Vijay DAHIPHALE, Gaurav BANSOD, Ankur ZAMBARE, Narayan PISHAROTY, 2020. Design and implementation of various datapath architectures for the ANU lightweight cipher on an FPGA. *Frontiers of Information Technology & Electronic Engineering*, 21(4):615-628. https://doi.org/10.1631/FITEE.1800681

Design and implementation of various datapath architectures for the ANU lightweight cipher on an FPGA

Key words: Lightweight cryptography; Internet of Things (IoT); Embedded security; Encryption; FPGA; Datapath design

Corresponding author: Vijay DAHIPHALE
E-mail: vijaydahiphale96@gmail.com
ORCID: https://orcid.org/0000-0002-7113-3666

Motivation

1. Since the dawn of the Internet of Things (IoT), data and system security has been the major concern for developers. Because most IoT devices operate on 8-bit controllers with limited storage and computation power, encryption and decryption need to be implemented at the transmitting and receiving ends, respectively, using lightweight ciphers.

2. Lightweight cipher implementation in hardware plays an instrumental role in IoT devices. Implementation of different novel datapath designs of lightweight cipher based on the applications will be the future trend in the constrained environments.

Main idea

1. Different datapath designs for lightweight cipher ANU for applications like IoT are proposed.

2. The ANU cipher is implemented at 4-, 8-, 16-, and 32-bit datapath sizes on four different field-programmable gate array (FPGA) platforms and the results are compared on every performance design metric.

3. Unlike previous ANU architectures, the new architectures have parallel substitution boxes (S-boxes) for high throughput and hardware optimization.

Method

1. 8-bit datapath of ANU cipher

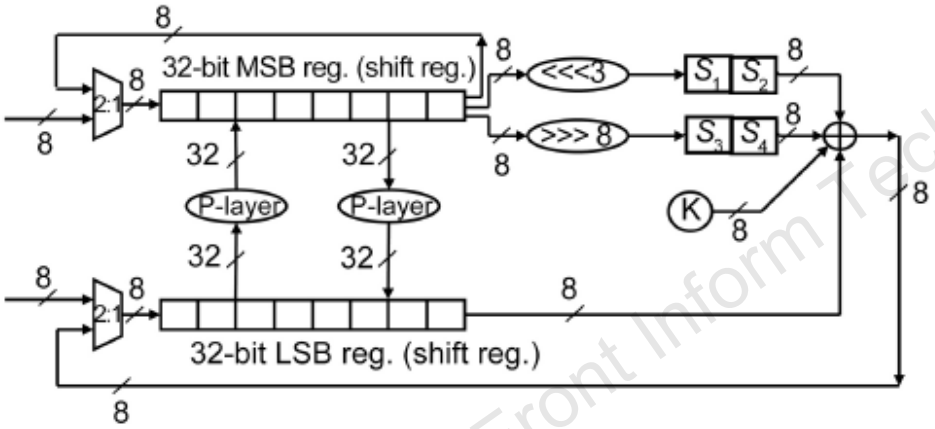

Fig. 10 8-bit datapath architecture of ANU

2. 32-bit datapath of ANU cipher

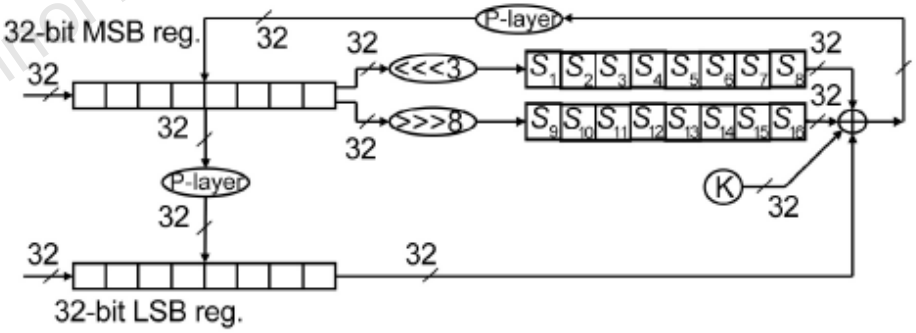

Fig. 13 32-bit datapath architecture of ANU

Major results

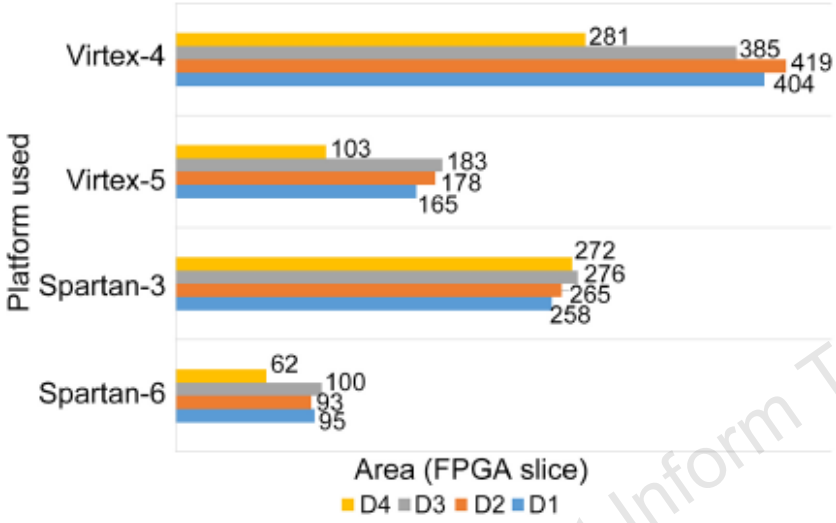

Fig. 17 Comparison of D1–D4 over the area used in terms of FPGA slices

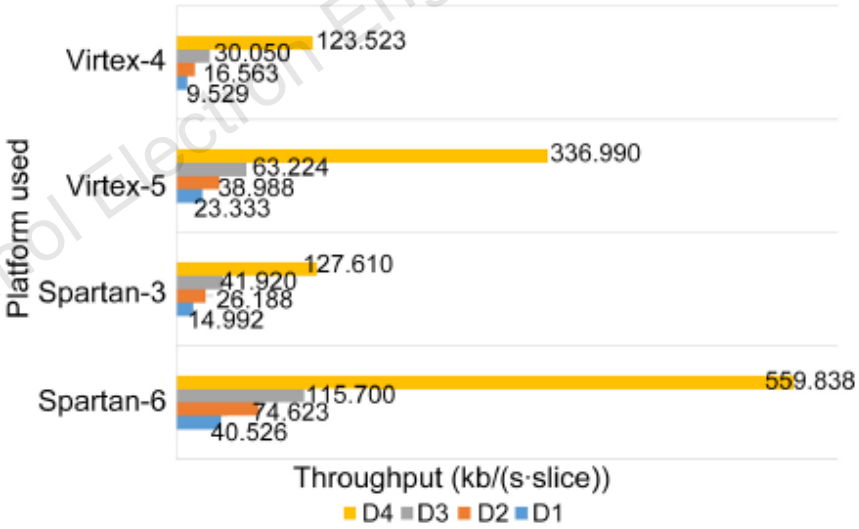

Fig. 23 Comparison of D1–D4 over the throughput per slice

Conclusions

1. In this study, we compared different ANU cipher architectures. The architectures were defined by different datapath sizes. D1–D4 each needed 64-bit data and a 128-bit key for encryption.

2. Depending on the datapath size, the performances varied significantly. The 4-bit datapath architecture was developed for slower applications where the time bound is flexible; similarly, the 32-bit datapath architecture was developed for faster applications where power consumption is not a major concern.

3. All the architectures were implemented on four different FPGA platforms. Among all these platforms, the Spartan platform allowed us to efficiently implement the hardware for a resource-constrained environment.