A Statement on Standardization

Orr Dunkelman[1], Atul Luykx[2], Léo Perrin[3]

[1]orrd@cs.haifa.ac.il
[2]Atul.Luykx@esat.kuleuven.be
[2]leo.perrin@uni.lu

March 7, 2017
Fast Software Encryption 2017

ISO/IEC

ISO, IEC

- ISO “promotes worldwide proprietary, industrial and commercial standards”.
- IEC “prepares and publishes International Standards for all electrical, electronic and related technologies”.

Together, they make ISO/IEC standards.

ISO/IEC

ISO, IEC

- ISO “promotes worldwide proprietary, industrial and commercial standards”.
- IEC “prepares and publishes International Standards for all electrical, electronic and related technologies”.

Together, they make ISO/IEC standards.

Example: ISO/IEC 29167 Part 11

Information technology – Automatic identification and data capture techniques –
Part 11: Crypto suite PRESENT-80 security services for air interface communications.

Algorithms Chosen

Previously

NIST and ISO/IEC standardized DUAL_EC PRNG[1]

[1] See summary in http://eprint.iacr.org/2015/767.pdf

Algorithms Chosen

Previously

NIST and ISO/IEC standardized DUAL_EC PRNG[1]

Currently

ISO/IEC is considering adding:

[1] See summary in http://eprint.iacr.org/2015/767.pdf

Algorithms Chosen

Previously

NIST and ISO/IEC standardized DUAL_EC PRNG[1]

Currently

ISO/IEC is considering adding:

- SIMON (NSA) [ISO/IEC 29192-2 (lightweight crypto)]
- SPECK (NSA) [ISO/IEC 29192-2 (lightweight crypto)]

[1] See summary in http://eprint.iacr.org/2015/767.pdf

Algorithms Chosen

Previously

NIST and ISO/IEC standardized DUAL_EC PRNG[1]

Currently

ISO/IEC is considering adding:

- SIMON (NSA) [ISO/IEC 29192-2 (lightweight crypto)]
- SPECK (NSA) [ISO/IEC 29192-2 (lightweight crypto)]
- Kuznyechik (FSB) [ISO/IEC 18033-3 (Encryption algorithms)]

[1] See summary in http://eprint.iacr.org/2015/767.pdf

Statement

We propose a statement along the lines of:

> *We believe that the continued involvement of intelligence agencies with a history of subversion in standardization organizations is detrimental to the integrity of cryptographic standards, and works counter to our mission of providing security tools benefiting society at large.*

Statement

We propose a statement along the lines of:

> *We believe that the continued involvement of intelligence agencies with a history of subversion in standardization organizations is detrimental to the integrity of cryptographic standards, and works counter to our mission of providing security tools benefiting society at large.*

Let us know what you think!