The ACRYPT Project

Results of the Second Round of the Triathlon

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

SnT, University of Luxembourg

22 March 2016

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!

Triathlon Competition

How do I win?

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

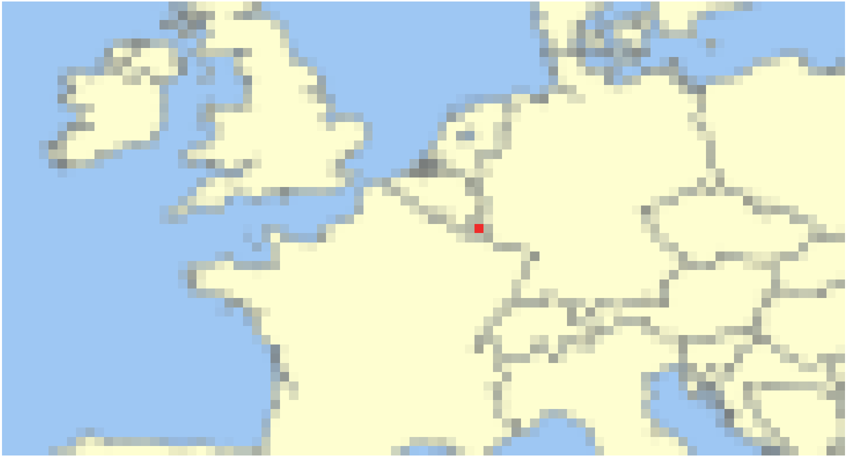
What targets? AVR, MSP, ARM

Scores Get points based on the implementation performance figures

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

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

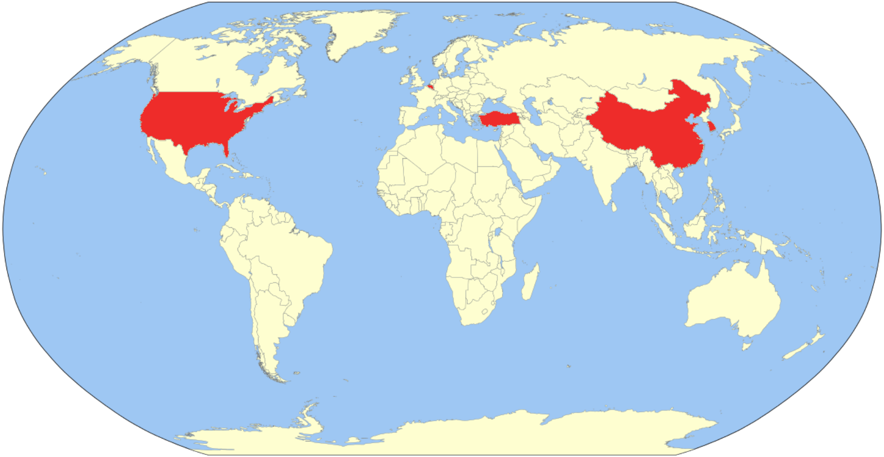
Before the Triathlon...



Some implementations...

A blurred picture of the implementation of LWC.

After the Triathlon!



Many implementations!

Much better understanding: rotations, assembly...

Winners of First Triathlon

Players/Teams

1. **Jason Smith and Yann Le Corre** – 3400 points
2. **Bryan Weeks, Jason Smith and Yann Le Corre** – 2920 points
3. **Bao Zhenzhen, Luo Peng and Zhang Wentao** – 2800 points

Implementations

1. **HIGHT_64_128_v21** – 1030 points – (*by Ilwoong Jeong*)
2. **Chaskey_128_128_v02** – 1010 points – (*by Mouha and Smith*)
3. **Speck_64_128_v02** – 910 points – (*by Smith and Weeks*)

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

Amazing Prices!

uni.lu
UNIVERSITÉ DU LUXEMBOURG

SnT
securityandtrust.lu

This is to acknowledge the contributions of

Bao Zhenzhen, Luo Peng and Zhang Wentao

to *Fair Evaluation of Lightweight Cryptographic Systems (FELICS)*
and the outstanding results achieved by their implementations
in the Second *Triathlon* competition

From the FNR ACRYPT project and the CryptoLUX team

22 March 2016

Triathlon Competition

Deadline for Next Lap

August 10, 2016

(before CHES 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 ↑↑