Coprocessador Criptográfico em Hardware para RISC-V

Pedro Sousa, Luís Cunha, Miguel Silva, Sandro Pinto, e Tiago Gomes
Centro ALGORITMI - Universidade do Minho
{a82041, a82307}@alunos.uminho.pt; {miguel.silva, sandro.pinto, mr.gomes}@dei.uminho.pt

***Resumo*—O novo paradigma da *Internet of Things* (IoT) incluí inúmeros dispositivos de baixo consumo e com características de conectividade com a Internet. Atualmente, estes dispositivos necessitam de cumprir requisitos de desempenho e de segurança, sendo este último de elevada importância, sobretudo ao nível das comunicações com a Internet. Este trabalho propõem o desenvolvimento de um acelerador em hardware, dedicado à execução de algoritmos criptográficos frequentemente utilizados pela pilha de rede, e.g., *Advanced Encryption Standard* (AES). O acelerador está a ser desenvolvido seguindo duas abordagens de acoplamento distintas: forte e fracamente acoplado. De modo a ser possível testar ambas as abordagens, a solução está a ser implementada numa plataforma baseada em RISC-V.**

***Index Terms*—*Internet of Things* (IoT), FPGA, RISC-V, coprocessador criptográfico.**

I. Introdução

O atual progresso tecnológico e a crescente procura por dispositivos de aplicação específica, cria inúmeras oportunidades para a evolução das áreas de sistemas embebidos. Este tipo de sistemas são capazes de proporcionar soluções economicamente viáveis com aplicações em diversas áreas, tais como, automação, saúde, sistemas de monitorização, etc., assegurando características de conectividade com a Internet. Esta característica fez surgir o novo conceito da *Internet of Things* (IoT) [1], que define um conjunto de "objetos" interligados entre si e directamente com a Internet, que em 2008 atingiu o marco histórico de mais objetos conectados que pessoas no mundo. Em 2020, todo o ecossistema IoT gerou cerca de 82 mil milhões USD, sendo esperado que este valor aumente consideravelmente com o aumento do número de dispositivos. Segundo as estimativas atuais existirão em 2030 cerca de 25 mil milhões de objetos conectados [2].

Dada a natureza insegura destes dispositivos, a sua constante conexão com a Internet, e o carácter sensível da informação recolhida e enviada pela rede, é necessário providenciar mecanismos de segurança que visam proteger e garantir a confidencialidade, integridade, e autenticidade dos dados, desde a origem até ao destinatário. Tradicionalmente, sistemas de recursos limitados utilizam mecanismos de segurança para protegerem a informação baseados em algoritmos de encriptação simples, como por exemplo, *Advanced Encryption Standard* (AES), *Rivest-Shamir-Adleman* (RSA) ou *Triple Data Encryption Standard* (TripleDES) [3]. Apesar de robustos, estes algoritmos podem ser executados em sistemas com baixo poder de computação, garantindo os requisitos mínimos de segurança da informação. O AES é um algoritmo de encriptação de chave simétrica, ou seja, a mesma chave é usada para as operações de encriptação e desencriptação dos dados. Este algoritmo apresenta uma fase inicial de expansão da chave, seguida de uma fase de encriptação/desencriptação do bloco de dados. Esta última é executada em várias rondas, usando as chaves geradas e efetuando substituições, transposições e combinações lineares dos bytes. Tradicionalmente, o AES é executado com recurso a bibliotecas de *software* providenciadas pelas camadas de rede do sistema operativo (SO). Contudo, e apesar de simples, o algoritmo exige algum poder de processamento devido ao elevado número de operações que necessita de executar, o que pode originar perdas de desempenho do dispositivo [4].

Recentemente tem-se assistido à utilização de tecnologia baseada em *field-programable gate array* (FPGA) em dispositivos IoT. As características desta, tais como a capacidade de reconfiguração, costumização, e paralelização de tarefas em *hardware*, contribuí para soluções de dispositivos IoT mais robustas que podem explorar a migração de tarefas de *software* para *hardware* dedicado [5]. Existem já várias implementações que utilizam FPGA para fornecer a dispositivos embebidos IoT funcionalidades da pilha de rede em hardware [6]. No entanto, apenas conseguem desenvolver soluções numa abordagem fracamente acoplada. Com o aparecimento do RISC-V, uma nova arquitectura de processadores de *Instruction Set Architecture* (ISA) aberto direcionado para diferentes classes de processadores [7,8], surgem novas oportunidades para a exploração de soluções de *hardware* que permitem o desenvolvimento de aceleradores como coprocessadores integrados no *datapath* do processador (fortemente acoplado) [9], ou como periféricos ligados ao processador através de barramentos de dados genéricos (fracamente acoplado) [6].

Este trabalho propõe o desenvolvimento de um acelerador em *hardware* usado para auxiliar as camadas de rede que necessitem de segurança ao nível das comunicações e utilizem protocolos baseados em algoritmos criptográficos simples, nomeadamente o AES ou o RSA. De forma a ser possível avaliar qual a melhor implementação, será feito um estudo comparativo entre a abordagem puramente *software*, com uma abordagem *hardware* com o acoplamento do acelerador segundo as abordagens fortemente acoplado e fracamente acoplado. Os resultados deverão avaliar as métricas de desempenho, consumo energético, e recursos de *hardware* necessários.

Este trabalho foi suportado pela FCT - Fundação para a Ciência e Tecnologia no âmbito do projeto UIDB/00319/2020.

II. Coprocessador Criptográfico em Hardware para RISC-V

Para o desenvolvimento deste coprocessador foi escolhida a placa de desenvolvimento Xilinx Arty-35T FPGA, a qual foi inicialmente programada com o *bitstream* de um processador RISC-V baseado na *framework* Rocket [10]. O coprocessador, implementado em Chisel, pretende acelerar a computação de algoritmos criptográficos, e.g., AES, RAS e TripleDES. A integração e teste deste coprocessador é feita seguindo duas abordagens distintas: (i) fracamente acoplado, e (ii) fortemente acoplado. A Figura 1 ilustra a arquitetura do sistema usando uma integração fracamente-acoplada do coprocessador. Neste cenário, a comunicação com o processador é feita através de uma interface *Memory-Mapped I/O* (MMIO) através de instruções *load* e *store*, o que facilita a portabilidade do acelerador para outros cores RISC-V.

Por sua vez, a Figura 2 ilustra a arquitetura do sistema quando o acelerador criptográfico é fortemente-acoplado à unidade de processamento central (CPU). Nesta abordagem, o acelerador criptográfico integra o RISC-V Rocket, comunicando com o CPU através da interface Rocket Custom Coprocessor (RoCC) e utilizando instruções próprias adicionadas ao ISA. Apesar de ser necessário alterar o datapath, estas modificações são completamente suportadas pelo gerador de cores Rocket, e consequentemente, não induzem nenhum tipo de *overhead* no funcionamento normal do processador.

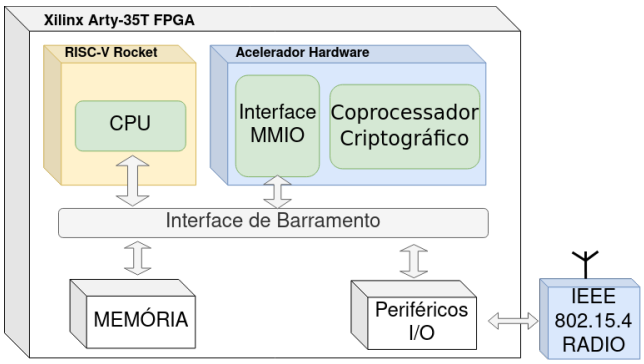

Figura 1. Coprocessador Fracamente-Acoplado.

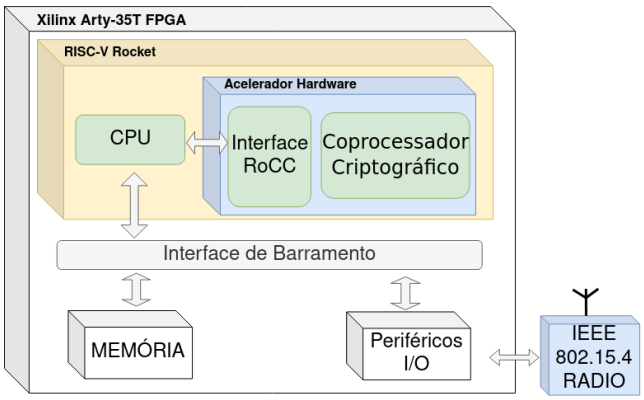

Figura 2. Coprocessador Fortemente-Acoplado.

III. Trabalho Atual

Utilizando as ferramentas de desenvolvimento Chipyard, Freedom E300, e Freedom Studio, o estado de desenvolvimento atual permite a execução e *debug* do sistema, tanto na FPGA como num emulador de código Chisel. Neste momento, encontram-se implementados em hardware os módulos de encriptação e desencriptação do algoritmo AES, sendo a comunicação com o coprocessador baseada numa abordagem fortemente acoplada utilizando instruções customizadas através da interface RoCC. Futuramente, na integração com o sistema operativo e a biblioteca criptográfica correspondente, o coprocessador será invocado através do uso de um conjunto de *APIs*, que irão substituir todas as funcionalidades que foram migradas para hardware, tornando a presença do acelerador transparente ao utilizador final.

IV. Linha de Investigação

Os próximos passos incluem a adição de pontos de configurabilidade no acelerador fortemente acoplado, tais como o tamanho da chave a usar (128, 192 ou 256 bits) ou o modo de operação do AES (ECB, CBC, CFB), bem como a implementação de *APIs* que permitam a utilização do coprocessador pelo software. Consecutivamente, será iniciada a integração do acelerador na pilha de rede do sistema operativo RIOT. Por último, o acelerador será alterado para uma abordagem fracamente acoplada, permitindo avaliar e comparar, em ambas abordagens, os *trade-offs* entre flexibilidade, portabilidade, performance, determinismo, consumo energético e recursos de *hardware*.

Referências

[1] D. J. Jackson and P. Caspi, "Embedded systems education: Future directions, initiatives, and cooperation," *SIGBED Rev.*, vol. 2, no. 4, p. 1–4, Oct. 2005.

[2] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[3] M.-H. Dao, V.-P. Hoang, V.-L. Dao, and X.-T. Tran, "An energy efficient aes encryption core for hardware security implementation in iot systems," in *2018 International Conference on Advanced Technologies for Communications (ATC)*, 2018, pp. 301–304.

[4] D. Canright and D. A. Osvik, "A more compact aes," in *Selected Areas in Cryptography*, M. J. Jacobson, V. Rijmen, and R. Safavi-Naini, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 157–169.

[5] M. Silva, A. Tavares, T. Gomes, and S. Pinto, "Chameliot: An agnostic operating system framework for reconfigurable iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 1291–1292, 2019.

[6] T. Gomes, S. Pinto, F. Salgado, A. Tavares, and J. Cabral, "Building ieee 802.15.4 accelerators for heterogeneous wireless sensor nodes," *IEEE Sensors Letters*, vol. 1, no. 1, pp. 1–4, 2017.

[7] Y. Lee, A. Waterman, H. Cook, B. Zimmer, B. Keller, A. Puggelli, J. Kwak, R. Jevtic, and S. Bailey, "An agile approach to building risc-v microprocessors," *IEEE Micro*, vol. 36, no. 2, pp. 8–20, 2016.

[8] K. Asanović and D. A. Patterson, "Instruction sets should be free: The case for risc-v," *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2014-146*, 2014.

[9] M. Silva, T. Gomes, and S. Pinto, "Leveraging risc-v to build an open-source (hardware) os framework for reconfigurable iot devices," in *CARRV2021*, 06 2021.

[10] D.-Z. Li, H.-R. Gong, and Y.-C. Chang, "Implementing riscv system-on-chip for acceleration of convolution operation and activation function based on fpga," in *2018 14th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT)*, 2018, pp. 1–3.