NIST Lightweight Cryptography Workshop 2015

Triathlon of Lightweight Block Ciphers for the Internet of Things

Daniel Dinu, Yann Le Corre, Dmitry Khovratovich,
Leo Perrin, *Johann Großschädl*, Alex Biryukov

UNIVERSITÉ DU LUXEMBOURG

Laboratory of Algorithmics, Cryptology and Security (LACS)
University of Luxembourg
http://lacs.uni.lu/members/johann_groszschaedl

Outline

- Lightweight Crypto for the IoT
- Benchmarking of Lightweight Ciphers
  - Two application scenarios
  - Implementation aspects
- Results
  - Execution time, RAM footprint, code size
  - 8-bit AVR, 16-bit MSP430, 32-bit ARM CortexM
  - Figure of Merit (FOM)
- Conclusions

What are “Things”?

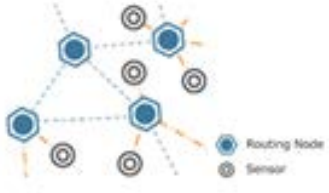
Vehicle, asset, person & pet controlling and monitoring

Agriculture automation

Energy consumption

Security & surveillance

Building management



M2M & wireless sensor network

Internet of Things
Smart Objects
Wirelessly connected

Embedded mobile

Source: nkonnect.com

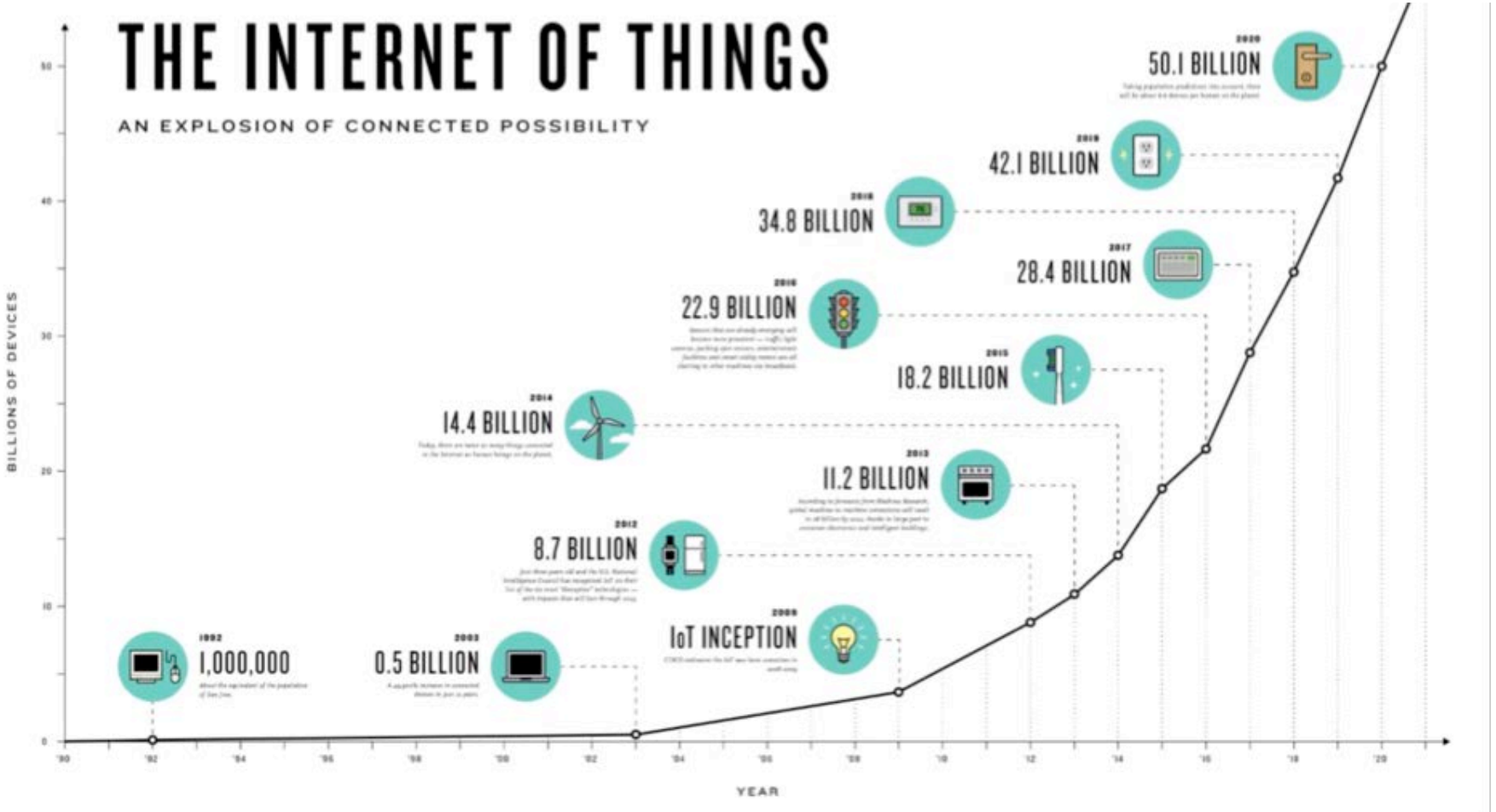
Everyday things

Smart homes

Telemedicine & healthcare

- Processors embedded into everyday objects (“things”)
- Wireless communication (WiFi, Bluetooth, ZigBee)

IoT Forecast by Cisco



Source: Cisco

Lightweight Cryptography

- Not meant to be Weak Cryptography
  - “Cryptographic primitives, schemes and protocols tailored to extremely constrained environments such as sensor nodes or RFID tags” (Gligor 2005)
- Requirements for IoT
  - Efficient in HW (performance, area, power)
  - Efficient in SW (performance, RAM, code size) on many 8, 16, and 32-bit platforms
  - Efficient protection against physical attacks
  - Support of different functionality (encryption, hashing)

Benchmarking of Lightweight Ciphers

- Fair and consistent evaluation
  - How well are existing LW suited for the IoT?
  - What are the promising directions for new designs?
- 3 Core Metrics
  - Execution time, RAM footprint, code size
  - Other metrics can be derived or estimated thereof (e.g. energy consumption)
- 3 Platforms
  - 8-bit AVR, 16-bit MSP430, 32-bit ARM CortexM
  - Further platforms may be supported in the future

13 Considered Ciphers

Cipher	Year	Block size	Key size	Round keys size	Rounds	Security level	Type	Target
AES	1998	128	128	1408	10	0.70	SPN	SW, HW
Fantomas	2014	128	128	0	12	NA	SPN	SW
HIGHT	2006	64	128	1088	32	0.69	Feistel	HW
LBlock	2011	64	80	1024	32	0.72	Feistel	HW, SW
LED	2011	64	80	0	48	NA	SPN	HW, SW
Piccolo	2011	64	80	864	25	0.56	Feistel	HW
PRESENT	2007	64	80	2048	31	0.84	SPN	HW
PRINCE	2012	64	128	192	12	0.83	SPN	HW
RC5*	1994	64	128	1344	20	0.90	Feistel	SW
Robin	2014	128	128	0	16	NA	SPN	SW
Simon	2013	64	96	1344	42	0.67	Feistel	HW, SW
Speck	2013	64	96	832	26	0.58	Feistel	SW, HW
TWINE	2011	64	80	1152	36	0.64	Feistel	HW, SW

* We use RC5 with increased number of rounds.

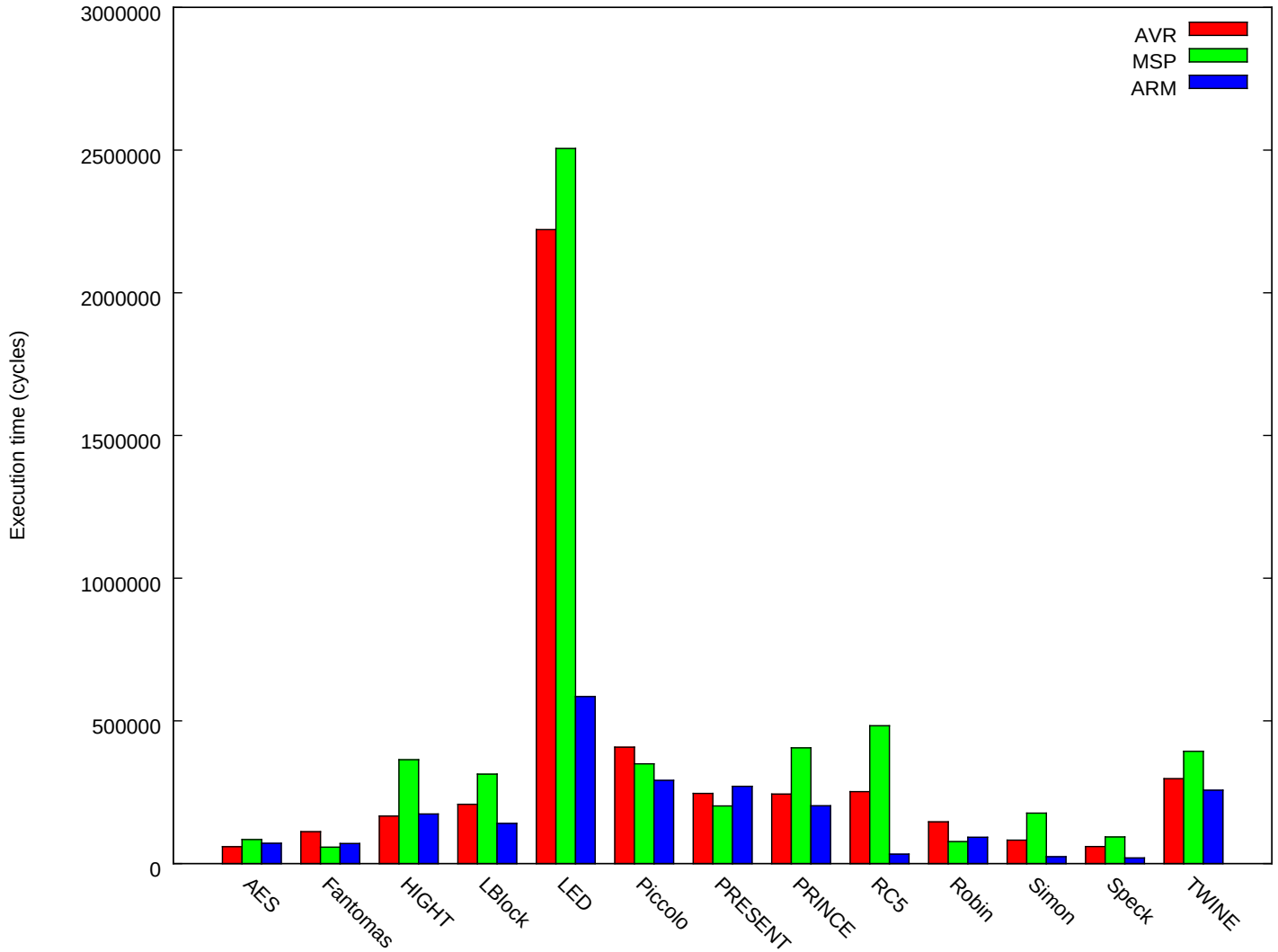
Application Scenarios

- Scenario 1: “Bulk Encryption”
  - Example: data transfer between two sensor nodes
  - 128 bytes of data, CBC mode, 80-bit key
  - We measure encryption + decryption + key schedule
  - Representative for “performance matters”
- Scenario 2: “Challenge-Response Authen.”
  - Example: access control, device authentication
  - 128 bits of data, CTR mode, 80-bit key
  - We measure encryption time (round keys pre-comp.)
  - Representative for “code size and RAM matter”

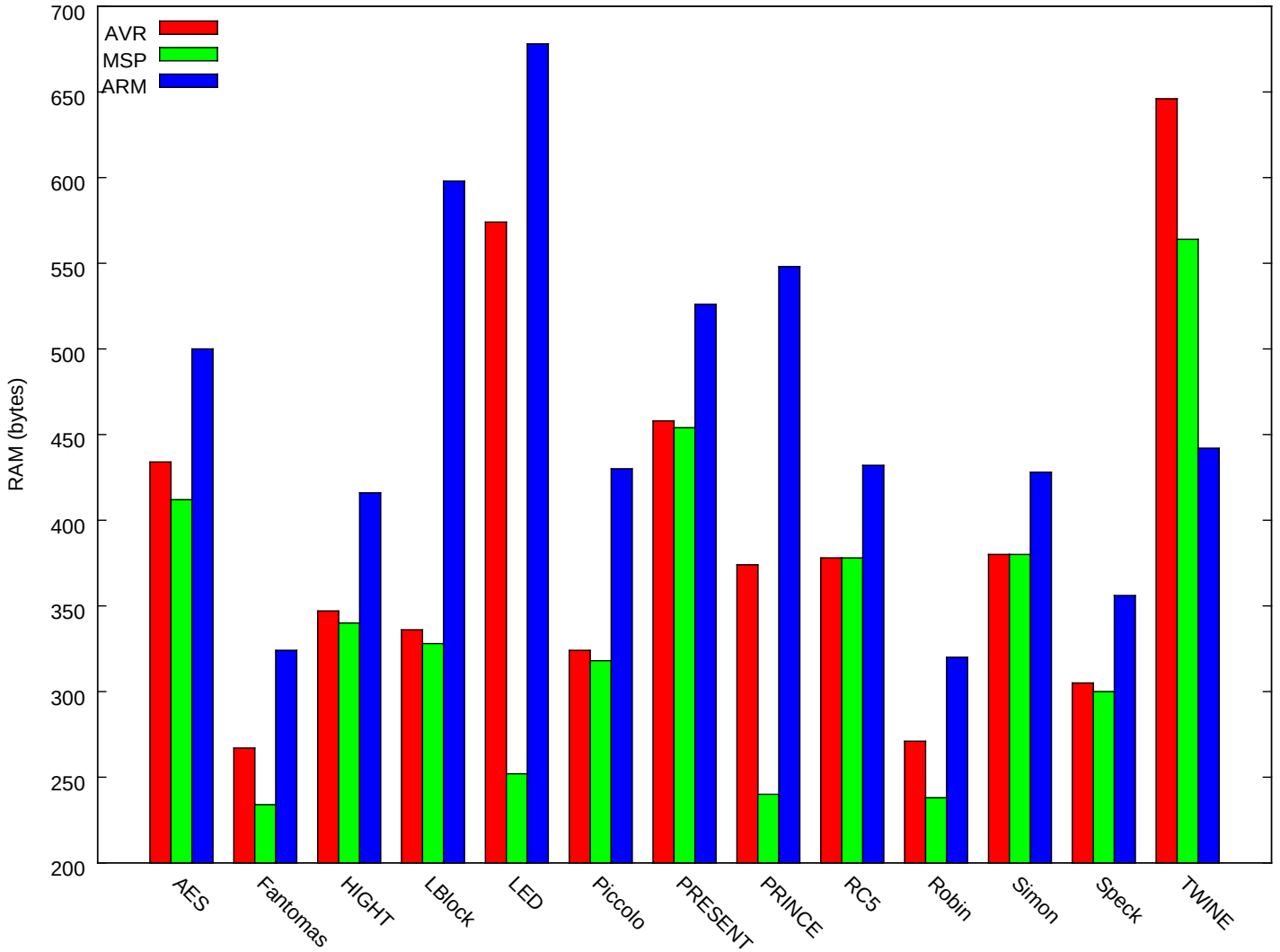
Implementations

- Several Implementations for each cipher
  - Between 2 and 24 implementations for each cipher (more than 100 in total)
  - Different trade-offs, at least one speed-oriented and one size-oriented implementation
- Written in ANSI C
  - Portability is very important in the IoT (many HW platforms and operating systems),
  - Useful to assess new ciphers in early stages of the design phase
  - Assembly implementations for AES and PRESENT

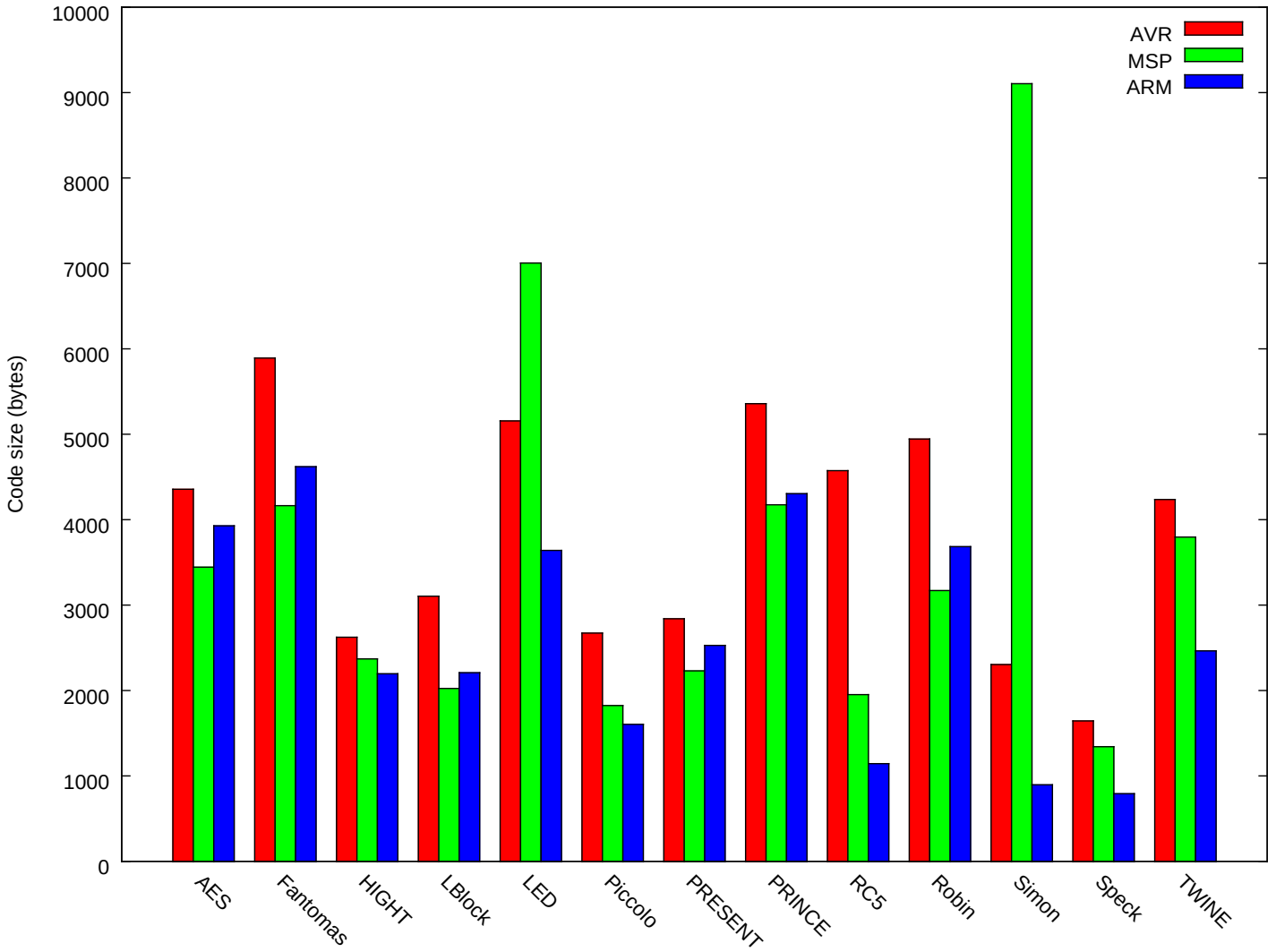
Scenario 1: Execution Time



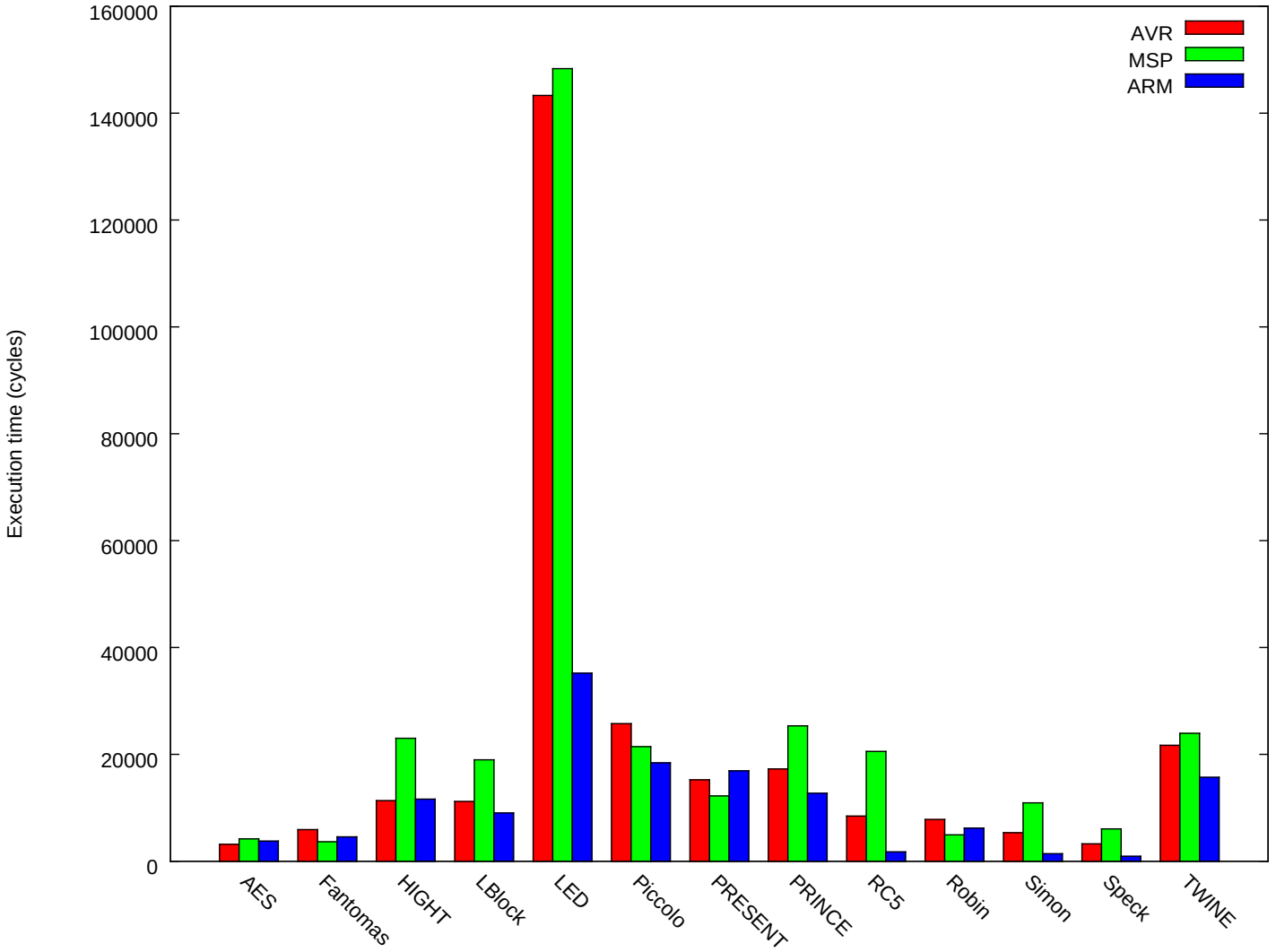
Scenario 1: RAM footprint



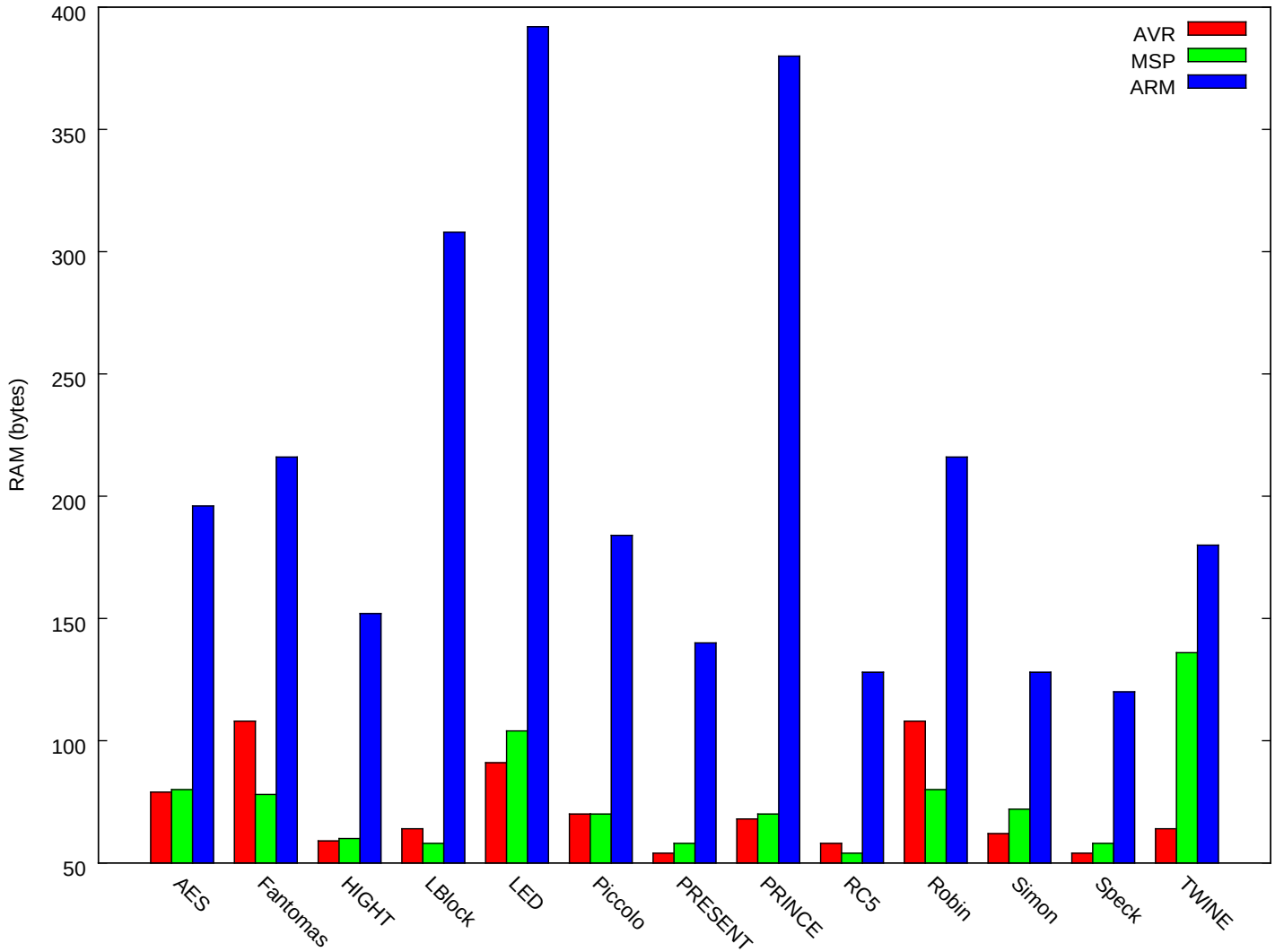
Scenario 1: Code Size



Scenario 2: Execution Time



Scenarion 2: RAM Footprint



Scenario 2: Code Size

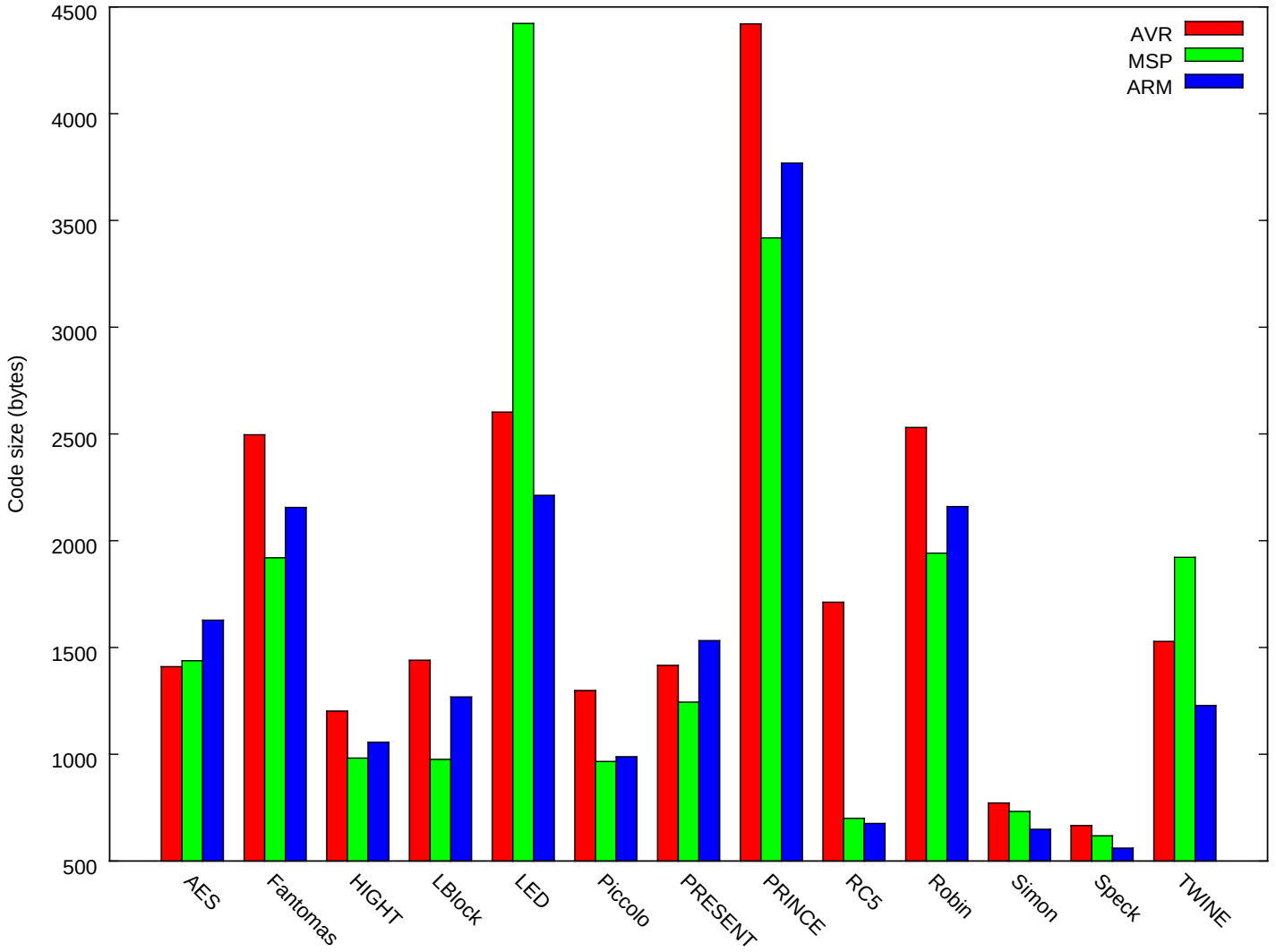


Figure of Merit (FOM)

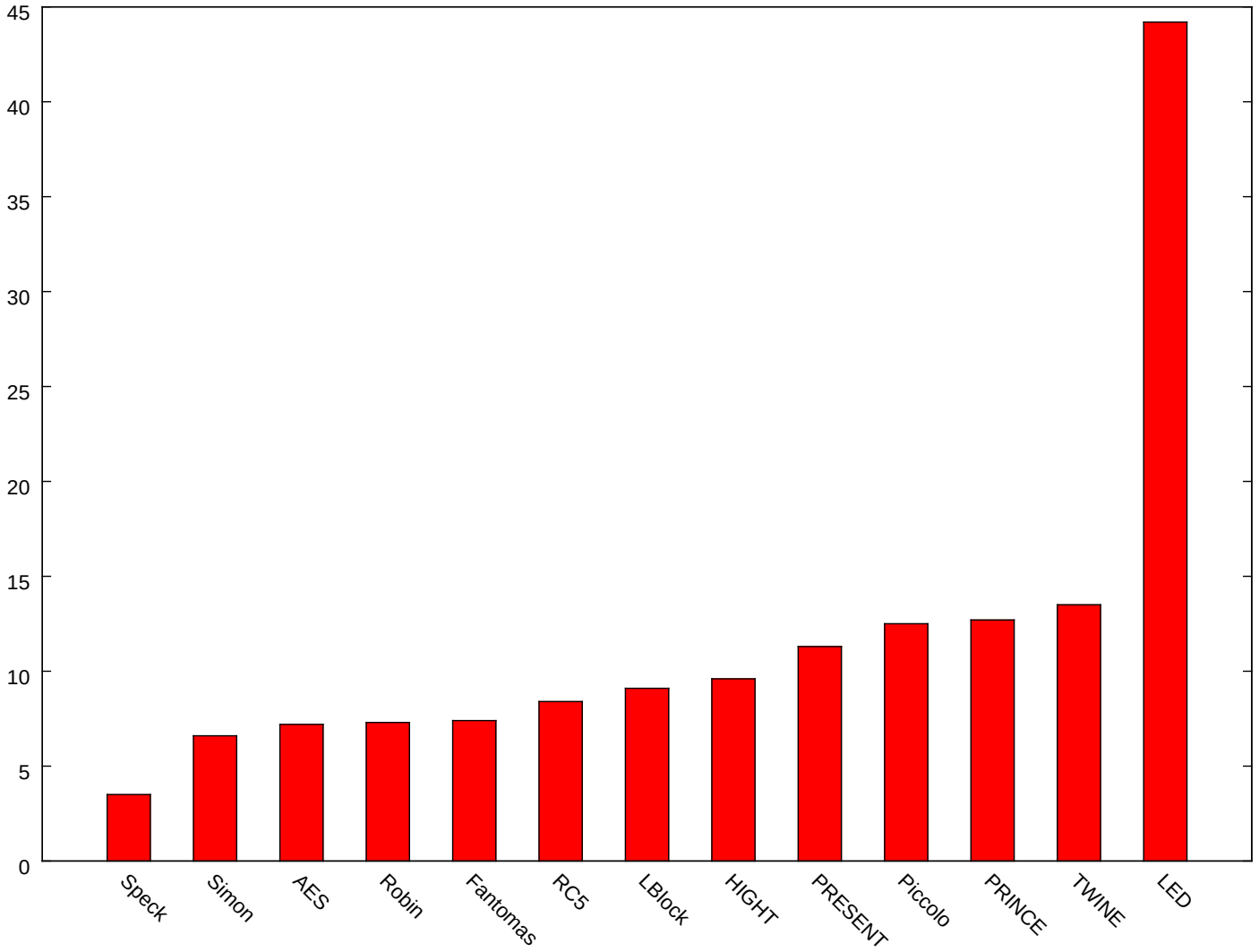
For each implementation i, and device d we calculate a *performance parameter* $p_{i,d}$, the value of which aggregates the three metrics $M = \{$ code size, RAM size, cycle count $\}$ as follows:

$$p_{i,d} = \sum_{m \in M} w_m \frac{v_{i,d,m}}{\min_i(v_{i,d,m})}, \tag{1}$$

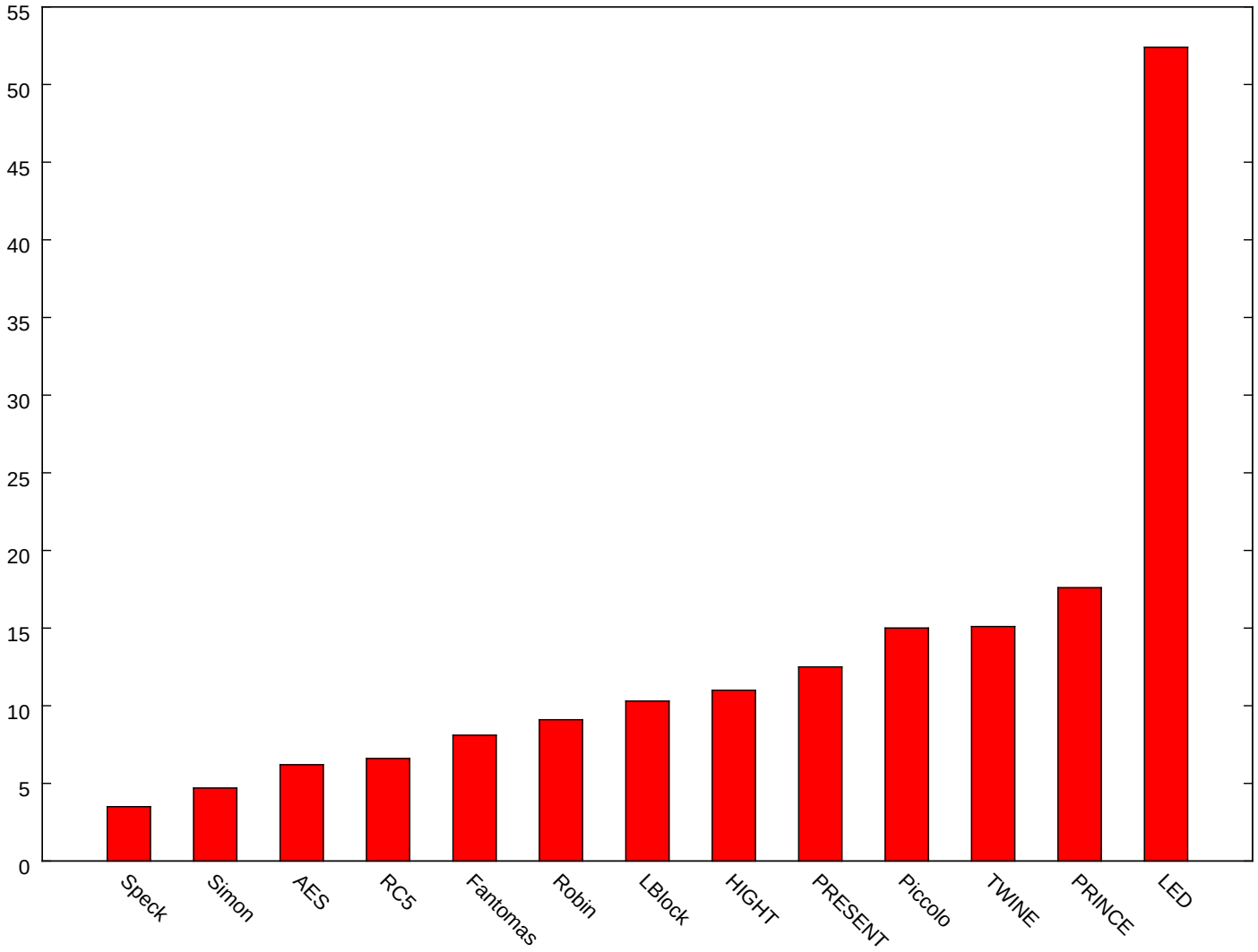
where $v_{i,d,m}$ is the value of the metric m for the implementation i on the device d; w_m is the *relative weight* of metric m and $\min_i(v_{i,d,m})$ represents the *minimum value* of the metric m from all considered implementations of all considered ciphers on the same device d. Finally, for each cipher and the selected set of implementations i_1, i_2, i_3 (one for each device) we calculate the Figure-of-Merit (FOM) value as the average performance value over three devices.

$$\mathrm{FOM}(i_1, i_2, i_3) = \frac{p_{i_1,AVR} + p_{i_2,MSP} + p_{i_3,ARM}}{3} \tag{2}$$

Scenario 1: FOM



Scenario 2: FOM



Conclusions

- Simon Wins Big!
  - Consistently fast and small on all three platforms
  - Best FOM score in both scenarios
  - Speck on 2nd place
  - Other advantages (small silicon area, SCA protection)
- Runner Up: LS Designs
  - Also fairly good on all three platforms
  - FOM score twice as high as Simon
  - Interesting from SCA perspective
  - More security analysis needed

Triathlon Competition

- Submit implementations (assembly/C) of existing lightweight block ciphers (published at well-known conferences) for the 3 target devices (AVR, MSP, ARM).
- Based on the implementation performance figures on the 3 target devices (AVR, MSP, ARM) in the 2 evaluation scenarios, you get a number of points.
- Collect as many points as possible to win the „Triathlon“
- The first 3 players/teams by the number of points will be rewarded with special prizes
- First deadline: September 6, 2015 (before CHES)
- More info: https://cryptolux.org