An Account of the ISO/IEC Standardization of Simon and Speck

Tomer Ashur, **Atul Luykx**

Imec-COSIC KU Leuven

ISO/IEC Meeting, Jaipur, India

Dual EC

- NSA-designed PRNG (DRBG)
- Backdoored
- Snowden revelations: Project Bullrun
- Standardized by ISO November 2005 (before NIST)
  - “a challenge in finesse” – NSA

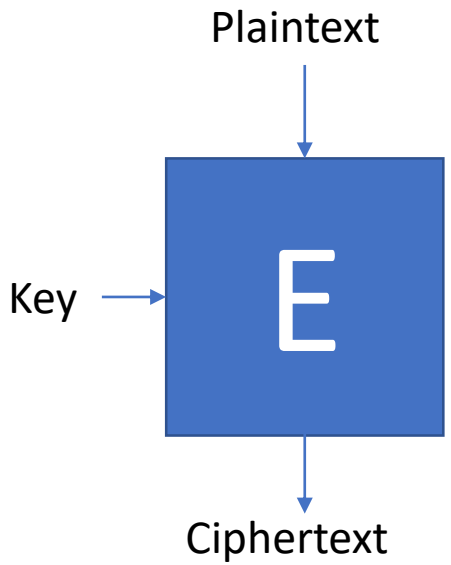
Bernstein, Lange, Niederhagen, “Dual EC: A Standardized Back Door”, eprint 2015/767

ISO/IEC Meeting, Jaipur, India

- Study Period on NSA proposal for new cryptographic algorithms
- Debby Wallner – US Head of Delegation

Simon and Speck

- Block cipher families
- Used in *modes of operation* for encryption, authentication/integrity, build hash functions, …



Block Size	Key Size
32	64
48	72 96
64	96 128
96	96 144
128	128 192 256

People are still making new block ciphers?

What's wrong with the AES? (Or triple DES…)

- Diversity
- Country preferences: China, Korea, Russia, Japan, …
- Research
  - Implementation-targeted ciphers
  - MPC-friendly ciphers
  - Side channel resistance
  - Performance, efficiency gains

In 2011, prompted by potential U.S. government requirements for lightweight ciphers (e.g., SCADA and logistics applications) and concerns that existing cryptographic solutions were unnecessarily restrictive, a team of cryptographic designers was formed within the Information Assurance Research Laboratory of NSA's Research Directorate, with the goal of designing foundational lightweight cryptographic block ciphers. SIMON and SPECK emerged from that research effort in 2013. See [Age16].

Beaulieu, Shors, Smith, Treatman-Clark, Weeks, Wingers, "Notes on the design and analysis of SIMON and SPECK", eprint 2017/560

Why Standardize at ISO?

- Country A develops algorithm X
- Country B does not like X, it blocks all products containing X

"… two key WTO Agreements … explicitly urge regulators to base their measures on relevant international standards to avoid unnecessary barriers to trade. These Agreements go as far as to say that measures that are based on relevant international standards are assumed to be in compliance with WTO rules."

Pascal Lamy, former director general WTO
https://www.iso.org/news/2011/09/Ref1463.html

What about NIST?

"We will encourage NSA to bring proposed algorithms to conferences and standards organizations – e.g., SIMON, SPECK"

John Kelsey, NIST

Real World Crypto 2015

Recap

- 2013: Simon and Speck made public on eprint
- Snowden revelations, Dual EC revoked from standards
- NIST tells NSA to get external vetting
- ISO comes with WTO benefit

Simon and Speck submitted for consideration to ISO/IEC October 2014

Rejected from ISO/IEC JTC 1 SC 27 April 2018

Goal

Shed some light on the process which leads governments and industries to agree upon the algorithms which secure their digital communications.

- When is ISO/IEC the right venue?
- Relationship with NSA?

- NOT: Tell you whether you should use Simon or Speck or not.

ISO/IEC JTC 1 SC 27 WG 2

- ISO: International Organization for Standardization
- IEC: International Electrotechnical Commission
- JTC 1: Information technology
- SC 27: IT Security techniques (21 SCs)
- WG 2: Cryptography and security mechanisms (5 WGs)

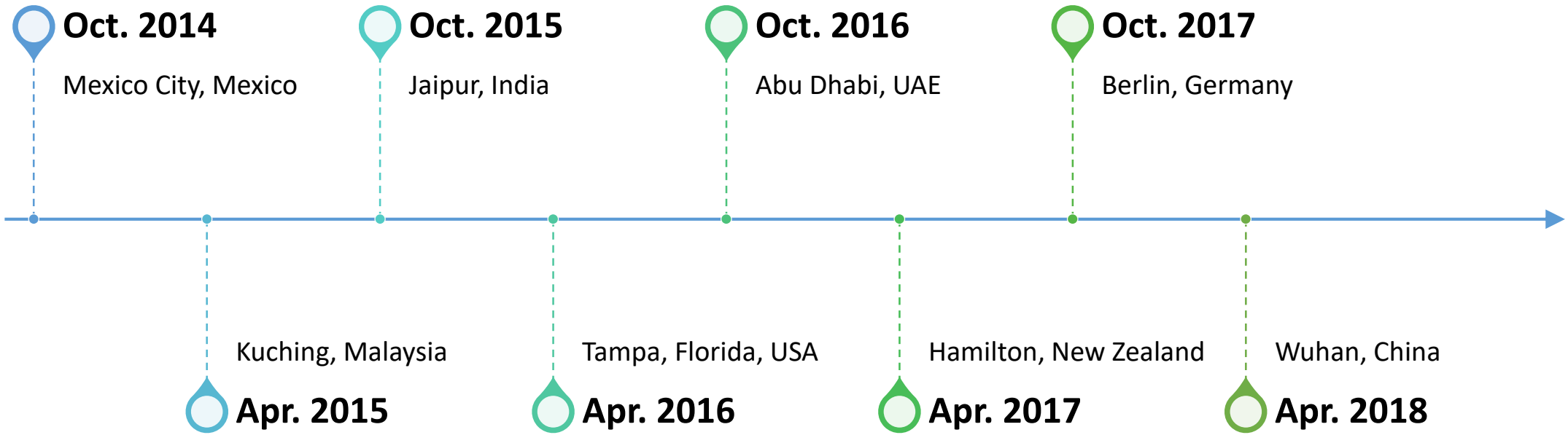
- (SC 31: Automatic identification and data capture techniques)
- (WG 4: Radio communications)

ISO/IEC Process

- Registration through national bodies
- Two-layered consensus: expert + national bodies
- Consensus = no sustained opposition (not the same as unanimity)
- Decisions made at physical meetings

1. Study period
2. Working draft
3. Committee draft
4. Draft International Standard
5. FDIS
6. Publication

Timeline


Oct. 2014
Mexico City, Mexico
Oct. 2015
Jaipur, India
Oct. 2016
Abu Dhabi, UAE
Oct. 2017
Berlin, Germany
Kuching, Malaysia
Apr. 2015
Tampa, Florida, USA
Apr. 2016
Hamilton, New Zealand
Apr. 2017
Wuhan, China
Apr. 2018

- Modes of operation for an n-bit block cipher algorithm (10116)
- Entity authentication (9798)
- Message authentication codes (MACs) (9797)
- Non-repudiation (13888)
- Digital signatures with appendix (14888)
- Hash-functions (10118)
- Key management (11770)
- Cryptographic techniques based on elliptic curves (15946)
- Time-stamping services (18014)
- Prime number generation (18032)
- Encryption algorithms (18033)
- **Lightweight cryptography (29192)**
- Anonymous entity authentication (20009)
- Anonymous digital signatures (20008)
- Secret sharing (19592)
- Study periods

Observations

- Consensus ill-defined – unclear when a vote needed to be taken by experts, national bodies, when a vote needed to be taken, how that vote should be taken
  - Positive outcome: all clarified during Simon and Speck process
- Significant amount of time and resources
  - Limits participation
  - Most participate for short periods of time
  - Lack of expertise
  - Usual suspects: France, Germany, US, UK, Japan, Korea, Russia, China, Belgium, Luxembourg
- Burden of proof on those dissenting
  - Not ideal for security standards

Resulting Difficulties

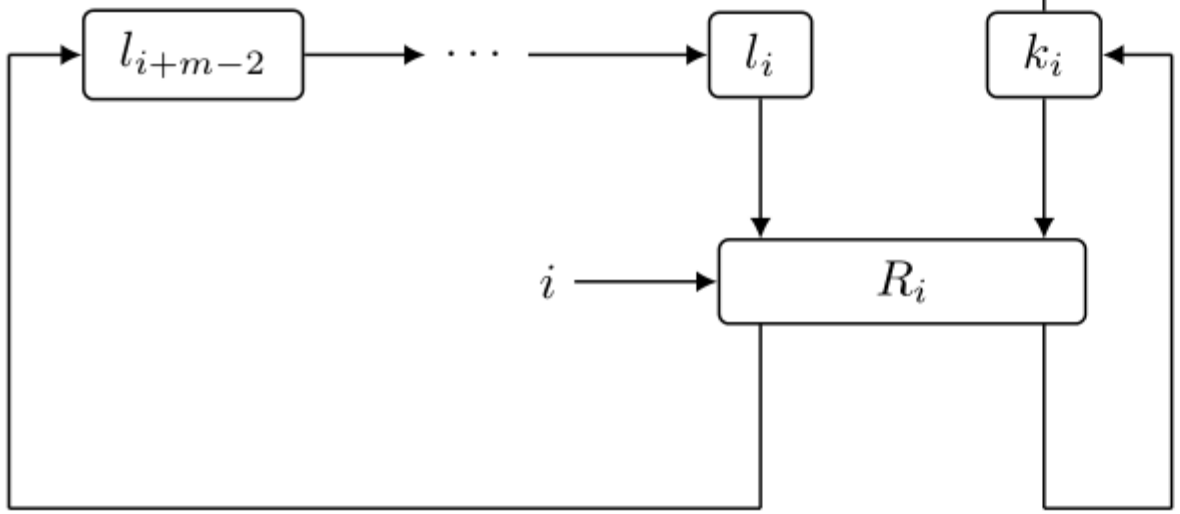
- 3.5 years from start to finish, despite significant opposition at every meeting
- Procedural mistakes, in favor of Simon and Speck standardization
- Each country needs to be approached individually, asking whether they were ok with the standardization of Simon and Speck, otherwise automatic approval

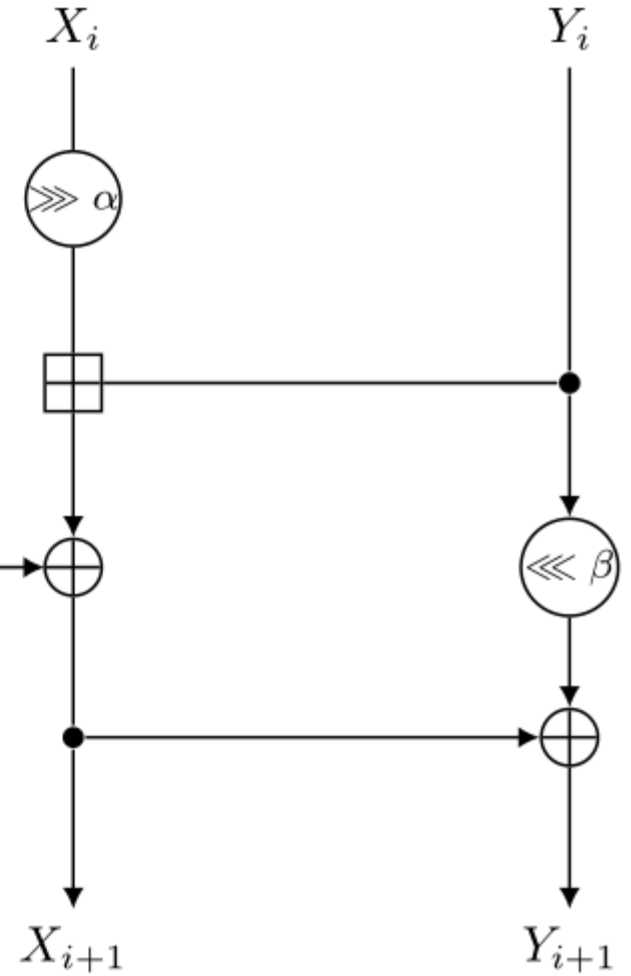
Technical Discussion

- Cryptanalytic Results
- Generic Attacks

Cryptanalysis

- Lack of security rationale (“can’t release internal analysis”)
- Many publications but…
  - Any attack is a new result
  - ARX ciphers generally less well understood in academia
  - Hardly any analysis on key schedule
- Aggressive decision: “30% security margin”





Generic Attacks

- Block ciphers always used in modes of operation: birthday bound attacks (Sweet32)
- Tiny block and key sizes
  - April 2016: defend 48 bit block sizes (CTR mode fixes birthday bound problems??)
  - October 2016: 48 bit removed, 64 bit remains
  - April 2017: all candidates below 128 bit block size removed

Block Size	Key Size
~~32~~	~~64~~
~~48~~	~~72~~ ~~96~~
~~64~~	~~96~~ ~~128~~
~~96~~	~~96~~ ~~144~~
128	128 192 256

Backdoors?

- “Where are we going to install a backdoor, in the AND or the XOR?”
- Is it possible to backdoor block ciphers?
  - Implies PKE
  - Whitebox crypto

Alternatives?

- AES is good for the vast majority of use cases
- Lightweight ciphers PRESENT, CLEFIA already standardized
- Chaskey, LEA, RC5
- Key schedules poorly understood: use permutation-based crypto
- Tweakable block ciphers much preferred to avoid birthday bound attacks
- NIST lightweight cryptography competition

Summary

- “Working Group 2 (WG 2) feels that both algorithms included in the amendment are not properly motivated and their security properties are not sufficiently understood.”
- Not a statement about the security or the quality of the algorithms nor about the work done by the designers nor the editors.
- Given the available information and the opposing opinions about the security of the algorithms they do not enjoy the level of confidence required for inclusion in ISO/IEC JTC 1/SC 27 standards.

Conclusions

Erosion of Trust

Lack of Necessity

It takes time to build these