# NIST Lightweight Cryptography (LwC) Project

Gopal Iyer
R&D Engineer,
DENSO International America Inc.
gopalakrishnan_iyer@denso-diam.com

# NIST LwC Project

- Initiated in 2013
- To address growing industry need for security in resource constrained devices
- To find new cryptographic primitives for constrained devices
- For new applications (Health tracking, Asset tracking(RFID), autonomous cars etc.)
- To gather industry feedback on suitability of current crypto. standards for constrained devices
- To create recommendations & standards for the use of Lightweight cryptography

*Source: https://www.nist.gov/programs-projects/lightweight-cryptography*

# LwC project Goals/Targets

- Understand the need/requirements/characteristics of real-world applications,
- Understand where current NIST-approved algorithms fall short
- Bring industry/academia/government together
- Think about future standardization of lightweight primitives.
- Aims to provide solutions tailored for resource-constrained devices
- Not weak crypto, but may be less misuse resistant, may have fewer features
- Initial focus on Symmetric Ciphers (Block ciphers, Hash functions, stream ciphers, MACs, Authenticated Encryption)

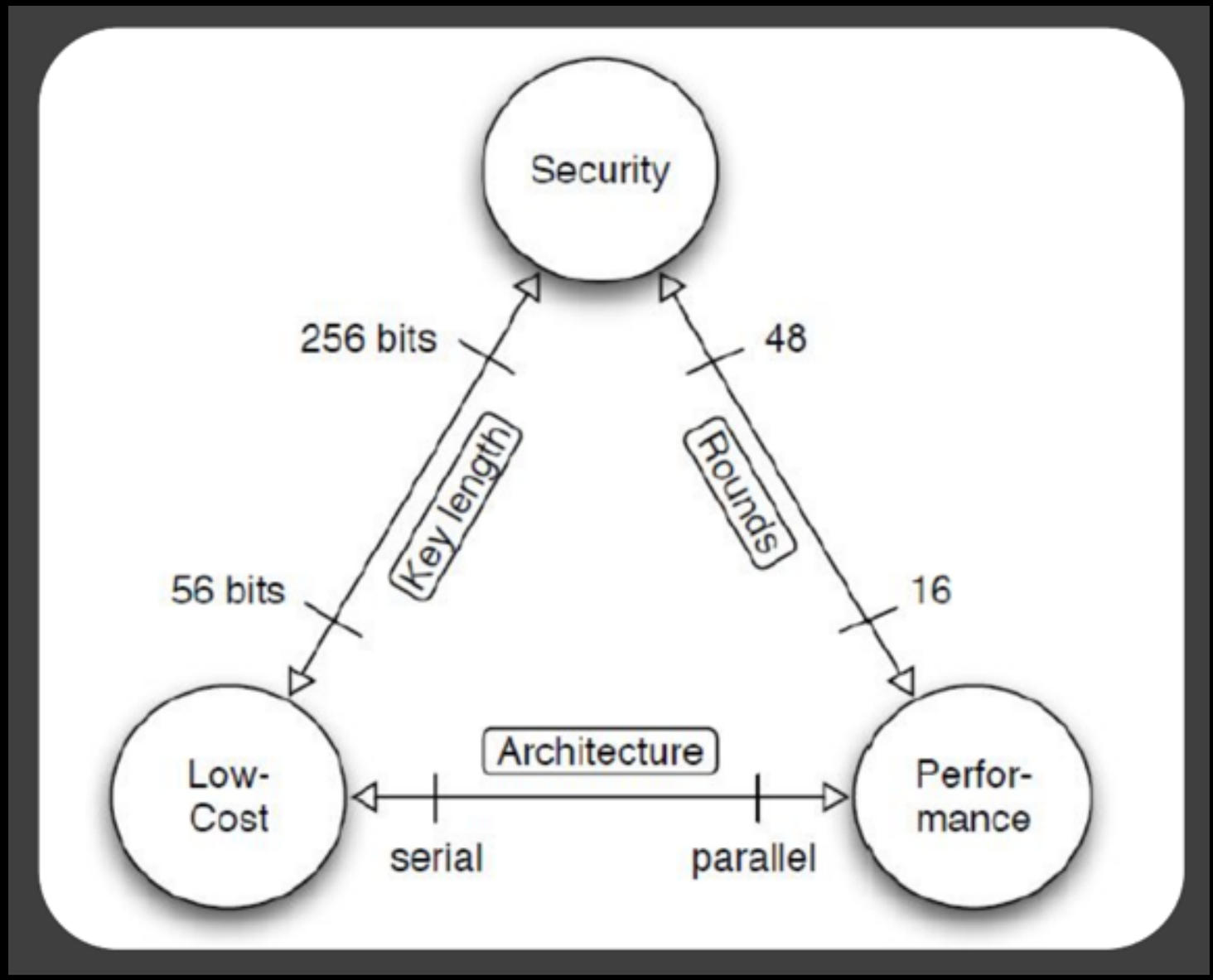
# Optimization criteria

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

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

*LwC Scope*

# Trade off points




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

# Activity

- First LwC Workshop in 2015
    - https://www.nist.gov/news-events/events/2015/07/lightweight-cryptography-workshop-2015
- Information Report published [Aug 2016]: http://csrc.nist.gov/publications/drafts/nistir-8114/nistir_8114_draft.pdf
    - Proposal for creating Profiles
    - Lightweight algorithms will be chosen from a an approved list to meet optimization criteria in profiles
    - Industry feedback solicited on profiles.
- Second LwC Workshop in 2016
    - https://www.nist.gov/news-events/events/2016/10/lightweight-cryptography-workshop-2016

# Profile parameters & Sample

| Physical characteristics | Performance characteristics | Security characteristics |
|---|---|---|
| Area (in GE) | Latency (in clock cycles) | Minimum security strength (bits) |
| Memory (RAM/ROM) | Throughput (cycles per byte) | Attack models |
| Implementation type (hardware, software, or both) | Power (µW) | Side channel resistance requirements |

| **Profile Sample_2** | |
|---|---|
| **Primitive** | Block cipher |
| **Physical characteristics** | Hardware or software implementation |
| **Performance characteristics** | Latency $\leq$ 20 ns |
| **Security characteristics** | 128-bit security, resistance to power analysis |
| **Design goals** | Authenticated encryption |

*Sample Profile*

# List of LwC Algorithms

- Lightweight Block Ciphers
  - PRESENT, SIMON, SPECK, RC5, TEA, XTEA, MISTY1, TWINE etc.
  - Non-exhaustive list: https://www.cryptolux.org/index.php/Lightweight_Block_Ciphers
- Lightweight Steam Ciphers
  - Grain, Trivium, Mickey, etc.
- Lightweight Hash Functions
  - PHOTON, Quark, SPONGENT, Lesamnta-LW, etc.
- Lightweight MAC
  - Chaskey, TuLP, LightMAC, etc.
- Lightweight DSA: WalnutDSA

# Performance of LwC Block Ciphers

- CryptoLUX, University of Luxembourg
  - Released FELICS framework (Fair Evaluation of Lightweight Cryptographic Systems)
  - https://www.cryptolux.org/index.php/FELICS

| Cipher Info | | | | Results | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | AVR | | | MSP | | | ARM | | | |
| Cipher | Block [b] | Key [b] | Sec. | Code [B] | RAM [B] | Time [cyc.] | Code [B] | RAM [B] | Time [cyc.] | Code [B] | RAM [B] | Time [cyc.] | FOM |
| Chaskey | 128 | 128 | 0.87 | 1510 | 229 | 22142 | 1136 | 244 | 23402 | 438 | 236 | 9851 | 4.3 |
| Speck | 64 | 96 | 0.69 | *966* | *294* | *39875* | *556* | *288* | *31360* | 492 | 308 | 15427 | 4.9 |
| Speck | 64 | 128 | 0.70 | *874* | *302* | *44895* | *572* | *296* | *32333* | 444 | 308 | 16505 | 5.0 |
| Chaskey-LTS | 128 | 128 | 0.43 | 1510 | 229 | 34814 | 1140 | 244 | 37626 | 438 | 236 | 12859 | 5.0 |
| Simon | 64 | 96 | 0.71 | *1084* | *363* | *63649* | *738* | *360* | *47767* | 600 | 376 | 23056 | 6.7 |
| Simon | 64 | 128 | 0.70 | *1122* | *375* | *66613* | *760* | *372* | *49829* | 560 | 392 | 23930 | 6.9 |
| RECTANGLE | 64 | 80 | 0.72 | *1152* | *352* | *66722* | *818* | *396* | *45688* | *670* | *426* | *36814* | 7.8 |
| RECTANGLE | 64 | 128 | 0.72 | *1118* | *353* | *64813* | *844* | *402* | *46196* | *654* | *432* | *37006* | 7.8 |
| LEA | 128 | 128 | -1 | *1684* | *631* | *61020* | *1130* | *626* | *47339* | *524* | *664* | *17417* | 8.0 |
| SPARX | 64 | 128 | 0.62 | *1198* | *392* | *65539* | *966* | *392* | *36766* | *1200* | *424* | *40887* | 8.6 |
| SPARX | 128 | 128 | 0.68 | *1736* | *753* | *83663* | *1118* | *760* | *53936* | *1122* | *788* | *67581* | 12.9 |
| HIGHT | 64 | 128 | 0.69 | *1414* | *333* | *94557* | *1238* | *328* | *120716* | *1444* | *380* | *90385* | 14.1 |
| AES | 128 | 128 | 0.70 | *3010* | *408* | *58246* | *2684* | *408* | *86506* | *3050* | *452* | *73868* | 15.3 |
| Fantomas | 128 | 128 | -1 | 3520 | 227 | 141838 | 2918 | 222 | 85911 | 2916 | 268 | 94921 | 17.2 |
| Robin | 128 | 128 | -1 | 2474 | 229 | 184622 | 1900 | 224 | 110527 | 3668 | 304 | 91909 | 18.0 |
| RC5-20 | 64 | 128 | 0.80 | 2782 | 372 | 275730 | 1240 | 378 | 386026 | 624 | 376 | 36473 | 18.9 |
| PRIDE | 64 | 128 | -1 | 1402 | 369 | 146742 | 2566 | 212 | 242784 | 2240 | 452 | 130017 | 21.5 |
| RoadRunneR | 64 | 80 | -1 | 2504 | 330 | 144071 | 3088 | 338 | 235317 | 2788 | 418 | 119537 | 22.1 |
| RoadRunneR | 64 | 128 | -1 | 2316 | 209 | 125635 | 3218 | 218 | 222032 | 2504 | 448 | 140664 | 22.2 |
| LBlock | 64 | 80 | 0.72 | 2954 | 494 | 183324 | 1632 | 324 | 263778 | 2204 | 574 | 140647 | 23.8 |
| PRESENT | 64 | 80 | 0.84 | *2160* | *448* | *245232* | *1818* | *448* | *202050* | *2116* | *470* | *274463* | 31.5 |
| PRINCE | 64 | 128 | 0.83 | 1954 | 369 | 299322 | 2028 | 236 | 386781 | 1700 | 448 | 233941 | 32.7 |

# Global Standardization

- ISO/IEC SC27 ( PRESENT, CLEFIA, PHOTON, SPONGENT, Lesamnta-LW, Enocoro,Trivium)
- ISO/IEC 29192-2:2012 Information technology -- Security techniques -- Lightweight cryptography -- Part 2: Block ciphers
- CRYPTREC JAPAN (Target ciphers: AES, Camellia, CLEFIA, PRESENT, LED, Piccolo, TWINE, PRINCE)
- ECRYPT eSTREAM Project [EU] – Stream Ciphers for Constrained Environments - 2008 (Mickey, Trivium, Grain)
- Industry-specific standards (Proprietary designs) (A5/1 in GSM, E0 in Bluetooth)
- NIST constrained SHA-3 implementation

# Get Involved

- Send Feedback: lightweight-crypto@nist.gov
- Join Forum/Mailing list: lwc-forum@nist.gov
- Project Site: http://www.nist.gov/itl/csd/ct/lwc-project.cfm
- Proposal to invite NIST LwC project members to speak at SAE meetings/ESCAR