An Optimized Hardware Implementation of Grain-128AEAD

Mattias Sönnerup and Ripudaman Khattar

In our daily life, electronic devices play an important role. Today it is hard to imagine a world without electronics. With the Internet of Things era being here more devices than ever are connected to the Internet, making the need for security greater.

Devices connected to the Internet send out information, which gets shared with other electronic media. The problem is that not all sensitive information flowing between devices are protected, which is where security is needed. One important aspect of security is cryptography. In encryption, the original information is transformed into a ciphertext, which can only be read by devices or people authorized to do so. Whereas, decryption converts the encrypted data back to a readable text. Integration of cryptography can be done in multiple ways but is usually constrained by the area, speed and power consumption of a device. One way to apply cryptography is with the use of stream ciphers, which can be very efficient when it comes area, speed and power consumption in hardware.

In this work, we implement several versions of Grain-128AEAD. It is a stream cipher that can also authenticate data. The implementations are optimized for area, speed and power consumption in hardware. For the high-speed designs, we utilize high-speed transistors to increase the speed and for the low area/power designs we utilize low power transistors. Moreover, several optimization methods are employed on the cipher to further improve them. In addition to that, we also present some area optimization of the hardware by reducing the number of transistors in the hardware used to make up the design.

The combined effect of all the optimizations enabled some designs to run at a throughput of 1.25-33.6 Gbit/s compared to 1 Gbit/s for the original non-optimized version of the design. The power also improved by approximately 52-94% when running the designs at a 10 MHz and a 100 kHz clock frequency respectively. In addition to that, the area improved by approximately 2-7% with the optimization methods and with an additional 1-12% by reducing the number of the transistors of the design.

Analyzing the result it turns out the most power efficient implementation is a suitable security solution for low power IoT devices. The throughput of the high-speed designs are also quite large and can be applied in IoT applications where high speed is a necessity. Finally, the area for the low area designs is quite small making it a suitable security solution for small IoT devices.

Figure 1: *IoT devices are becoming increasingly common and often require transmitted data to be encrypted and authenticated.*