University of Kerbala
College of Computer Science & Information Technology
Computer Science Department

Cryptographic Hardware: Design of AES and RSA accelerators

الأسم: عبد الله محمد جاسم
بأشراف: د. اياد حميد موسى

Introduction

- **What is this report about?** This comprehensive report analyzes the hardware microarchitecture and system-level design of cryptographic accelerators, focusing specifically on the Advanced Encryption Standard (AES) for symmetric cryptography and the RSA algorithm for asymmetric (public-key) cryptography.
-

- **Why is this topic important?** As the technology landscape shifts towards Cloud Computing, edge devices, and the Internet of Things (IoT), the volume of sensitive data transmitted across networks has grown exponentially. Software-based encryption is no longer sufficient to handle this massive throughput. Dedicated cryptographic hardware is essential because it guarantees robust data confidentiality and authentication at multi-gigabit speeds, minimizes the massive processing load on the main CPU, and drastically reduces dynamic power consumption in energy-constrained mobile and embedded systems.

The Problem

- **What problem does this system solve?** Cryptographic operations are mathematically intensive. When executing these algorithms, standard CPUs suffer from massive performance bottlenecks, high power dissipation, and vulnerability to side-channel attacks (such as cache-timing attacks).

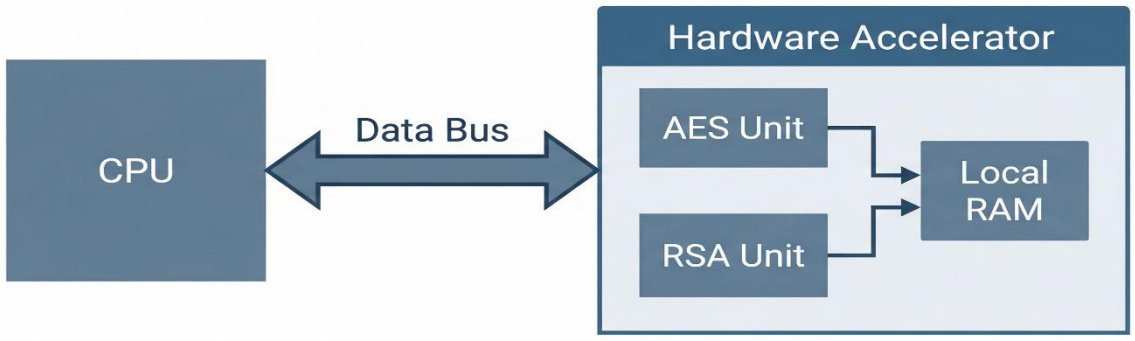
- **What was the old way of doing things?** Traditionally, systems executed cryptographic algorithms purely as software instructions on a general-purpose processor's Arithmetic Logic Unit (ALU).

- **Why wasn't the old method good enough?** A general-purpose CPU is optimized for sequential logic and standard 32-bit or 64-bit arithmetic.
    - For **AES**, software execution requires repeatedly fetching data from memory to access "S-boxes" (Substitution boxes). This causes frequent Cache Misses, wasting hundreds of clock cycles just waiting for memory access.
    - For **RSA**, the algorithm relies on modular exponentiation of massive integers (typically 2048-bit or 4096-bit numbers). A standard 64-bit CPU must break this down into thousands of smaller instructions, taking millions of clock cycles to compute a single RSA key exchange. This chokes the CPU pipeline and causes unacceptable latency in secure real-time communications.

System Design / How it Works

- **The Big Picture:** The system consists of dedicated electronic circuits (such as FPGAs or ASICs) built for the sole purpose of performing cryptographic calculations. The accelerator contains a dedicated AES section for processing fast data streams, and a dedicated RSA section for handling complex keys and massive numbers.

- **Include a Diagram:**



- **Explain the Diagram:** The main processor sends raw data and encryption keys to the accelerator. The accelerator acts as an independent device, rapidly performing the complex encryption operations, and then sends the encrypted data back to the processor. This frees up the CPU to perform other tasks.

Key Feature or Innovation

- **Most important part:** The most innovative feature is the implementation of "Parallel Processing" in AES units and the use of the "Montgomery Multiplier" in RSA units.

- **How it works:** Instead of executing operations step-by-step (like in software), the logic circuits in the AES unit perform multiple encryption steps simultaneously. In the RSA unit, the "Montgomery Multiplier" allows the circuits to multiply huge numbers (like 2048-bit keys) using fast "shift" operations rather than incredibly slow mathematical division.

- **Trade-offs:** The downside to this feature is the increase in "Chip Area" and cost. Designing dedicated circuits for these algorithms requires more silicon space inside the processor or motherboard, making it more expensive to manufacture compared to software-only solutions.

Analysis and Results

- **How well does it perform?** Hardware accelerators provide performance that is exponentially superior to executing the same algorithms purely through software.

- **Data and Numbers:** Using a dedicated hardware accelerator for AES can speed up the encryption process by 10 to 100 times (1000% to 10000%) compared to a standard CPU. Additionally, in IoT (Internet of Things) devices, these accelerators can reduce energy consumption by up to 80%.

- **Why it gets those results:** The system achieves these impressive results because the physical logic gates are custom-wired to execute the encryption equations directly, without wasting time on the "instruction fetch and decode" cycles that traditional processors need just to understand what to do.

Conclusion

- **Summarize the main point:** In summary, AES and RSA cryptographic hardware accelerators are essential components for providing high-level data security without sacrificing device speed or draining battery life.

- **Final thought (The future):** The future of this technology is focused on designing "flexible" accelerators capable of adapting to run Post-Quantum Cryptography (PQC) algorithms, protecting data against the future threats posed by quantum computers.

References

1. Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.

2. National Institute of Standards and Technology (NIST). (2001). *Advanced Encryption*

   Standard (AES). FIPS PUB 197.

3. Kocher, P., Jaffe, J., & Jun, B. (1999). *Differential Power Analysis*. Advances in Cryptology — CRYPTO '99.