many
  - ternary discretisation
- => sparse representation
- add fake nonzero entries for privacy



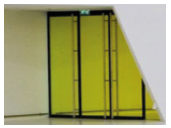


Optimal attacks on qubit-based Quantum Key Recycling

Daan Leermakers and Boris Škorić

Security proof for
Round Robin Differential Phase Shift QKD

Daan Leermakers and Boris Škorić



What's next?

Machine Learning challenge

- to be announced at WIFS 2017 special session
- data set courtesy of Pinkse (Univ. Twente) and Mosk (Univ. Utrecht)
  - speckle patterns from different PUFs
- derive a transmission matrix from multiple speckle images
- distinguish real from synthetic data
- distinguish responses from different PUFs