The ACRYPT Project

Lightweight Cryptography for the Internet of Things

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

Presented by Zhe Liu

SnT, University of Luxembourg

15 September 2015

Lightweight Crypto Lounge

- A Zoo about lightweight symmetric primitives
- Design principles and cryptographic properties
- Best attacks
- Hardware implementation footprint (if available)
- 50+ primitives!

Let us know if you have new results!

https://www.cryptolux.org/index.php/Lightweight_Block_Ciphers

Benchmarking Framework

FELICS – **F**air **E**valuation of **Li**ghtweight **C**ryptographic **S**ystems

- Open-source software benchmarking framework
- Similar to SUPERCOP, but for embedded devices
- 3 different platforms (8-bit AVR, 16-bit MSP, 32-bit ARM)
- 3 different metrics: execution time, RAM, code size
- Different usage scenarios
- 100+ different implementations of block and stream ciphers!

Contributions are welcome!

https://www.cryptolux.org/index.php/FELICS

Implementation Competition

Win Luxembourgish Chocolate/Beer!

Triathlon Competition

How do I win?

What to submit? Implementations (assembly/C) of published lightweight block ciphers

What targets? AVR, MSP, ARM

Scores Get points based on the implementation performance figures

Who gets a prize? First 3 players/teams *and* first 3 implementations

~~First Deadline~~: ~~**September 6, 2015** (before CHES 2015)~~

Website: https://www.cryptolux.org/index.php/FELICS_Triathlon

Winners of First Triathlon

Players/Teams

1. **Jason Smith** – *1440* points
2. **Dongsoo Lee** and **Ilwoong Jeong** – *1290* points
3. **Jason Smith** and **Bryan Weeks** – *1240* points

Implementations

1. **LEA**_128_128_v03 – *750* points
2. **Speck**_64_96_v04 – *730* points
3. **Chaskey**_128_128_v02 – *690* points

Details: https://www.cryptolux.org/index.php/FELICS_Triathlon

Triathlon Competition

Second Deadline

March 13, 2016
(before FSE 2016)

Website: https://www.cryptolux.org/index.php/FELICS_Triathlon

Conclusion

↓↓ Click on this link ↓↓

https://www.cryptolux.org/index.php/Lightweight_Cryptography

↑↑ Click on this link ↑↑