Energy Efficient CGRA Accelerators for Cryptography and Medical Image Diagnosis

Name: Duong Thi Sang
Laboratory's name: Computing Architecture
Supervisor's name: Yasuhiko Nakashima

Abstract:
Ensuring security in advanced applications such as blockchain and IoT, there is a pressing need for hashing hardware that combines low power consumption, high performance, and adaptability to process large-scale message loads. Traditional configurable hashing architectures struggle to meet the demands of massive message processing, often limited by inefficiencies in hardware utilization and performance bottlenecks. Addressing these challenges is critical as data security becomes more integral to IoT infrastructures. In parallel, the National Institute of Standards and Technology (NIST) has standardized ten lightweight cryptography (LWC) algorithms, designed to protect data efficiently on resource-constrained IoT devices. Implementing these algorithms in hardware can optimize both speed and energy efficiency, yet existing hardware architectures often fail to provide the flexibility needed to support different LWC algorithms while maintaining high speed and low power consumption. This limitation presents significant obstacles in adapting to the diverse security requirements of gateway and edge devices in IoT systems. Additionally, algorithms such as Advanced Encryption Standard (AES) and Ascon are compact and highly secure, making them suitable for fog computing within IoT frameworks. However, current research lacks a hardware architecture that can implement these algorithms with the flexibility and power efficiency required for IoT devices, thus hindering their potential for widespread, efficient deployment in fog computing environments. In the realm of AI-driven diagnostics, energy-efficient processing of medical images is essential, particularly for mobile or remote scenarios where traditional GPU-based solutions are impractical due to power and size constraints. Both two-dimensional (2D) and three-dimensional (3D) convolutional neural networks (CNNs) are valuable in computer vision and medical diagnostics, with 3D CNNs offering enhanced performance in tasks like visual recognition. However, these models impose substantial computational demands, potentially impacting the efficiency of real-time applications. Similarly, the 2D U-Net model, widely used for medical image segmentation, faces performance bottlenecks when deployed on traditional GPU platforms, limiting its effectiveness in resource-limited or high-throughput diagnostic settings. The development of efficient CGRA (Coarse-Grained Reconfigurable Array) architectures that integrate specialized accelerators for hashing, lightweight cryptography, and U-Net processing presents a promising solution to these challenges. By enabling adaptable, power-efficient computation for secure IoT and medical diagnostic applications, such architectures can bridge the gap between performance and efficiency, paving the way for more robust and versatile solutions in both domains.