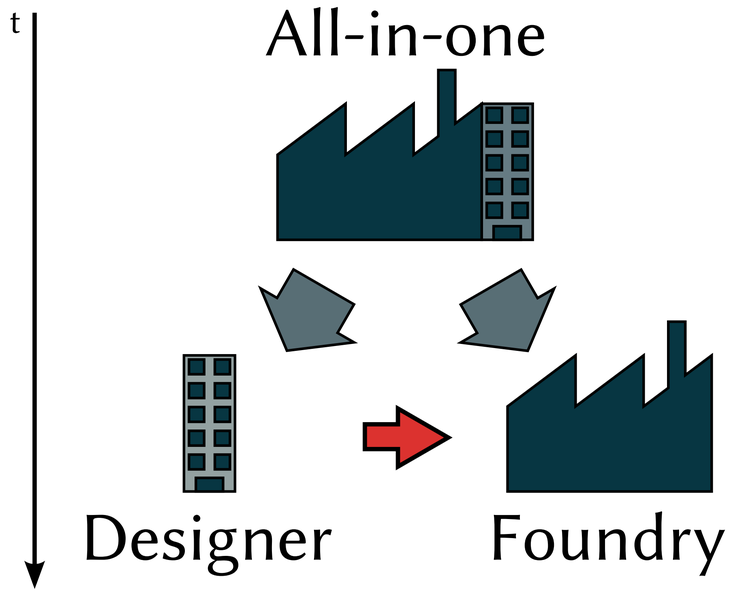
Secure remote activation scheme for integrated circuits

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/



Problem

Once the design is provided to the foundry, the designer cannot control **how many** copies are produced.

~10% of the electronics market is counterfeit **(>$20 billion)**

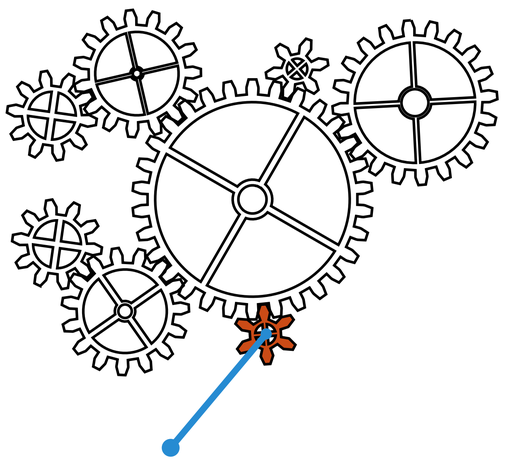
Proposed solution

• The design is modified to make the produced circuit **locked.**

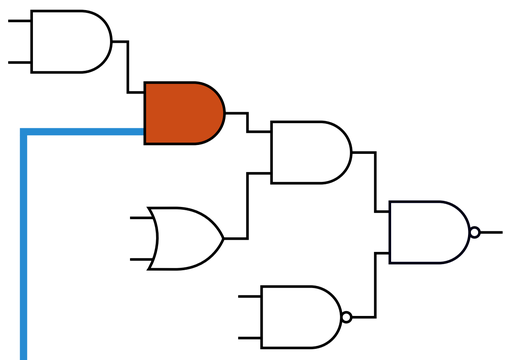
• After production, each circuit must be **individually unlocked** by the original designer who sends a **unique activation key**.

Make the design **lockable**

Gears



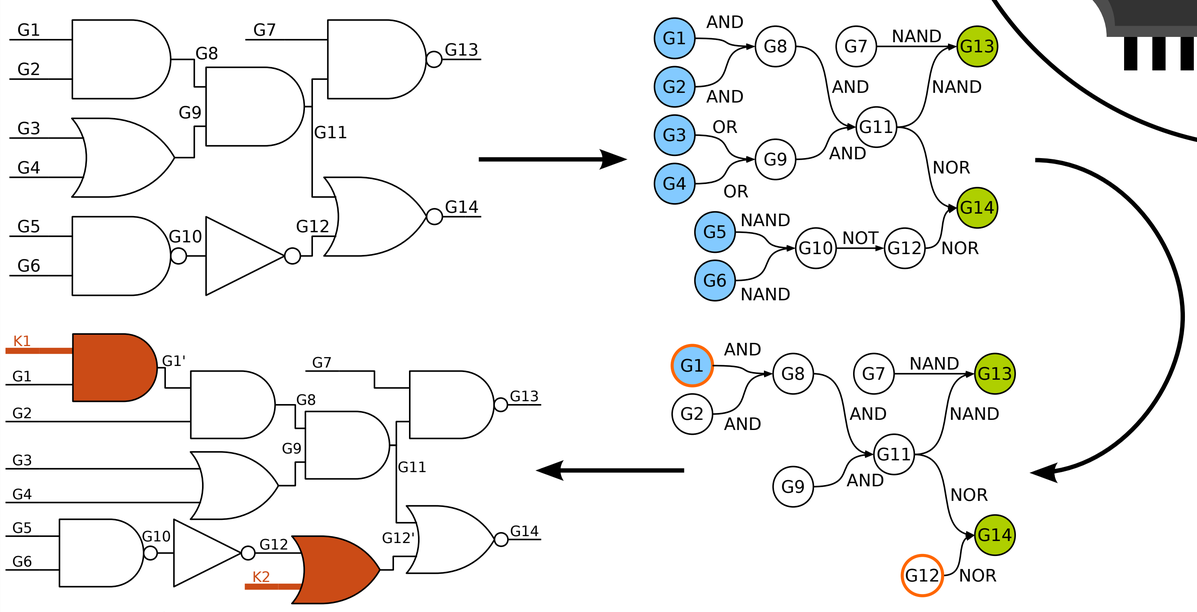
Logic gates



Existing parts
Added, controllable parts
Controller

Force the outputs to a fixed value

Insertion algorithm:

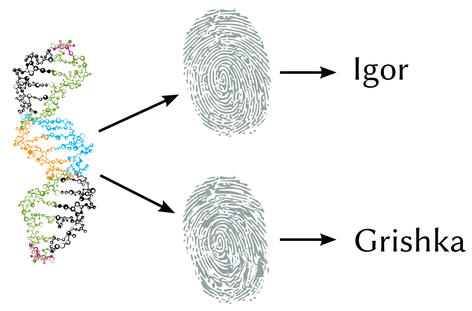


Results:

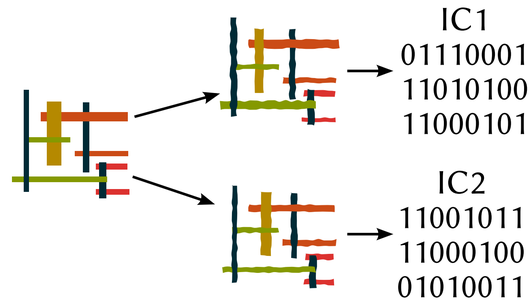
- Only 3% area overhead on average,
- 10000x faster than existing insertion algorithms.

Make the design **uniquely identifiable**

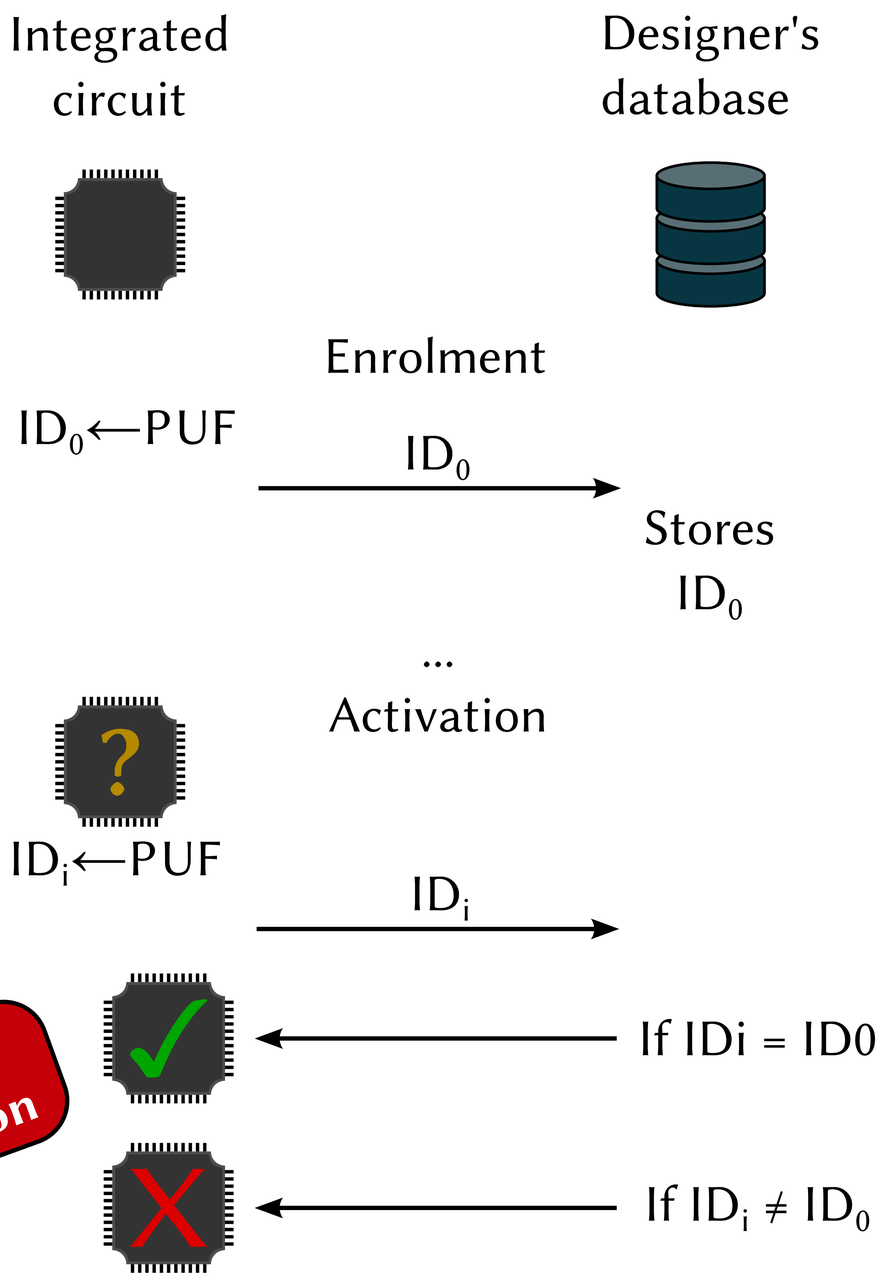
Fingerprint for twins



PUFs for ICs



Extract a unique ID from random physical variations



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".