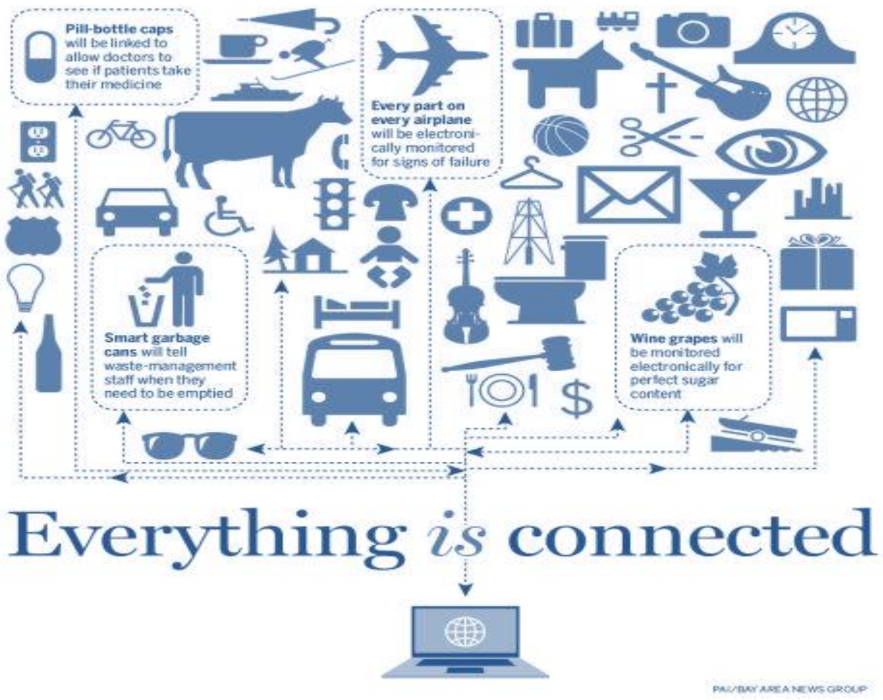
Towards a Lightweight Cryptography Standard

Meltem Sonmez Turan

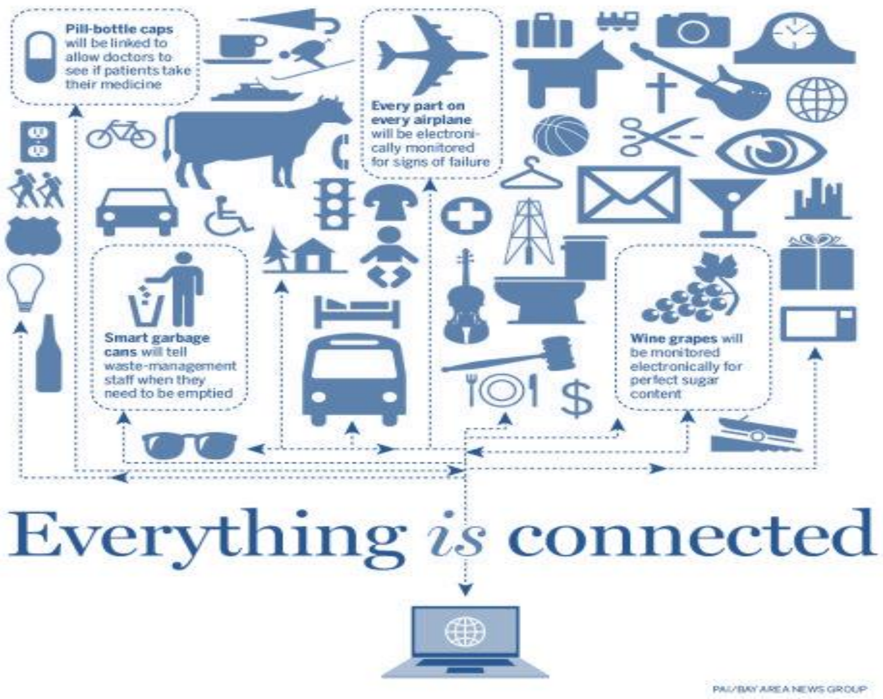
Lightsec 2015, Bochum Germany

September 10, 2015


Pill-bottle caps will be linked to allow doctors to see if patients take their medicine
Every part on every airplane will be electronically monitored for signs of failure
Smart garbage cans will tell waste-management staff when they need to be emptied
Wine grapes will be monitored electronically for perfect sugar content
Everything *is* connected
PAI/BAY AREA NEWS GROUP

- New concepts e.g. Internet of Things (IoT), pervasive computing, ubiquitous computing, ambient intelligence, calm computing
- New applications e.g. Healthcare monitoring systems, automated management of supply chain, public transportation, telephone cards

http://www.mercurynews.com/business/ci_24836116/internet-things-seen-bonanza-bay-area-businesses


Pill-bottle caps will be linked to allow doctors to see if patients take their medicine
Every part on every airplane will be electronically monitored for signs of failure
Smart garbage cans will tell waste-management staff when they need to be emptied
Wine grapes will be monitored electronically for perfect sugar content
Everything is connected
PAI/BAY AREA NEWS GROUP

- New concepts e.g. Internet of Things (IoT), pervasive computing, ubiquitous computing, ambient intelligence, calm computing
- New applications e.g. Healthcare monitoring systems, automated management of supply chain, public transportation, telephone cards

Cryptographic solutions tailored to constrained devices are needed.

http://www.mercurynews.com/business/ci_24836116/internet-things-seen-bonanza-bay-area-businesses

Lightweight Cryptography – Academic Research

Active research on Lightweight Crypto for the last 10 years

- Over 1600 papers on *lightweight cryptography* (according to Google Scholar)
- Dedicated workshops e.g. Lightsec, RFIDsec, Lightweight Crypto Day, Four workshops sponsored by the ECRYPT project

What has been done in academia? New Designs

- *Efficient implementations*
- *Modifications of well-analyzed algorithms* e.g. DESL, DESXL
- *Old interesting algorithms* e.g. RC5, TEA, XTEA
- *New dedicated block ciphers, AE primitives, hash functions, MAC algorithms* e.g. CLEFIA, Fantomas, HIGHT, ICEBERG, KASUMI, LBlock, LED, KATAN/KTANTAN, Klein, mCrypton, MIBS, NOEKEON, Piccolo, PRESENT, PRINTcipher, PUFFIN, PUFFIN2, PRINCE, PRIDE, SEA, SIMON, SPECK, TWIS, TWINE, Jambu, ALE, Quark, Photon, CHASKEY

What has been done in academia? New Approaches

Characteristics of the new designs

- Smaller algorithm parameters, such as block sizes (64, 80 bits), key length (80, 96, 112 bits), internal state size of the algorithms.
- Simply linear and nonlinear transformations, e.g. XORs, rotation, 4X4 Sboxes, bit permutations that allow implementation tradeoffs to the resources available on the target platform
- Many iterations of simple rounds
- Simplify key schedules, that can generate sub-keys on the fly
- Smaller security margins by design, many of them broken.

What has been done in academia? New Threat Models

- *Limits on the number of plaintext/ciphertext pairs.* Justified by the limitations of the devices (e.g. battery life), or message formats defined by the protocol. E.g. Prince claims 126-*n* bit security for an attacker with access to an 2^n input/output pairs
- *Less concern about related key attacks to simplify key schedule.* From *ideal cipher* to *ideal permutation* assumption. This can be accepted assuming that keys are generated randomly. E.g. For Prince, Decryption is free = encryption with a related key.
- *Side channel attacks.* More serious for cheaper devices. With countermeasures, the area increases by a factor of 3 to 5 (Fisher, Gammel, ’05). New designs with side channel resistance: Fides, LS family, PICARO.

Ecrypt eSTREAM Project

A 4-year network of excellence funded project started in 2004 by European Network of Excellence for Cryptology (ECRYPT)

Goal: To identify new stream ciphers that might be suitable for widespread adoption and to stimulate work in stream ciphers.

Profile I : for software applications with high throughput requirements with key size of 256 bits.

Profile II : **for hardware applications with restricted resources with key size of 80 bits.**

Ecrypt eSTREAM Project

Finalists of Profile II

- *Grain:*
  - Widely analyzed, tweaked twice, flexible
  - A new version Grain128a, featuring authentication
- *Trivium:*
  - Widely analyzed
  - Not tweaked, simple and elegant, flexible
  - Only supports 80-bit keys
- *Mickey:*
  - Lightly analyzed, security depends on the hardness of analysis.
  - Less implementation flexibility, due to irregular clocking
  - Susceptible to timing and power analysis attacks

What has been done by Standards Developing Organizations?

ISO
International Organization for Standardization
NFC FORUM
IEEE
CRYPTREC
Cryptography Research and Evaluation Committees
IEC
INTERNATIONAL ELECTROTECHNICAL COMMISSION
cen
European Payments Council
IETF
oma
Open Mobile Alliance
For a Connected World
ANSI
Bluetooth
SPECIAL INTEREST GROUP
ETSI
World Class Standards
RSA
Federal Office for Information Security
3GPP
A GLOBAL INITIATIVE
TRUSTED COMPUTING GROUP
W3C
ZigBee Alliance

What has been done by SDOs? ISO/IEC

International Organization for Standardization

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ISO/IEC 29192-1:2012 : Lightweight cryptography

- *Part I:* General, First edition, 2012
- *Part II:* Block ciphers, 2012, includes 64-bit PRESENT (80, 128 bit key) and 128-bit CLEFIA (128, 192 or 256-bit key)
- *Part III:* Stream ciphers, 2012, includes Enocoro (80, 128 bits key) and Trivium (80 bit key)
- *Part IV:* Mechanisms using asymmetric techniques, 2013, includes Identification scheme cryptoGPS, authentication and key exchange mechanism ALIKE, ID-based signature scheme IBS
- *Part V:* Hash functions – under development.

What has been done by SDOs? ISO/IEC

ISO/IEC 29167: Automatic identification and data capture techniques -- Part 1: Security services for RFID air interfaces

- A number of cryptographic suites designed for protecting application information transmitted across the RFID air interface, product authentication, and protecting access to resources on the tag.
- Ten parts, include the algorithms:
  - PRESENT-80, ECC-DH, Grain-128A, AES OFB,

    Crypto suite XOR, ECDSA-ECDH, cryptoGPS, RAMON

What has been done by SDOs? CRYPTREC

Cryptography Research and Evaluation Committees

- Project to evaluate and monitor the security of cryptographic techniques used in Japanese e-Government systems.
- Cryptrec publishes e-Government Recommended/Candidate Recommended/Monitored cipher lists.
- Cryptorec has a LWC working group, the target algorithms are:
  - *AES, Camelia, Clefia, Present, Led, Piccola, Twine, Prince*
- Deliverables on LWC (in Japanese).

CRYPTREC
Cryptography Research and Evaluation Committees

Industry-specific standards

- Proprietary designs
- E.g. A5/1 (in GSM), E0 (in Bluetooth), Crypto1 (in Mifare RFID tags), Cryptomeria (C2) (for digital rights managements), Dect (cordless phones), DST40 (TI), KeeLoq (authentication in car locks), Kindle stream cipher

- Most reversed engineered, practically broken.

IoT Protocols

- *Alljoyn:* open source project run by AllSeen Alliance, industry stakeholders Qualcomm, Microsoft and AT&T
- *Iotivity:* open source project associated with AllSeen Alliance, industry stakeholders Intel, Samsung, Cisco
- *Thread:* open protocol run by Thread group, industry stakeholders ARM, Samsung, Qualcomm.

Protocol	Asymmetric	Bulk encryption	Authentication
Alljoyn	RSA, ECDSA, ECDHE P256	AES CCM	AES CCM
Iotivity	RSA, DSA/DHE, ECDSA/ECDHE (NIST curves)	AES, AES CCM, AES GCM, 3DES	HMAC-SHA1, HMAC-SHA2
Thread	RSA, DSA/DHE, ECDSA/ECDHE (NIST curves)	AES, AES CCM, AES GCM, 3DES	HMAC-SHA1, HMAC-SHA2

Slide credit: Dan Shumov

Lightweight Cryptography Project at NIST

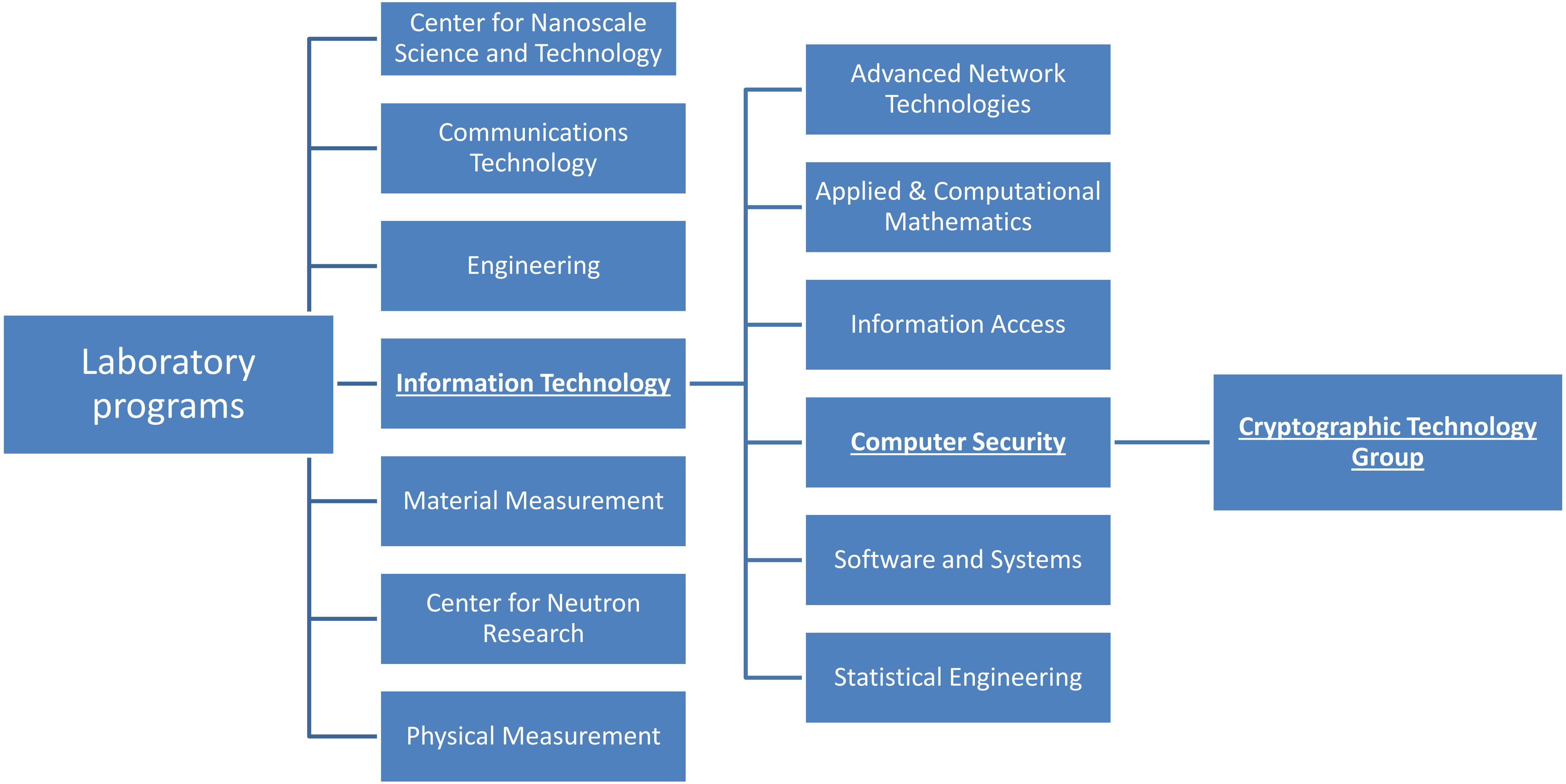
NIST

National Institute of
Standards and Technology
U.S. Department of Commerce

- Measurement science lab.
- Part of the US Department of Commerce
- Located at Gaithersburg, Maryland
- Founded in 1901, known as the National Bureau of Standards (NBS) prior to 1988
- Around 2700 employees, and 1,800 associates.

NIST's mission

to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade and improve the quality of life.



Laboratory programs

Center for Nanoscale Science and Technology

Communications Technology

Engineering

Information Technology

Material Measurement

Center for Neutron Research

Physical Measurement

Advanced Network Technologies

Applied & Computational Mathematics

Information Access

Computer Security

Software and Systems

Statistical Engineering

Cryptographic Technology Group

What do we do?

- *Algorithm specifications:*
  - Federal Information Processing Standards (FIPS) and Special Publications (SPs) specify a number of approved cryptographic algorithms.
- *General guidance on the use of cryptography:*
  - Covering selection, implementation, deployment and use of cryptography.
- *Guidelines in application-specific areas:*
  - Areas of particular need for the US government (e.g., PIV, TLS).
- *Testing:*
  - Providing assurance that crypto is implemented properly (e.g., FIPS 140 and CMVP)

Who do we work with ?

- *Academic Researchers:*
  - Development of new algorithms/modes/schemes, to advance science of cryptography
- *Industry:*
  - On adoption of cryptographic algorithms, feedback mechanism on standards
- *Standards Developing Organizations:*
  - Adoption and development of new standards
- *Government:*
  - Core user community

How do we develop standards?

- *International Competitions*
  - Engage community through an open competition
  - *e.g., AES, SHA-3*
- *Adoption of Existing Standards*
  - Collaboration with accredited standards organizations
  - *e.g., RSA, HMAC*
- *Open call for proposals*
  - Ongoing open invitation
  - e.g. modes of operations (SP 800 38)
- *Development of New Algorithms*
  - Used if no suitable standard exists
  - e.g., DRBGs

NIST IR 7977 *NIST Cryptographic Standards and Guidelines Development Process*

NIST-**approved** Cryptographic Algorithms

Block ciphers:

- FIPS 197- Advanced Encryption Standard (AES), FIPS 46-3 – Triple DES (TDEA), FIPS 185 – Skipjack

Block ciphers modes:

- ECB, CBC, CFB, OFB, CTR (for encryption)
- CMAC, CCM, GCM, (for authenticated encryption)
- KW, KWP, TKW (for key wrapping)

Hash functions:

- SHA-1, SHA-2 family (six algorithms), SHA-3 family (four algorithms)

Digital signatures:

- DSA, RSA, ECDSA

Approved algorithms on constrained devices (1)

- Approved algorithms like AES, SHA-2, SHA-3 etc. were not designed to for constrained environments!
  - Selected to perform good on variety of platforms.

- *Constrained AES implementations:*
  - In hardware, 2400 GEs (Moradi et al., Eurocrypt 11), 2090-gate design (Mathew et al, 2014)
  - In software, using 8-bit AVR microcontrollers, 124.6 and 181.3 cpb for encryption/decryption with a code size < 2 Kbyte (Osvik et al.,FSE10).
  - **AES should be used whenever possible!**

Approved algorithms on constrained devices (2)

- *SHA-3 Hash functions*
  - Sponge construction, using a 1600-bit permutation.
  - Smaller permutations with width {25, 50, 100, 200, 400, 800} are also defined in FIPS 202.
  - Reusing permutation for AE, hashing, etc.
  - Lightweight Keccak uses 200-bit permutation with, r=40, c=160, 12 rounds, with security strength of 80 bits.

- *Constrained SHA-3 implementations:*
  - 9.3 kGE on a 130 nm CMOS process technology, by designers
  - Kavun & Yalcin implemented 200, 400, 800 and 1600 versions with 2.52kGE, 5.09kGE, 13kGE and 20.79kGE, respectively.
  - Pessle & Hutter showed that 1600-bit version can be implemented with less than 5.5kGEs.
    - Low, but acceptable, throughput
    - 800-bit with 4.6kGE. (900GE less than full permutation and twice as fast.)
    - Don’t include side channel resistance.

Lightweight Crypto Project at NIST

After receiving some concerns on lack of suitable lightweight cryptographic algorithms from industry, 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.

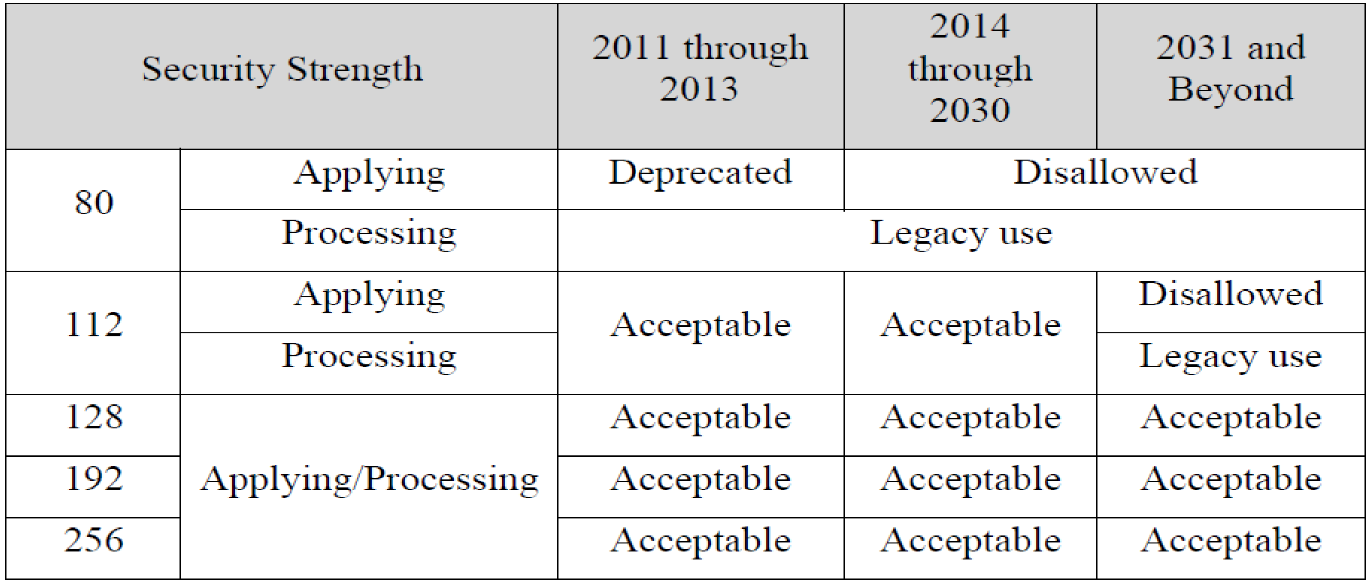
Tentative Timeline

Phase	*Objectives*	*Time*
Phase I	- Announce intent - Identify and evaluate the need - Survey latest developments - Workshop @NIST on July 20-21,2015 - Consider requirements and solutions	Late 2014 - December 2015
Phase II	- Define specific plan - Develop SP (if applicable) - Maintenance	2016 -

Challenges in Lightweight Crypto Standardization (1)

Selection of key sizes:

- Proposals use shorter key sizes to reduce area requirements.
- According to SP 800-57, key sizes shorter than 112 is not allowed. We don’t plan to use shorter keys.



Security Strength		2011 through 2013	2014 through 2030	2031 and Beyond
80	Applying	Deprecated	Disallowed	
	Processing	Legacy use		
112	Applying	Acceptable	Acceptable	Disallowed
	Processing			Legacy use
128	Applying/Processing	Acceptable	Acceptable	Acceptable
192		Acceptable	Acceptable	Acceptable
256		Acceptable	Acceptable	Acceptable

Challenges in Lightweight Crypto Standardization (2)

Bridging the gap b/w industry and academia:

Optimal tradeoff depends between security/cost/performance depends on the target technology.

- Prince, and Chaskey are examples of successful collaboration.
- Dedicated workshops, meetings are useful.

Challenges in Lightweight Crypto Standardization (3)

Misuse Prevention

- Less flexibility, less misuse resistant, more constraints, assumptions about attackers.
- Challenge to enforce the limitations, e.g., # of known/chosen plaintext/ciphertext blocks, Uniqueness of the IVs (e.g. AES GCM), related key resistance
- May be done in protocol level.

Lightweight Crypto Workshop at NIST

- NIST held the Lightweight Crypto Workshop at NIST on July 20-21, 2015.
- Around 80 attendees from industry, government, and academia
- Program included 24 papers, 2 invited talks and a panel.
- Received some new design proposals (block ciphers, MAC, stream ciphers, signature schemes, protocols), benchmarking results, some position papers
- Presentations/papers available athttp://www.nist.gov/itl/csd/ct/lwc_workshop2015.cfm

Some of the feedbacks we received …

- AES bring performance compromise in RFIDs, when the LWC standards are implemented they provide performance advantage.
- No need for lightweight crypto for software for IoT devices/tables/smart phones, with possible exception for microcontrollers.
- Smaller key sizes should not be used.
- Implementation flexibility is very important.
- Competition can be useful to bring attention, but might be hard to frame. A block cipher, stream cipher, symmetric, asymmetric? Or an AE scheme for short payloads?
- A small portfolio of algorithms addressing complementary parts of IoT ecosystem would be useful.

Next Steps

- By the end of 2015, publish a survey report.
- Narrow down the scope/target application/target devices
- New workshop in 2016

- Final standard may include an algorithm or a portfolio of algorithms
  - Adoption of existing standards
  - Open ongoing call for proposals
  - Unlikely a competition due to time constraints

Some Research Ideas

- New dedicated proposals, e.g. an AE primitive for short payload, new modes of operations, authentication mechanisms for stream ciphers, tweakable block ciphers with small block size
- Analysis recent lightweight crypto proposals, such as Present, Prince, Chaskey, Simon/Speck, etc.
- Analysis of smaller Keccak variants using 200, 400, 800 bits.
- Efficient implementations of lightweight crypto proposals on constrained environments
  - Contribute to FELICS (Fair Evaluation of Lightweight Cryptography Systems) by University of Luxembourg: Open source software benchmarking framework, with three different platforms (8-bit AVR, 16-bit MSP, 32-bit ARM)

THANKS!

Contact emails: meltem.turan@nist.gov
lightweight-crypto@nist.gov

e-mail forum: lwc-forum@nist.gov

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