# Password based Hardware Authentication using PUFs

Raghavan Kumar
Wayne Burleson

Department of Electrical and Computer Engineering
University of Massachusetts Amherst

# Outline

Introduction

Problem Statement

Proposed Solution

Results

Conclusion

# Outline

# Introduction

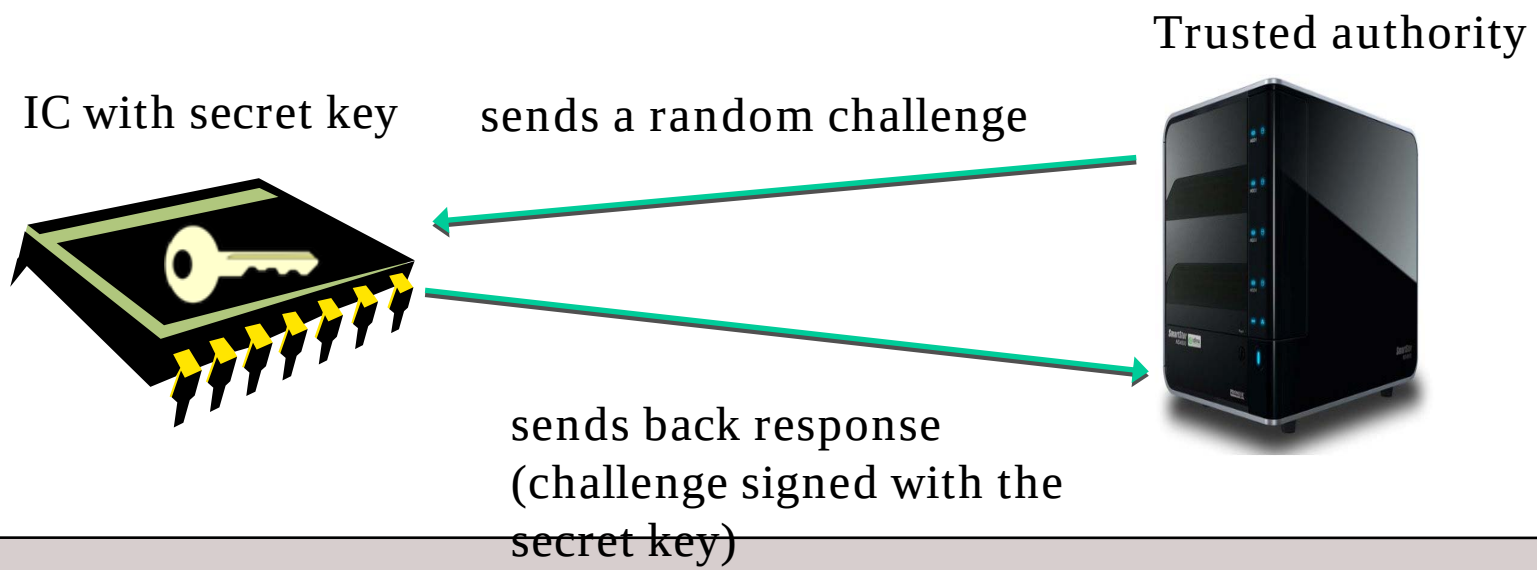
**Key Security Challenges**

- Secure authentication of devices [4]
  - keycards, RFIDs, mobile phones
  - counterfeit detection
- Protection of sensitive IP on devices
  - digital content, personal information
  - software on mobile/embedded systems
- Secure communication among devices

# Introduction

**Traditional Solution**

- Key/Signature stored in non-volatile memory
- Use the Key/Signature for authentication and also other security operations like IP protection



# Introduction

**Problems with key storage [1]**

- Vulnerable to attacks (active and passive)
- EEPROM adds complexity to system
- Non-Volatile memory may be expensive in resource constrained platforms

**Key question: "How to generate inexpensive, secure and unique keys/signatures in an IC?"**

[1] G. Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. In Proceedings of the 44th annual Design Automation Conference (DAC '07). ACM, New York, NY, USA

# Introduction

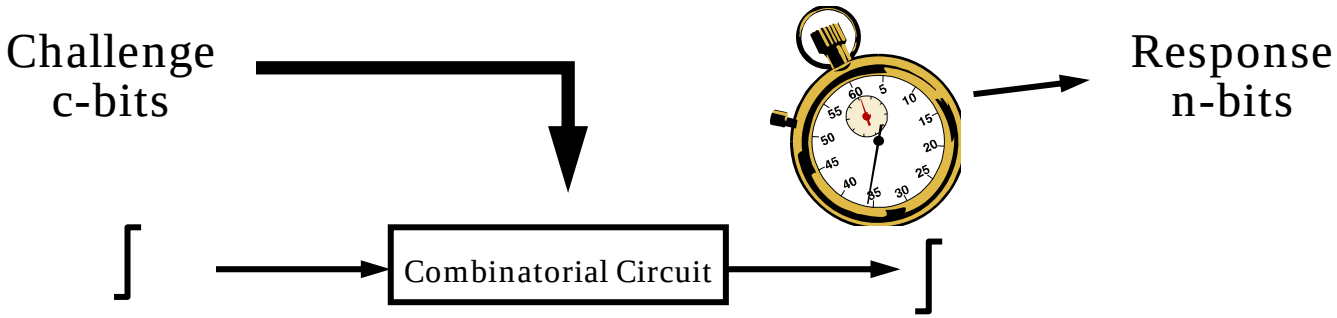
**Physical Unclonable Functions (PUF) [1,4,5]**

- Extracts secret keys from inherent manufacturing/process variations
- Due to process variations, **no two integrated circuits with same layout is identical**
  - Variations are random and hard to predict
  - Relative variations are increasing with shrinking of gate dimensions

# Introduction

**Arbiter PUF (delay-based)**

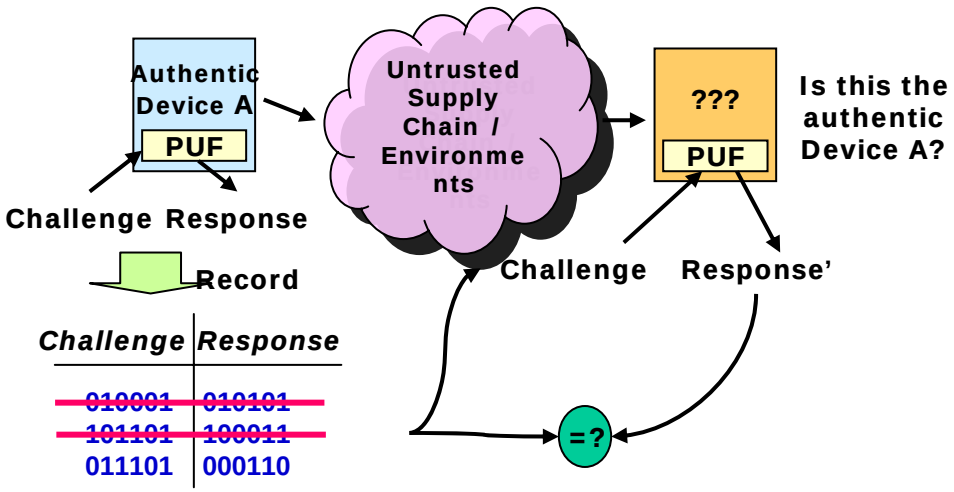
- Generate secret keys using **unique delay characteristics** of each processor chip
- Delay differences arise from variations in gate dimensions, threshold voltage and interconnects



# Outline

# Problem Statement

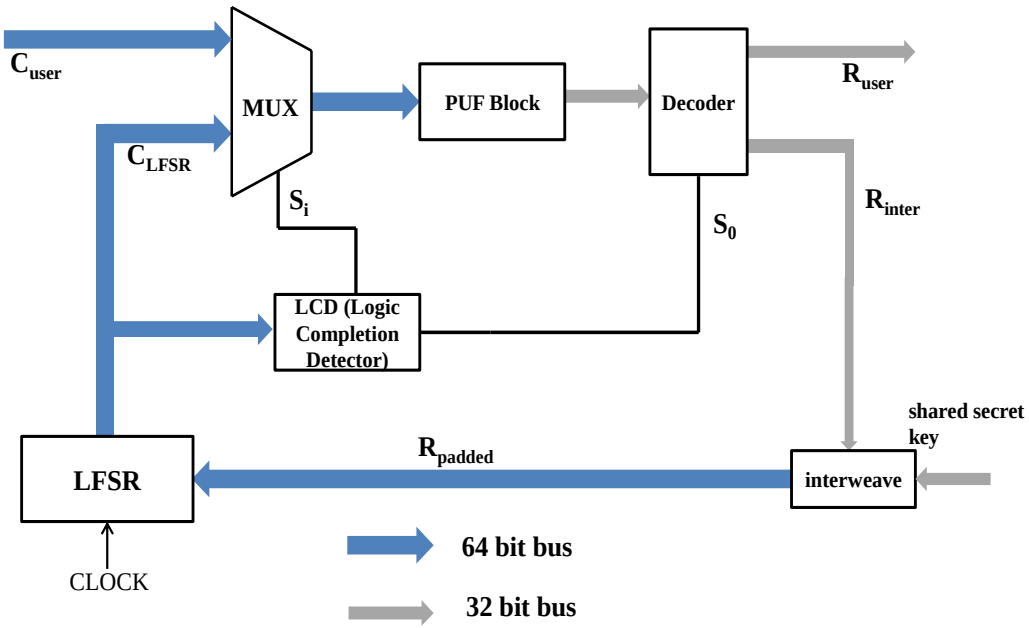
- Arbiter PUFs are vulnerable to machine learning attacks [2]
  - Arbiter PUFs are essentially linear classifiers of challenges and responses in n-dimensional space (n-number of CRP pairs)
- Also, existing PUF based authentication protocols authenticate only the device
  - Even an adversary possessing trusted hardware can use the features



# Outline

# Proposed Solution

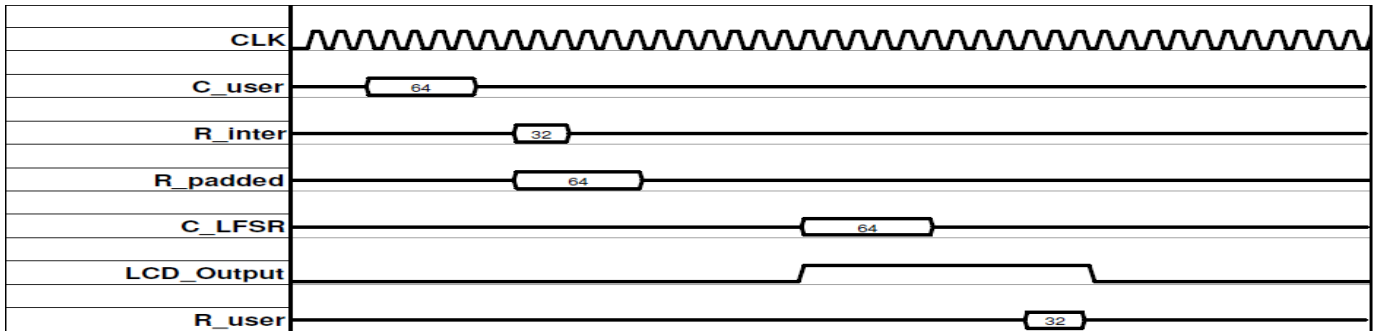
## Password based Hardware Authentication using PUFs (PHAP)




| Signal | Description | Length |
|---|---|---|
| $C_{user}$ | External challenge | 64 |
| $R_{inter}$ | Intermediate PUF response | 32 |
| $R_{padded}$ | Padded PUF response with password | 64 |
| $C_{LFSR}$ | New PUF challenge generated by LFSR | 64 |
| $R_{user}$ | Final PUF response | 32 |

# Proposed Solution

## Timing Diagram




## Authentication Protocol

| **Authenticate - User and Device *S* authentication to trusted authority** |
|---|
| - *S* initiates the authentication request to *TA*<br>- *TA* sends back the pointer to the user<br>- User sends back the tuple <(*ID*,*hash*(user password))> to *TA*<br>- *TA* sends back user authentication acknowledgement if user password is corrrect along with $C_{user}$<br>- User sends back $R_{user}$ after computation<br>- *TA* computes $R_{TA}$ using $D(S)$ and *Sim*<br>- Hardware is authenticated if $R_{TA} = R_{user}$ and time taken for $R_{user}$ computation is $\leq t_{max}$ |

# Proposed Solution

- Simulation algorithm for PUF block can be made public
- Trusted authority can obtain response after authentication is initiated
  - Eliminates cumbersome “enrollment” process
  - Similar in properties to SIMPL systems [3]
- Trusted Authority’s database can be built dynamically

**Sample Trusted Authority’s database**

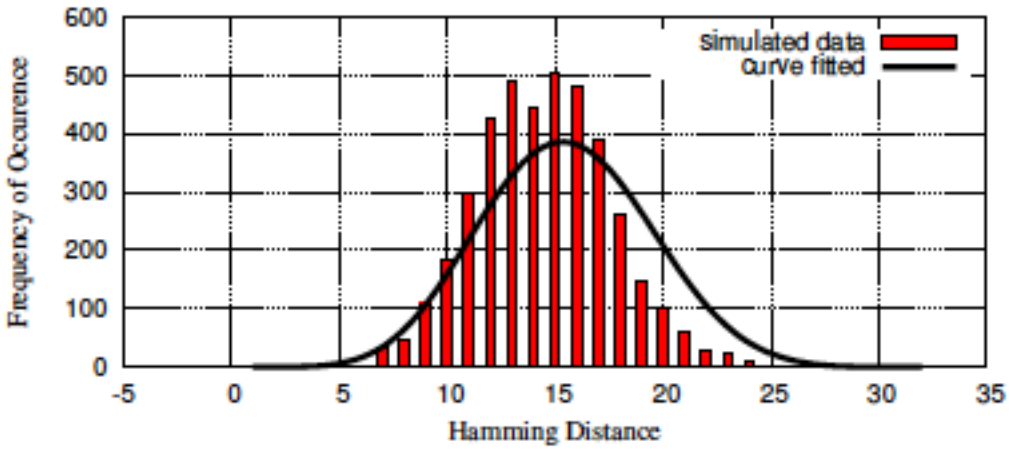
| | Challenge | Response |
|---|---|---|
| $<(ID_1, hash(\text{user password}_1 .. \text{user password}_k)>$ | $C_1 \ldots\ldots C_k$ | $R_1 \ldots\ldots R_k$ |
| $<(ID_2, hash(\text{user password}_1 .. \text{user password}_k)>$ | $C_1 \ldots\ldots C_k$ | $R_1 \ldots\ldots R_k$ |
| ... | ... | ... |
| $<(ID_n, hash(\text{user password}_1 .. \text{user password}_k)>$ | $C_1 \ldots\ldots C_k$ | $R_1 \ldots\ldots R_k$ |

[3] U. Rührmair, “Simpl systems, or: can we design cryptographic hardware without secret key information?” in Proceedings of the 37th international conference on Current trends in theory and practice of computer science, ser. SOFSEM’11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 26– 45

# Outline

# Results

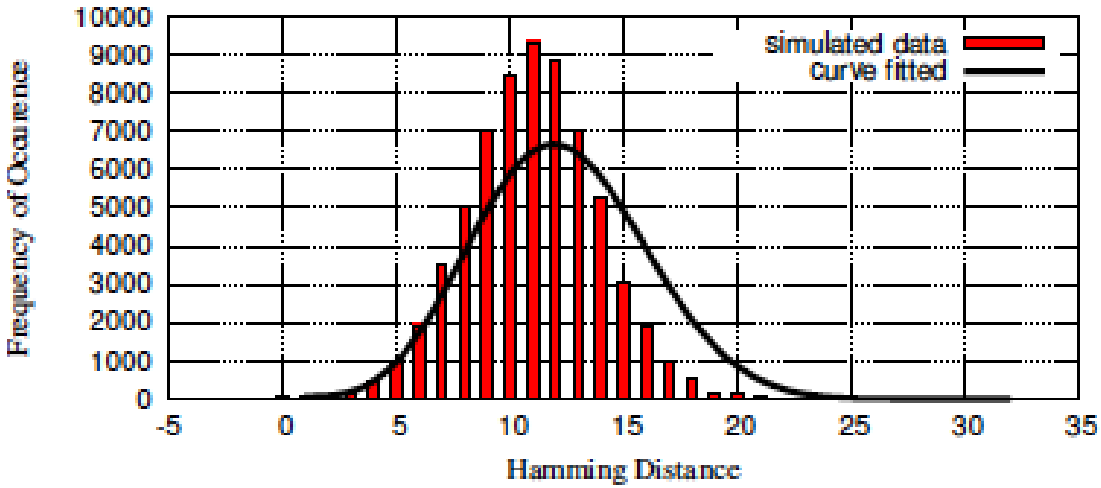
- Uniqueness is one of the major performance metrics of a PUF
  - Computed by analyzing hamming distance (HD) distribution
  - Monte-carlo simulations were run to capture process variations
- Mean Hamming distance = 16 (50% uniqueness)



# Results

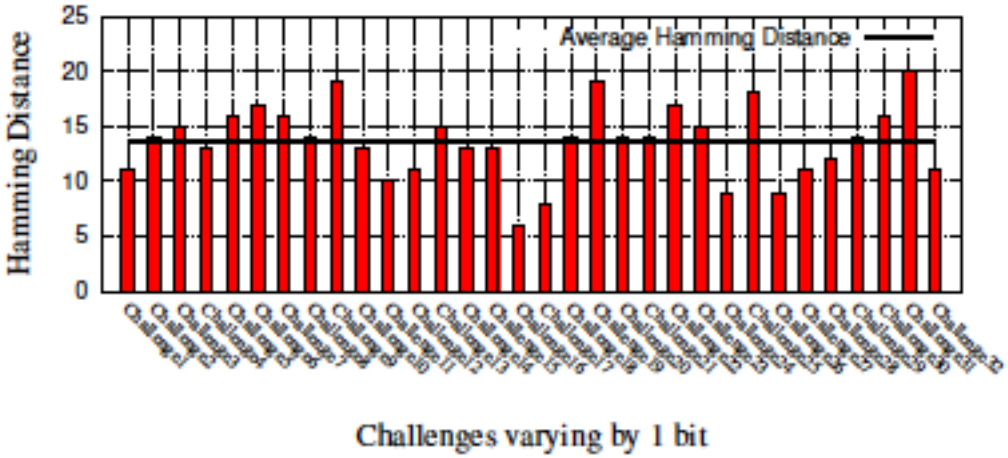
**Sensitivity to various session passwords**

- Around 100 random session passwords were chosen for the experiment
- LFSR rounds was set to 50,000
  - Different number of rounds can be set in runtime
- Mean uniqueness of 41%



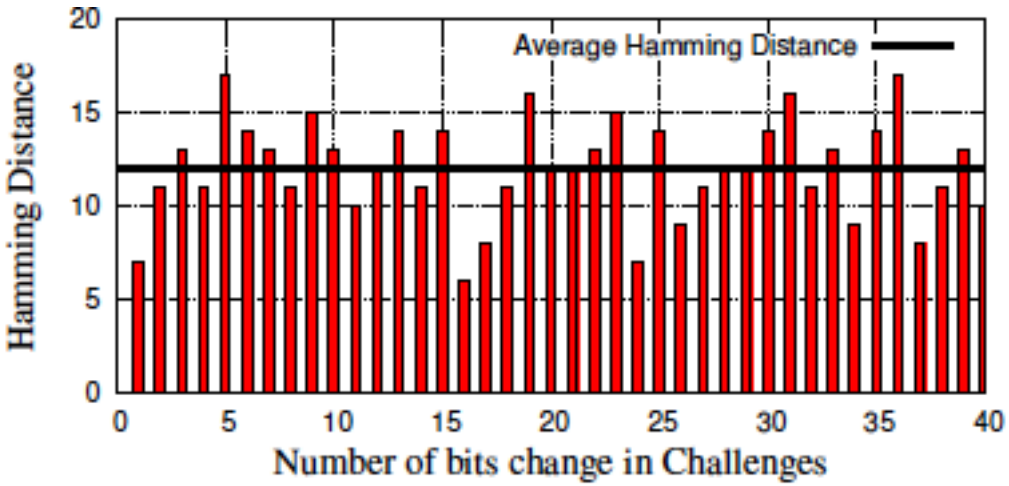
# Results

- Sensitivity to $R_{padded}$ varying by 1 bit
  - Analysis done by carefully picking challenge ($C_{user}$) and session password
- PHAP produces an average of 42% output bit flips for 1 bit change in $R_{padded}$



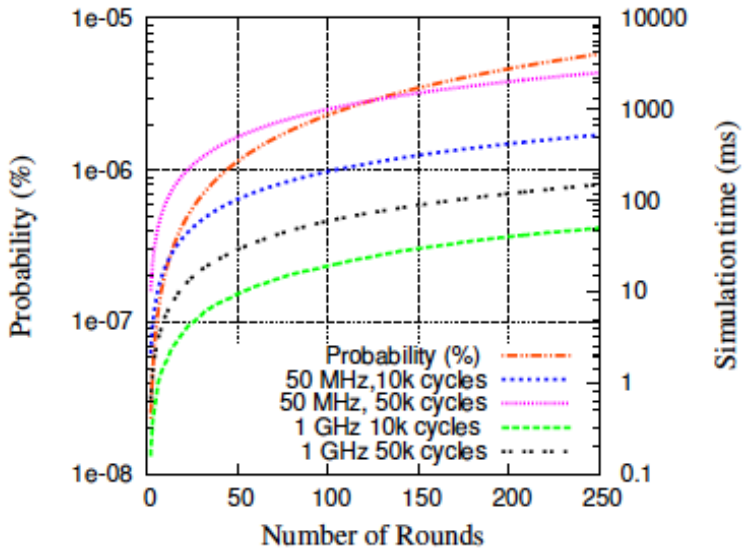
# Results

- Sensitivity to $R_{padded}$ varying from 1 to 40 bits
  - Analysis done by carefully picking challenge ($C_{user}$) and session password
- PHAP produces an average of 38% output bit flips for 1 bit change in $R_{padded}$



# Results

- Simulation time vs. attack probability
  - Attack probability of lower than $10^{-5}$ %, even after 250 rounds
- Authentication interrupted after $t_{max}$ is elapsed



# Outline

# Conclusion

- PUF based authentication protocol presented
- Authentication of both user and hardware
- Uniqueness of system is not compromised
- Future Work:
  - Analysis of reliability under noise
  - Machine learning vulnerabilities

# References

[1] G. Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. In Proceedings of the 44th annual Design Automation Conference (DAC '07). ACM, New York, NY, USA

[2] Ulrich Rührmair, Frank Sehnke, Jan Sölter, Gideon Dror, Srinivas Devadas, and Jürgen Schmidhuber. 2010. Modeling attacks on physical unclonable functions. In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10). ACM, New York, NY, USA, 237-249.

[3] U. Rührmair, "Simpl systems, or: can we design cryptographic hardware without secret key information?" in Proceedings of the 37th international conference on Current trends in theory and practice of computer science, ser. SOFSEM'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 26– 45.

[4] Leonid Bolotnyy and Gabriel Robins. 2007. Physically Unclonable Function-Based Security and Privacy in RFID Systems. In Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications (PERCOM '07). IEEE Computer Society, Washington, DC, USA, 211-220.

[5] L. Lin, D. Holcomb, D. K. Krishnappa, P. Shabadi, and W. Burleson, "Low-power sub-threshold design of secure physical unclonable functions," in Proceedings of the 16th ACM/IEEE international symposium on Low power electronics and design, ser. ISLPED '10.

# Thank You