КРИПТОНИТ

Can RFID tag use MGM?

Victoria Vysotskaya, Lev Vysotsky

September 17, 2020

RFID technology

Определение

RFID (Radio Frequency Identification) is a contactless data exchange technology based on the use of radio frequency electromagnetic radiation, which is used for automatic identification and accounting of objects.

RFID systems are used in retail and logistics, contactless cards and access control, animal identification and healthcare.

Lightweight cryptography

Definition

Lightweight cryptography is a field of cryptography with the goal of developing algorithms for use in devices with limited resources (memory, power supply, size).

Note

Not all RFID must be lightweight!

Parameters minimization

Minimize by a complex of parameters:

- area, LUTs
- frequency, Hz
- throughput, bit/sec
- power consumption, W
- memory, bit
- other.

Note
As the frequency of the circuit increases, the bandwidth increases, but so does the power.

Base operations

Lightweight operations

- bitwise XOR
- (cyclic) bit shift
- bit fixation
- zero padding and truncation

Non-lightweight operations

- multiplication (including multiplication in non-trivial fields)
- memory access at a given index

Lightweight algorithms

World
International standard ISO/IEC 29167. Part 21: SIMON

Russia
Russian algorithms were developed without regard to lightweight requirements. Therefore, the question arises: are these algorithms applicable for use in RFID tags?

Idea

Note

Requirements for labels depend on the manufacturer and the purpose, so it’s hard to talk about «universally good» algorithms.

Idea

Compare Russian algorithms with their international lightweight analogues.

Algorithms

- Base ciphers: Magma vs Simon.
- Block length is 64 bit, key length is 256 bit.
- AEAD: MGM vs Silc v3.
- Optimization by area.

Realization

Why FPGA, not ASIC?

- Easier to develop.
- Can be tested in hardware.
- The ratio «more–less» is preserved during the transition from FPGA to ASIC.

Realization

- **Language:** Verilog
- **Modeling on** Xilinx Vivado Design Suite
- **FPGA:** Xilinx XA Zynq-7000
- **Parameters:**
    - 485 I/O pins,
    - 78 600 LUTs,
    - 157 200 flip-flop
- **Frequency:** 400 MHz and 100 KHz

Results. Encryption

	Simon	Magma	Simon	Magma
Frequency (MHz)	400	400	0.1	0.1
Area (LUTs)	183	71	151	68
Throughput (Kbit/sec)	533 333	800 000	133	200
Power (mW)	136	162	123	123
Memory (FFs)	171	130	171	130

Results. Authenticated encryption

	Silc-Simon	Silc-Magma	MGM-Magma	Silc-Simon	Silc-Magma	MGM-Magma
Frequency (MHz)	400	400	400	0.1	0.1	0.1
Area (LUTs)	975	991	1390	944	956	1309
Throughput (Kbit/sec)	245 208	365 714	186 861	62	91	47
Power (mW)	163	171	185	123	123	123
Memory (FFs)	508	408	639	508	408	639

Results

Note

When implementing circuits on FPGAs, it turned out that it was impossible to measure their real power consumption, since the static power consumption of the circuit itself is high (approximately 123 mW).

Conclusion

- Russian analogues of international low-resource algorithms coincide up to an order of magnitude (further optimization is possible).
- The results obtained can be useful when starting the development of real devices.
- Power consumption requires future research.

GitHub link

github.com/VysotskayaVictory/RFID