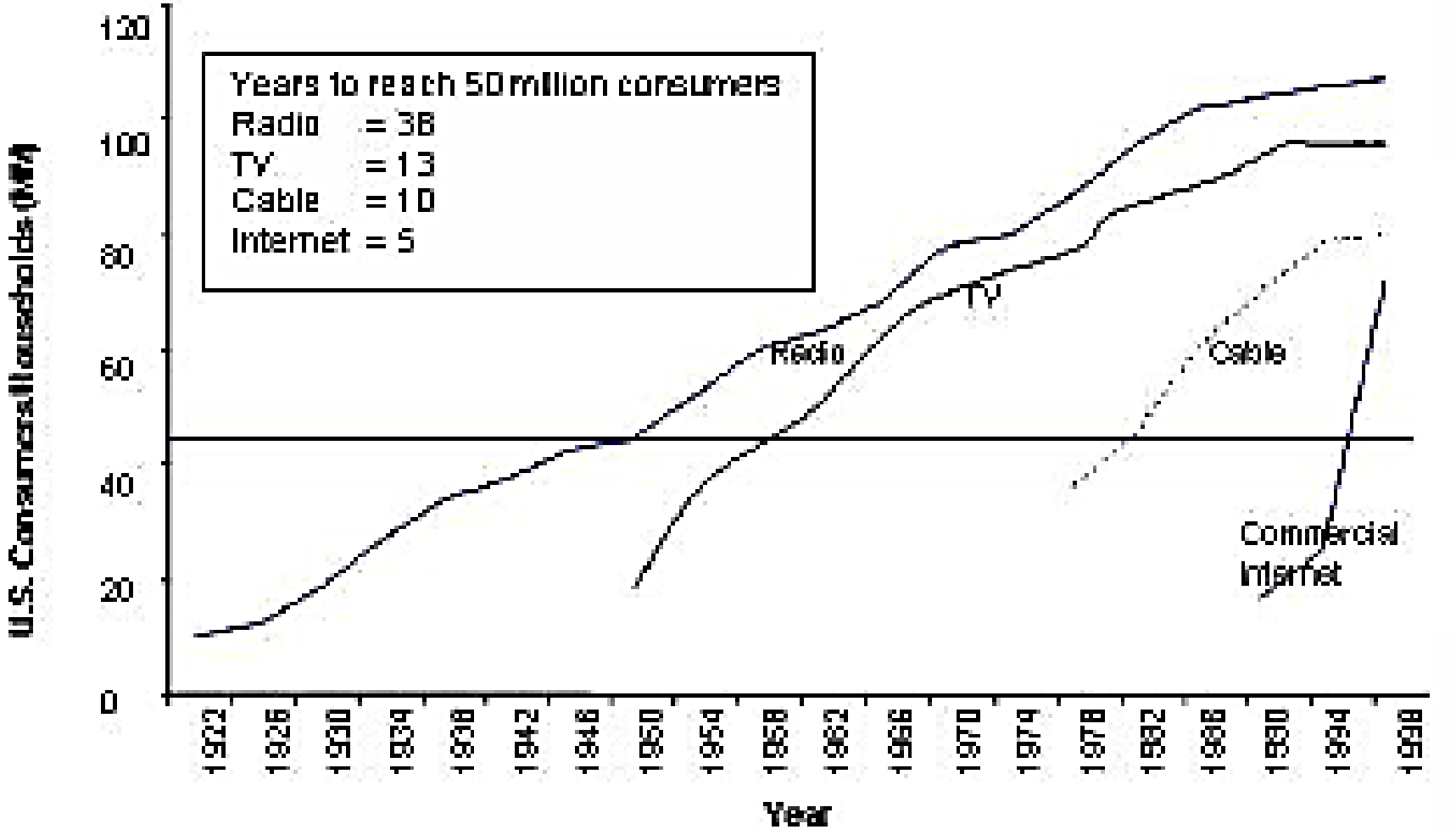
Основные достижения и тенденции развития теоретической криптологии

Ассоциация РусКрипто

РусКрипто 2012



Ассоциация РусКрипто

РусКрипто 2012

Internet of Things — An action plan for Europe

Communication from the Commission to the European Parliament, the Council, the European economic and Social Committee and the Committee of the Regions

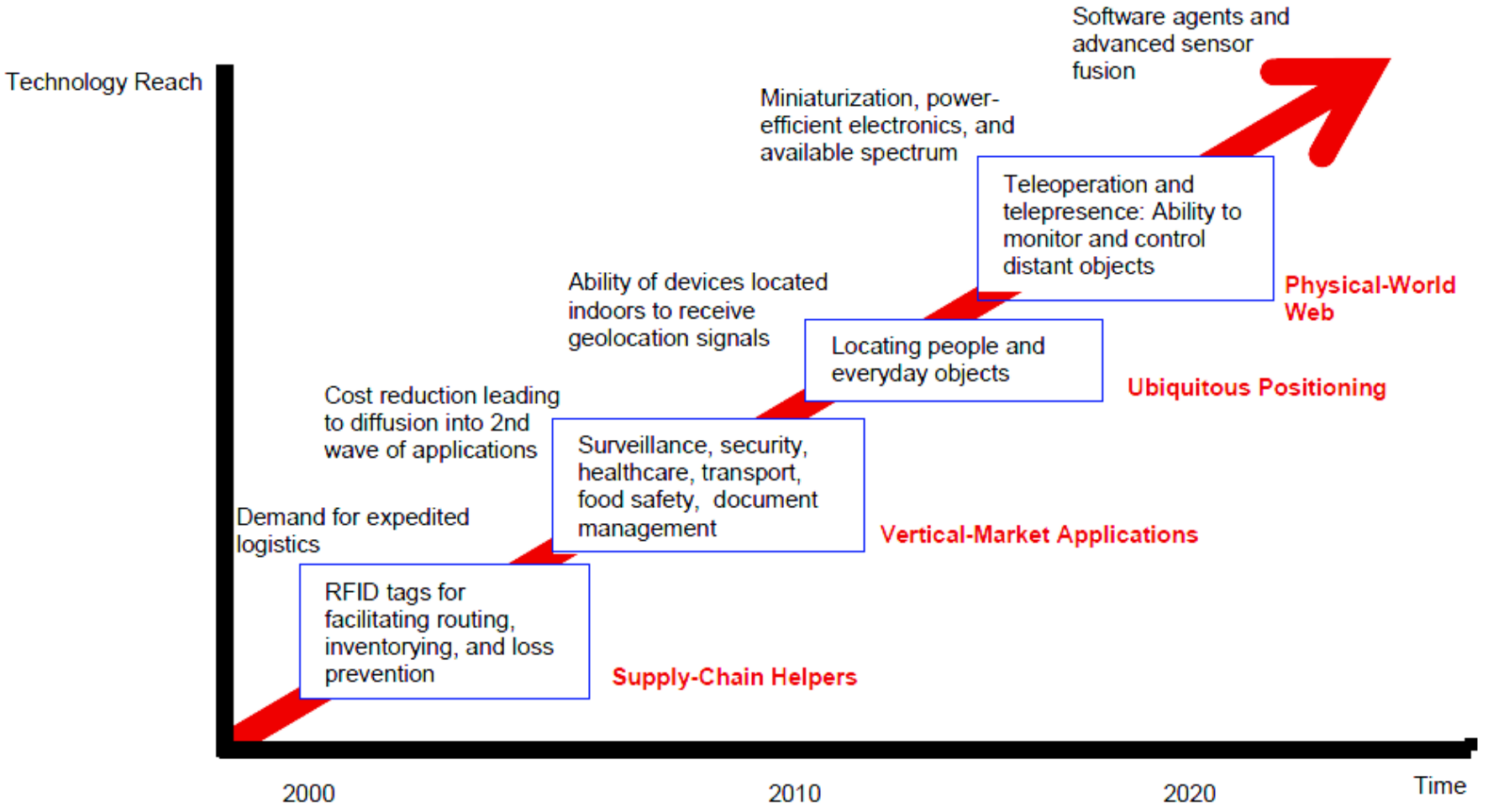
От Интернента PC к Интернету вещей (IoT)

- В 2008 г. число устройств, подключенных к Интернету превысило число жителей Земли К 2020 г. таких устройств будет 50 миллиардов

"... by 2012 your fridge, your heart monitor, your bathroom scales and your shoes might work together to monitor (and nag you about) your cardiovascular health"

F. Stajano. *Security for Ubiquitous Computing*. Wiley, 1st ed., 2002.

TECHNOLOGY ROADMAP: THE INTERNET OF THINGS



Ассоциация РусКрипто

РусКрипто 2012

- В 2008 г. число устройств, подключенных к Интернету превысило число жителей Земли К 2020 г. таких устройств будет 50 миллиардов
- В ближайшие 5 лет 20 типичных европейских домохозяйств будут генерировать больше интернет-трафика, чем весь Интернет в 2008 г.
- Благодаря протоколу IPv6 у нас появятся 340282366920938463463374607431768211456 интернет-адресов.

- **A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in information processes. Services are available to interact with these 'smart objects' over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues.**

"SAP IoT Definition".
SAP Research. Retrieved 2011-03-18.

- A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in information processes. Services are available to interact with these 'smart objects' over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues

"SAP IoT Definition".
SAP Research. Retrieved 2011-03-18.

Lightweight Cryptography for the Internet of Things

Легковесная криптография

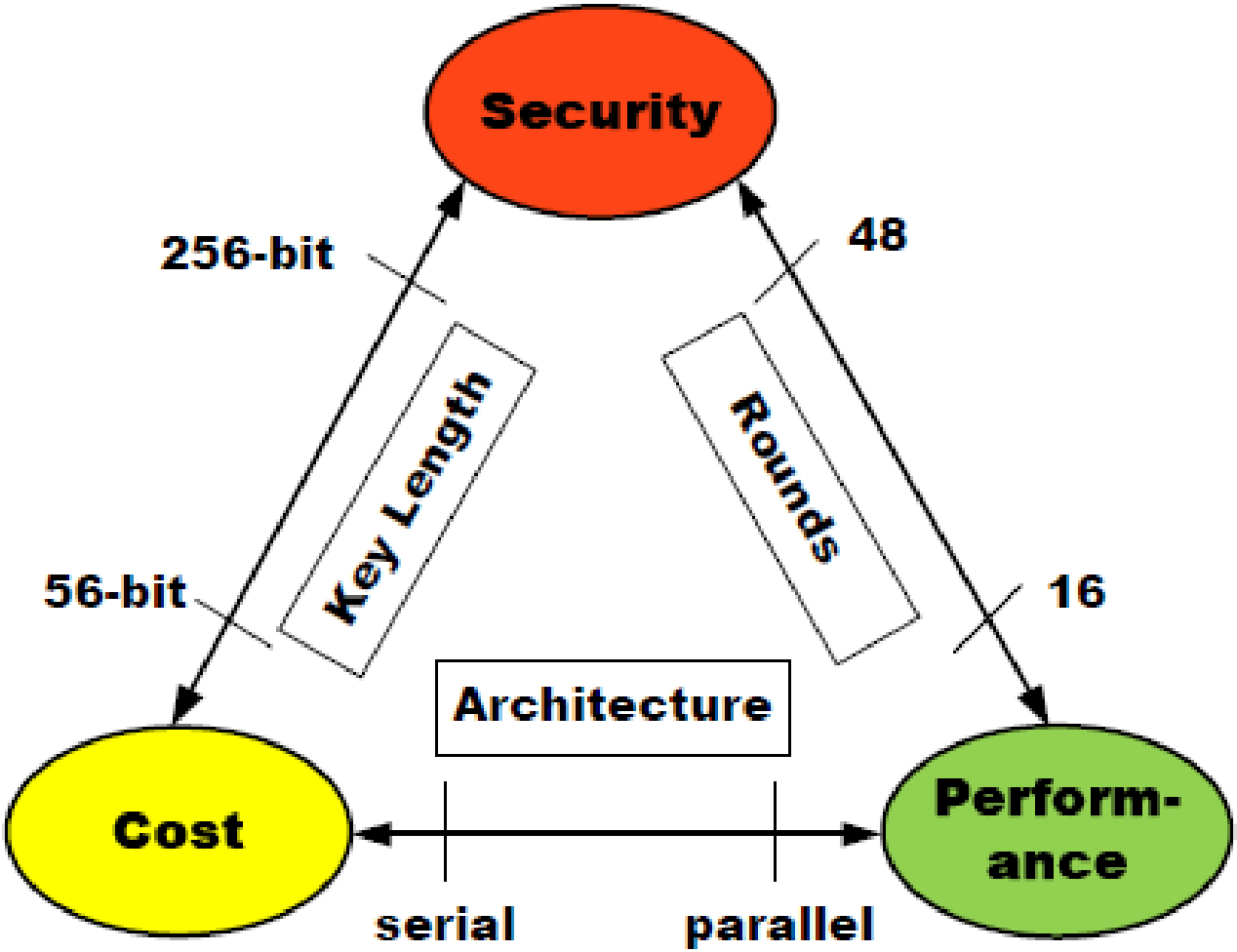
Легковесная криптография (низкоресурсная криптография)

- **ISO/IEC FDIS 29192-1 -- 29192-4.**
  -- Information technology
  -- Security techniques
  -- Lightweight cryptography
  - **Part 1: General.**
    Стадия: 50.60 (2012-03-18)
  - **Part 3: Stream ciphers.**
    Стадия: 50.20 (2012-02-16)
  - **Part 4: Mechanisms using asymmetric techniques. Стадия: 40.20 (2011-12-22)**

Ассоциация РусКрипто

РусКрипто 2012

- ECRYPT Workshop on Lightweight Cryptography (Belgium) –November 28-29, 2011.
- Workshop on Cryptographic Hardware and Embedded Systems 2011 –CHES'2011 (Japan) – секция LWC
- Eurocrypt'2011
- AFRICACRYPT'2011
- CRYPTO'2011
- FSE'2011
- SAC'2011


Security
256-bit
48
Key Length
Rounds
56-bit
16
Architecture
Cost
Perform-
ance
serial
parallel

Lightweight Block Ciphers

64-bit block	96-bit block	128-bit block
• 3-DES (112-168) • IDEA (128) • MISTY1 (128) • KASUMI (64-128) • HIGHT (128) • PRESENT (80-128) • TEA (128) • mCRYPTON (96) • GOST (256) • KATAN64 (80) • KTANTAN64 (80) • KLEIN (64-96-128) • DESXL (184)	• SEA (96) • PRINTcipher-96 (160)	• AES (128-192-256) • CAMELLIA • RC6 • CLEFIA

Lightweight Block Ciphers

Algorithm	Reference	key size	block size	datapath width	cycles/ block	Throughput [Kbps]	Logic [μm]	Area [GE]
KATAN-32	[Cannière et al.'09]	80	32	–	256	12.5	0.13	802
KATAN-64		80	64	–	255	25.1	0.13	1,027
PRESENT-80	[Rolfes et al.'08]	80	64	4	547	11.7	0.18	1,075
PRESENT-128		128	64	4	559	11.45	0.18	1,391
DES	[Leander et al.'07]	56	64	4	144	44.4	0.18	2,309
DESXL		184	64	4	144	44.4	0.18	2,168
AES-128	[Feldhofer et al.'04]	128	128	8	1,032	12.4	0.35	3,400
AES-128	[Hämäläinen et al.'06]	128	128	8	160	44.4	0.13	3,100
HIGHT	[Hong et al.'06]	128	64	64	1	6,400	0.25	3,048
mCrypton	[Lim et al.'05]	96	64	64	13	492.3	0.13	2,681
SEA	[Standaert et al.'06]	96	96	96	93	103.23	0.13	3,758

Lightweight Block Ciphers

CHES 2011

Piccolo: An Ultra-Lightweight Blockcipher

Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai

64-bit blockcipher supporting 80 and 128-bit keys.

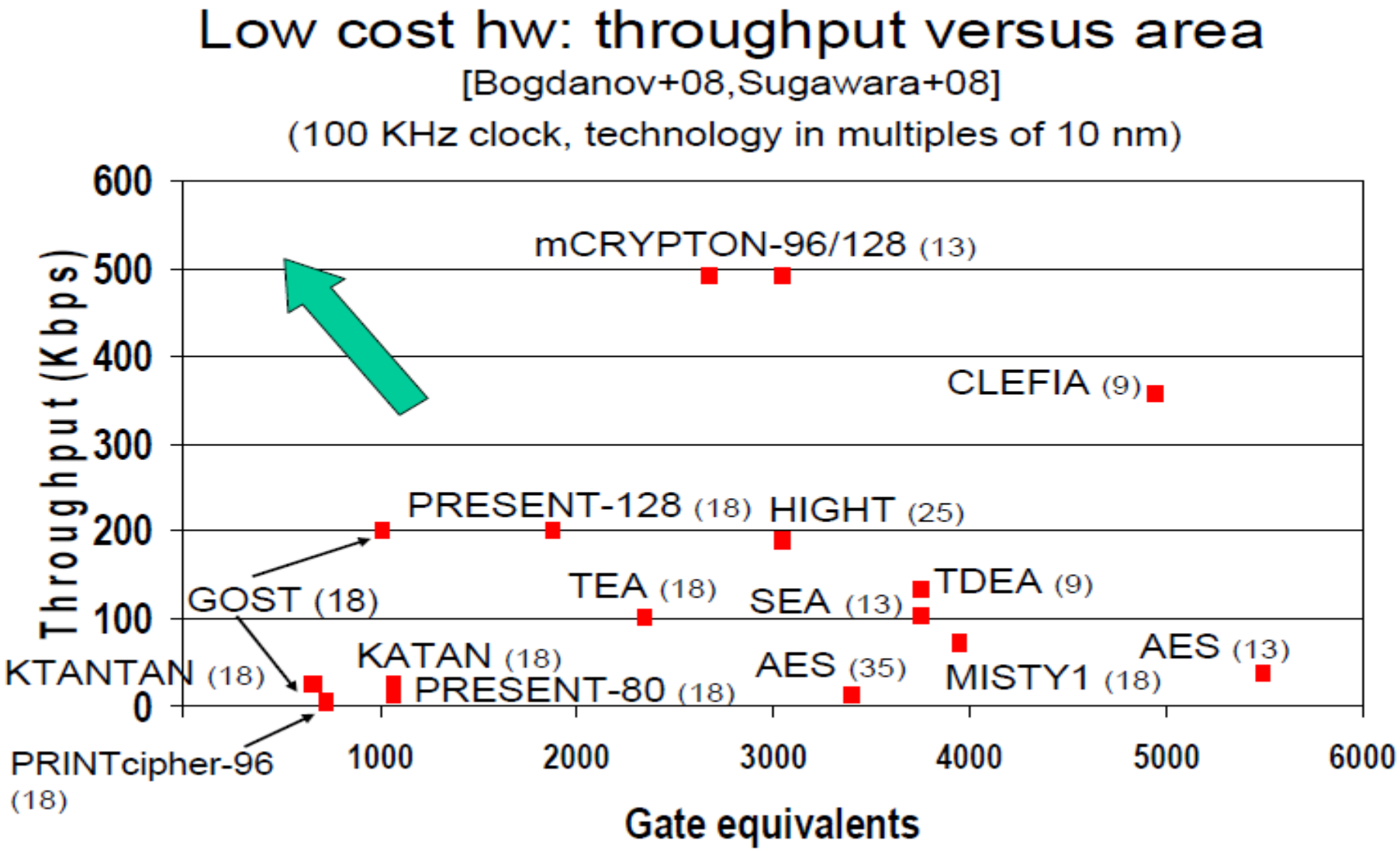
The hardware requirements for the 80 and the 128-bit key mode are only 683 and 758 gate equivalents, respectively.

Lightweight Block Ciphers

Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices

Daniel Engels, Xinxin Fan, Guang Gong, Honggang Hu and Eric M. Smith (CANADA, USA)

Hummingbird is a combination of block cipher and stream cipher structures with 16-bit block size, 256-bit key size, and 80-bit internal state.

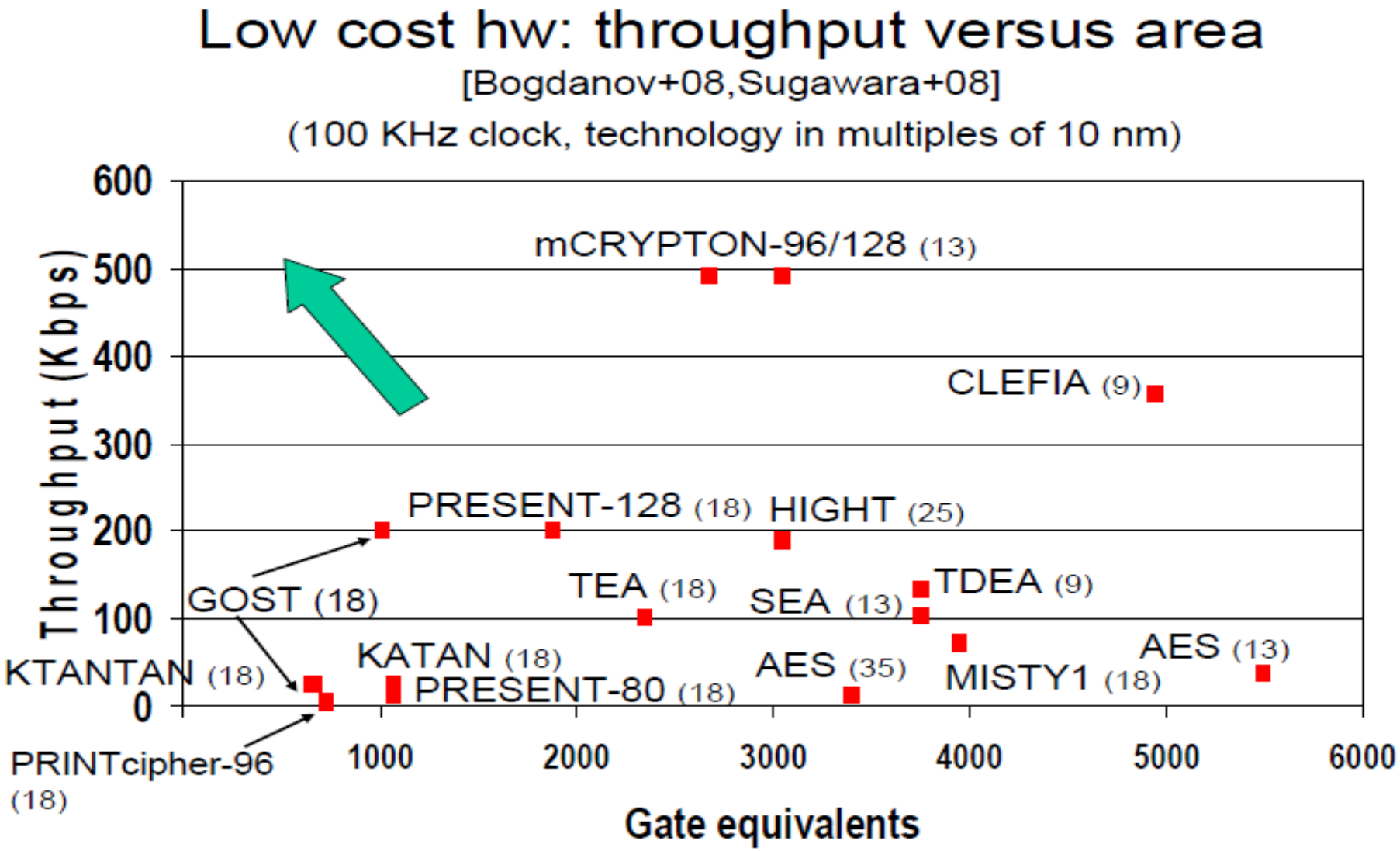

Low cost hw: throughput versus area
[Bogdanov+08,Sugawara+08]
(100 KHz clock, technology in multiples of 10 nm)
Throughput (Kbps)
600
500
400
300
200
100
0
mCRYPTON-96/128 (13)
CLEFIA (9)
PRESENT-128 (18)
HIGHT (25)
GOST (18)
TEA (18)
SEA (13)
TDEA (9)
KTANTAN (18)
KATAN (18)
PRESENT-80 (18)
AES (35)
MISTY1 (18)
AES (13)
PRINTcipher-96 (18)
1000
2000
3000
4000
5000
6000
Gate equivalents

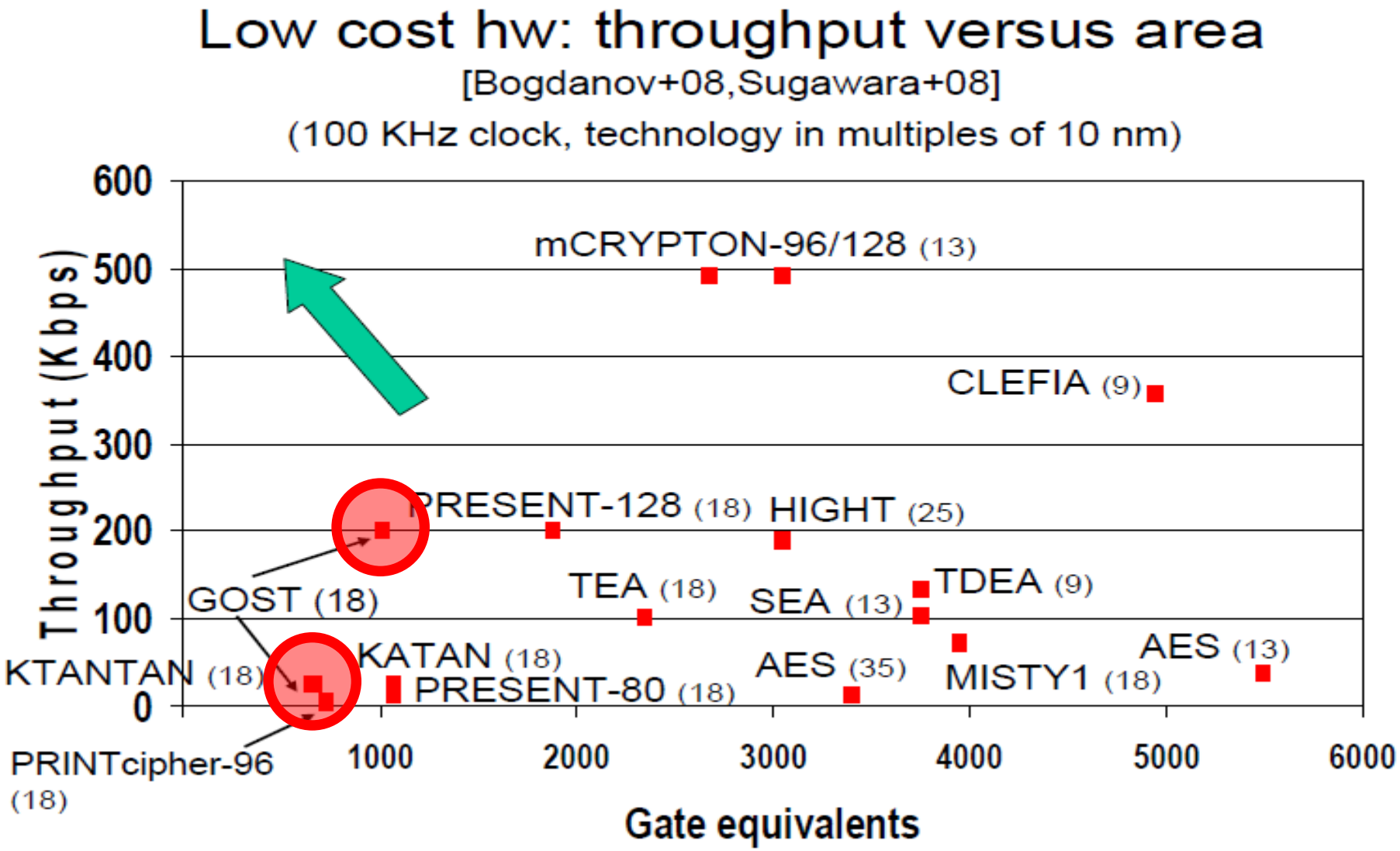
Lightweight Block Ciphers

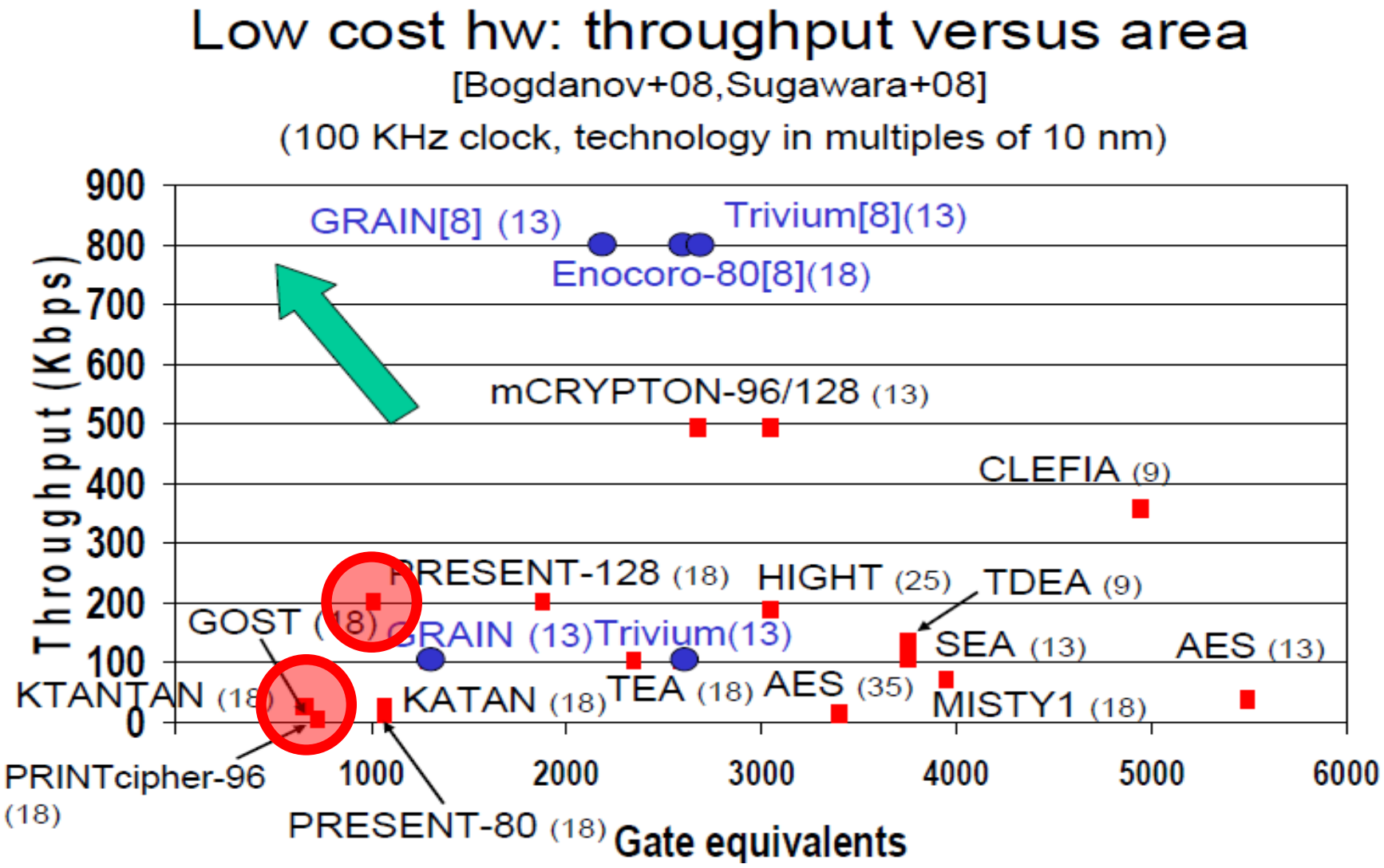
Axel Poschmann, San Ling, and Huaxiong Wang: *256 Bit Standardized Crypto for 650 GE GOST Revisited,* In CHES 2010, LNCS 6225, pp. 219-233, 2010.

Faculty of Electrical Engineering and Information Technology
Ruhr-University Bochum, Germany

Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University, Singapore


Low cost hw: throughput versus area
[Bogdanov+08,Sugawara+08]
(100 KHz clock, technology in multiples of 10 nm)
Throughput (Kbps)
600
500
400
300
200
100
0
mCRYPTON-96/128 (13)
CLEFIA (9)
PRESENT-128 (18)
HIGHT (25)
GOST (18)
TEA (18)
SEA (13)
TDEA (9)
KTANTAN (18)
KATAN (18)
PRESENT-80 (18)
AES (35)
MISTY1 (18)
AES (13)
PRINTcipher-96 (18)
1000
2000
3000
4000
5000
6000
Gate equivalents


Low cost hw: throughput versus area
[Bogdanov+08,Sugawara+08]
(100 KHz clock, technology in multiples of 10 nm)
Throughput (Kbps)
600
500
400
300
200
100
0
mCRYPTON-96/128 (13)
CLEFIA (9)
PRESENT-128 (18)
HIGHT (25)
GOST (18)
TEA (18)
SEA (13)
TDEA (9)
KTANTAN (18)
KATAN (18)
PRESENT-80 (18)
AES (35)
MISTY1 (18)
AES (13)
PRINTcipher-96 (18)
1000
2000
3000
4000
5000
6000
Gate equivalents


Low cost hw: throughput versus area
[Bogdanov+08,Sugawara+08]
(100 KHz clock, technology in multiples of 10 nm)
Throughput (Kbps)
900
800
700
600
500
400
300
200
100
0
1000
2000
3000
4000
5000
6000
Gate equivalents
GRAIN[8] (13)
Trivium[8](13)
Enocoro-80[8](18)
mCRYPTON-96/128 (13)
CLEFIA (9)
PRESENT-128 (18)
HIGHT (25)
TDEA (9)
GOST (18)
GRAIN (13)
Trivium(13)
SEA (13)
AES (13)
KTANTAN (18)
KATAN (18)
TEA (18)
AES (35)
MISTY1 (18)
PRINTcipher-96 (18)
PRESENT-80 (18)

- FSE'2011 *Takanori Isobe*
  A Single-Key Attack on the Full GOST Block Cipher
- IACR 2011/211 *Nicolas T. Courtois*
  Security Evaluation of GOST 28147-89 In View Of International Standardisation
- IACR 2011/312 *Nicolas T. Courtois and Michal Misztal*
  Differential Cryptanalysis of GOST
- IACR 2011/489 *A. N. Alekseychuk and L. V. Kovalchuk*
  Towards a Theory of Security Evaluation for GOST-like Ciphers against Differential and Linear Cryptanalysis
- IACR 2011/558 *Itai Dinur and Orr Dunkelman and Adi Shamir*
  Improved Attacks on Full GOST
- IACR 2011/619 *Bo Zhu and Guang Gong*
  Multidimensional Meet-in-the-Middle Attack and Its Applications to GOST, KTANTAN and Hummingbird-2
- IACR 2011/626 *Nicolas T. Courtois*
  Algebraic Complexity Reduction and Cryptanalysis of GOST

Single-key Attacks on the Full GOST

Reference	Data (KP)	Mem.	Time	Self-Sim. Property
T. Isobe. *A Single-Key Attack on the Full GOST Block Cipher*. FSE 2011	2^{32}	2^{64}	2^{224}	Reflection
N. Courtois. *Security Evaluation of GOST 28147-89 in View of International Standardisation*. Cryptology ePrint Archive, Report 2011/211 (2011)	2^{64}	2^{64}	2^{248}	
N. Courtois and M. Misztal. *Differential Cryptanalysis of GOST.* Cryptology ePrint Archive, Report 2011/312 (2011)	2^{64}	2^{64}	2^{226}	Differential
Itai Dinur, Orr Dunkelman and Adi Shamir *Improved Attacks on Full GOST* Cryptology ePrint Archive, Report 2011/558 (2011)	2^{64}	2^{36}	2^{192}	fixed point
Itai Dinur, Orr Dunkelman and Adi Shamir *Improved Attacks on Full GOST* Cryptology ePrint Archive, Report 2011/558 (2011)	2^{64}	2^{19}	2^{204}	fixed point
Itai Dinur, Orr Dunkelman and Adi Shamir *Improved Attacks on Full GOST* Cryptology ePrint Archive, Report 2011/558 (2011)	2^{32}	2^{36}	2^{224}	Reflection
Itai Dinur, Orr Dunkelman and Adi Shamir *Improved Attacks on Full GOST* Cryptology ePrint Archive, Report 2011/558 (2011)	2^{32}	2^{19}	2^{236}	Reflection

Security Evaluation of GOST 28147-89 In View Of International Standardisation

Nicolas T. Courtois

University College London, Gower Street, London, UK,
n.courtois@cs.ucl.ac.uk

be possible. It appears that also that it is for the first time in history that a major standardized block cipher intended to provide a military-grade level of security and intended to protect also classified and secret documents, for the government, large banks and other organisations, is broken by a mathematical attack.

Clearly GOST is deeply flawed, in more than one way, and GOST does not provide the security level required by ISO. A plethora of other attacks

Improved Attacks on Full GOST

Itai Dinur[1], Orr Dunkelman[1,2] and Adi Shamir[1]

[1] Computer Science department, The Weizmann Institute, Rehovot, Israel
[2] Computer Science Department, University of Haifa, Israel

cache of modern microprocessors, with a small penalty in the running time). The lowest time complexity of our attacks is 2^{192}, which is 2^{32} times better than previously published attacks but still very far from being practical. Consequently, we are concerned about the weaknesses which were demonstrated in the design of GOST (especially in its simplistic key schedule), but do not advocate that its current users should stop using it right away.

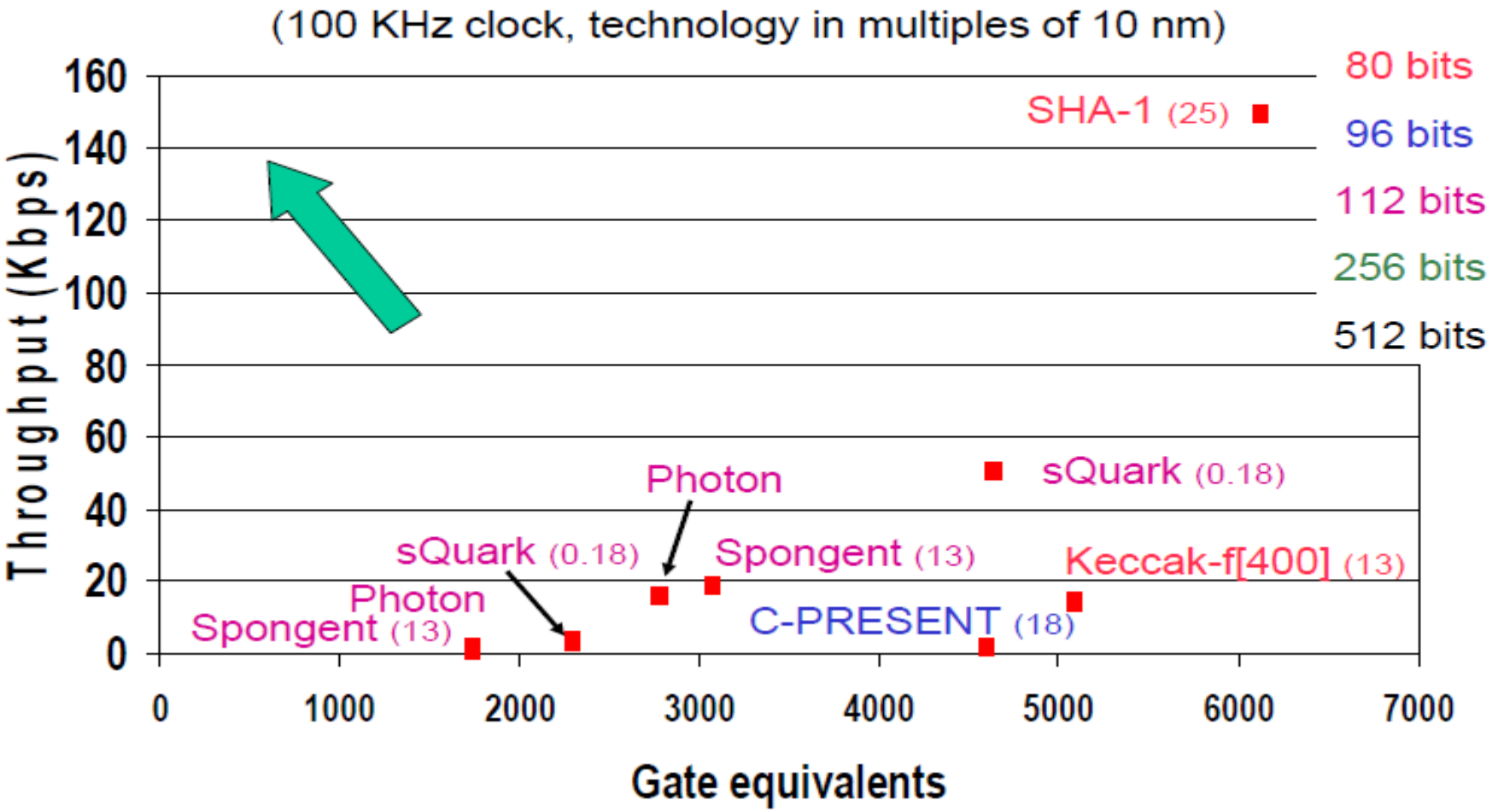
Свойства S-блоков размера 4×4

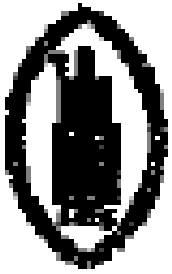
- Markku-Juhani O. Saarinen (Revere Security, USA)
  Cryptographic Analysis of All 4×4-Bit S-Boxes
  SAC 2011
- *Nicolas T. Courtois, Daniel Hulme and Theodosis Mourouzis*
  Solving Circuit Optimisation Problems in Cryptography and Cryptanalysis
  Cryptology ePrint Archive, Report 2011/475 (2011)
- *Markus Ullrich, Christophe De Canniere, Sebastiaan Indesteege, Ozgul Kucuk, Nicky Mouha, Bart Preneel*
  Finding Optimal Bitsliced Implementations of 4×4-bit S-boxes

Lightweight Hash Functions

Hash Functions	Reference	output size	datapath width	cycles/ block	Throughput [Kbps]	Logic [μm]	Area [GE]
U-QUARK	[Aumasson et al.'10]	128	–	33	242.42	0.18	1,379
D-QUARK		160	–	547	14.63	0.18	1,702
T-QUARK		224	–	33	387.88	0.18	2,296
PRESENT80-based	[Bogdanov et al.'08]	64	64	33	242.42	0.18	2,213
			4	547	14.63	0.18	1,600
PRESENT128-based	[Bogdanov et al.'08]	128	64	33	387.88	0.18	2,530
			4	559	22.9	0.18	1,886
AES128-based	[Bogdanov et al.'08]	128	8	$> 1,032$	< 12.4	estimiate	$> 4,400$

Low cost hw: throughput versus area





ECRYPT

http://www.ecrypt.eu.org

Perspectives on Lightweight Cryptography

Bart Preneel

COSIC, K.U.Leuven, Belgium