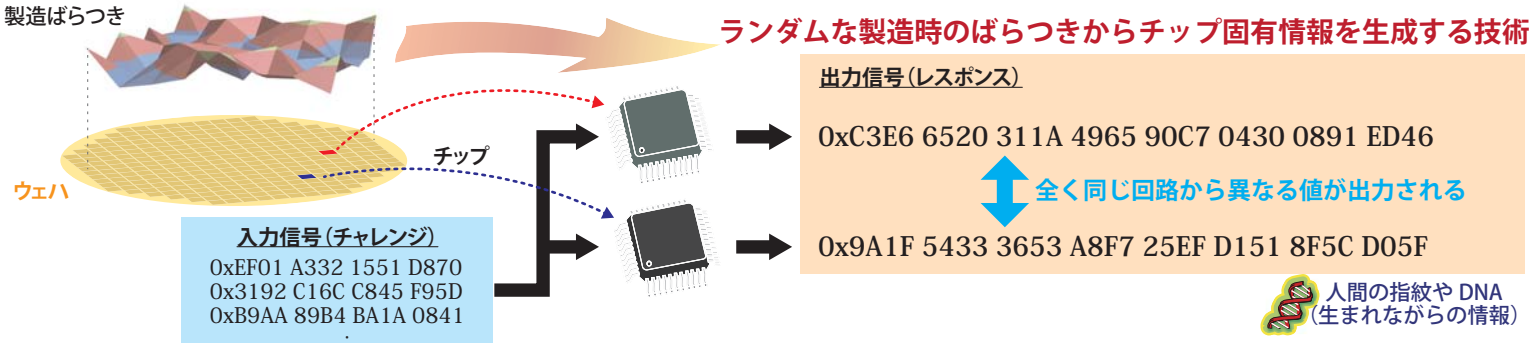
耐タンパディペンダブルVLSIシステムの開発・評価

- 人為的攻撃による内部機密情報の漏洩・複製を防止するVLSIの実現 -

立命館大学，産総研，名城大学，三菱電機グループ

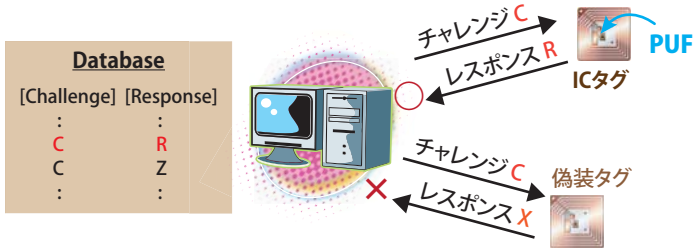
Physical Unclonable Function (PUF)



【特長】 同一入力信号（チャレンジ）を LSI に与えても，内在する製造ばらつきはチップ毎に異なるため出力信号（レスポンス）チップ毎に異なる
また，製造ばらつきを人工的に制御・複製するのは困難

PUF のアプリケーション

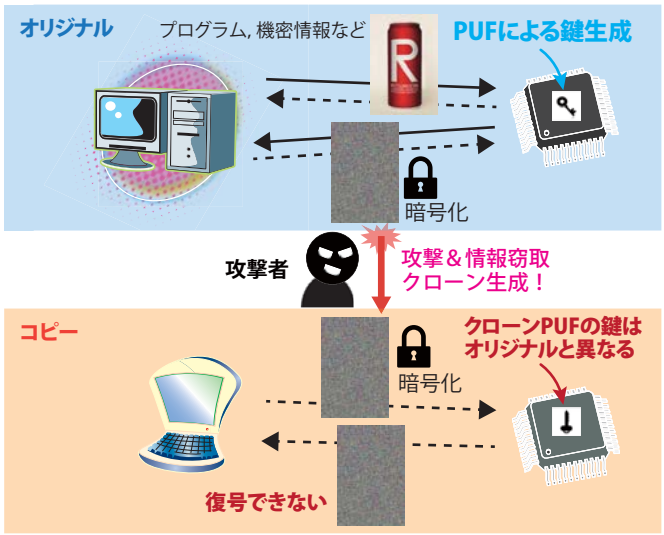
【識別・認証】



不揮発メモリを必要としない安価な IC タグが実現可能

【偽造・複製防止対策】

半導体の模造品が大きな問題
- 模造品発見数は年々増加
- 半導体模造品市場は世界の半導体市場の 5%



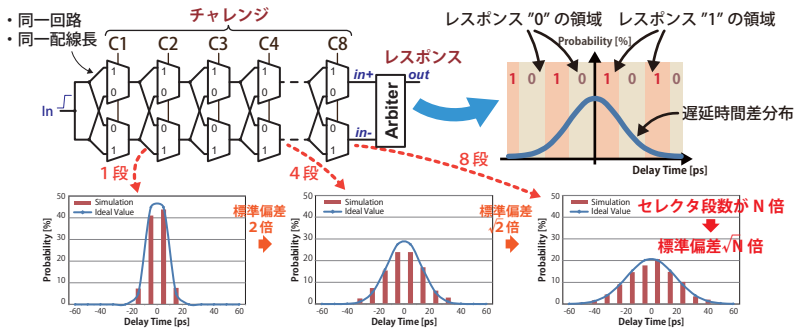
唯一，暗号化したチップだけが復号できる！

試作 PUF 回路

65nm CMOSプロセスで試作
- PUFを用いた暗号鍵生成
- チャレンジ・レスポンス認証　を実証

RG-DTM PUF

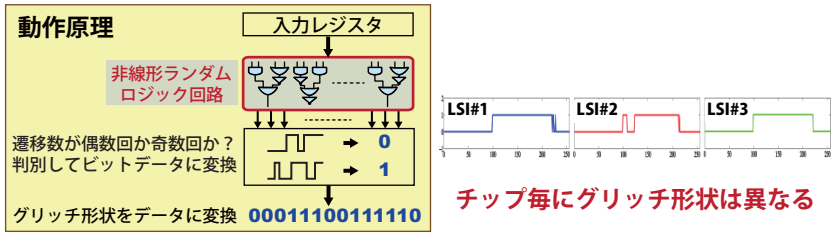
- 製造ばらつきによる遅延特性の差異を利用
- 時間遅延差を測定してマッピングされたレスポンスを生成
- 数多いチャレンジ・レスポンスペアが生成可能



遅延時間差分布は段数増加に伴って広がる

Glitch PUF

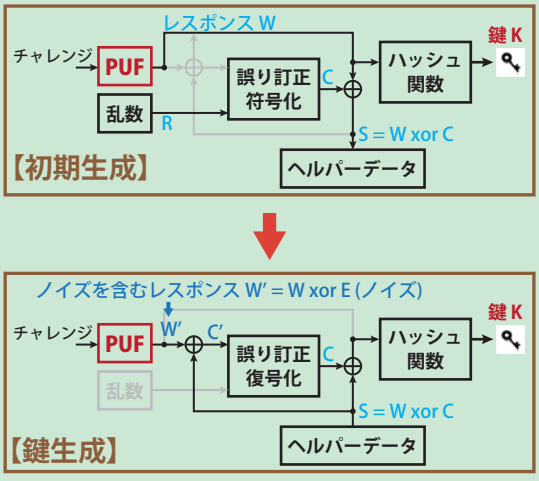
- 既存の攻撃法に耐性があり，且つレイアウト設計での最適化が不要なPUFを開発
- ランダムロジック出力のグリッチ形状に着目した独自方式
- 入手可能な遅延のばらつきパラメータを用いて，設計段階で PUFの情報量とエラーレートの評価が可能



チップ毎にグリッチ形状は異なる

PUF による鍵生成手法

PUFには出力が安定しないビットが存在するので，
誤り訂正を用いて安定した鍵を生成する



独立行政法人 科学技術振興機構 Japan Science and Technology Agency
CREST Core Research for Evolutional Science and Technology