UNIVERSITÀ
DELLA CALABRIA

Using a PUF-based Identification Tag for Goods Tracking via Blockchain

Domenico Saccà, University of Calabria

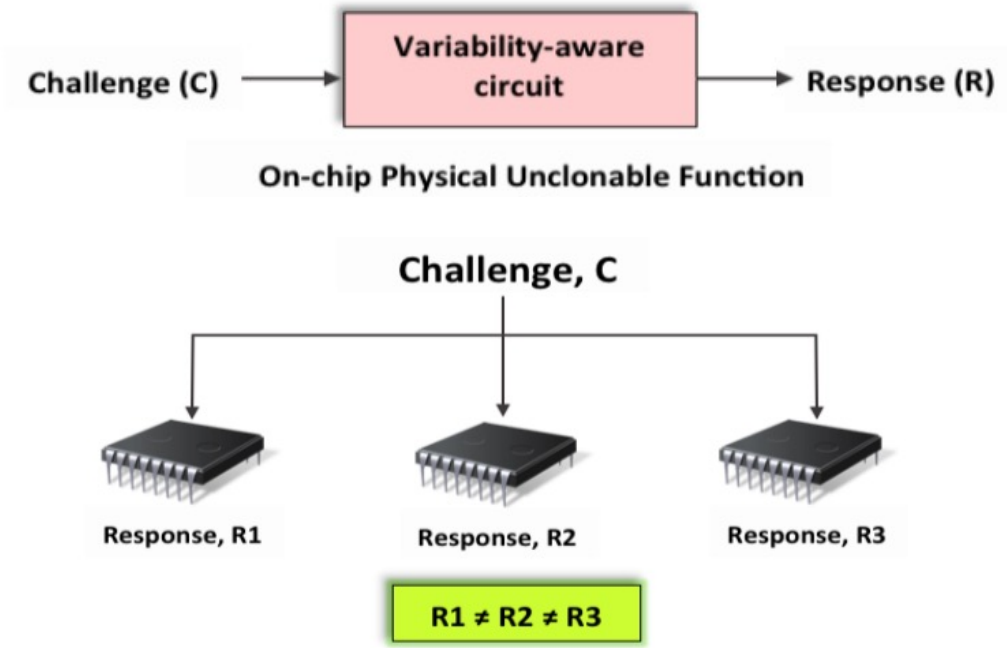
Joint Work with *F. Crupi, R. De Rose, C. Felicetti, M. Lanuzza, A. Rullo, M. Vatalaro*

SILICON PUF

(Silicon) Physically Unclonable Functions (PUFs) use the unique pattern or '**silicon fingerprint**' due to inherent deep ***sub-micron process variations*** in the production process.

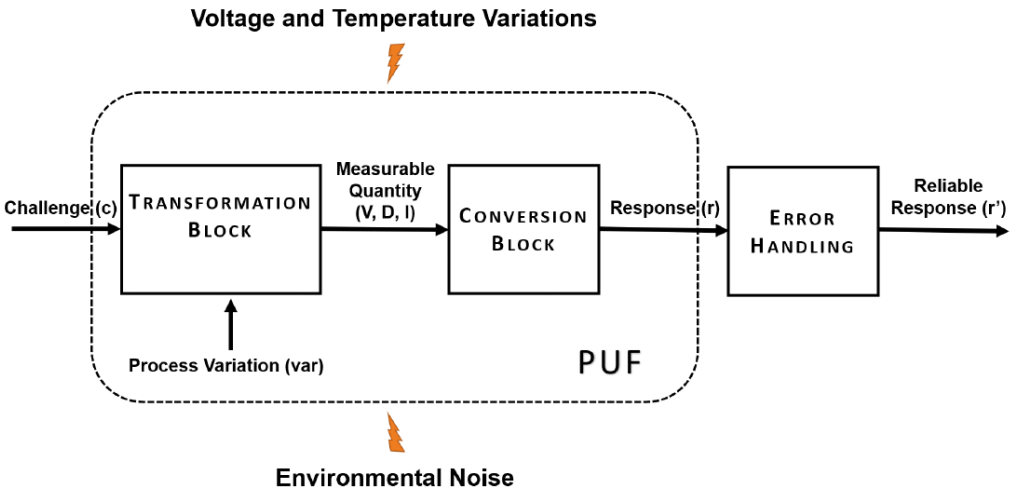
They are virtually impossible to clone or predict!

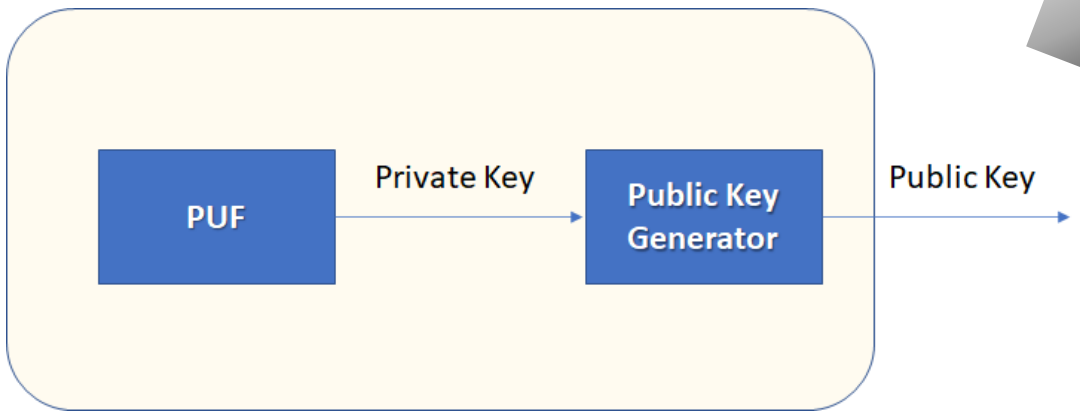
- *Secure key generation and storage*
- *Device authentication*
- *Flexible key provisioning*
- ***Asset management***

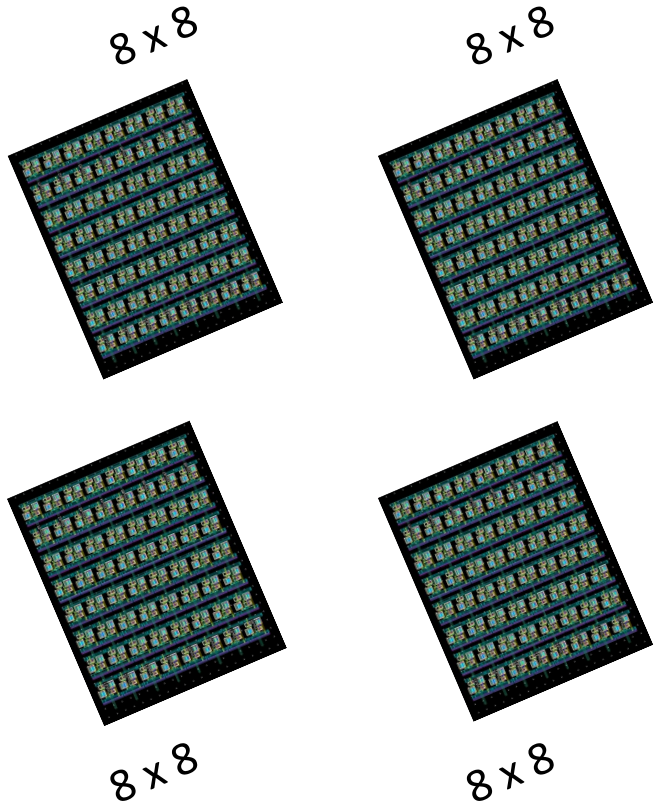


UNIVERSITÀ DELLA CALABRIA

PUF ARCHITECTURE



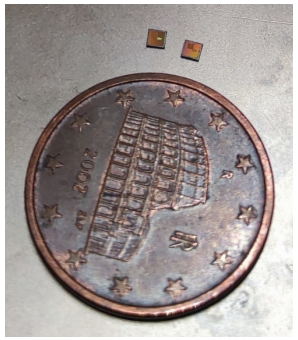


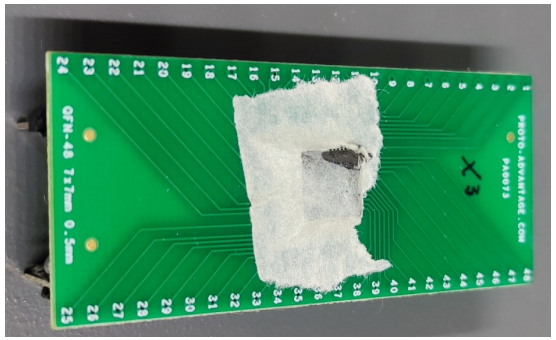


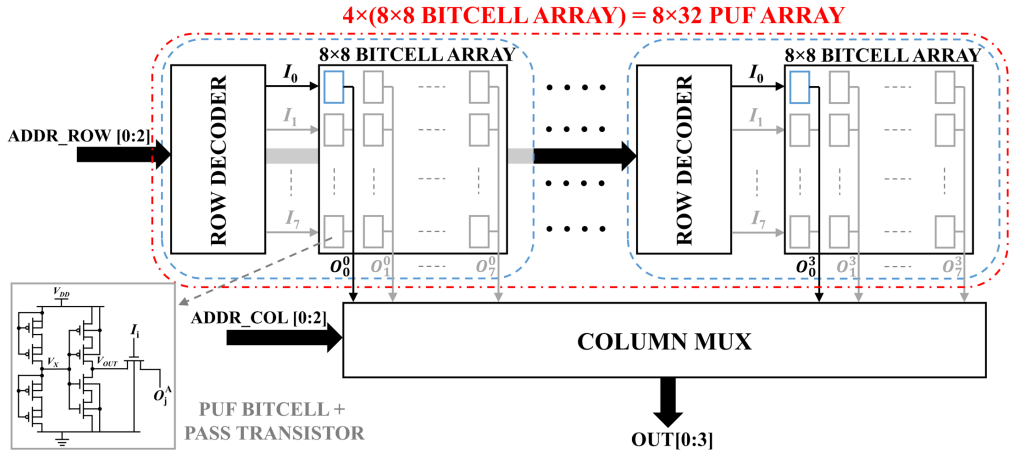
= 256 bit

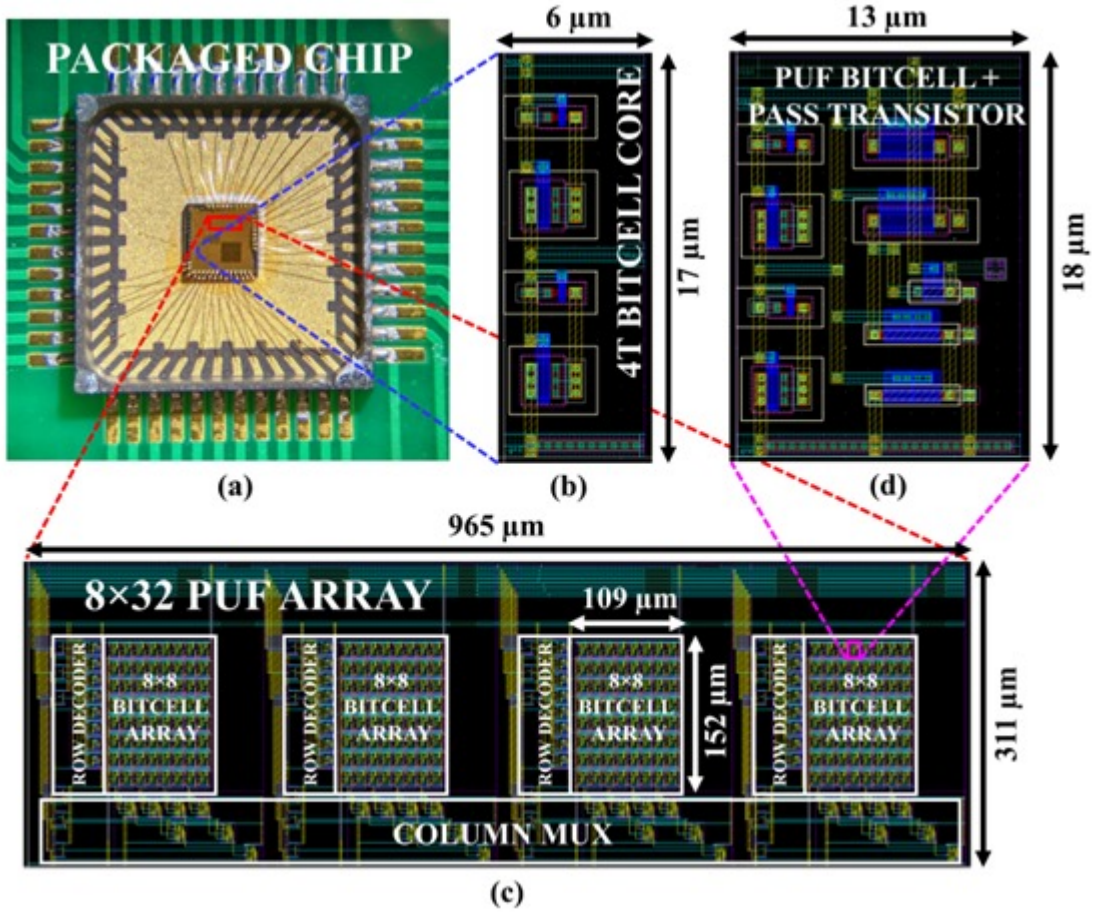
UNIVERSITÀ DELLA CALABRIA

PUF DESIGN AND REALIZATION



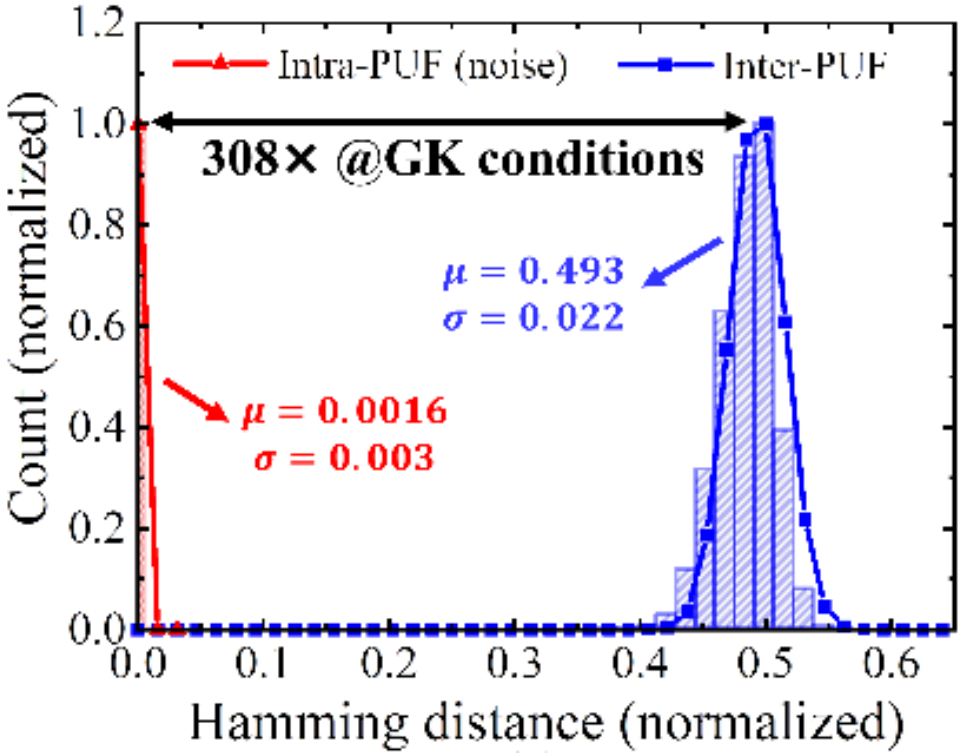


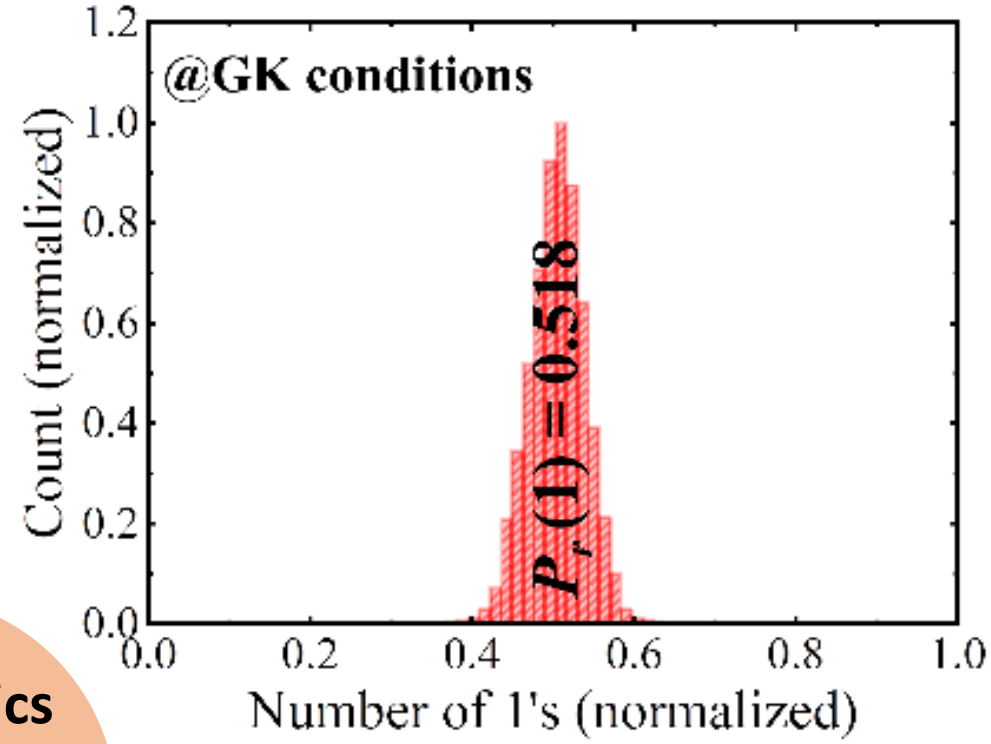




UNIVERSITÀ DELLA CALABRIA

TEST RESULTS





Key Metrics

- Reliability
- Uniqueness
- Randomness

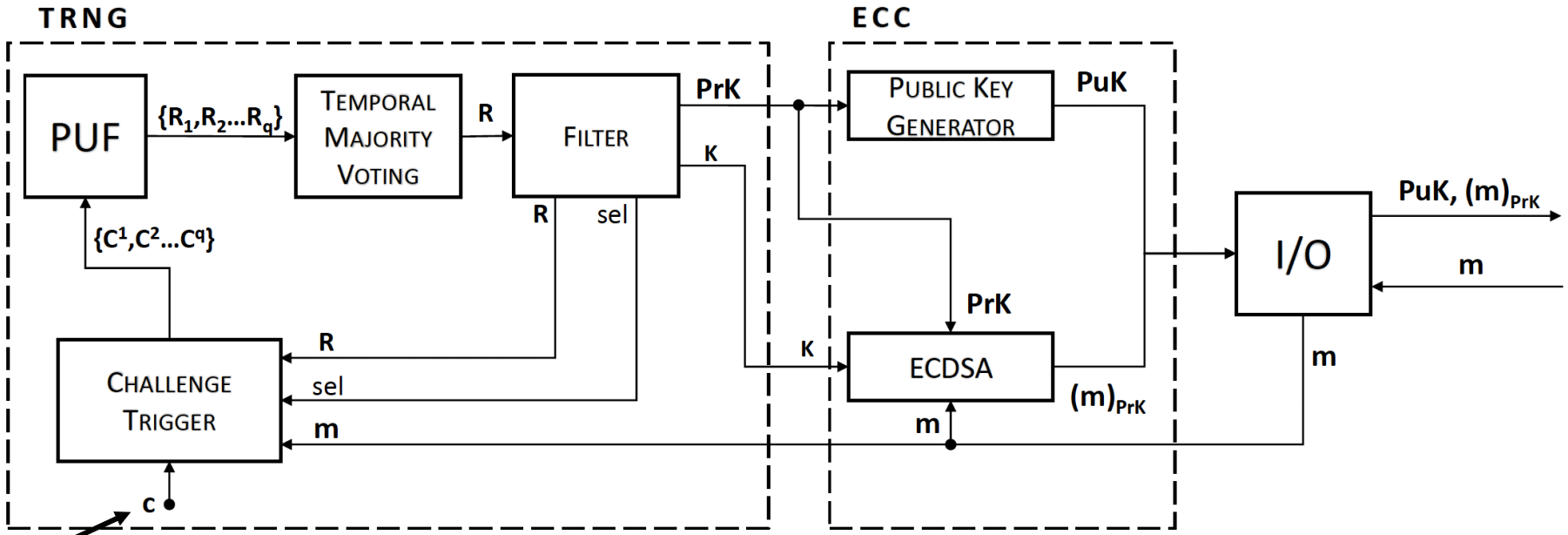
PASSED

NIST TEST:

"A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications"

UNIVERSITÀ DELLA CALABRIA

DEVICE ARCHITECTURE



Built-In Challenge

TRNG

DIGITAL FINGERPRINT

ECC

PUBLIC KEY

SIGNATURE

I/O

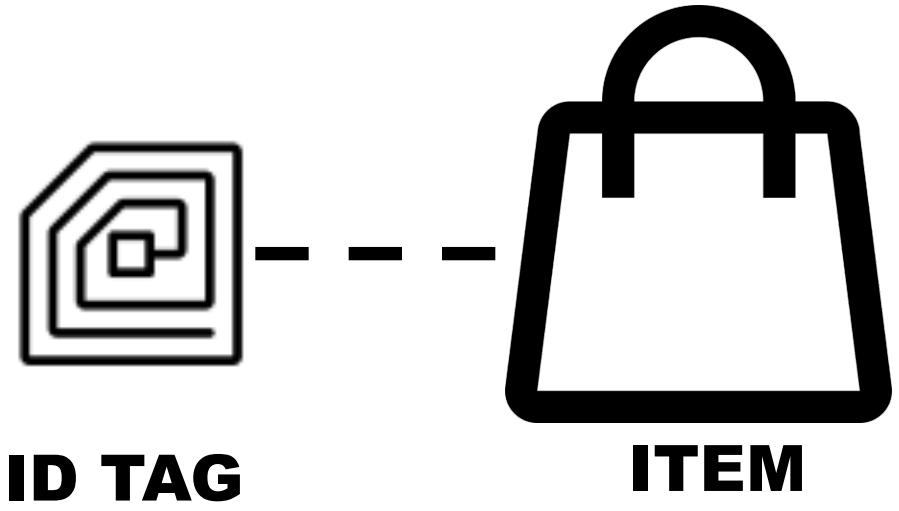
INTERFACE

(*) **Felicetti, C.**, Lanuzza, M., Rullo, A., Sacca', D., Crupi, F., «Exploiting Silicon Fingerprint for Device Authentication Using CMOS-PUF and ECC». The 5th IEEE International Conference on Smart Internet of Things. IEEE SmartIoT 2021 - August 13-15, 2021, Jeju Island, South Korea.

UNIVERSITÀ DELLA CALABRI

USING ID TAG FOR TRACKING PHYSICAL OBJECTS VIA BLOCKCHAIN

Pairing ID Tag and Physical Object (Item)



UNIVERSITÀ DELLA CALABRI

BLOCKCHAIN APPLICATION SCENARIOS

THREE PHASES IN PAIRING ID TAG AND ITEM

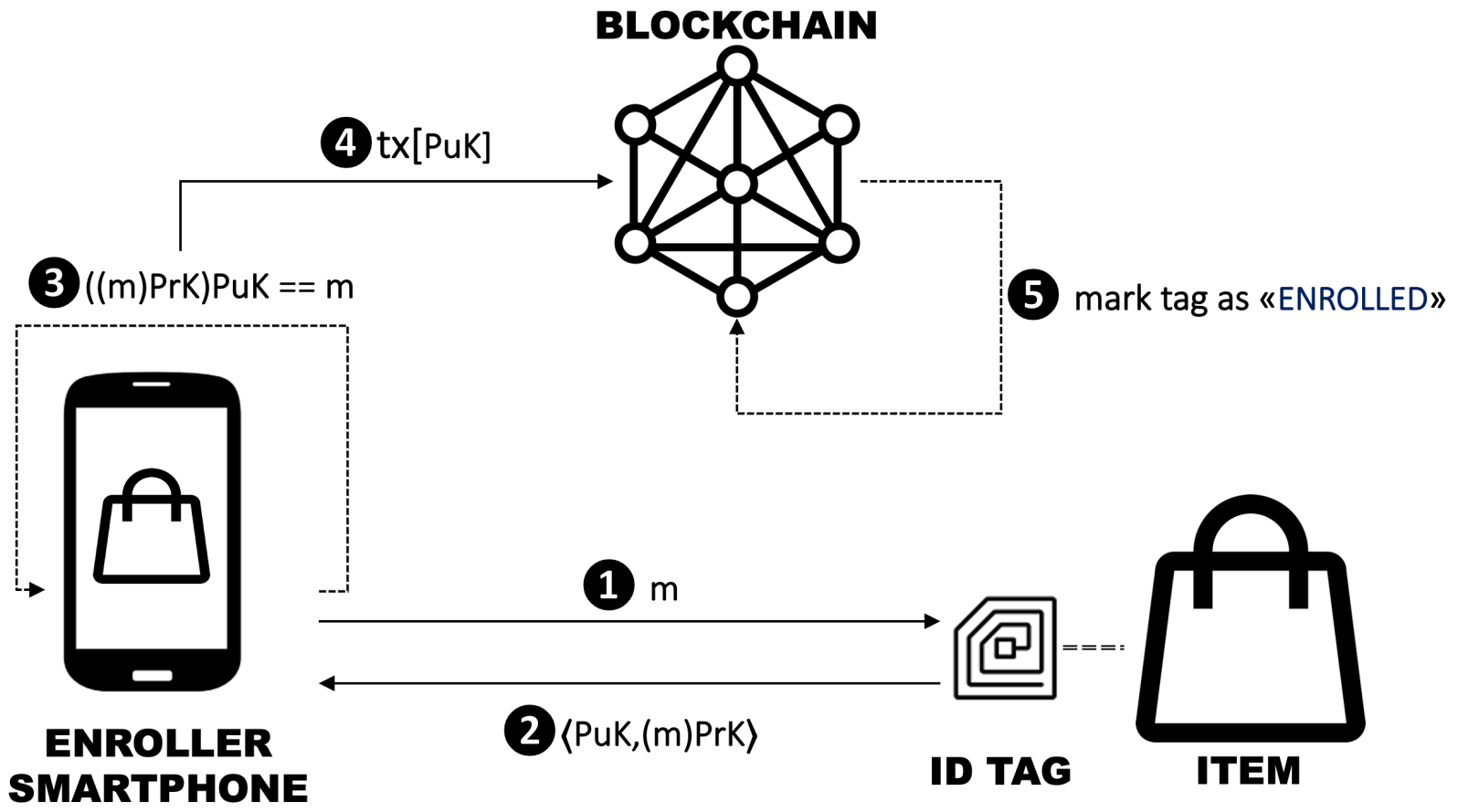
- Enrolment
- Verification
- Consumption

TWO TYPES OF PAIRING

- Uncoupled
- Coupled

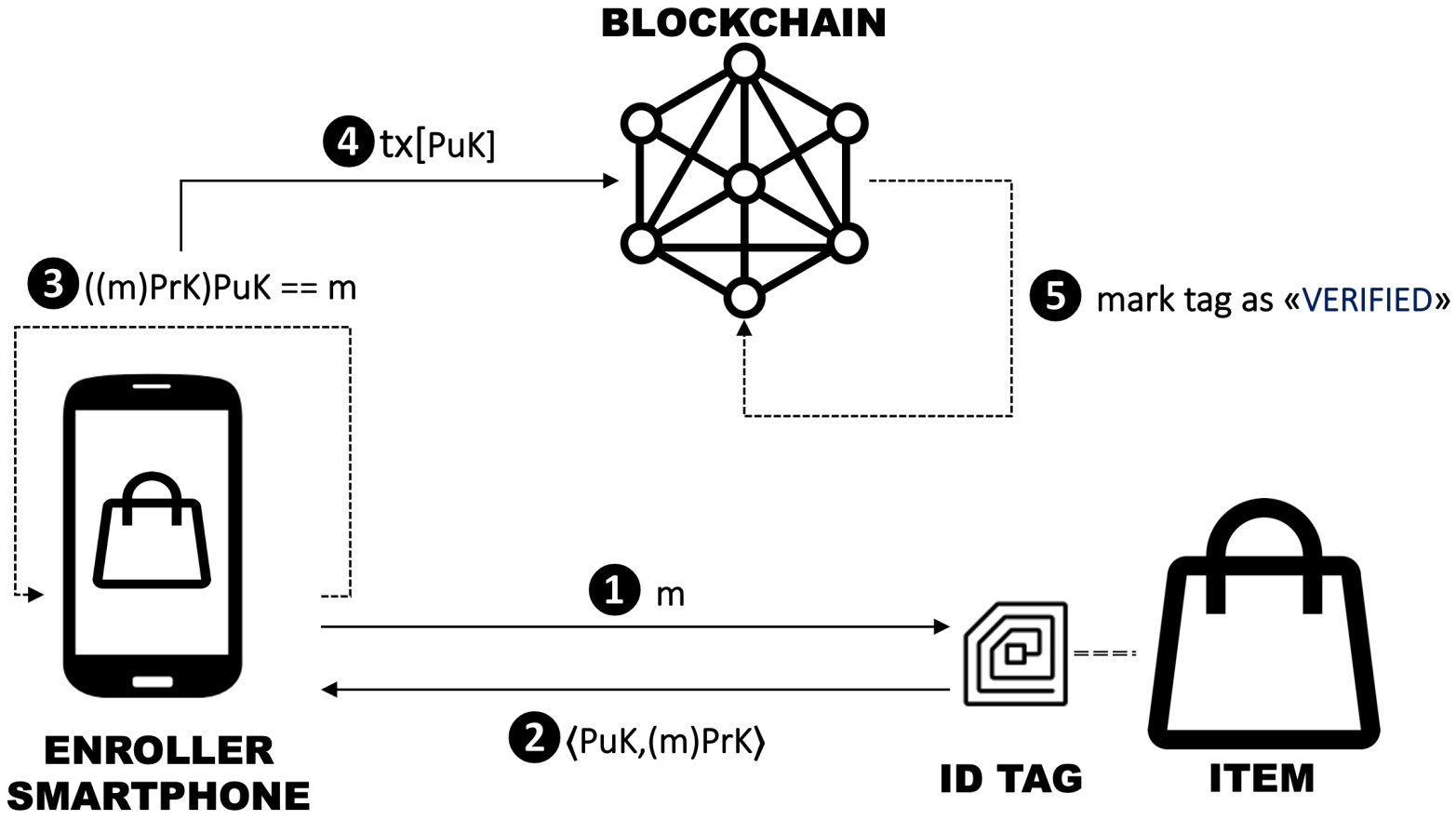
UNIVERSITÀ DELLA CALABRIA

ENROLMENT PHASE



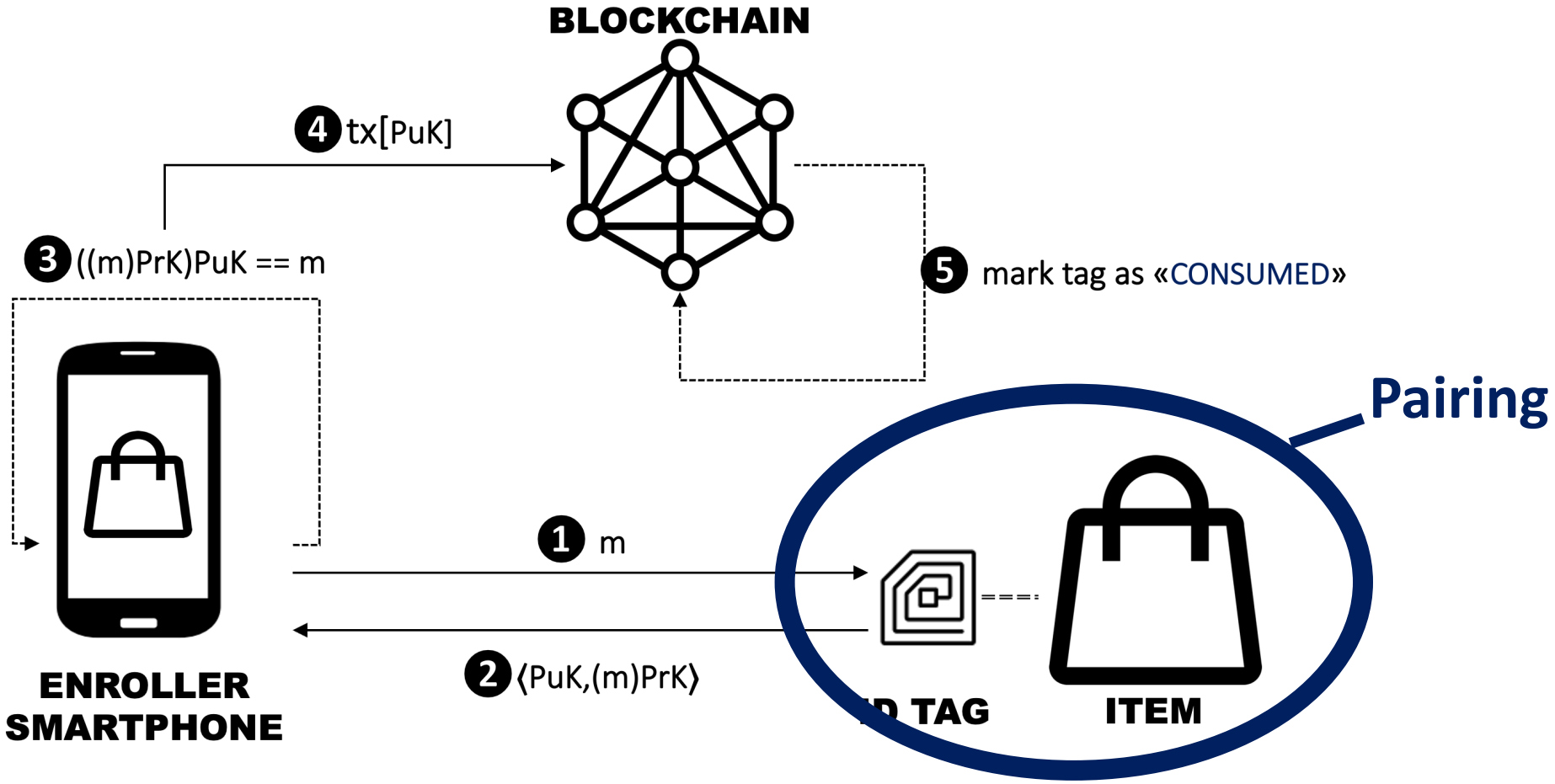
UNIVERSITÀ DELLA CALABRIA

VERIFICATION PHASE



UNIVERSITÀ DELLA CALABRIA

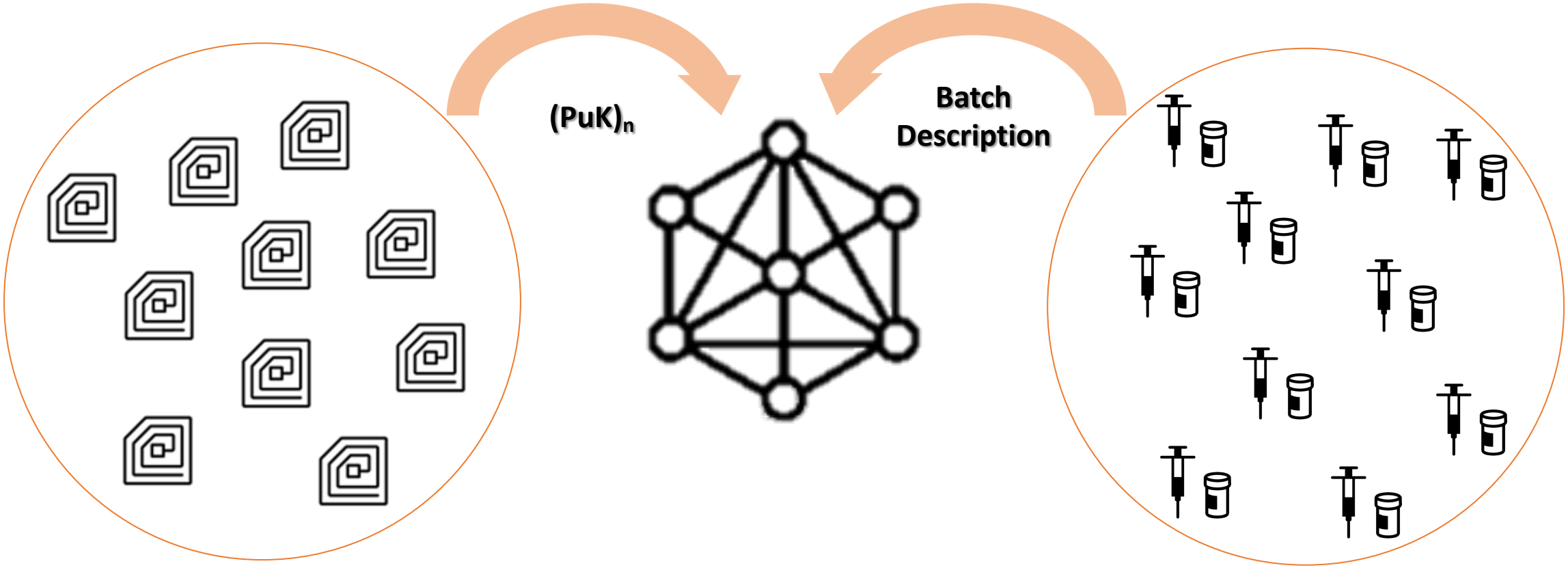
CONSUMPTION PHASE



UNIVERSITÀ DELLA CALABRIA

UNCOUPLED BATCH

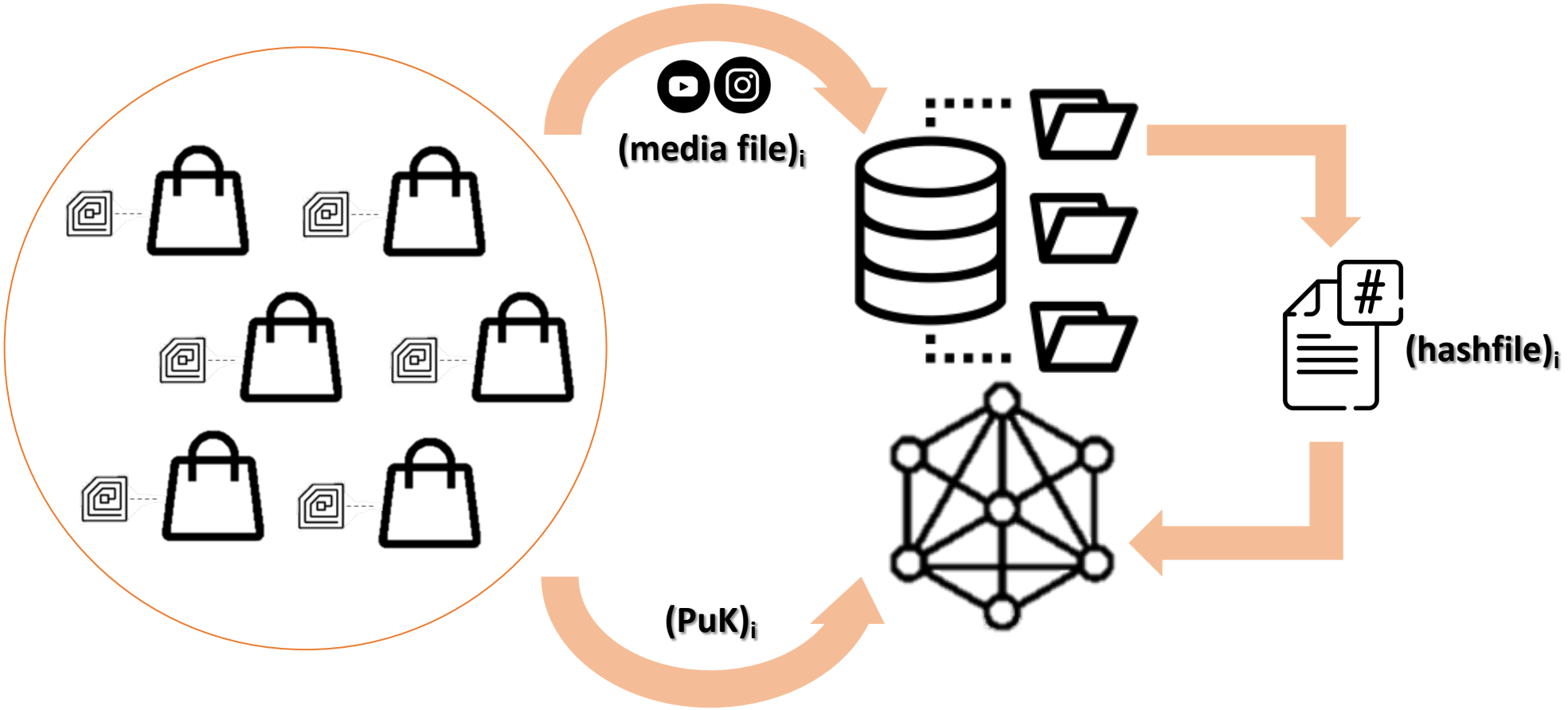
Batch of n products is associated with n tags
without direct coupling between products and tags



UNIVERSITÀ DELLA CALABRIA

COUPLED BATCH

Each Item of the batch is associated with a tag



UNIVERSITÀ DELLA CALABRI

A Related Issue to ID Tag & Physical Object

Pairing ID Tag and Digital Object