

# Digital Security for Physical World

Slava Voloshynovskiy

University of Geneva  
Switzerland

# Outline

- Physical object security
- Why not traditional security?
- Proposed solutions for
  - ▶ Object recognition
  - ▶ Design verification
  - ▶ Object identification
- Benefits

# Global Scope of Counterfeiting



The Association for Packaging  
and Processing Technologies

Global value of  
counterfeit goods annually  
**\$1.5 trillion**

Counterfeit is increasing  
**3% per year**  
worldwide

**ATP** PRODUCTS FOR MODERN LIVING

**ATP** INVERTERS

**ATP** "A" Battery ELIMINATOR

**TOPS IN KNOBS**

**LOOK! Boys Wanted**

**BOGUS!**

**ELECTRONIC MANUFACTURING AND CONSUMERS CONFRONT A RISING TIDE OF COUNTERFEIT ELECTRONICS**

By Michael Pecht & Sanjay Tiku

**Jupiter POWERFUL!**

**SompSin ELECTRIC COMPANY**

Photo Collage: Laura Azran

Special Edition/July-August 2011

**Supply & Demand Chain Executive**

Solutions-based Intelligence for Supply Chain ROI

**The COUNTERFEIT Crisis**

Critical strategies to meet the growing challenge

**Setting the International Standard**  
Global standards to preserve your role in the supply chain  
p. 8

**Supply Chain Best Practices**  
Keys to avoiding counterfeit parts and supplier risk  
p. 12

**Fighting the Fakes**  
L3 Communications' award-winning solution  
p. 18

CYGNUS

**IEEE SPECTRUM**

FOR THE TECHNOLOGY INDUSTRY \$3.95

**FAKE**

Scavenged chips passed off as new are cropping up in U.S. military equipment. Are they in passenger jets and cars, too? **p.36**

TEACHING A COPTER TO FLY ITSELF: A full-size craft takes solo **p. 24**

THE QUANTUM TRANSISTOR: Can it break Moore's Law just? **p. 30**

DAVID SARRNOFF'S SECRET GARDEN: Discoveries in a remote corner of a remote corner **p. 42**

CHINA'S INVADE: BY WINNING MAN: What's about to happen in China? **p. 48**

[SPECTRUM.IEEE.ORG](http://SPECTRUM.IEEE.ORG)

IEEE

ID docs



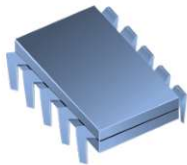
Certificates



Banknotes



Electronics



Luxury objects



Art objects



Packaging



## Risks of counterfeiting

- Danger for life
- Market loss
- Damage of brand reputation

## Restraints

- Inefficient authentication technologies
- High cost of track and trace infrastructure
- Lack of awareness for product originality

# Global anti-counterfeit packaging market 2020 - \$143 Billion

## Authentication packaging technologies:

- Security Inks and Dyes
- Holograms
- Watermarks
- Taggants

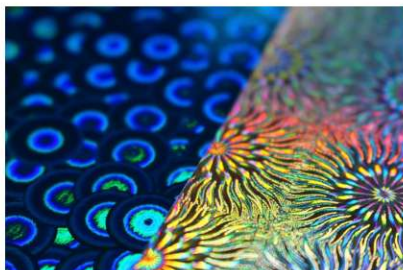
## Track and Trace packaging technologies:

- Barcodes
- RFID

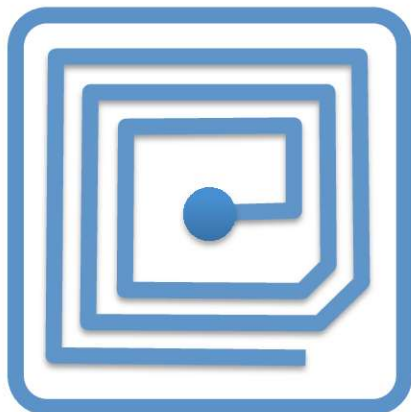


## Why not “traditional” security?

### Main restrictions of existing security technologies for physical objects:



- **Proprietary technologies** (rare or expensive materials, inks, holograms, etc.)
  - **obsolete** and **easy to clone** by modern means
  - **expensive** for mass markets
  - **special equipment/special knowledge** are required



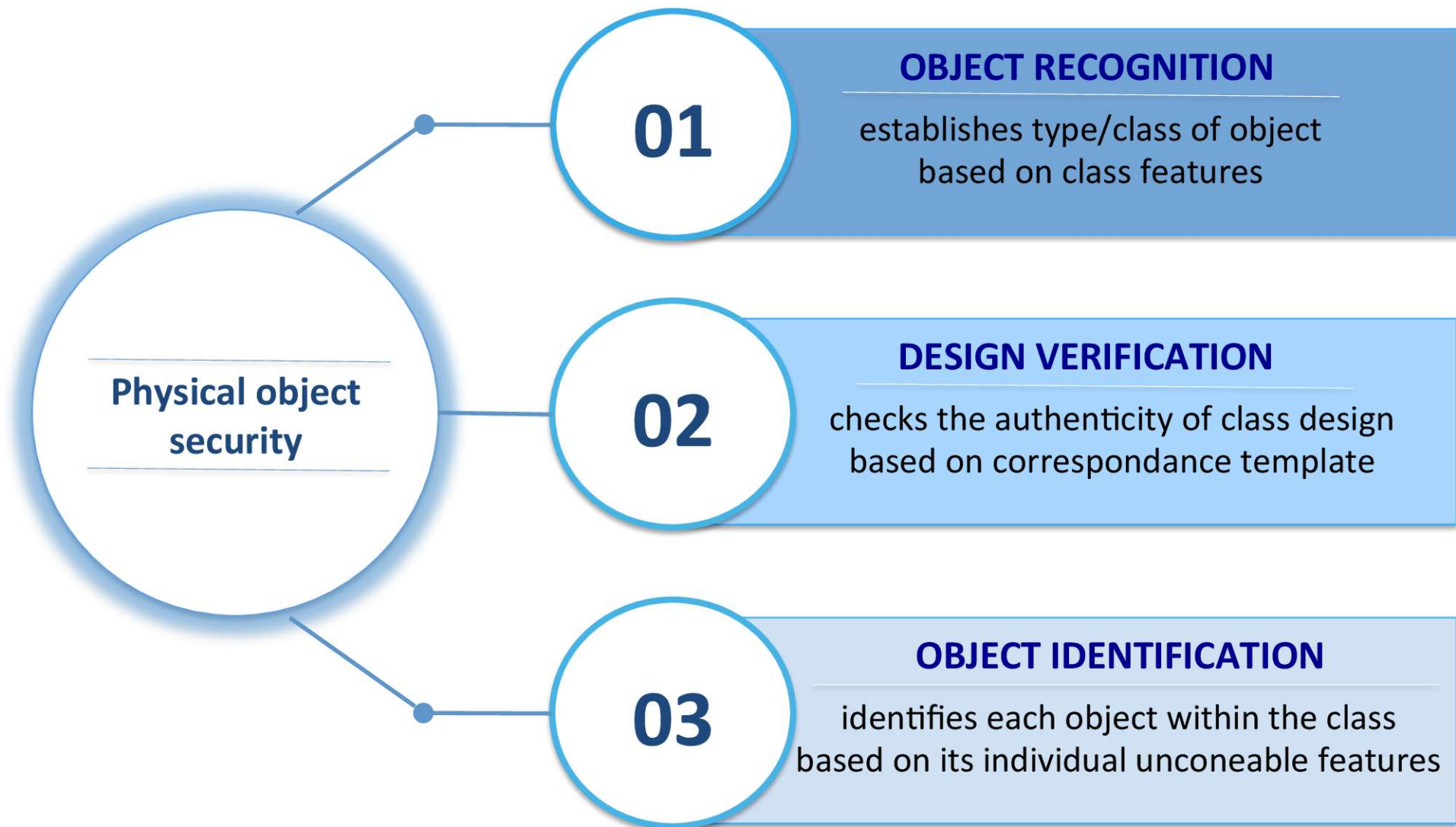
- **Crypto security**
  - very sensitive to noisy and can not be directly applied to analog/physical data
- **RFID/Connected devices/Internet of Things**
  - still quite expensive
  - serious security concerns
  - not always applicable

## Requirements to modern physical object security



- **easy to verify authenticity but difficult to clone**  
cloning should be economically inefficient
- **non-proprietary: based on physical-crypto principles**  
protection mechanism is assumed to be public
- **no special equipment required**  
preferably on mobile phone (in possession of everyone)
- **no special training required**  
any user can validate it
- **cheap and scalable to mass markets**  
millions or billions of products
- **non-invasive**  
products and production should not be modified





# Object recognition



## Goal

Accurately recognize each object on mobile phone



## Challenges

- Billions of items
- Very similar



# Object recognition

Enrollment from physical object



Enrollment from digital template

Feature extraction



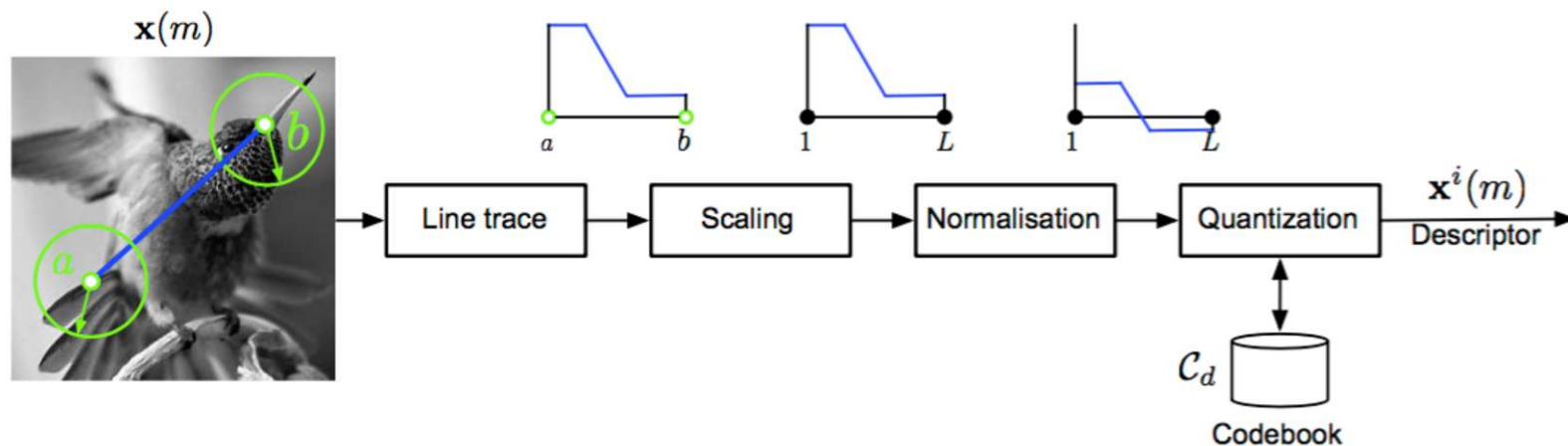
# Object recognition

## Image parsing



## SketchPrint main idea

Extract a sketch connecting two reference points

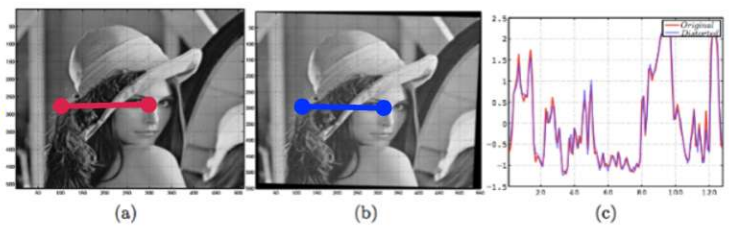




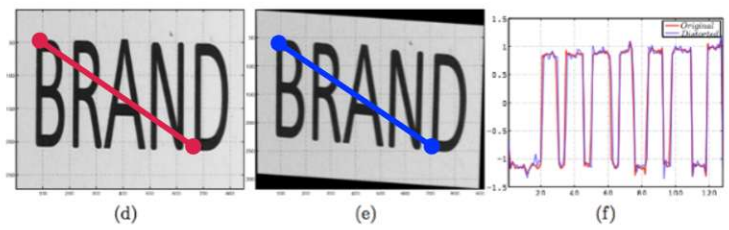
# Object recognition

## SketchPrint

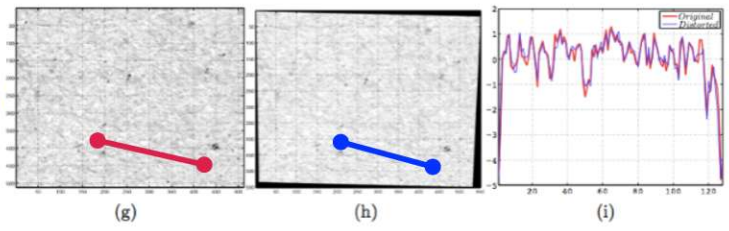
Natural images



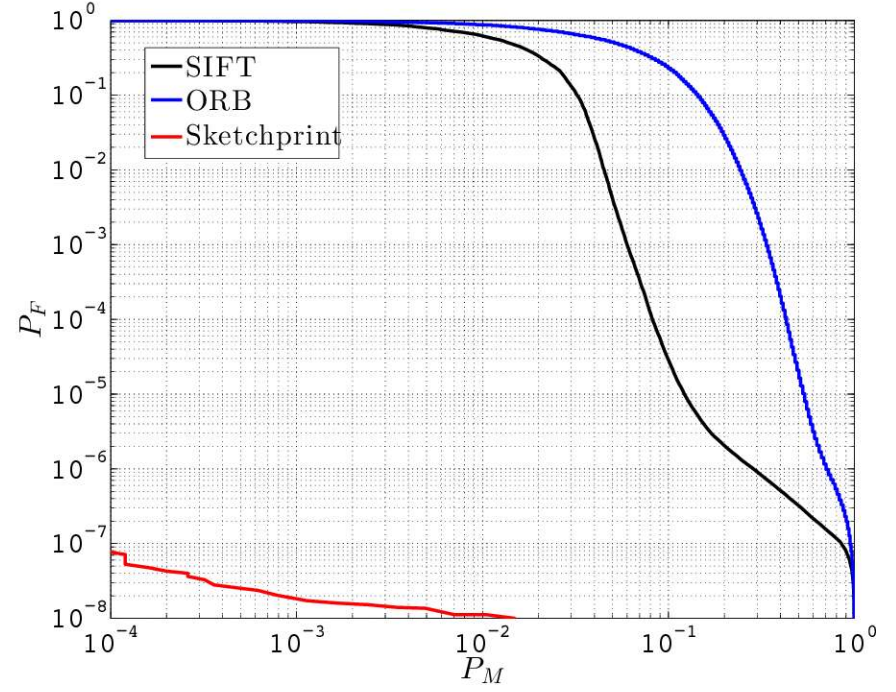
Text & logos



Random images



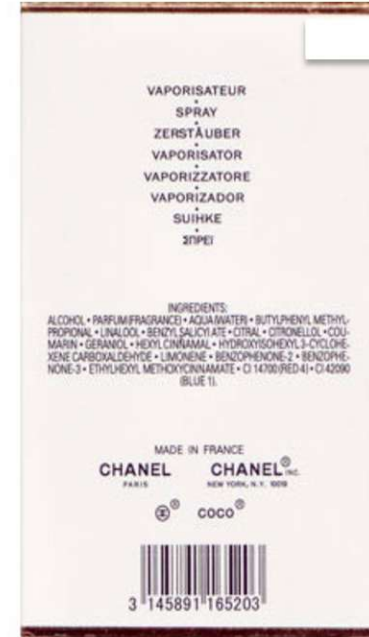
## Performance





# Object authentication

**Given:** a package



source: originalideas.info

**Question:**

- Is this package authentic?

**Remark:** you have never seen it or remember its design roughly...

**Your thinking:** well....quality of print looks OK

.....logo seems OK

.....I buy it from a reputable vendor

.....so probably authentic!

# Object authentication



source: originalideas.info

**Observation:** if we know the original design, we can easily verify its authenticity.

## Question:

- Can we perform the design verification automatically?
- And how accurately (say with the precision about 10-15 microns)?

# Design verification

Enrollment from physical object



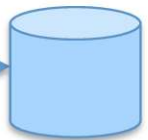
Enrolled image



Feature extraction



Cloud storage and computing



Enrollment from digital template



# Design verification

## Integral verification

Text  
Graphics  
Images  
Microstructures  
Halftoning



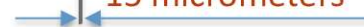
Authentic



Not authentic

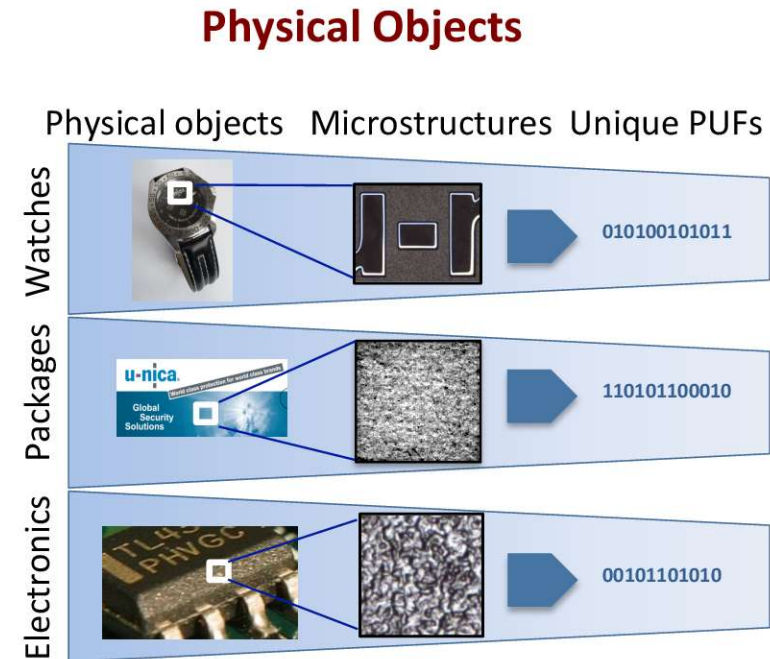
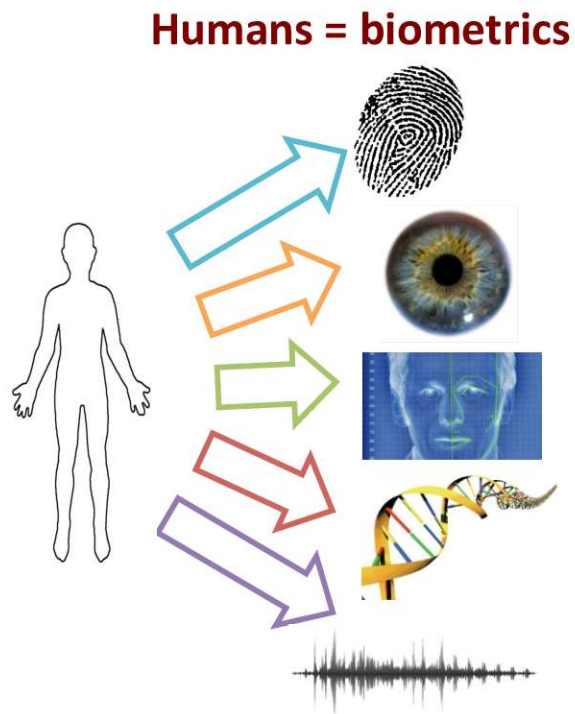


15 micrometers



# Object identification

## Intuition behind physical uncloneable functions (PUFs)



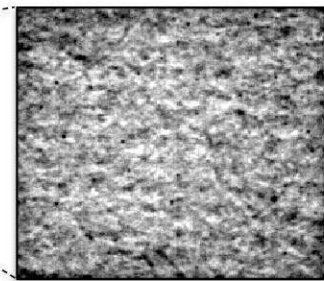
**All physical objects are unique like humans**



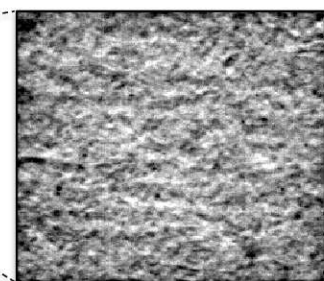
# Object identification

Paper microstructures = PUFs

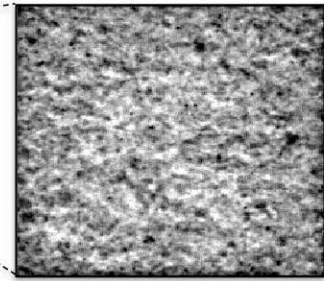
Package 1



Package 2



Package M



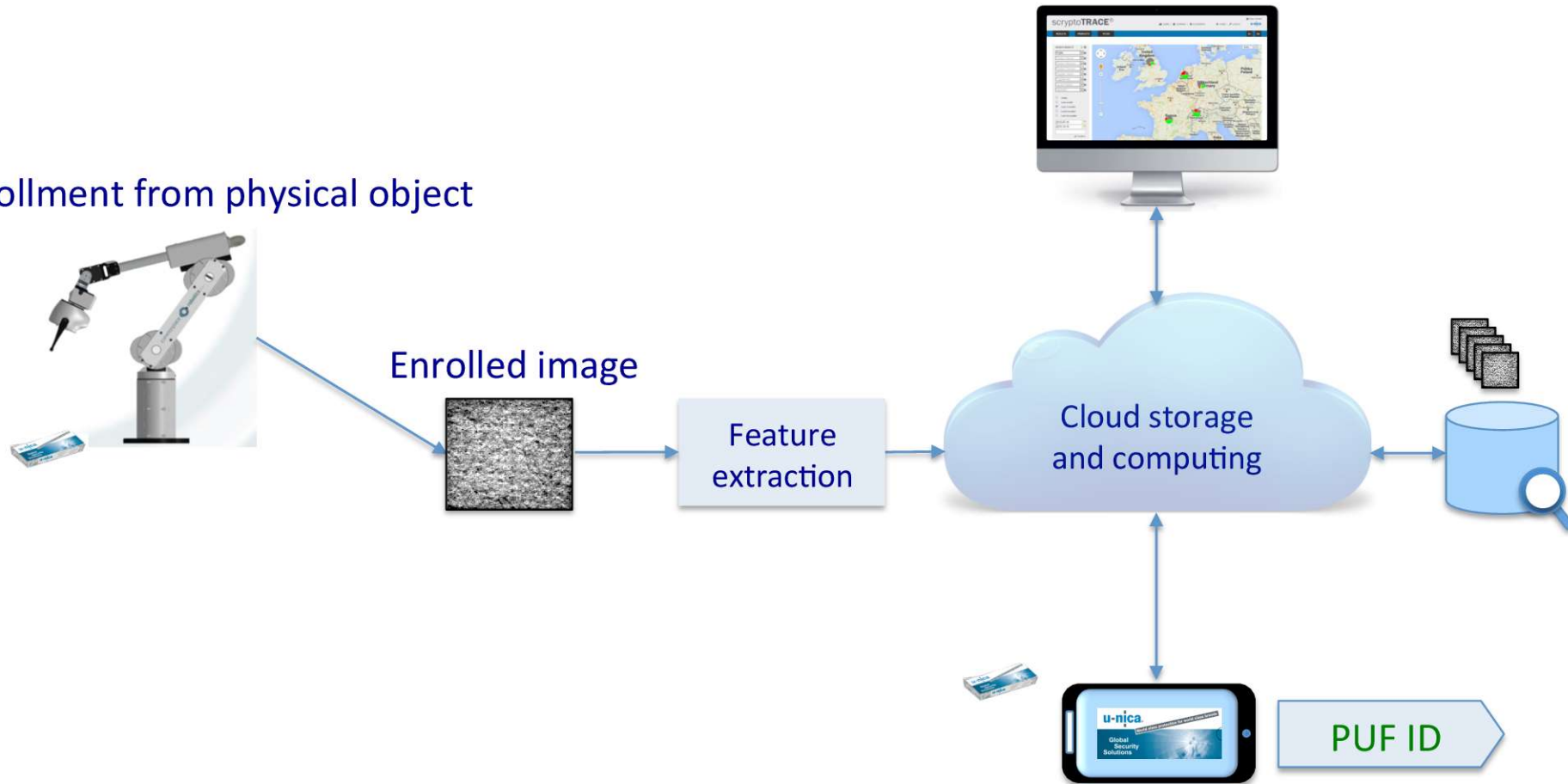
Individually unique PUFs

= unique identifier for Track&Trace

Visibly packages look identical

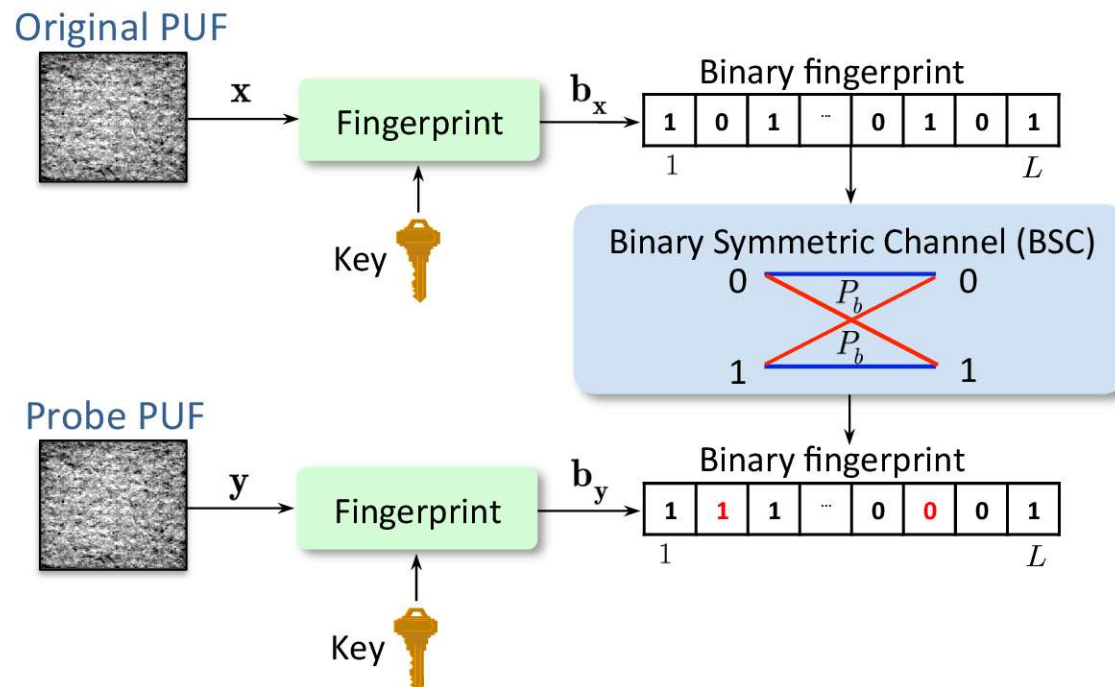
# Object identification

Enrollment from physical object



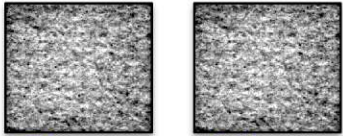
## Open issue:

## Big Data (millions of objects with high-dimensional features)

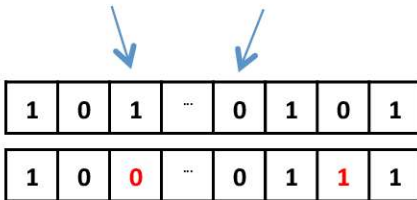


# Properties of PUFs: Close PUFs = close fingerprints

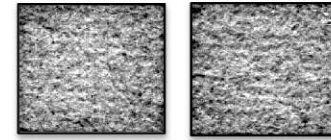
Correct acceptance



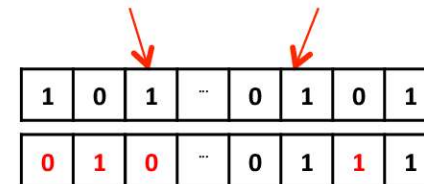
The same object



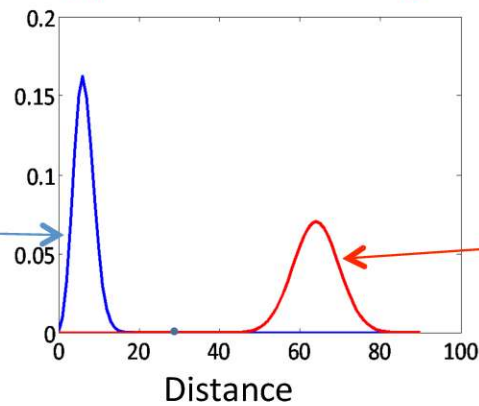
Correct rejection



Two different objects



Hypothesis testing



## Benefits



### Recognize physical objects

Direct interaction with  
physical objects



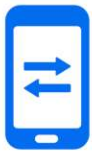
### Detect fake objects

Prevent end user consuming  
fake objects



### Track market activity

Tracking goods, market  
trends and activity



### Smartphone app

Public app not requiring  
any special training



### Real-time reporting

Dynamic reporting and  
visual analytics



### Mobile marketing

Consumer engagement and  
product promotion



For more details: **Swiss Pavilion Halle 6, Stand E30**



Digital Security for Physical World

UNIVERSITÉ DE GENÈVE

Object Recognition

Design Verification

Surface Authentication

[www.unige.ch](http://www.unige.ch)

The banner features a dark blue background with glowing, curved lines in shades of blue and red. The text is arranged in a diagonal sequence from top-left to bottom-right. The bottom section of the banner shows a glowing orange and yellow light trail with binary code (0s and 1s) overlaid on it.

## University of Geneva

Department of Computer Science  
7 rout de Drize  
CH-1227 Carouge/Geneva  
Switzerland

## Industrial partner

U-nica Solutions AG  
Industriestrasse 4  
CH-7208 Malans  
Switzerland

---

[svolos@unige.ch](mailto:svolos@unige.ch) | [sip.unige.ch](http://sip.unige.ch)

# Acknowledgment

Our research has been partially supported by



FONDS NATIONAL SUISSE  
SCHWEIZERISCHER NATIONALFONDS  
FONDO NAZIONALE SVIZZERO  
SWISS NATIONAL SCIENCE FOUNDATION



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Commission for Technology and Innovation CTI



UNIVERSITÉ  
DE GENÈVE

FACULTÉ DES SCIENCES

