ADVENTURES IN CRYPTOGRAPHIC STANDARDIZATION

Orr Dunkelman (CS Dept, Univ. of Haifa)

In cooperation with so many people: Leo Perrin, Tomer Ashur, Eran Lambooij, Erez Waisbard …

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

ISO 3591

- Defines the glass that should be used in the process of wine tastings

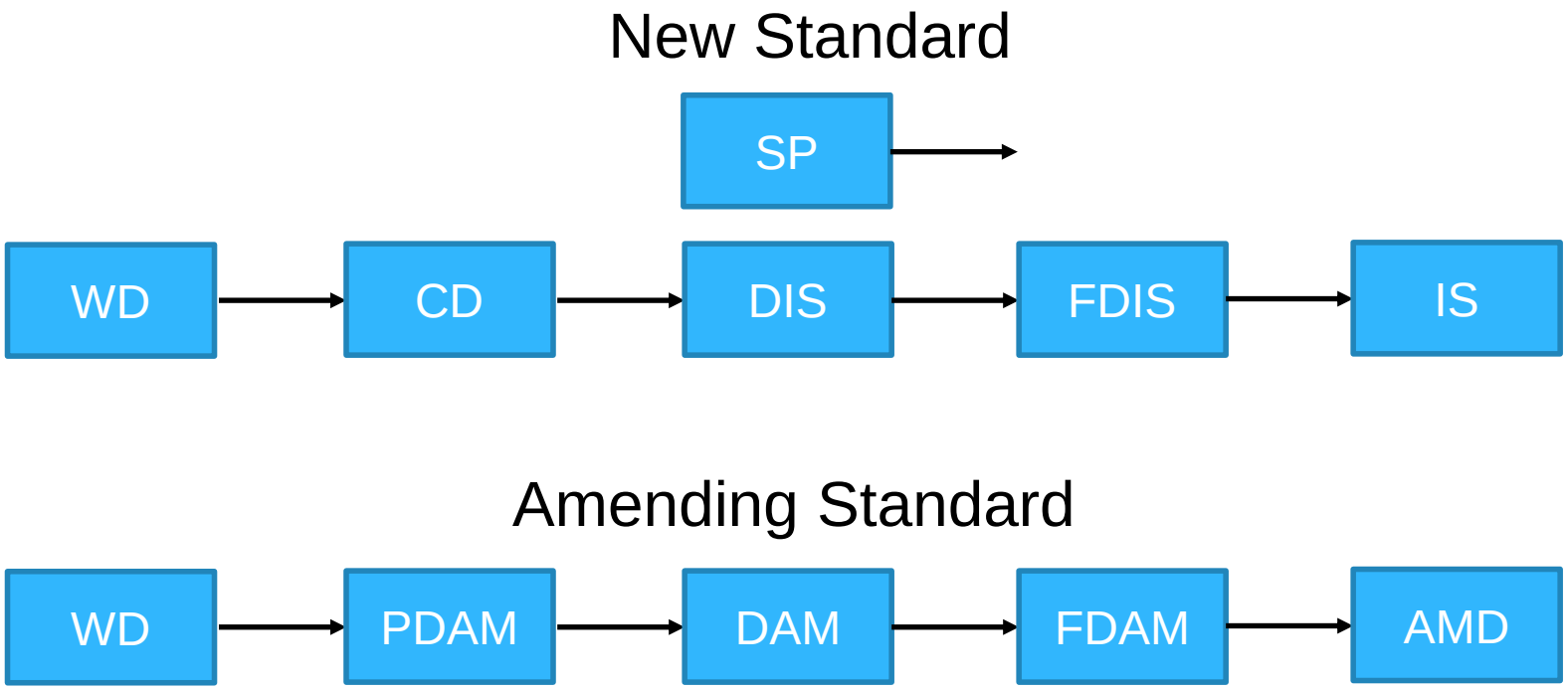
ISO 216

- Defines the sizes of papers, the A, B, and C series

International Standardization Organization

- Covers different types of standards
- Divided into different committees
  - we discuss ISO/IEC JTC 1 (ICT technologies)
- Committees are further divided into subcommittees:
  - SC27 – IT Security Techniques
  - SC31 – Automatic identification and data capture techniques
  - SC37 – Biometrics
- Subcommittees are further divided into working groups:
  - SC27/WG2 – Cryptography and security mechanisms
  - SC27/WG3 – Security evaluation, testing and specification

The ISO Process (Simplified)

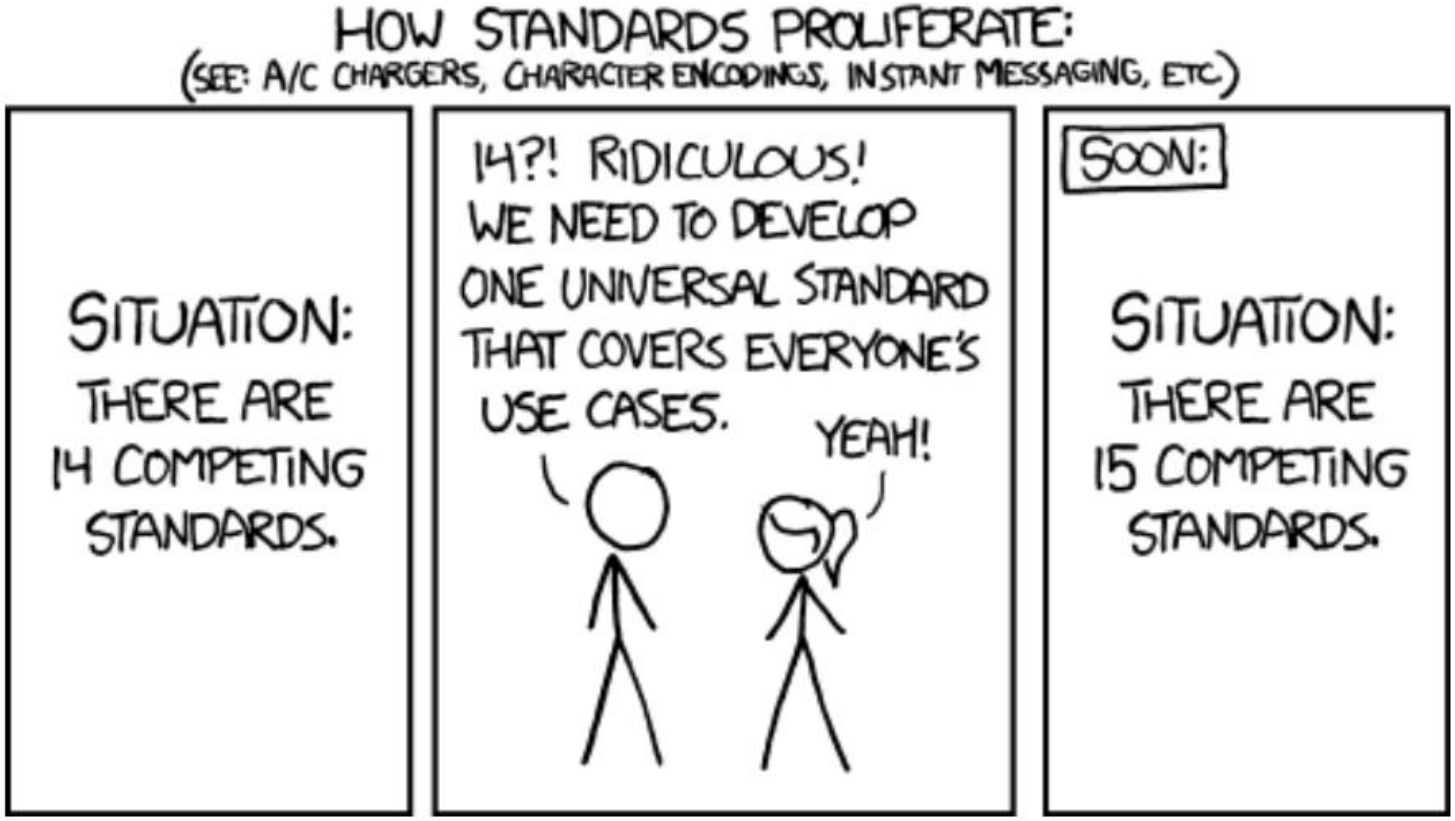


Pre-Working Draft

- Preliminary:
  - Announcement
  - Study Period (Discussion)
  - Decision – Continue to Proposal/Go back to SP/Cancel
- Proposal:
  - Registration
  - Vote
  - Study Period + Improvements
  - Decision – Continue to WD/Go back to SP/Cancel

- See codes at https://www.iso.org/stage-codes.html

Cryptographic Standardization



"The good thing about standards is that there are so many to choose from" — Andrew S. Tanenbaum

Cryptographic Standards of ISO

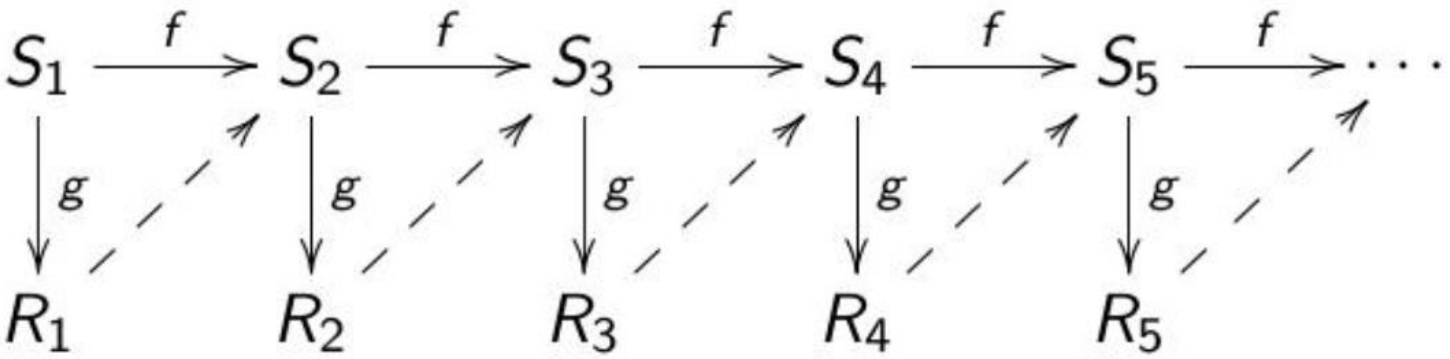
- Offer multiple options for the same task
- ISO 9797-1 (Block Cipher-based MACs):
  - Defines 6(!) different approaches for using an n-bit block cipher to produce m-bit tag
  - 3 different paddings, 2 different initial transformations, 3 different output transformation
  - + Truncation! (rightmost bits)
  - Alg. 1: CBC-MAC
  - Alg. 5: CMAC
  - For more details – purchase ISO 9797-1:2011 for **just 158 CHF**

Cryptographic Standards of ISO

- ISO 9796: Signatures with message recovery
- ISO 9797: MACs
- ISO 9798: Security Authentication
- ISO 18033-2: Asymmetric encryption
- ISO 18033-3: Block ciphers: 3DES, Misty1, CAST128, HIGHT, AES, Camellia, SEED
- ISO 18033-4: Stream ciphers
- ISO 10118: Hash Functions: SHA224, RIPEMD128, RIPEMD160, SHA1, SHA256, SHA384, SHA512, Whirlpool
- ...

The ISO 18031 Fiasco

- A.K.A. Dual EC DBRG
- Early 2000's introduced by the NSA for the people!
- 2005: ISO 18031 adoption
- June '06: ANSI SP 800-90A
- Crypto '07: Dan Shumow & Niels Fergueson – "It's a point? It's another point? It's a backdoor!"
- 2013: Snowden revelations



How ISO Works

- Votes are done by country (NB)
- During the meeting (every 6 months), the WG can have as many experts representing a NB
- Votes then are “advisory”
- After the meeting of WG (and during the meeting), a HoD vote takes place
- After that HoD vote, a plenary of the SC takes place

- In parallel, votes are held throughout the year, where each NB has one vote

How ISO Does Not Work

- QKD (Quantum Key Distribution) is an *emerging technology*
- Chinese companies want to sell ISO-complaint QKD equipment
- CN tries to standardize QKD at SC27/WG2
- CN fails (contact me later for details)
- CN tries to standardize “methods for security evaluation of QKD” in SC27/WG3

Kuznyechik

- Designed by TC 26 as an effort to generate a new ~~Soviet~~ Russian standard for encryption
- A 128-bit block, 256-bit key
- Uses SPN structure:
  - 16 parallel 8-bit S-boxes,
  - A linear transformation, (LFSR over 16 words)
  - Key addition (XOR)

On the Importance of Good S-boxes

- At the beginning there was a linear scheme, and the cryptanalysts rejoiced.
- And Shannon said, let there be confusion, and there was a great confusion, as everybody got really confused what did he mean.
- And the agreement many years later was that S-boxes should be highly non-linear.
- And there was much rejoicing in the camp.

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

S-boxes

- The choice of S-boxes has a great impact on the security of the scheme
- Good S-boxes are usually adopted from “good families”, sets of S-boxes that we have studied very well, or picked at random
- Now, if the S-box is not good enough, the scheme may be weak
- Or if the S-box is backdoored…

Backdooring Crypto 101

- Subliminal Channels [Simmons83]
- Kleptography [YoungYung97]
- DES-like backdoored scheme [Paterson99]
- RSA keys [CrepeauSlakmon03]
- Malicious constants in Hashing [Albertini++14]
- AES-like subspace scheme [BannierBodinFiloil16]
- And … The Underhanded Crypto Contest - https://underhandedcrypto.com/

The Kuznyechic S-box

- See Streebog S-box
- Seriously.
- This S-box was generated as part of Streebog, Russian hash function (replaces GOST-hash)
- Standardized in RFC 6986 and in ISO 10118-3:2018

The Streebog S-box

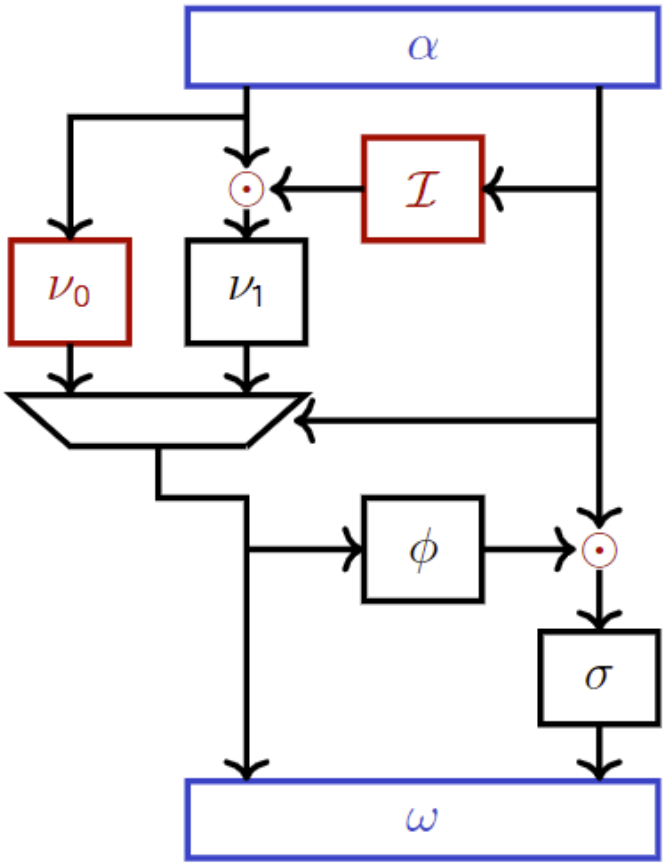
- During the standardization process of Streebog at ISO, the full design rationale was not requested
- However, during the Berlin meeting (November 2017), when the discussion of the S-box generation surfaced, RU delegation mentioned that the S-box was chosen at random
- More precisely, different S-boxes where chosen at random until a good one was found (good differential/linear/algebraic properties)

In the Ivory Tower

- Eurocrypt 2016: Biryukov, Perrin, Udovenko: Reverse-engineering the S-box of Streebog, Kuznyechik and STRIBOBr1
- FSE 2017: Perrin, Udovenko. Exponential S-Boxes: a Link Between the S-Boxes of BelT and Kuznyechik/Streebog
- FSE 2019: New decomposition of the S-box

- Three decompositions to rule them all!

Previous decompositions: the TU-decomposition



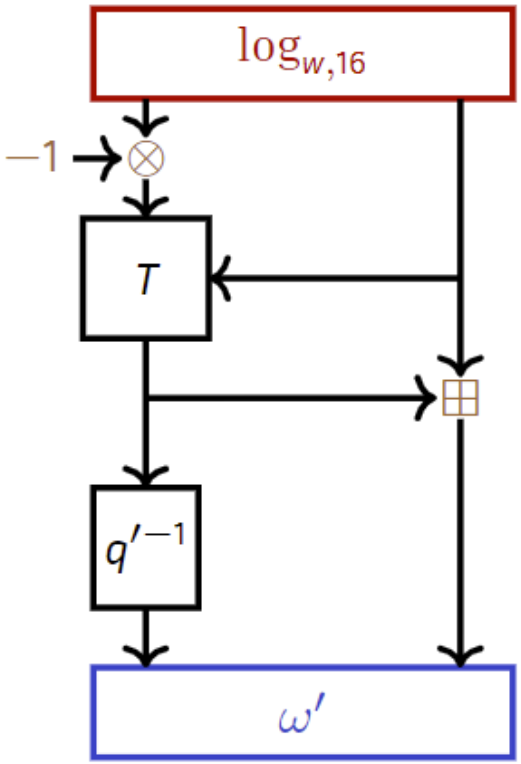
- $\odot$ Multiplication in $\mathbb{F}_{2^4}$
- $\mathcal{I}$ Inversion in $\mathbb{F}_{2^4}$
- ν_0 $\approx$ Discrete logarithm in $\mathbb{F}_{2^4}$
- ν_1, σ 4×4 permutations
- ϕ 4×4 function
- α, ω Linear permutations

Published in 2016[1].

Taken (with permission & blessings) from Leo Perrin

[1] A. Biryukov, L. Perrin, A. Udovenko. *Reverse-engineering the S-box of streebog, kuznyechik and STRIBOBr1*. EUROCRYPT'16.

Previous decompositions: log-based

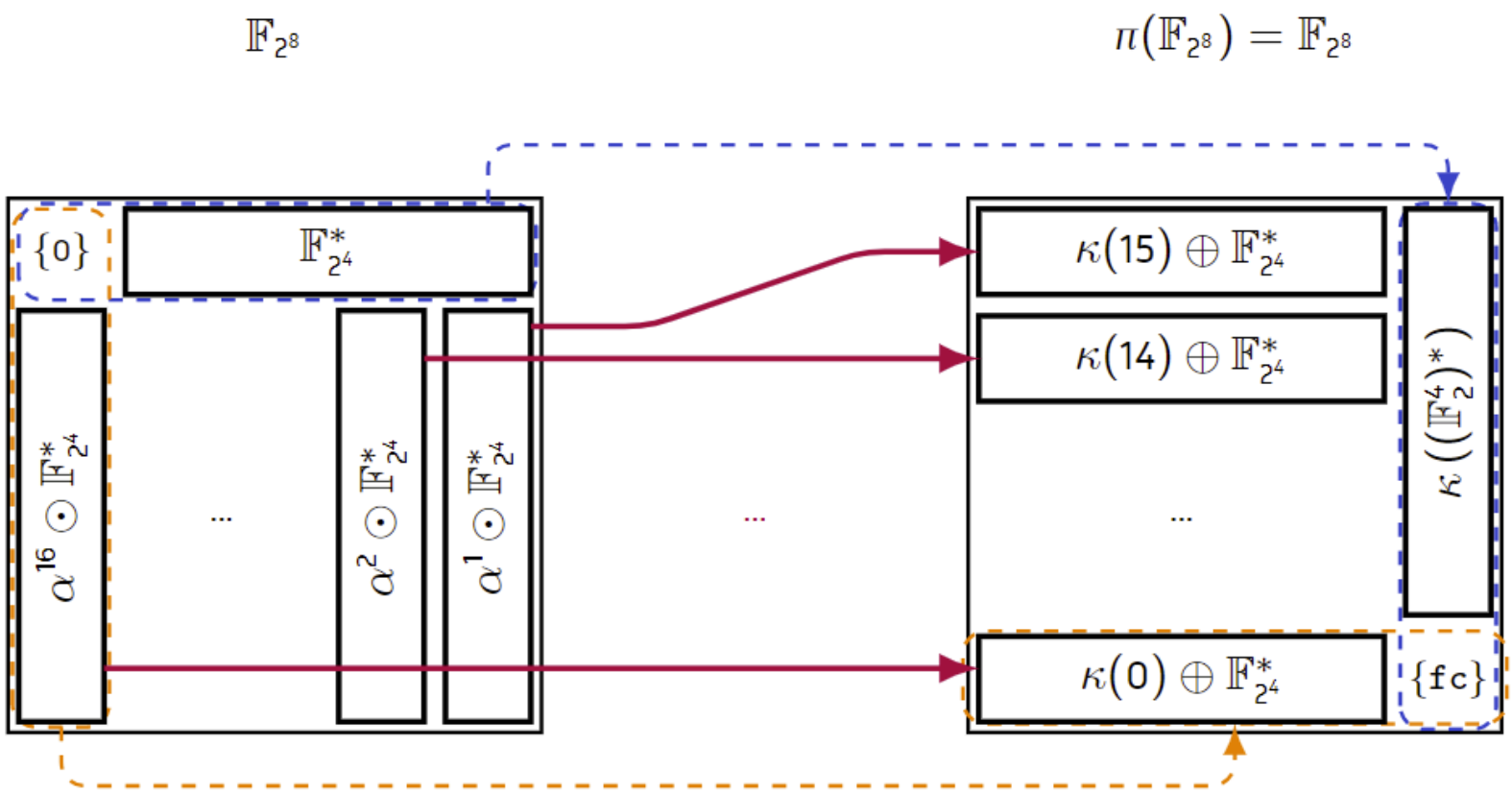


- Published in 2017[2]
- Completely different decomposition!
- Uses a $\approx$ discrete log. in $\mathbb{F}_{2^8}$.

Taken (with permission & blessings) from Leo Perrin

[2] L. Perrin, A. Udovenko. *Exponential S-Boxes: a Link Between the S-Boxes of BelT and Kuznyechik/Streebog*. ToSC vol. 16.

Cosets to cosets



π maps the partition of $\mathbb{F}_{2^8}$ into multiplicative cosets of $\mathbb{F}_{2^4}^*$
to its partition into additive cosets of $\mathbb{F}_{2^4}^*$!

Taken (with permission & blessings) from Leo Perrin

Meaning

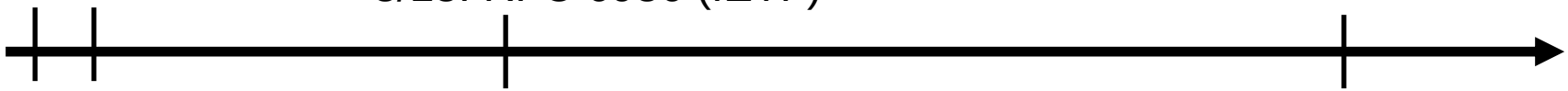
- Well, the three structures suggest that the S-box was not generated at random
- Or, that the S-box was generated at random, and by chance, has this structure

Timeline

7/12: Streebog standardized in RU

6/15: Kuznyechic standardized in RU

8/13: RFC 6986 (IETF)



3/16: RFC 7801 (IETF)

2/17: 2nd decomposition

5/16 1st decomposition

10/18: ISO standardizes Streebog (10118-3)

12/18 Last decomposition published

4/19 – ISO meeting @ Tel Aviv – What to do with Kuznyechic?

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

The ISO Discussion

Complicated situation:

- No attack on the scheme
- No attack based on the decompositions
- RU delegation insists that S-boxes were chosen at random

To make life even harder

- The “ISO project” is composed of two amendments to 18033-3
  - Kuznyechic (RU)
  - SM4 (CN) [The algorithm that was used to be called SMS4, the base of WAPI, the Chinese WPA]
  - Chinese very upfront about their design – more public scrutiny, no weird things, supplied all design documents even without being asked for

Discussion on April 2019 (Tel Aviv)

Illustration of Toshio-San

- First option – move forward in standardization of both schemes
- Second option – drop the entire project
- Third option – separate the project into two new ones
- Fourth option – postpone decision to next meeting

- Discussion is led by Toshio Tatsuta, the vice convenor of WG2

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

Discussion until October 2019

- RU key arguments:
  - We choose S-boxes at random, but lost the code
  - S-boxes always have structure, also the AES one
  - When putting requirements on the security of the S-box, the structure will appear
  - Until there is an attack, you should allow us in the standard
  - The C language generates these structures
  - This is an anti-Russia bias!

RU Main Argument

- Number of 8-bit bijective S-boxes with some structure (partial list):

	Special polynomials	2^{22}
	Generation using paths (?)	
†	TU_4-decomposition (w/ mult)	
→	**TU_4-decomposition (called "F-co**	
†	Feistel 1r	
	Feistel 1r (wei	
†	Mist	2^{88}
		2^{781}
		2^{104}
		2^{88}
	ypton v1)	2^{152}
	SPN 2r (CLEFIA-style)	2^{177}
†	Lai-Massey (FLY-style)	2^{152}
†	Lai-Massey (Whirlpool-style)	2^{88}
†	Perrin (neither mine nor a permutation)	2^{304}
	LFSRs	2^{12}
	Total (with affine-equivalence)	$\approx 2^{1488}$

But there are 2^{1684} such S-boxes
Probability of Structure – 2^{-196}

Decision in October 2019 (Paris)

- The project was cancelled

- The RU delegation could have tried to resurrect the project in the April 2020 meeting
- which conveniently was supposed to take place in St. Petersburg
- Which took place online

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

Thank you for your attention!

מתי
THE STANDARDS INSTITUTION OF ISRAEL

Special thanks to TC26:

אוניברסיטת חיפה
University of Haifa
جامعة حيفا