Reliable PUF Design
Using Machine Learning for CRP Enrollment
Xiaolin Xu and Wayne Burleson
Electrical and Computer Engineering
University of Massachusetts Amherst

Abstract
Physical Unclonable Functions (PUFs) that leverage uncontrollable process variations during manufacture, are promising hardware security primitives. However, its operation is sensitive to transient and aging noise, moreover, the impact is of sub-nanometer and sub-picosecond level, thus is difficult (or even impossible) to detect. We proposed a statistical model based on Machine Learning (ML) modeling method, that can effectively mimic the disordered silicon process variations, and help with filtering out unwanted noise with 99.99% precision.

Why Hardware Security?
Examples: - Embedded systems
- Content and IP protection
- Implantable medical devices
- Payment systems.
Solutions: Secure key-storage based on Lightweight PUF;

What is a PUF ?
Naturally disordered process variations make PUFs a promising platform for key generation and storage as well as new keyless PUF-based protocols.

PUFs are sensitive to noise
• Sensitive to environmental noise, like temperature and supply voltage variations;
• Sensitive to device aging;

Machine Learning model
• No need to know the exact sub-nanometer and sub-picosecond process variations, but can model them!
• Model the disordered process variations with hyper-planes;
• Use some known input/output to train a PUF model, that can mimic the PUF behavior, >99.9% prediction rate can be achieved with 3000 CRPs.
• PUF model are of high correlation with that of practical process variation parameters, >99.9% correlation.

Performance
Discard the sensitive inputs while just employing the robust ones:

Raw challenges

Our model

Sensitive to noise? NO employed

• As high as 100% reliability can be achieved, while discarding more suspected CRPs.