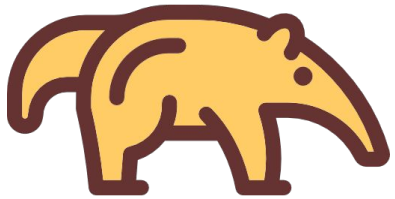


The BugEaters

University of California, Irvine

Team Leader: **Peter the Bugeater**

Presented by: **Jinyao Xu** | **Zuhair Taleb**

Zhanhao Ruan | **Yintong Luo**

Richard Sima | **Songhao Wang (Emeriti)**

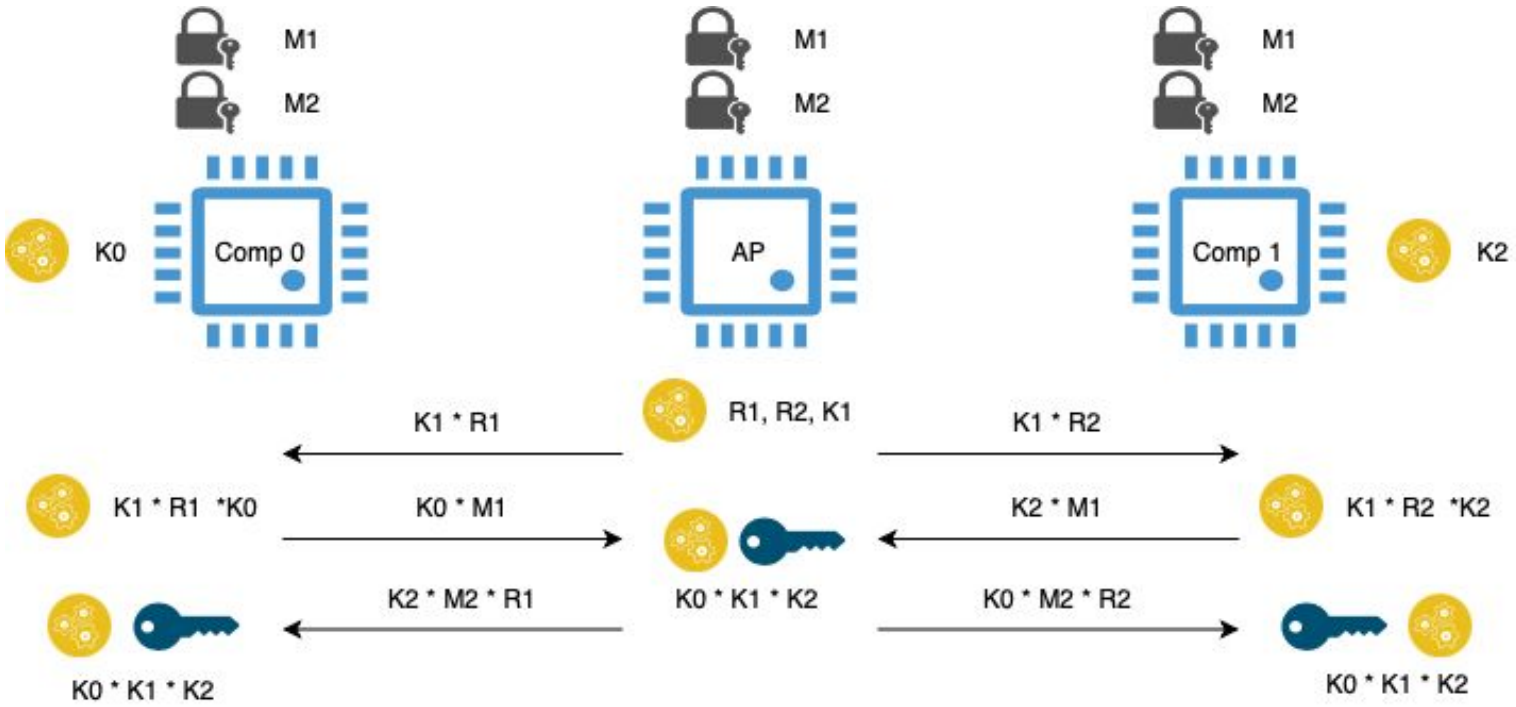
Advised by: **Professor Ian G. Harris**

Outline

- **Towards a Secure Design**
  - Mask-on Key-Exchange-Verify
  - Random-Nonce-Based Communication
- **Towards a Robust Attack**
  - Weak Crypto & Weak Design
  - Brute Force Attack
- **2025-ECTF Directions**

Mask-On Key-Exchange-Verify

- A One-Time-Pad XOR-based Key Synthesis Protocol
  - Randomization of AES key for 3 devices: Prevent Board Switching.

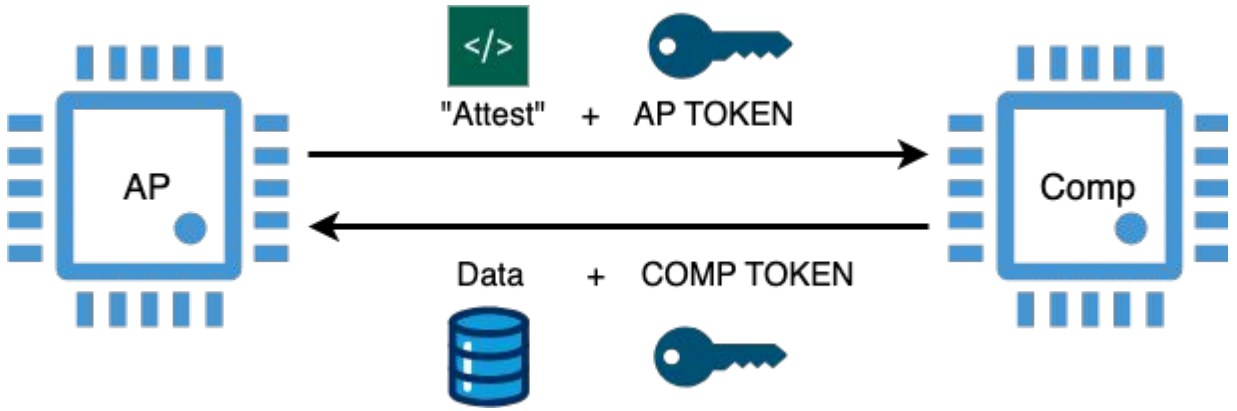


Nonce-Based Communication

- Communication protocols
  - Pre-boot: Two-way handshake
  - Post-boot: Three-way handshake
- Attacks we considered when developing our design
  - Brute force
  - Replay attacks
  - Man-in-the-middle (MitM)
- Attacks we didn’t consider
  - Side channel 😭

Weak Crypto & Weak Design

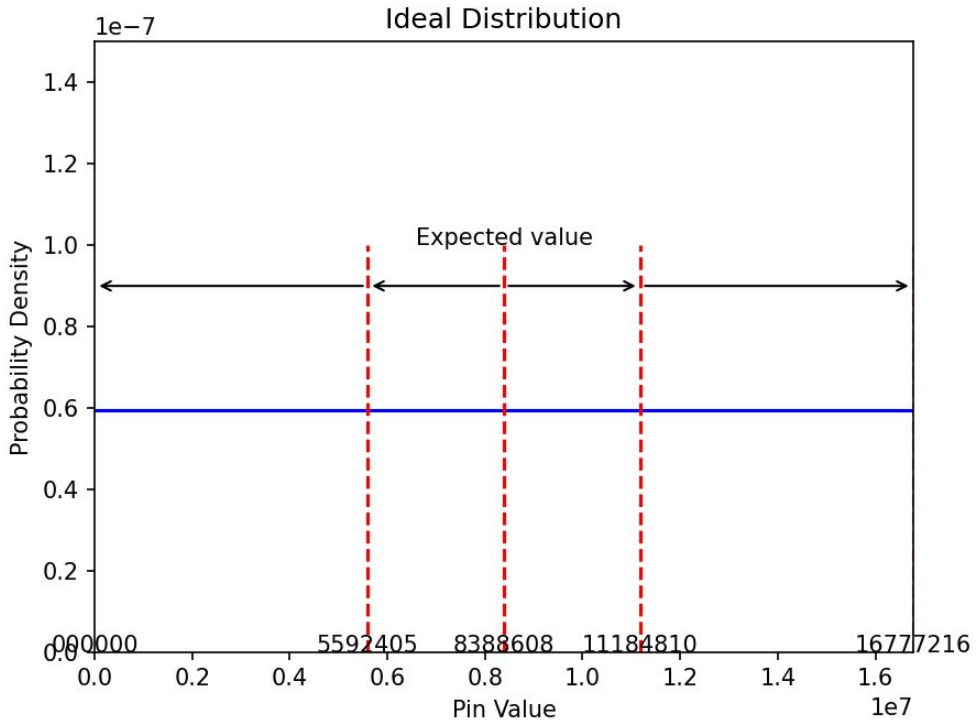
- Replay Attack to Get Firmware Token(Recognition Key)
  - The design validates the authenticity of the firmware by sending and validating tokens.
  - The tokens are static once built and are sent in plain text.
  - We built a malicious component with their codes and printed out the AP(Application Processor) token through the message sent from AP.
  - We used the acquired AP token to build a malicious AP and used it to trick the real Component to send the Component token back.



Brute Force Attack — Simple but effective

- Target designs with no lock-out time delay for incorrect input

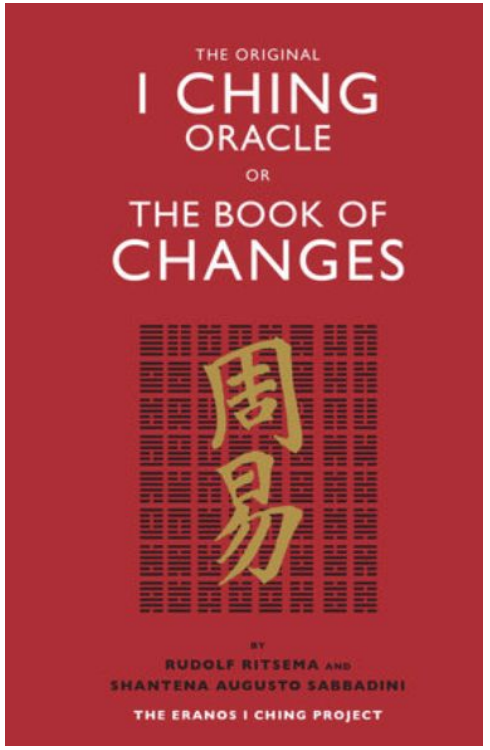
Strategy:



$$E[X] = \int_a^b x \; 1/(b-a) \; dx$$

$$= 1/(b-a) \int_a^b x \; dx$$

$$= (a+b)/2$$



Looking Ahead: 2025

- Secure designs against our attacks
  - Time delay (prevents brute force)
  - Nonced encryption: prevents replay attacks

- Would some of your attacks also be successful against your own system?
  - Our design was heavily designed with replay attacks in mind, as well as a secure key exchange algorithm and thus none of the attacks we conducted would’ve been successful

- With more time and resources, what other things would you have done?
  - We’d only realized that side channel attacks were much more feasible and effective than we expected once we entered the attack phase, so that’s an aspect we’d like to learn to perform and defend against for next year. Additionally, we tried to but were unsuccessful in setting up a breadboard to perform a man-in-the-middle attack

Additional Acknowledgement

- **Additional Members**
  - Xiaozheng Li
  - Emma Xiao
  - Yeseong Moon
  - Zhengxuan Li

Criticism Or Questions?