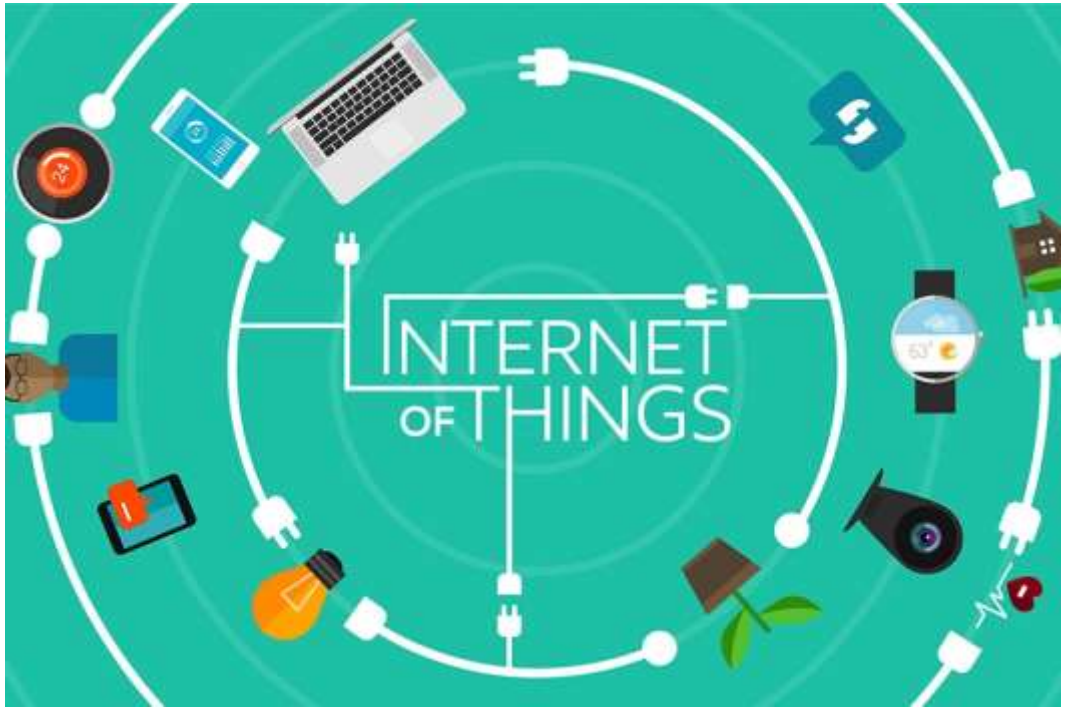
A Reliable Authentication Method for the Internet of Things Devices

Arslan G. Mustafaev , Abdulhamid Y. Buchaev
Department of Information Technologies and Management
Dagestan State University of National Economy
Makhachkala, Russia
arslan_mustafaev@mail.ru

Internet of Things security challenges

Constraints on IoT devices limit the ability to process information at speed – there is a limited CPU, memory, and energy budget. Challenging forms of security are required which satisfy the competing goals of strong performance and minimal resource consumption. The constraints in size and power impact most significantly on efforts to maintain confidentiality and integrity in IoT systems.



Internet of Things security challenges

For example, the largest physical layer packet in ZigBee or 6LoWPAN is 127 bytes. Frame overhead could be 25 bytes, the maximum frame size in the media access control layer is 102 bytes. To protect confidentiality encryption can be applied.

If AES-CCM-128 (mode of operation designed to provide both authentication and confidentiality) were to be used, this would need 21 bytes, leaving only 81 bytes available. Using AES-CCM-32 would consume 9 bytes, leaving 93 available. Designing appropriately secure and robust systems is challenging, since communication between nodes is often over 'lossy and low-bandwidth channels'.

ZigBee®

6LoWPAN

Internet of Things security challenges

For security through digital signatures, a public key infrastructure is required, and this is a significant challenge to IoT systems. Public key infrastructure can protect against both loss of confidentiality and loss of integrity. However, even the encryption process with the public key requires computational and memory resources that are beyond many wireless sensor systems, especially when frequent data transmission is required.

Internet of Things security challenges

Authentication within the IoT is critical, since without appropriate authentication the confidentiality, integrity, and availability of systems can be compromised. This is because if an adversary can authenticate as a legitimate user, they will have access to any data that the user has, and can see (compromising confidentiality), modify (compromising integrity), and delete or restrict availability (compromising availability) in the same way that the user can.

Physical Unclonable Function, introduction

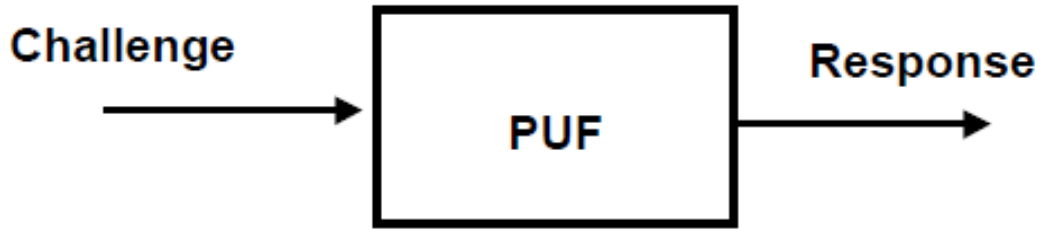
A Physical Unclonable Function (PUF) is a function that is:

- Based on a physical system
- Easy to evaluate (using the physical system)
- Its output looks like a random function
- Unpredictable even for an attacker with physical access

Because of process variations, no two identical Integrated Circuits (IC).
Experiments in which identical circuits with identical layouts on different ICs show that path delays vary enough across ICs to use them for identification.

Physical Unclonable Function, introduction

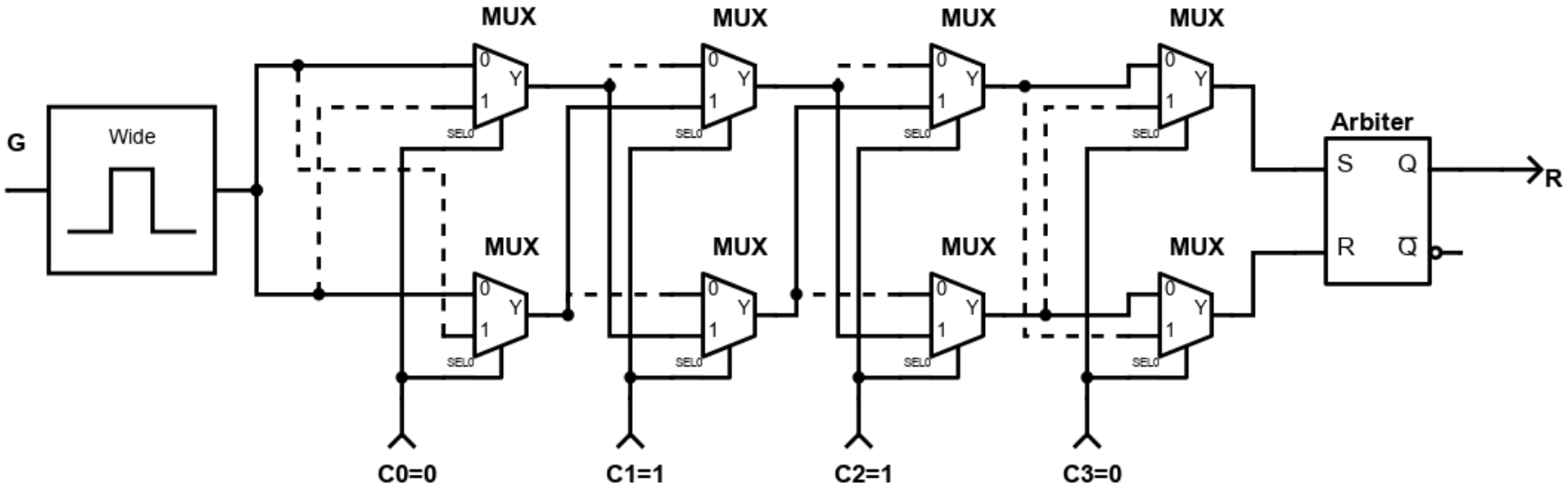
- Very hard (“impossible”) to produce two PUFs with similar challenge-response behavior
- Easy to construct and evaluate a random PUF



Requirements:

- For two random PUFs, difference between expected responses to same challenge, should be large;
- For single random PUF, difference between two measured responses to same challenge, should be small (noise, aging, temperature effects);
- For single random PUF, uncertainty about response to challenge is large, when one does not have access to this PUF instance.

Arbiter PUF scheme*



* switch block: e.g. two muxes;
arbiter: e.g. a latch or a flip-flop;
n switch blocks gives *2n* "different" delays.

- Each challenge creates two paths through the circuit that are excited simultaneously. The digital response is based on a (timing) comparison of the path delays.
- Path delays in an IC are statistically distributed due to random manufacturing variations.

PUF Applications

System identification

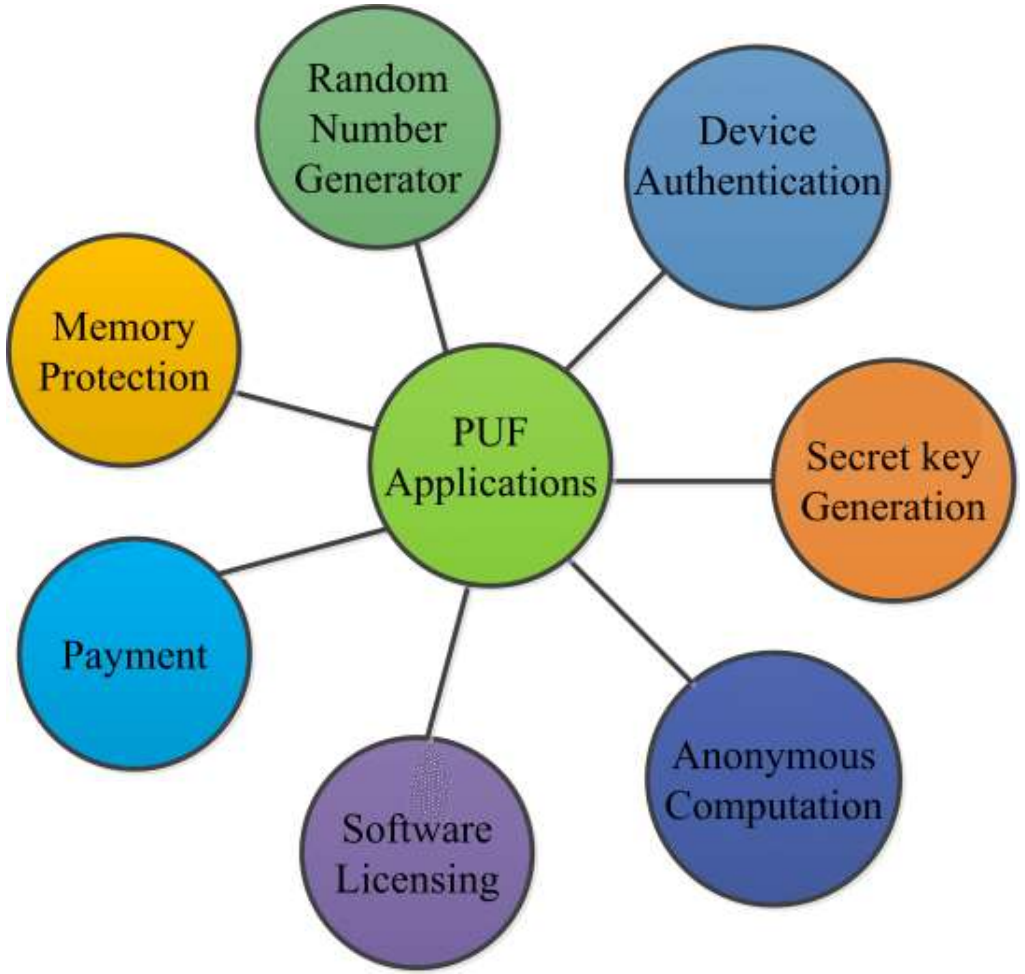
- anti-counterfeiting
- hardware binding
- hardware metering

Secret Key Generation

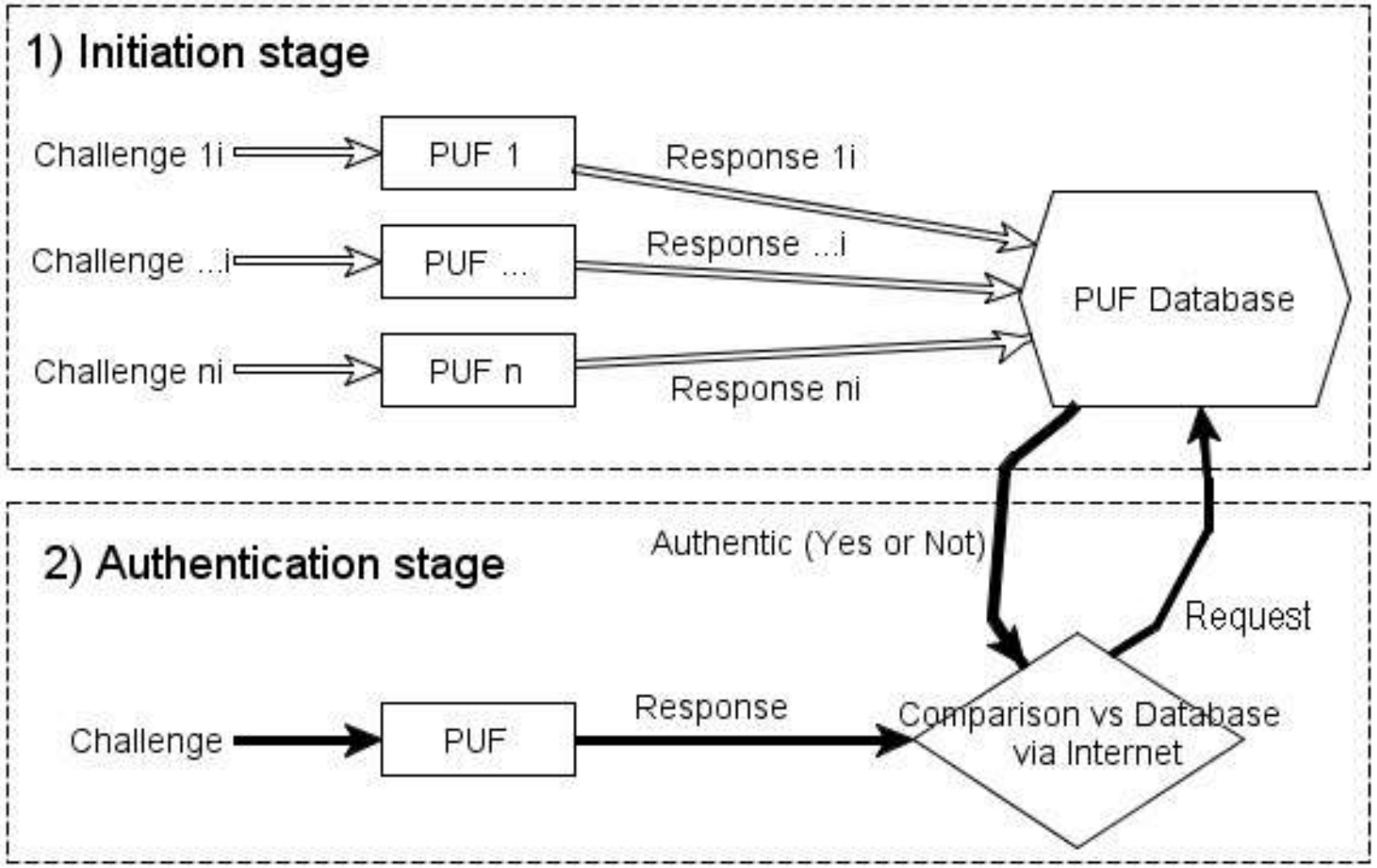
- secure key storage
- secure key distribution

Hardware Entangled Cryptography

- side-channel resistance



Simple implementation of PUF



Questions???