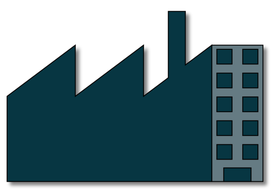
Key reconciliation protocols for correcting errors in PUF responses

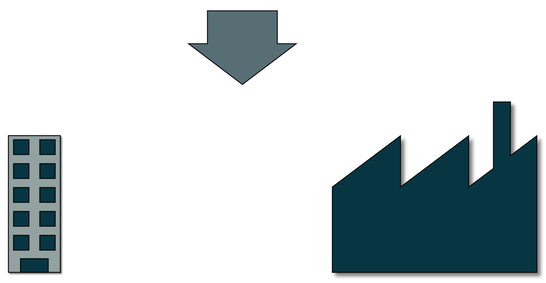
Brice Colombier, Lilian Bossuet
Université de Lyon, UJM-Saint-Etienne, CNRS,
UMR5516, Laboratoire Hubert Curien,
F-42023, SAINT-ETIENNE, France

David Hély
Univ. Grenoble Alpes, LCIS
F-26000, VALENCE, France

b.colombier@univ-st-etienne.fr
www.univ-st-etienne.fr/salware/

All-in-one





How to prevent overbuilding and illegal copying of integrated circuits ?

PUF: generate a secret ID for each circuit

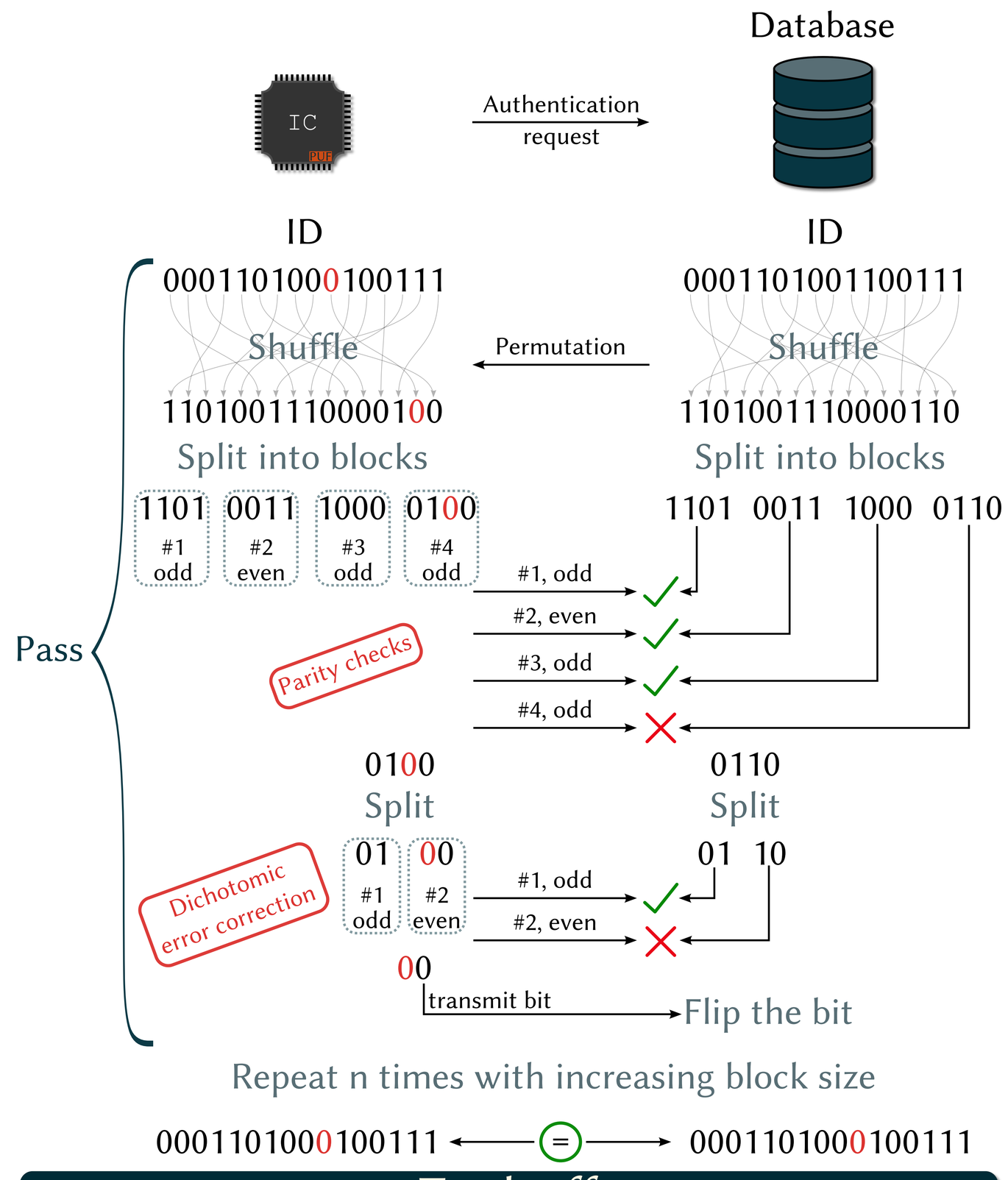
Problem

PUFs are *physical*
IDs change over time

Error correction is **necessary**

How can we make it **lightweight**?

CASCADE reconciliation protocol [1]



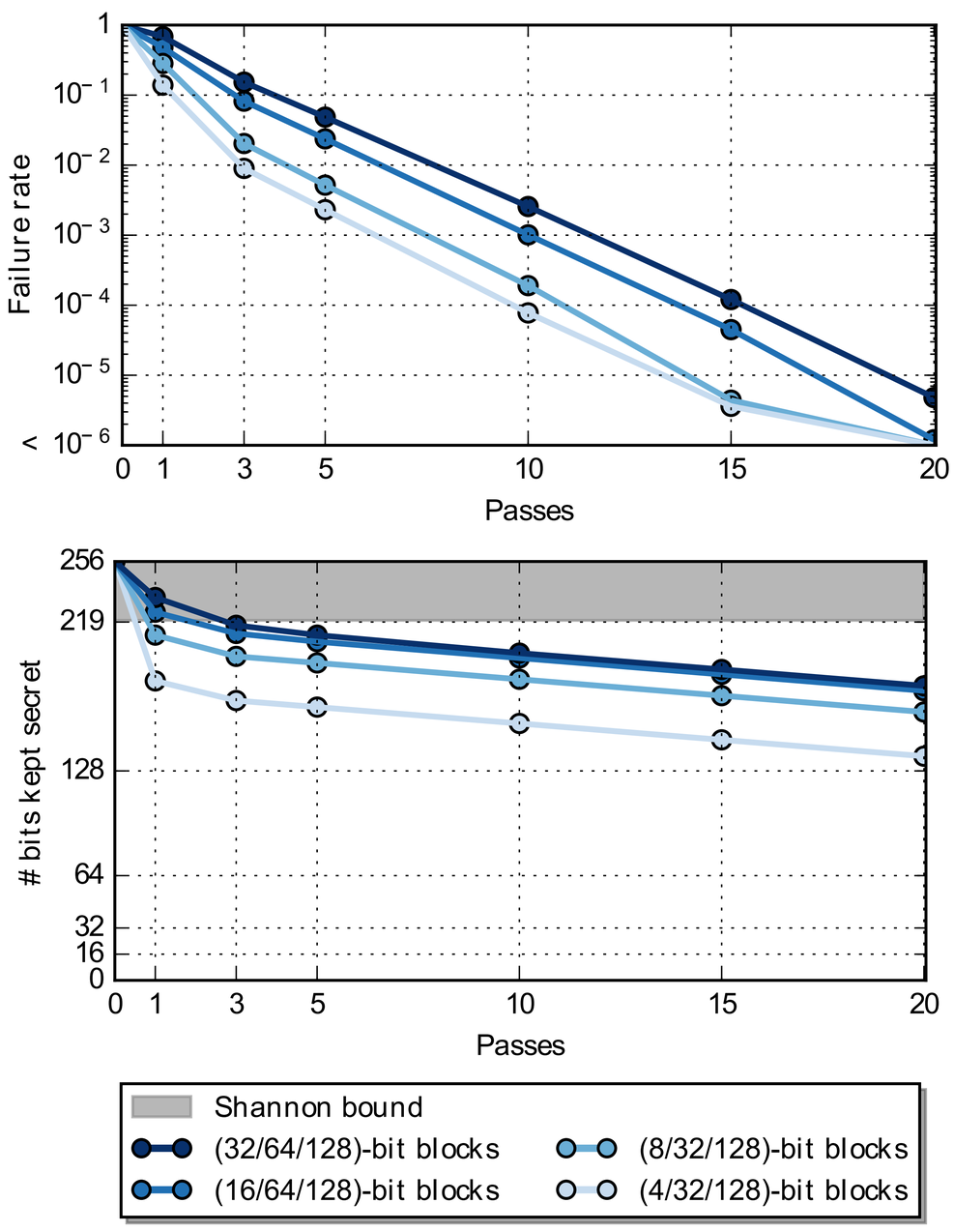
Tradeoff

Leakage VS Failure rate

More passes :
- more errors corrected
- more bits leaked

Experimental results

PUF that generates a 256-bit ID with a 2% error rate



Compared to state-of-the-art:
- same latency or less
- 3x less logic resources

To do next:

- Pair it on a circuit with a real PUF,
- Integrate it in the overall protection scheme.

[1] Brassard, G. & Salvail, L. *Secret-Key Reconciliation by Public Discussion* **EUROCRYPT**, 1993

The work presented in this paper was realized in the frame of the SALWARE project number ANR-13-JS03-0003 supported by the French "Agence Nationale de la Recherche" and by the French "Fondation de Recherche pour l'Aéronautique et l'Espace", funding for this project was also provided by a grant from "La Région Rhône-Alpes".