NIST’s Lightweight Crypto Project

MELTEM SONMEZ TURAN, NIST

Motivation

- Shift from general-purpose computers to dedicated resource-constrained devices
- New applications e.g. health tracking, self-driving cars, etc.
- Collection of private data
- Security problems
- Lack of cryptographic standards that are suitable for resource-constrained devices

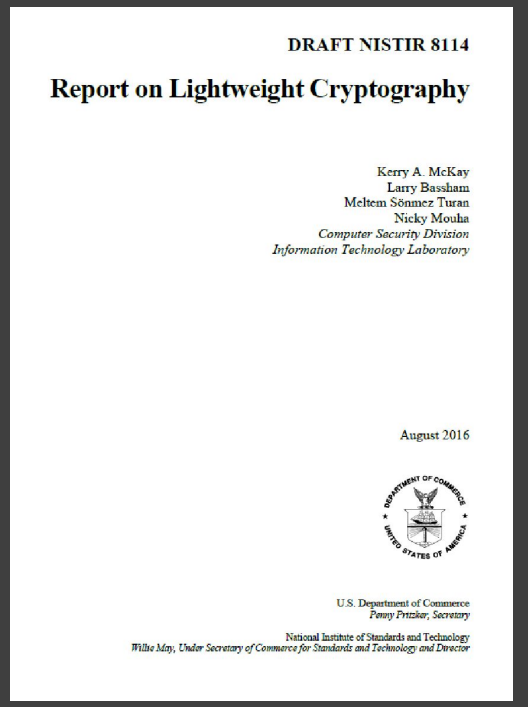
NIST's Lightweight Crypto Project

After receiving some concerns from industry in 2014, NIST initiated the lightweight crypto project

- to understand the need/requirements/characteristics of real-world applications,
- to understand where the NIST-approved algorithms fall short,
- to bring industry/academia/government together,
- to think about future standardization of lightweight primitives.

So far …

- Meetings with industry partners
- The First Lightweight Crypto Workshop at NIST on July 20-21, 2015
- Invited talks at Fast Software Encryption 2015, Lightweight Crypto Day 2015, Lightsec 2015, Cybersecurity Innovation Forum etc.
- Followed the developments in the academic literature (new designs, new efficient implementations of crypto standards etc.)
- Followed the developments in standardization of lightweight crypto
- Draft NISTIR 8114 Report on Lightweight Cryptography, August 2016


DRAFT NISTIR 8114

Report on Lightweight Cryptography

Kerry A. McKay
Larry Bassham
Meltem Sönmez Turan
Nicky Mouha
Computer Security Division
Information Technology Laboratory

August 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Initial Questions

???

- What do we mean by lightweight cryptography?
- How do the current NIST-approved crypto standards perform on constrained devices?
- Which constrained devices should we consider? What are the restrictions of the devices/applications?
- Are there solid academic solutions?
- Do we need to add new lightweight algorithms to our cryptographic toolkit? If yes, what should be the process? A competition? An open call?
- What should be the scope of the project?

Lightweight Cryptography

- Subfield of cryptography
- Aims to provide solutions tailored for resource-constrained devices
- It is not weak crypto, but it may be less robust, less misuse resistant, may have fewer features.

“Weight” of a Crypto Primitive

Amount of resources needed to run the primitive.

Depends on the target platform!

For Hardware Applications:
Area, latency, throughput, power/energy consumption etc.

For Software Applications:
Execution time, latency, memory (ROM/RAM) requirements, power/energy consumption etc.

Target Devices

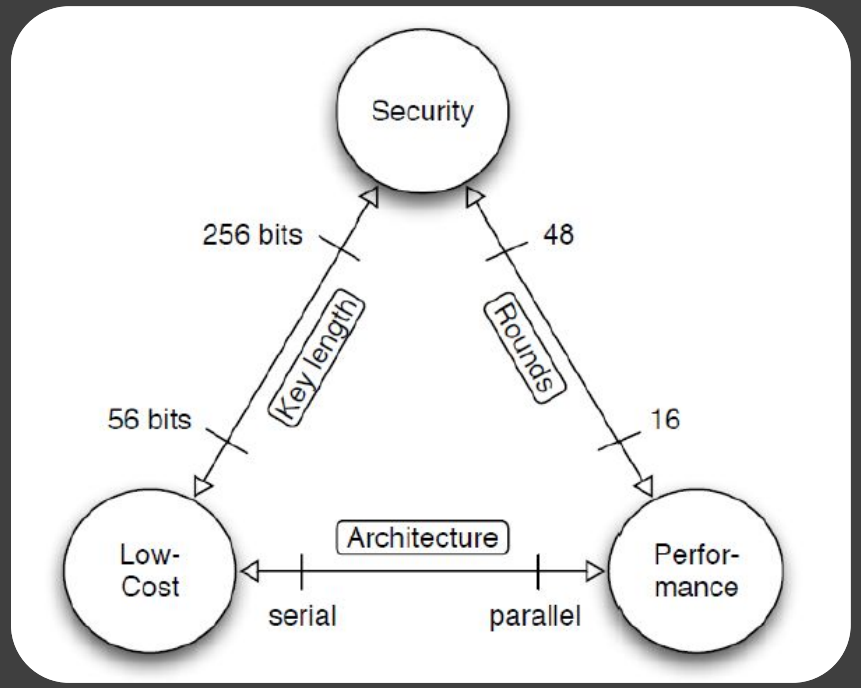
Servers and Desktops	Conventional Cryptography
Tablets and Smartphones	
Embedded Systems	Lightweight Cryptography
RFID and Sensor Networks	

Lightweight Crypto Research

- New lightweight primitives: Modifications of well-analyzed algorithms, old interesting algorithms, new dedicated algorithms
- Cryptanalysis of the new designs
- Benchmarks (e.g. FELICS project), improved implementations of crypto standards

Lightweight Crypto Research

Security-Performance-Cost Tradeoff



- Optimal tradeoff depends on the target technology.
- Small security margin by design
- Different optimizations: size, power, energy, latency, code size, RAM/ROM consumption

Figure: A. Poschmann, *Lightweight Cryptography: Cryptographic engineering for a pervasive world*

Advances in Crypto Design

- Simpler key schedules
- Many iterations of simple rounds
- Simpler operations (e.g. XORs, rotation, 4X4 S-boxes, bit permutations)
- Smaller block/internal/output/message sizes
- New designs with inherent resistance against side channel attacks

Different Attack Models

- Limited number of known plaintexts/ciphertexts imposed by the limitations of the devices (e.g. battery life)
- Less concern about related key attacks (if keys are generated using KDF standards).
- Side channel and fault attacks

Overview of Standardization Efforts

- ISO/IEC SC27 (PRESENT, CLEFIA, PHOTON, SPONGENT, Lesamnta-LW, Enocoro, Trivium)
- CRYPTREC (Target ciphers: AES, Camellia, CLEFIA, PRESENT, LED, Piccolo, TWINE, PRINCE)
- ECRYPT eSTREAM Project – Stream Ciphers for Constrained Environments - 2008 (Mickey, Trivium, Grain)
- Industry-specific standards (Proprietary designs) (A5/1 in GSM, E0 in Bluetooth)

NIST Standards on Constrained Devices

Constrained AES implementations:

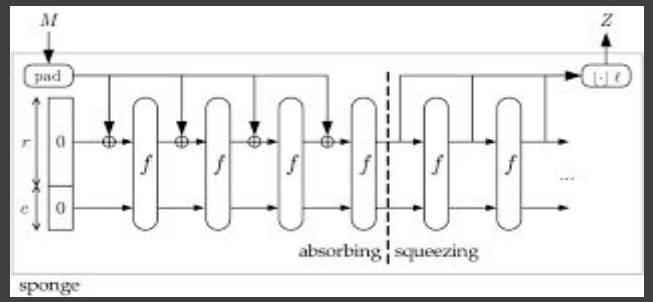
- 1947/2090 GEs (8-bit serial implementation) (Mathew et al., 2015)
- 2400 GEs (Moradi et al., 2011)
- 8-bit AVR microcontrollers 124.6 and 181.3 cpb for encryption/decryption with a code size < 2 Kbyte (Osvik et al., 2010).
- On RL78 16-bit microcontroller, combined enc/dec implementation is not possible within 512 bytes of ROM and 128 bytes of RAM (Moriai, 2016).

Constrained SHA-3 implementations:

- Area requirement of SHA-3 is around 5500GEs, with low, but acceptable, throughput.

SHA-3 and Small Permutations of KECCAK

- Permutation based sponge construction, with widths {25, 50, 100, 200, 400, 800, 1600}.



- Lightweight instance: e.g. 200-bit permutation with r=40, c=160, 12 rounds, 80-bit security.
- Offers tradeoffs
- Reusing permutation for authenticated encryption, hashing, etc.

More research needed for small permutations of Keccak

NIST's Lightweight Crypto Project - The Scope

All cryptographic primitives and modes that are needed in constrained environment!

Initial focus :

Symmetric Cryptography (Block Ciphers, Hash Functions, MACs, Stream Ciphers, Authenticated Encryption Schemes)

NIST's Lightweight Crypto Project - The Approach

How do we develop standards?

- *International competitions* (*e.g., AES, SHA-3)*
- *Adoption of existing standards: (e.g., RSA, HMAC)*
- *Open call for proposals:* (e.g. modes of operations)
- *Development of new algorithms* if no suitable standard exists (e.g., DRBGs)

For Lightweight Crypto

- *Open call for proposals*
- *Portfolio of algorithms with limited use*

NIST's Lightweight Crypto Project - The Profiles

- Evaluate and recommend algorithms based on ***Profiles***.
- Profiles include set of design goals, physical characteristics of target devices, performance characteristics imposed by the applications, and security characteristics.
- Profiles will be determined by NIST, based on the feedback we receive from the industry.

Next Steps

- Get feedback to develop profiles
- Announce the profiles - 2017
- Call for submissions for the profiles (submission requirements, guidelines, and set of evaluation criteria will be published on our project webpage).
- Third Lightweight Crypto Workshop in 2018 to discuss proposals

Feedback

- The proposed approach
- The questions listed in NISTIR 8114
- Evaluation process
- Timeline

Contact info

Send your feedbacks to: lightweight-crypto@nist.gov

Lightweight Crypto Email Forum : lwc-forum@nist.gov

Project website: http://www.nist.gov/itl/csd/ct/lwc-project.cfm

THANKS!