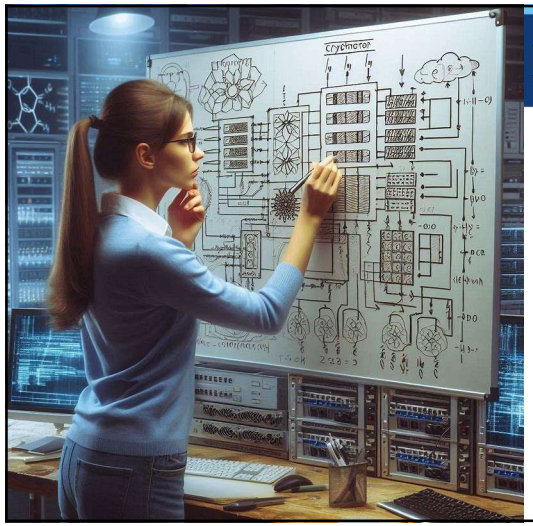


KU LEUVEN

COSIC

Block cipher design pre- and post-AES

Bart Preneel
COSIC-KU Leuven
firstname.lastname(AT)esat.kuleuven.be
@bpreneel1 preneel@infosec.exchange
Gausta, April 2026

1

Claude Shannon
(1916-2001)

Communication Theory of Secrecy Systems*

By C. E. SHANNON

Bell System Technical Journal, vol. 28-4, pp. 656-715, Oct. 1949.

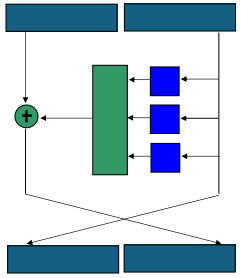
Various methods of mixing applicable to statistical sequences of the type found in natural languages can be devised. One which looks fairly good is to follow a preliminary transposition by a sequence of alternating substitutions and simple linear operations, adding adjacent letters mod 26 for example. Thus we might take

$$F = LSLSLT$$

where T is a transposition, L is a linear operation, and S is a substitution.

2

Horst Feistel
(1915-1990)

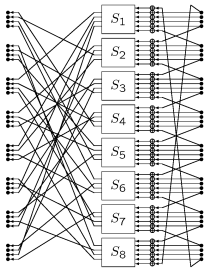


- Lucifer (1971) block and key lengths:
  - 48/48, 32/64, 128/128
- patent: 1971

3

Don Coppersmith
(1950-)

Walter Tuchman

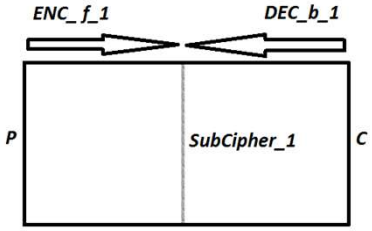


- DES (1976) block and key lengths:
  - 64/56
- S-box controversy

4

Martin Hellman (1945-)

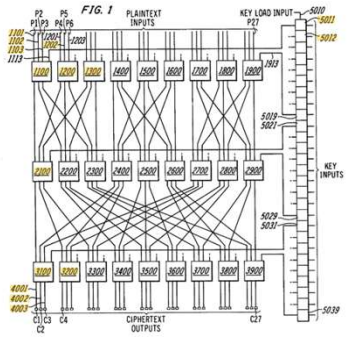
Whitfield Diffie (1944-)



- Meet-in-the-middle attack on double DES (1977)

5

George Davida (1944-2025)

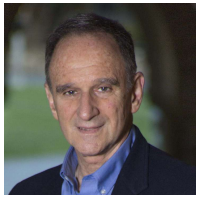


George I. Davida, John B. Kam

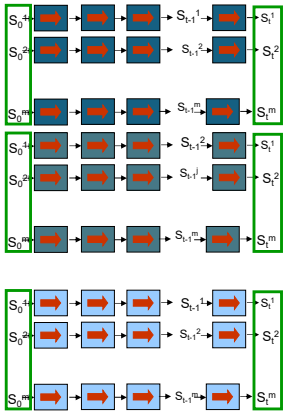
- Complete substitution permutation enciphering and deciphering circuit, 1978
- Structured Design of Substitution-Permutation Encryption Networks. IEEE Trans. Computers 28(10): 747-753 (1979)

6

- Time-Memory Trade-off for key search
- 1980

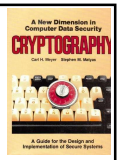


Martin Hellman (1945-)



7

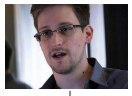
Work on DES in the 1980s



- Carl H. Meyer, Stephen M. Matyas, Cryptography: A New Dimension in Computer Data Security--A Guide for the Design and Implementation of Secure Systems, 1st Edition, 1982.
- Ingrid Schaumüller-Bichl: Cryptonalysis of the Data Encryption Standard by the Method of Formal Coding. EUROCRYPT 1982: 235-255
- Adi Shamir: On the Security of DES. CRYPTO 1985: 280-281
- David Chaum, Jan-Hendrik Evertse: Crytanalysis of DES with a Reduced Number of Rounds: Sequences of Linear Factors in Block Ciphers. CRYPTO 1985: 192-211
- Donald W. Davies, Sean Murphy: Pairs and Triplets of DES S-Boxes. J. Cryptol. 8(1): 1-25 (1995)

8

Cryptography Timeline



kings, generals & diplomats | wireless & commerce | finance | finance comms | Internet, GSM EMV | crypto-currencies | messaging | PQC

pre-1920 | 1920-1960 | 1960-1975 | 1975-1990 | 1990-2013 | 2013-2025 | 2026

mechanical | electro-mechanical | electronics | large-scale adoption | mass adoption end-2-end | ubiqui-tous

software

9

What else happened in the 1980s?

- Donald W. Davies: A Message Authenticator Algorithm Suitable for A Mainframe Computer. CRYPTO 1984: 393-400
- Ron Rivest: RC4, 1987 (trade secret)
- Ron Rivest: RC2, 1989.
- Xuejia Lai, James L. Massey: A Proposal for a New Block Encryption Standard. EUROCRYPT 1990: 389-404
- Ralph C. Merkle: Fast Software Encryption Functions. CRYPTO 1990: 476-501 (Khufu and Khafre)
- Ralph C. Merkle: A Fast Software One-Way Hash Function. J. Cryptol. 3(1): 43-58 (1990) (Snefru)
- Shoji Miyaguchi: The FEAL Cipher Family. CRYPTO 1990: 627-638

Under a voluntary scheme, Xerox submitted Khufu and Khafre to the US National Security Agency (NSA) prior to publication. NSA requested that Xerox not publish the algorithms, citing concerns about national security. Xerox, a large contractor to the US government, complied. However, a reviewer of the paper passed a copy to John Gilmore, who made it available via the sci.crypt newsgroup.

10

FEAL was a source of inspiration

- Henri Gilbert, Guy Chassé: A Statistical Attack of the FEAL-8 Cryptosystem. CRYPTO 1990: 22-33
- Sean Murphy: The Cryptanalysis of FEAL-4 with 20 Chosen Plaintexts. J. Cryptol. 2(3): 145-154 (1990)
- Eli Biham, Adi Shamir: Differential Cryptanalysis of Feal and N-Hash. EUROCRYPT 1991: 1-16
- Anne Tardy-Corfdir, Henri Gilbert: A Known Plaintext Attack of FEAL-4 and FEAL-6. CRYPTO 1991: 172-181
- Mitsuru Matsui, Atsuhiro Yamagishi: A New Method for Known Plaintext Attack of FEAL Cipher. EUROCRYPT 1992: 81-91

11

Resulting in theoretical breaks of DES

- Eli Biham, Adi Shamir: Differential Cryptanalysis of DES-like Cryptosystems. CRYPTO 1990: 2-21
- Mitsuru Matsui: Linear Cryptanalysis Method for DES Cipher. EUROCRYPT 1993: 386-397
- Eli Biham, Adi Shamir: Differential Cryptanalysis of the Full 16-Round DES. CRYPTO 1992: 487-496

12

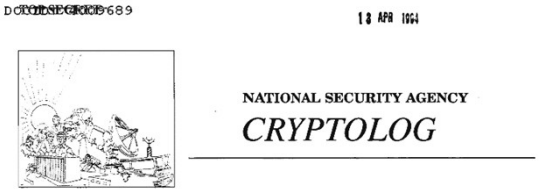
The real break of DES

- Michael J. Wiener, Efficient DES Key Search, Carleton University, Technical Report TR-244 ('94) (1 M$, 3.5h)
- EFF Deep Crack FPGA ('98) (250K $, 50h)
- COPACABANA FPGA ('07) (10 K$, 6.4 days)

13

1990: academics

- Field growing slowly but only 3 conferences:
  - Crypto, Eurocrypt, Auscrypt/Asiacrypt
- Increasing number of submissions yet no parallel sessions (competition)
- Shift towards theory



14

CryptoLog 1994 (Vol. 20 no. 1)
NSA internal newsletter
Report on Eurocrypt'92

https://nsarchive.gwu.edu/sites/default/files/documents/5301816/National-Security-Agency-Cryptolog-Vol-20-No-1.pdf

> Three of the last four sessions were of no value whatever, and indeed there was almost nothing at Eurocrypt to interest us (this is good news!). The scholarship was actually extremely good; it's just that the directions which external cryptologic researchers have taken are remarkably far from our own lines of interest.

> There were no proposals of cryptosystems, no novel cryptanalysis of old designs, even very little on hardware design. I really don't see how things could have been any better for our purposes.

15

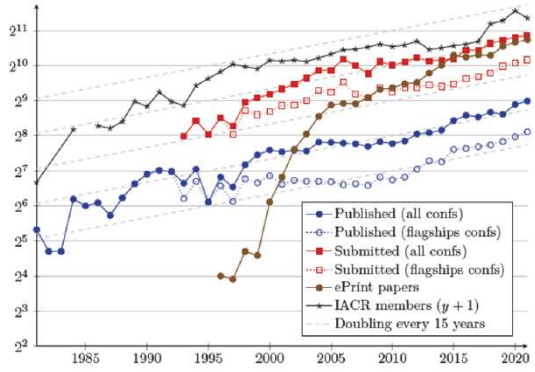
CryptoLog 1994 (Vol. 20 no. 1)
NSA internal newsletter
Report on Eurocrypt'92

https://nsarchive.gwu.edu/sites/default/files/documents/5301816/National-Security-Agency-Cryptolog-Vol-20-No-1.pdf

> Those of you who know my prejudice against the "zero-knowledge" wing of the philosophical camp will be surprised to hear that I enjoyed the three talks of the session better than any of that ilk that I had previously endured. The reason is simple: I took along some interesting reading material and ignored the speakers. That technique served to advantage again for three more snoozers, Thursday's "digital signature and electronic cash" session, but the final session, also on complexity theory, provided some sensible listening

16

IACR publications and members



Credit: Gaëtan Leurent

17

1990: academics

More competitive resulting in harsh reviews for applied cryptography:

- Donald Davies' first shortcut attack on DES rejected from Crypto'88
- ASIC design for RSA: "This is hardware which I don't understand. Reject."
- Stream cipher design: "This looks too simple. Reject."

IACR eprint only launched in 1999

Hardware community always had the option to shift to IEEE

18

Creation of FSE: "Fast Software Encryption"

- 1993 (Ross Anderson, Eli Biham, Cunsheng Ding, Dieter Gollman, James Massey, Bart Preneel)
- Focused on symmetric key design and cryptanalysis
- Propose concrete designs with working code and test values
- Sponsored by IACR since 2003

Ross Anderson
1956-2024

19

First Fast Software Encryption Workshop (Cambridge, December 1993)

- James L. Massey: SAFER K-64: A Byte-Oriented Block-Ciphering Algorithm. 1-17
- Joan Daemen, René Govaerts, Joos Vandewalle: A New Approach to Block Cipher Design. 18-32 (3-way, 96/96)
- Burton S. Kaliski Jr., Matthew J. B. Robshaw: Fast Block Cipher Proposal. 33-40
- Bruce Schneier: Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish). 191-204
- Adina di Porto, William Wolfowicz: VINO: A Block Cipher Including Variable Permutations. 205-210
- Lars R. Knudsen: Practically Secure Feistel Cyphers. 211-221

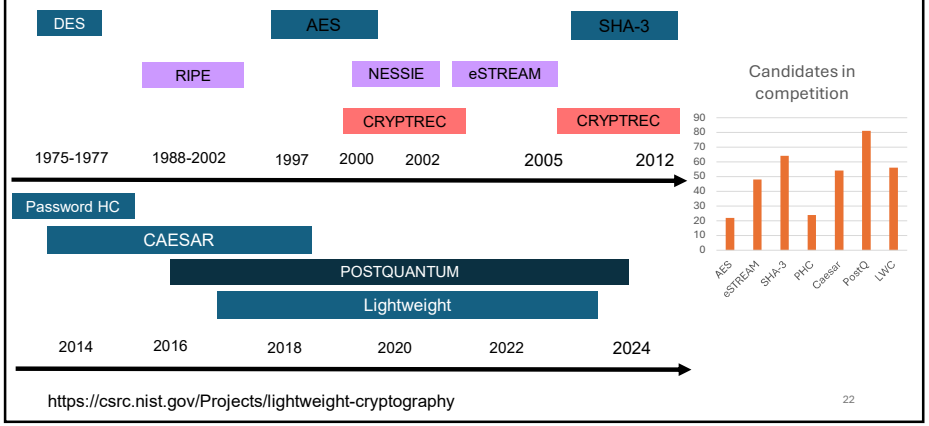
20

Second Fast Software Encryption Workshop (Leuven, December 1994)

- Ronald L. Rivest: The RC5 Encryption Algorithm. 86-96
- Matt Blaze, Bruce Schneier: The MacGuffin Block Cipher Algorithm. 97-110
- Lars R. Knudsen: Truncated and Higher Order Differentials. 196-211
- James L. Massey: SAFER K-64: One Year Later. 212-241
- Vincent Rijmen, Bart Preneel: Improved Characteristics for Differential Cryptanalysis of Hash Functions Based on Block Ciphers. 242-248
- Burton S. Kaliski Jr., Matthew J. B. Robshaw: Linear Cryptanalysis Using Multiple Approximations and FEAL. 249-264
- Uwe Blöcher, Markus Dichtl: Problems with the Linear Cryptanalysis of DES Using More Than One Active S-box per Round. 265-274
- Joan Daemen, René Govaerts, Joos Vandewalle: Correlation Matrices. 275-285
- Serge Vaudenay: On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER. 286-297
- Vincent Rijmen, Bart Preneel: Cryptanalysis of McGuffin. 353-358
- David J. Wheeler, Roger M. Needham: TEA, a Tiny Encryption Algorithm. 363-366

21

Open competitions in cryptography



https://csrc.nist.gov/Projects/lightweight-cryptography

22

22

AES competition

- MARS: multiplication, outer layers
- RC-6: ARX
- Rijndael
- Serpent: bit slicing and simple S-boxes
- Twofish: secret S-boxes

23

Immediately after the AES competition

- Nicolas T. Courtois, Josef Pieprzyk: Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. ASIACRYPT 2002: 267-287
- Daniel J. Bernstein, Cache timing attacks on AES, https://cr.yp.to/antiforgery/cachetiming-20050414.pdf
- Dag Arne Osvik, Adi Shamir, Eran Tromer: Cache Attacks and Countermeasures: The Case of AES. CT-RSA 2006: 1-20

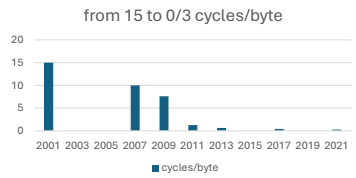
24

The lightweight rage

- Sanjay E. Sarma, Stephen A. Weis, Daniel W. Engels: RFID Systems and Security and Privacy Implications. CHES 2002: 454-469
- Daniel W. Engels, Ronald L. Rivest, Sanjay E., Sarma, Stephen A. Weiss, Security and privacy aspects of low-cost RFID systems, SPC 2003, https://saweis.net/pdfs/spc-rfid.pdf
- Adi Shamir: Stream Ciphers: Dead or Alive? ASIACRYPT 2004: 78

25

AES Implementations



Fast software
7.6 cycles/byte on Intel
0.3 cycle/byte on Intel with AES instruction

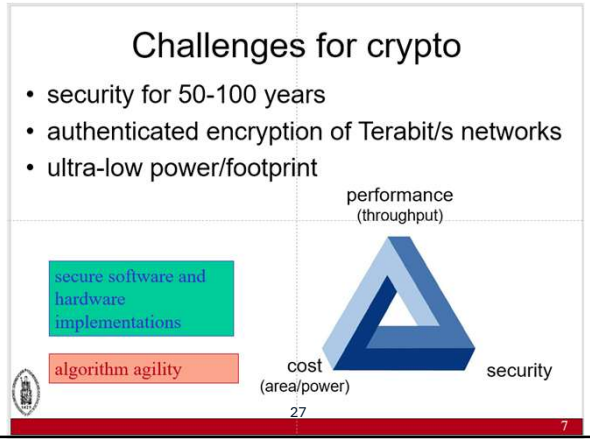
Tiny software
49 bytes of RAM on 8051

Fast hardware
(.15 mm²) (45 nm)
53 Gbit/s
125 mW
434 Gbps/W

Tiny hardware
(2400 GE) (180 nm)
56 Kbit/sec
3.7 μW
15 Gbps/W or 65 pJ/bit

26

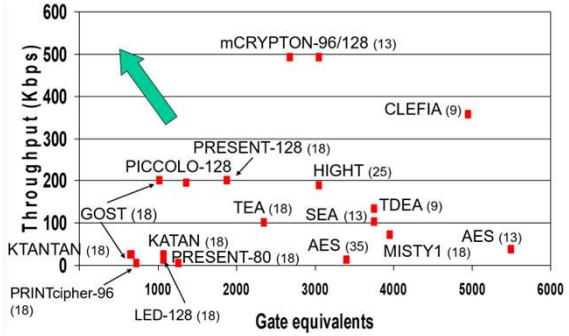
The 2004 perspective



27

Low cost hw: throughput versus area

[Bogdanov+08,Sugawara+08]
100 KHz clock, technology in multiples of 10 nm)

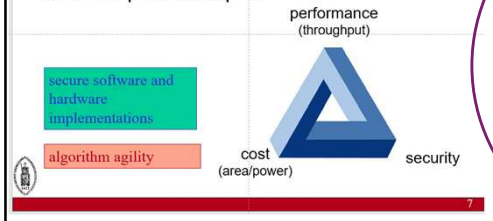


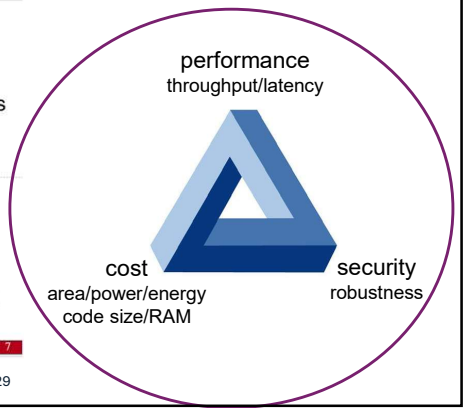
28

The 2004 perspective changes

Challenges for crypto

- security for 50-100 years
- authenticated encryption of Terabit/s networks
- ultra-low power/footprint

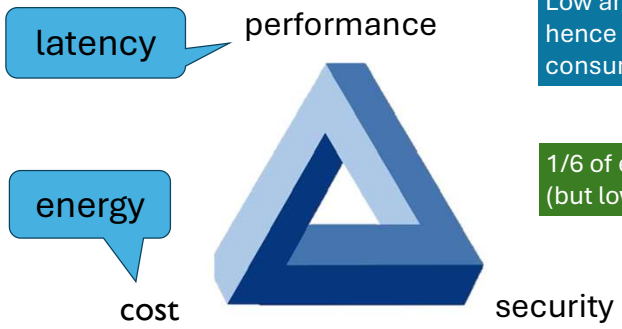




29

29

Lightweight Crypto: Can we improve over AES?

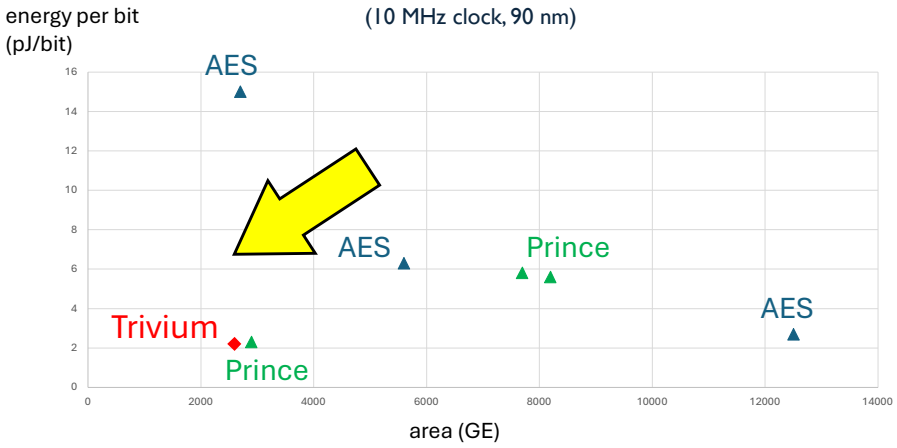


Low area is slow hence higher energy consumption

1/6 of energy/bit (but lower security)

30

Lightweight crypto: energy per bit versus area [Banik+15]



31

Lightweight: lessons learned

- Simplify designs
- Pushing the limits of designs helps to identify new weaknesses or attacks to avoid
- But mostly following the traditional DES, AES or ARX model

- Low latency still challenging

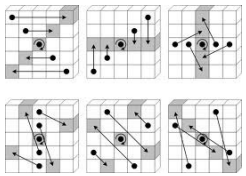
32

Permutation (this is not a block cipher)

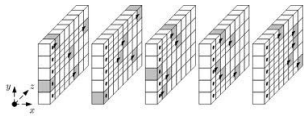
- Early designs inspired by cellular automata (Subterranean)
- Designs for hash functions and AEAD:
  - Keccack: 25, 50, 100, 200, 400, 800, 1600 bits
  - Ascon: 320 bits
- Block ciphers: 3-Way (92 bits), BaseKing (196 bits), Nokeon (128)

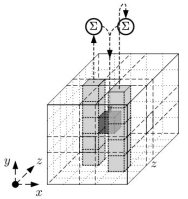
33

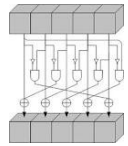
Keccak/SHA-3/FIPS 202



$$R = \iota \circ \chi \circ \pi \circ \rho \circ \theta, \text{with}$$







permutation: 25, 50, 100, 200, 400, 800, 1600

nominal version:

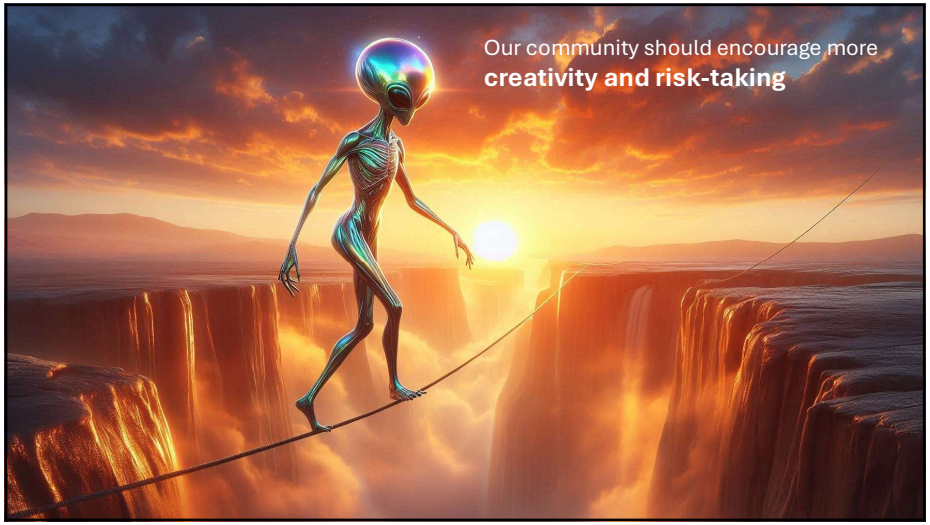
- 5x5 array of 64 bits
- 24 rounds of 5 steps

34

Designs

- SPN, Feistel and variants, Lai-Massey,…
- Tweakable block ciphers,…
- S-boxes: permutations of 4 to 8 bits, mappings of 8 to 64 bits, ….
- Linear layer: bit permutation, xor, MDS, non-aligned,…
- ARX: designed for CPU,…
- …

35



36

Bart Preneel

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven

WEBSITE: homes.esat.kuleuven.be/~preneel/

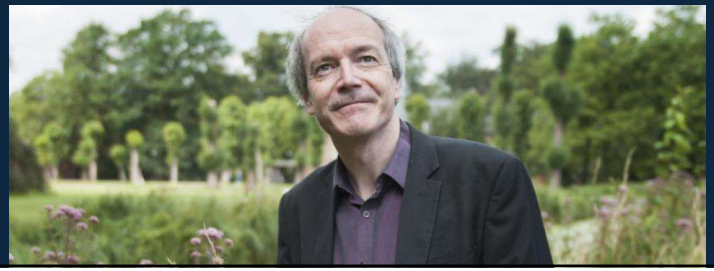
EMAIL: Bart.Preneel@esat.kuleuven.be

MASTODON: bpreneel@infosec.exchange

TWITTER: @bpreneel1

TELEPHONE: +32 16 321148

KU LEUVEN COSIC



37

37