SCIENCE CHINA
Information Sciences

• LETTER •

April 2022, Vol. 65 149404:1–149404:2
https://doi.org/10.1007/s11432-020-3206-2

An energy-efficient dynamically reconfigurable cryptographic engine with improved power/EM-side-channel-attack resistance

Chenchen DENG[1], Min ZHU[2], Jinjiang YANG[3], Youyu WU[2], Jiaji HE[4], Bohan YANG[4], Jianfeng ZHU[4], Shouyi YIN[4], Shaojun WEI[4] & Leibo LIU[4]*

[1]*Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing* 100084*, China;*
[2]*Wuxi Micro Innovation Integrated Circuit Design Company, Wuxi* 214000*, China;*
[3]*Wuxi Research Institute of Applied Technology, Tsinghua University, Wuxi* 214000*, China;*
[4]*Institute of Microelectronics, Tsinghua University, Beijing* 100084*, China*

Received 17 November 2020/Revised 19 February 2021/Accepted 10 March 2021/Published online 11 March 2022

Citation Deng C C, Zhu M, Yang J J, et al. An energy-efficient dynamically reconfigurable cryptographic engine with improved power/EM-side-channel-attack resistance. Sci China Inf Sci, 2022, 65(4): 149404, https://doi.org/10.1007/s11432-020-3206-2

Dear editor,

With the prevalence of Internet of things (IoT) applications, energy efficiency is an essential feature for cryptographic engines besides the high security under resource constraints [1]. In the meanwhile, security protocols normally involve various types of cryptographic algorithms, and both protocols and cryptographic algorithms are undergoing rapid evolution [2], posing significant flexibility challenges for cryptographic engines. Application specific integrated circuit accelerators have significant advantages in energy efficiency but cannot change their functionality after fabrication. General purpose processor (GPP)-based cryptographic engines are highly flexible to accommodate different algorithms; however, their throughput is fundamentally limited by the instruction-based architecture of GPPs as they normally function based on the fetch-decode-execute principle in series. Dynamically reconfigurable cryptographic engines featured with a coarse-grained computing architecture (CGRA) have the potential to simultaneously satisfy these essential requirements for high energy efficiency while maintaining flexibility and security. In this study, we propose a dynamically reconfigurable cryptographic engine called Transcryptor. We leverage the flexibility of a custom instruction set-based controller to accelerate algorithm switching and execute control-intensive tasks, serving as a perfect counterpart for high-performance reconfigurable computing arrays that are specialized for computation-intensive tasks.

Transcryptor consists of a coarse-grained reconfigurable computing array and a configuration controller, as shown in Figure 1. As the computing engine for cryptographic algorithms, the reconfigurable computing array has 32 basic computing units (BCUs) and one shared memory. The data flow and configuration flow of each BCU can be independently scheduled by a pipelined configuration controller. Each BCU is composed of four 32-bit processing elements (PEs), register files, a data load/store unit, and a hybrid-RAM. To implement various types of cryptographic algorithms, the PE operator includes basic operations such as arithmetic, shift, and permutation operations, which are commonly used in symmetric-key cryptographic algorithms and hash functions. The data load/store unit can actively load/store data for PEs without interference from the configuration controller to support different data dependencies in the computation of various algorithms. A hybrid-RAM is shared by 4 PEs in a BCU. Computation logics are added to the RAM address and data line to perform operations such as shift and XOR, commonly accompanied by S-box operations in cryptographic algorithms. In this way, different S-box structures are implemented without affecting the efficiency of the pipeline. Using several PEs to accelerate the computation inevitably involves a large amount of intermediate data, and the cache mechanism of these data greatly affects the overall performance. A configurable task-scheduling-based multi-read and multi-write shared RAM is used to transfer intermediate data between BCUs to improve efficiency. The shared memory consists of 8 dual-port RAMs, and each of them has dedicated read and write ports, respectively. Multi-R/W logic can be configured to enable concurrent access of PEs in different BCUs. In the meanwhile, scheduling tools ensure the conflicts are avoided in most cases to reduce undesirable effects.

The configuration controller utilizes configuration contexts, similar to the bitstream of field programmable gate array (FPGA), to control and schedule the reconfiguration computing array. The configuration controller's mechanism affects algorithm switching, which is common during the im-

* Corresponding author (email: liulb@tsinghua.edu.cn)

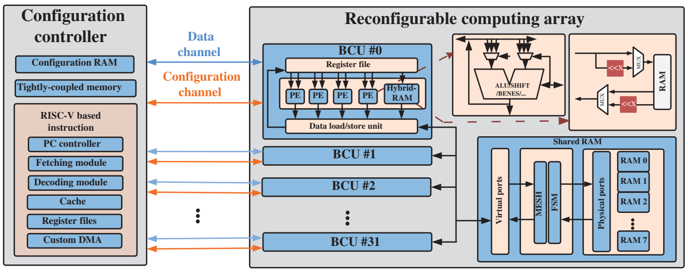

Figure 1 (Color online) The architecture of Transcryptor.

plementation of protocols. An instruction set architecture extension to RISC-V is designed and implemented adopting a pipelined instruction architecture, which has the flexibility of software programs, to accelerate the algorithm switching. Based on RISC-V, custom instructions are derived from commonly used cryptographic operations, such as S-box lookup tables, Benes network, finite field multiplication, and multivariate operation. Through the pipelining of the custom instruction set-based controller, block ciphers, stream ciphers, and hash functions can be switched within one cycle. In addition, special instructions involving jumps are included to reduce the waiting time and to accelerate algorithm switching. In total, 32 controllers support up to 128 instructions in parallel to achieve precise control of each PE and ensure the hardware utilization rate can reach more than 98%.

Results. The chip was fabricated in a 55 nm TSMC process, and measurements are made at a frequency of 500 MHz with 1 V supply voltage. Several representative algorithms of block ciphers, stream ciphers, hash function, and authenticated encryption are supported. Two winner algorithms of CAESAR finalized after the fabrication of this chip are also implemented, demonstrating potential compatibility for future algorithms. Based on these two algorithms, the throughput of the proposed reconfigurable cryptographic engine is 1.4× (AEGIS) and 33.1× (OCB) as high as that of FPGA solutions[1]. Compared with state-of-the-art studies, the proposed work has competitive performance for both advanced encryption standard (AES) and the hash function. When normalized to the same process, our reconfigurable cryptographic engine outperforms others in terms of AES energy efficiency by 17.6× [3], 1.7× [4], 2.4× [5], respectively. The normalized energy efficiency of the hash function of this work is 1.1× and 1.4× better than the studies by [4, 5].

There are two major advantages of the dynamically reconfigurable architecture in terms of countermeasures against side-channel attacks (SCA). One is that the reconfigurable computing array is dynamically configured, which means that configuration can be paralleled with computation, therefore, hiding sensitive information. The other is that the dynamic reconfiguration of PEs can be performed randomly in both spatial and temporal dimensions [6]. In this way, the correlation between intermediate values and power consumption/EM emanations is reduced. Correlation power analysis (CPA) and test vector leakage assessment are utilized to evaluate the effectiveness of side-channel resistance. If no dynamic reconfiguration is performed, the key can be recovered from 100000 instant power traces in a CPA attack. A fixed vs. random Welch's t-test is also performed, and the max $|t|$ value is 11.37. With the proposed countermeasures, the max $|t|$ value is 1.77, and the key cannot be recovered with one million power traces. From this perspective, the resistance against power attacks is increased by at least one order of magnitude. To evaluate the electromagnetic (EM) analysis attack resistance, the same AES implementation as power-SCA is configured. Although the keys are not recovered within one million traces, the comparison of right key guess ranking and the correlation value indicates an improved EM-SCA resistance. The tradeoffs between resistance and overhead can be made by adjusting the randomness of degree [6].

Conclusion. Utilizing the hardware resource of CGRA effectively, Transcrytor has substantial flexibility to comply with new cryptographic protocols while maintaining energy efficiency as the basic functions of fundamental primitives tend not to change much. In addition, the intrinsic reconfigurability feature allows upgrading countermeasures when new vulnerabilities appear, which is particularly useful for IoT devices with a long lifespan. Moreover, Transcrytpor also has the potential to be compatible with other types of algorithms such as baseband processing and compression/decompression, which are often related to cryptographic algorithms in IoT applications. The multiplexing of reconfigurable resources can improve area efficiency.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grant Nos. 61804088, 61672317, 62004112).

References

1 Yang K, Blaauw D, Sylvester D. Hardware designs for security in ultra-low-power IoT systems: an overview and survey. IEEE Micro, 2017, 37: 72–89

2 Yang J, Johansson T. An overview of cryptographic primitives for possible use in 5G and beyond. Sci China Inf Sci, 2020, 63: 220301

3 Bohnenstiehl B, Stillmaker A, Pimentel J J, et al. KiloCore: a 32-nm 1000-processor computational array. IEEE J Solid-State Circ, 2017, 52: 891–902

4 Zhang Y Q, Xu L, Dong Q, et al. Recryptor: a reconfigurable cryptographic cortex-M0 processor with in-memory and near-memory computing for IoT security. IEEE J Solid-State Circ, 2018, 53: 995–1005

5 Banerjee U, Wright A, Juvekar C, et al. An energy-efficient reconfigurable DTLS cryptographic engine for securing Internet-of-things applications. IEEE J Solid-State Circ, 2019, 54: 2339–2352

6 Wang B, Liu L B, Deng C C, et al. Against double fault attacks: injection effort model, space and time randomization based countermeasures for reconfigurable array architecture. IEEE Trans Inform Forensic Secur, 2016, 11: 1151–1164

[1] Homsirikamol E, Farahmand F, Diehl W, et al. Benchmarking of round 3 CAESAR candidates in hardware: methodology, designs and results. https://cryptography.gmu.edu/athena/index.php?id=CAESAR.