The Need for Parallel Ultra Fast Cryptographic Designs for Emerging Technologies

Danilo Gligoroski and Svein Johan Knapskog and Simona Samardjiska

Presented by

Prof. Danilo Gligoroski

Department of Telematics

Faculty of Information Technology, Mathematics and Electrical Engineering

Norwegian University of Science and TechnologyTechnology - NTNU, NORWAY

NTNU

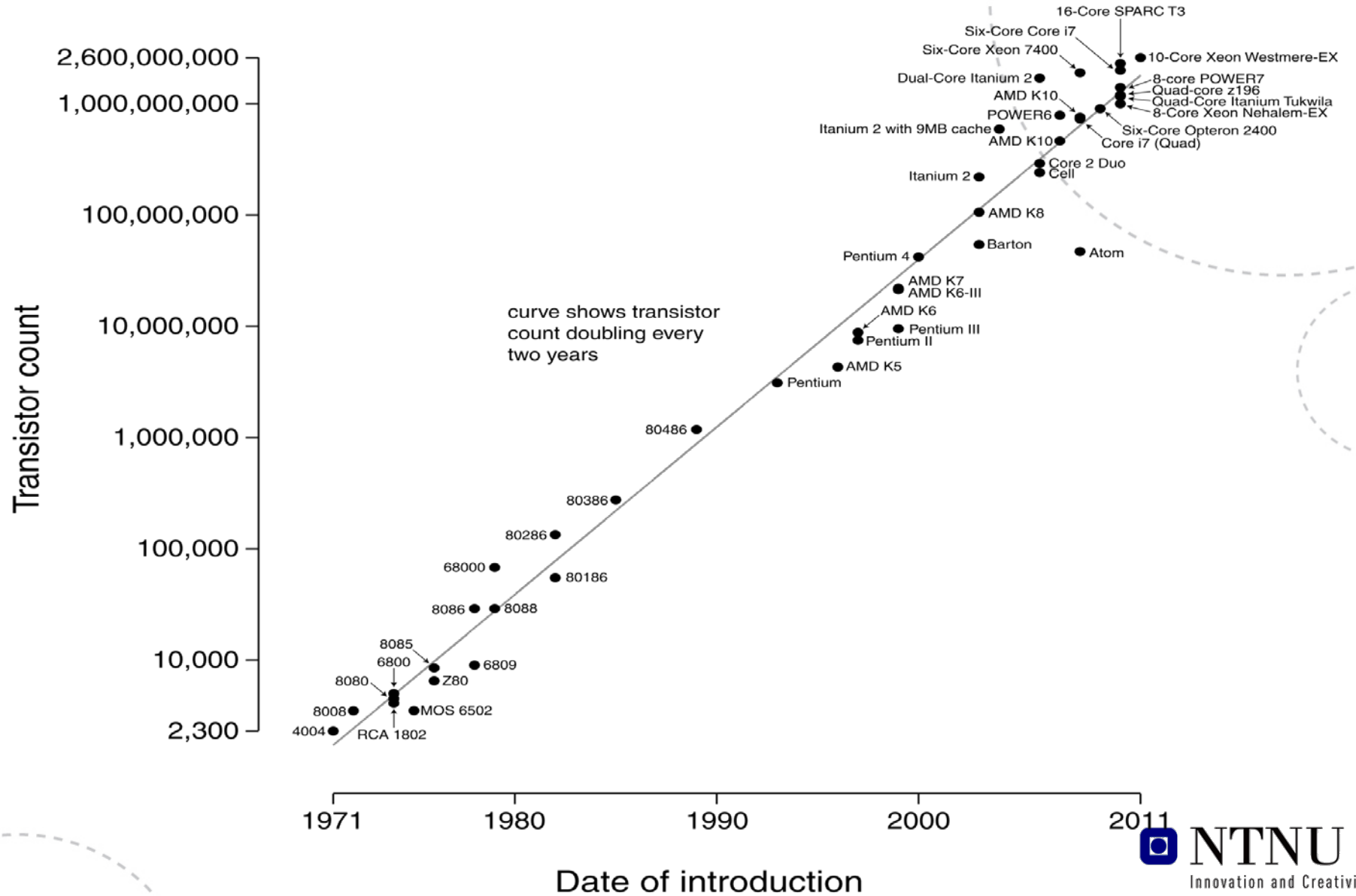
Innovation and Creativity

Outline (in a form of abstract)

- The exponential growth of computing power
- Was not followed by the development of the cryptographic designs in
  - Hash functions and
  - Public Key Cryptography
- The current trends in the Digital Universe
  - Either use less secure primitives like MD5
  - Or hit the wall of massive usability even with the obsolete security parameters (around 2^{80} crypto computations)
- We offer arguments that there are technological and theoretical preconditions for design of new parallel and ultrafast cryptographic primitives
- And we propose establishment of a regular mechanism "Cryptographic Contests" for addressing the cryptographic challenges for the emerging technologies

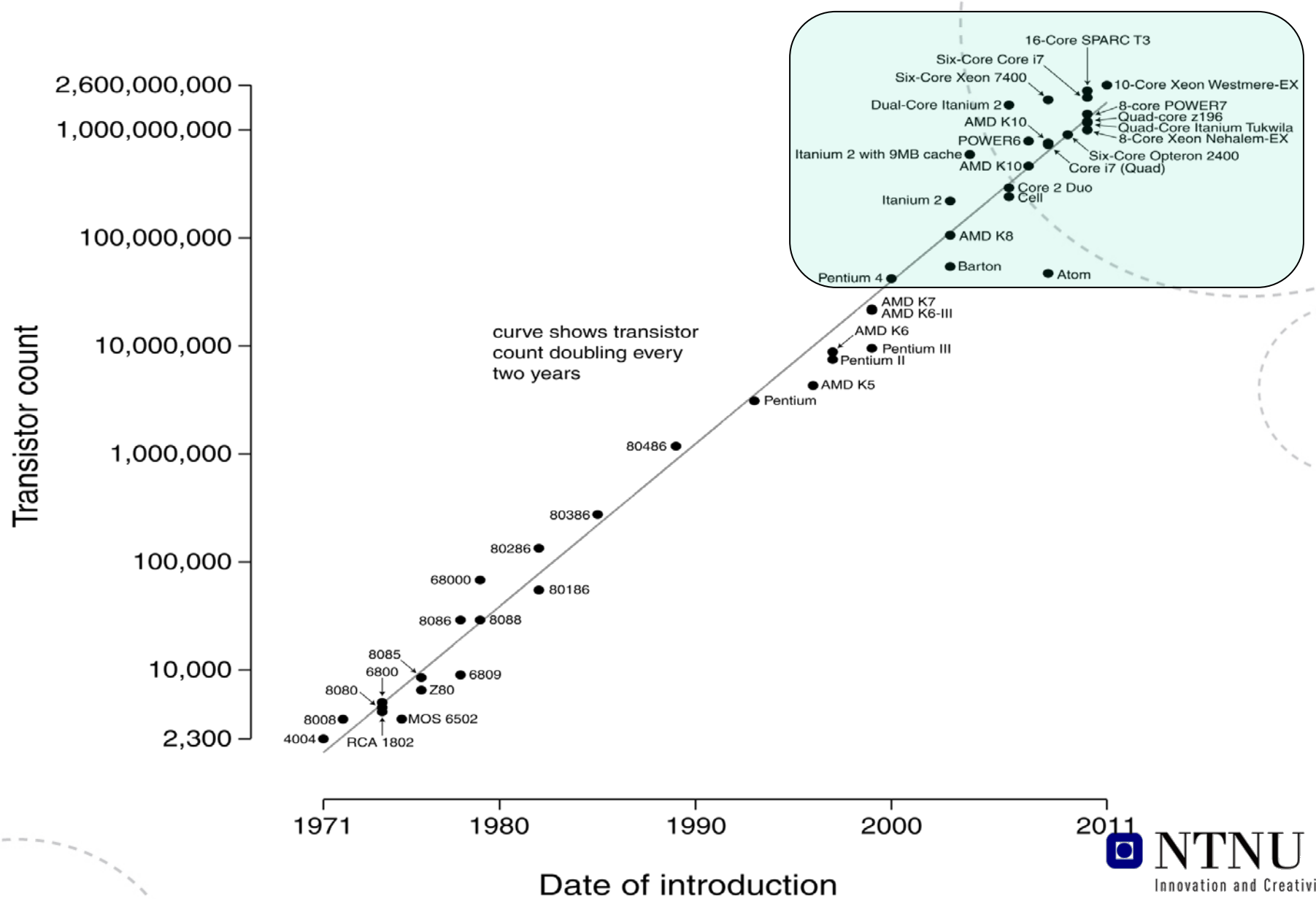
NTNU
Innovation and Creativity

Microprocessor Transistor Counts 1971-2011 & Moore's Law

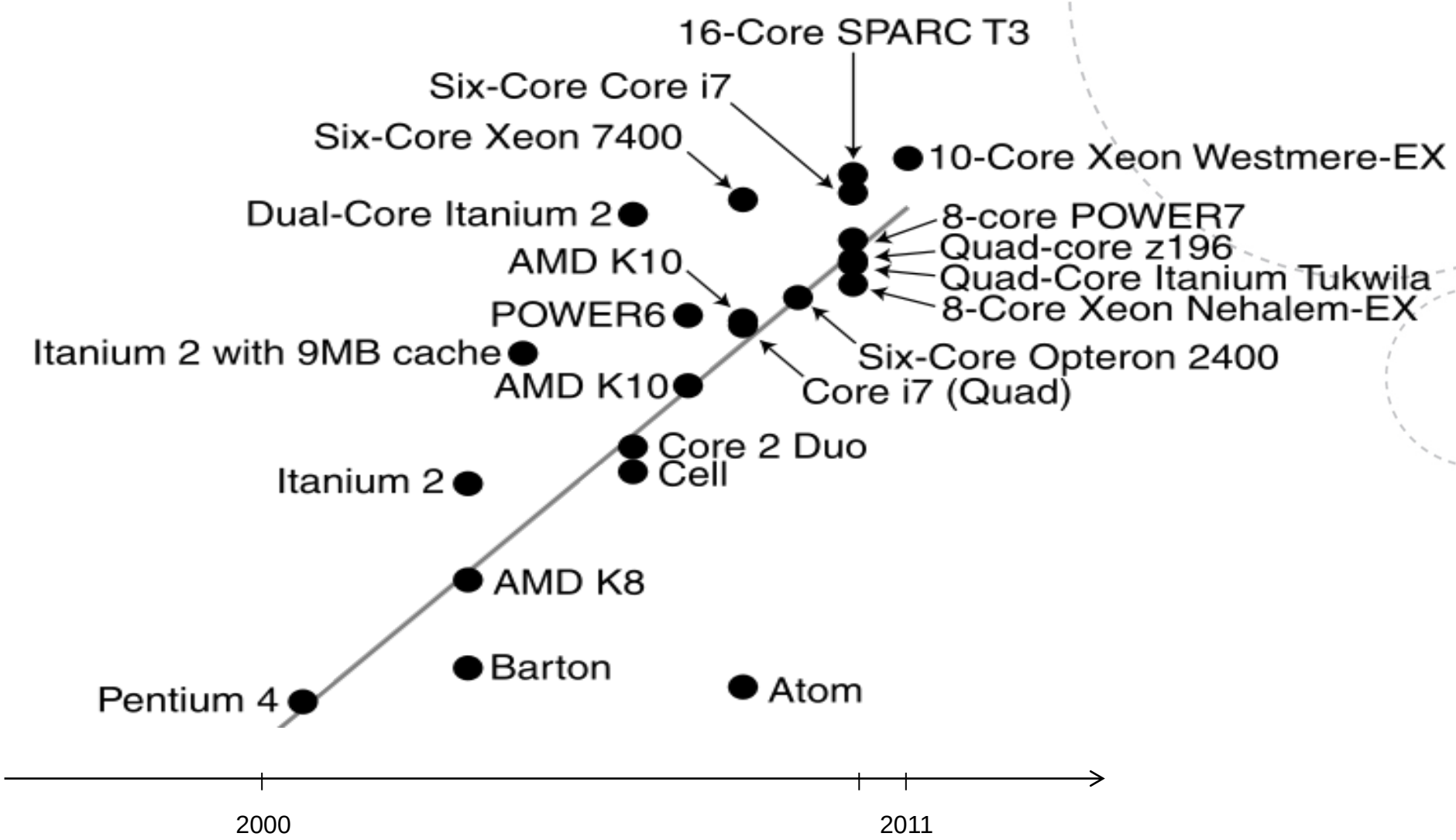


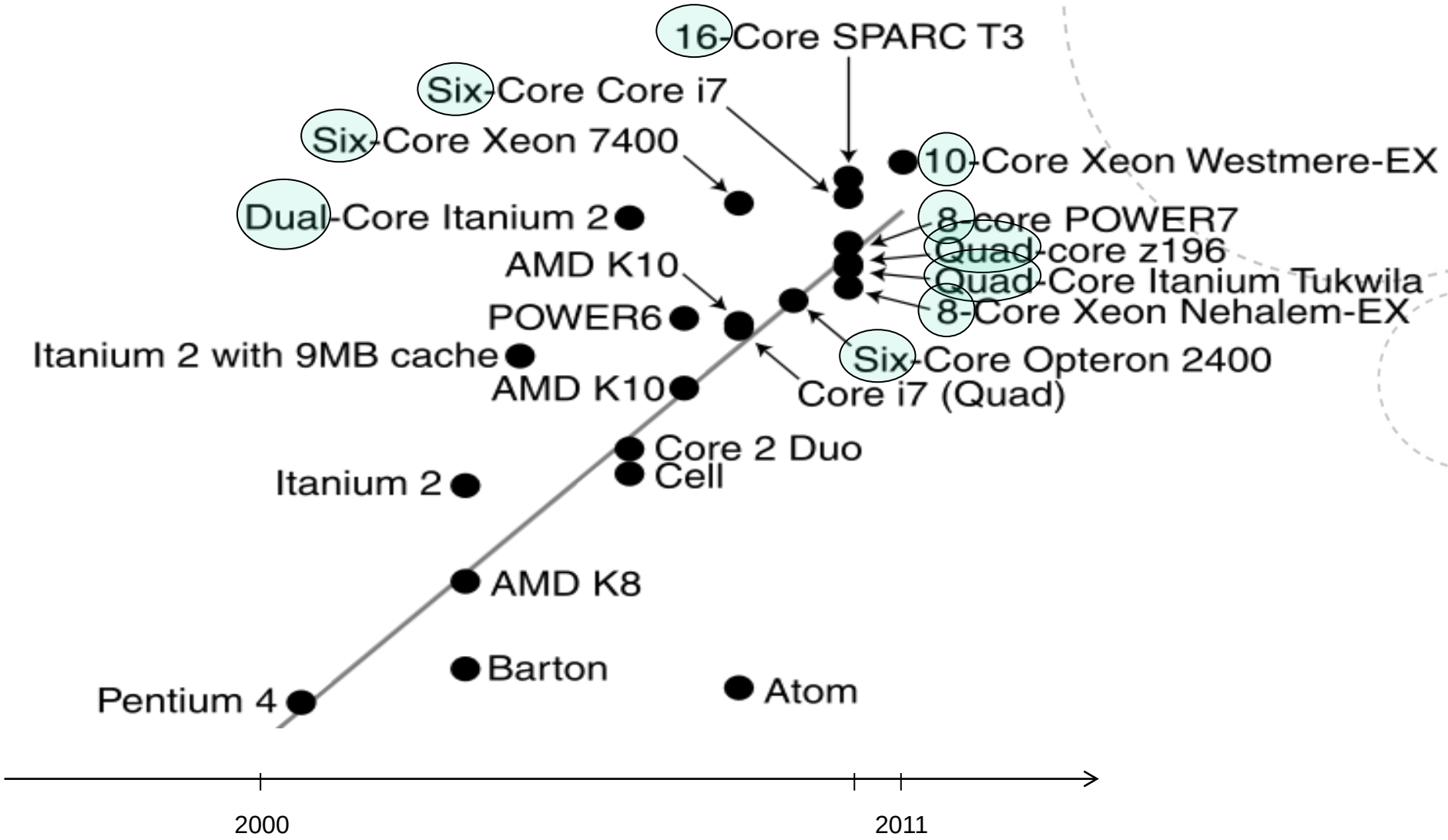
NTNU
Innovation and Creativity

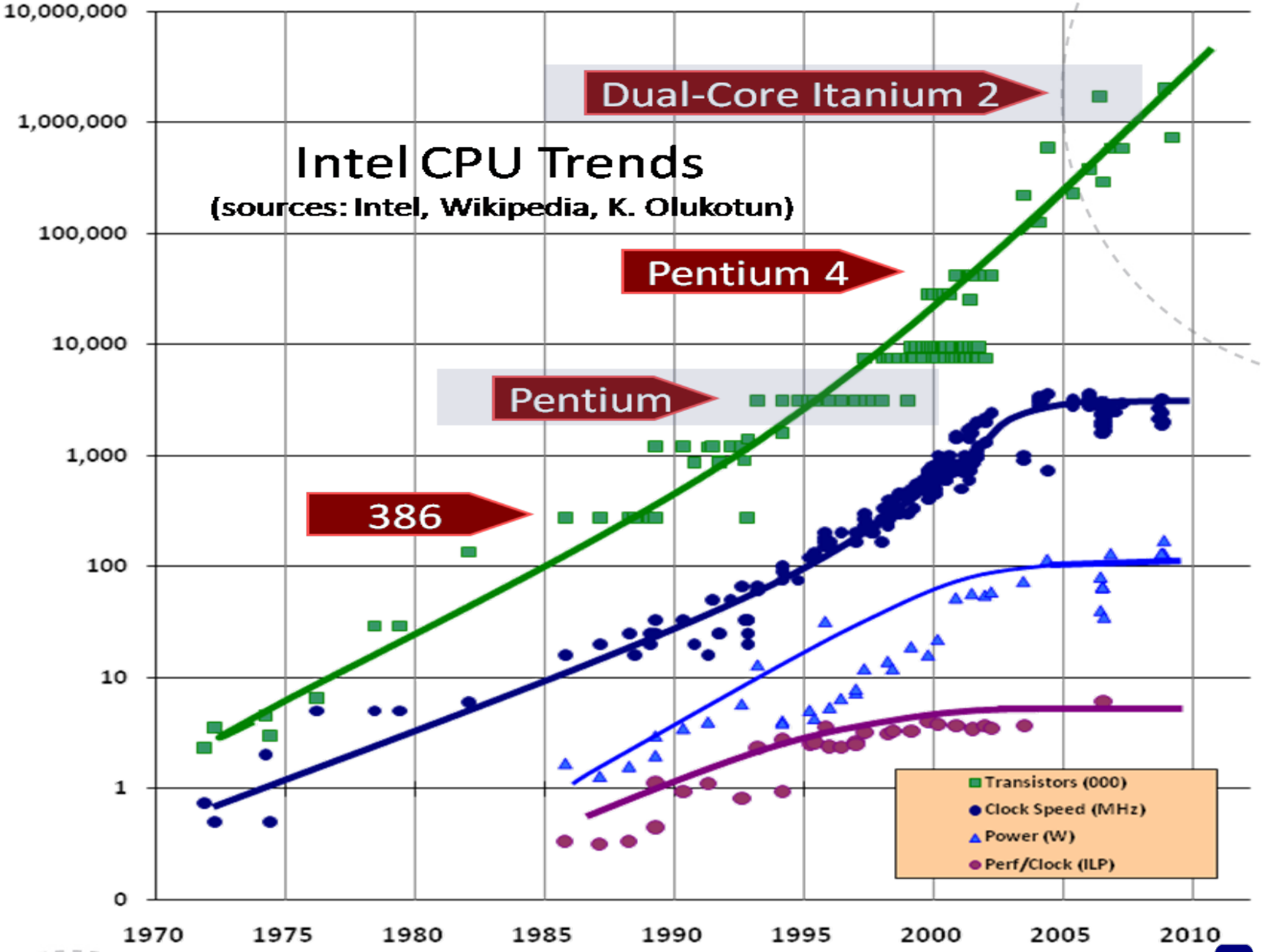
Microprocessor Transistor Counts 1971-2011 & Moore's Law



NTNU
Innovation and Creativity


16-Core SPARC T3
Six-Core Core i7
Six-Core Xeon 7400
10-Core Xeon Westmere-EX
Dual-Core Itanium 2
8-core POWER7
Quad-core z196
AMD K10
Quad-Core Itanium Tukwila
8-Core Xeon Nehalem-EX
POWER6
Itanium 2 with 9MB cache
Six-Core Opteron 2400
AMD K10
Core i7 (Quad)
Core 2 Duo
Cell
Itanium 2
AMD K8
Barton
Atom
Pentium 4
2000
2011

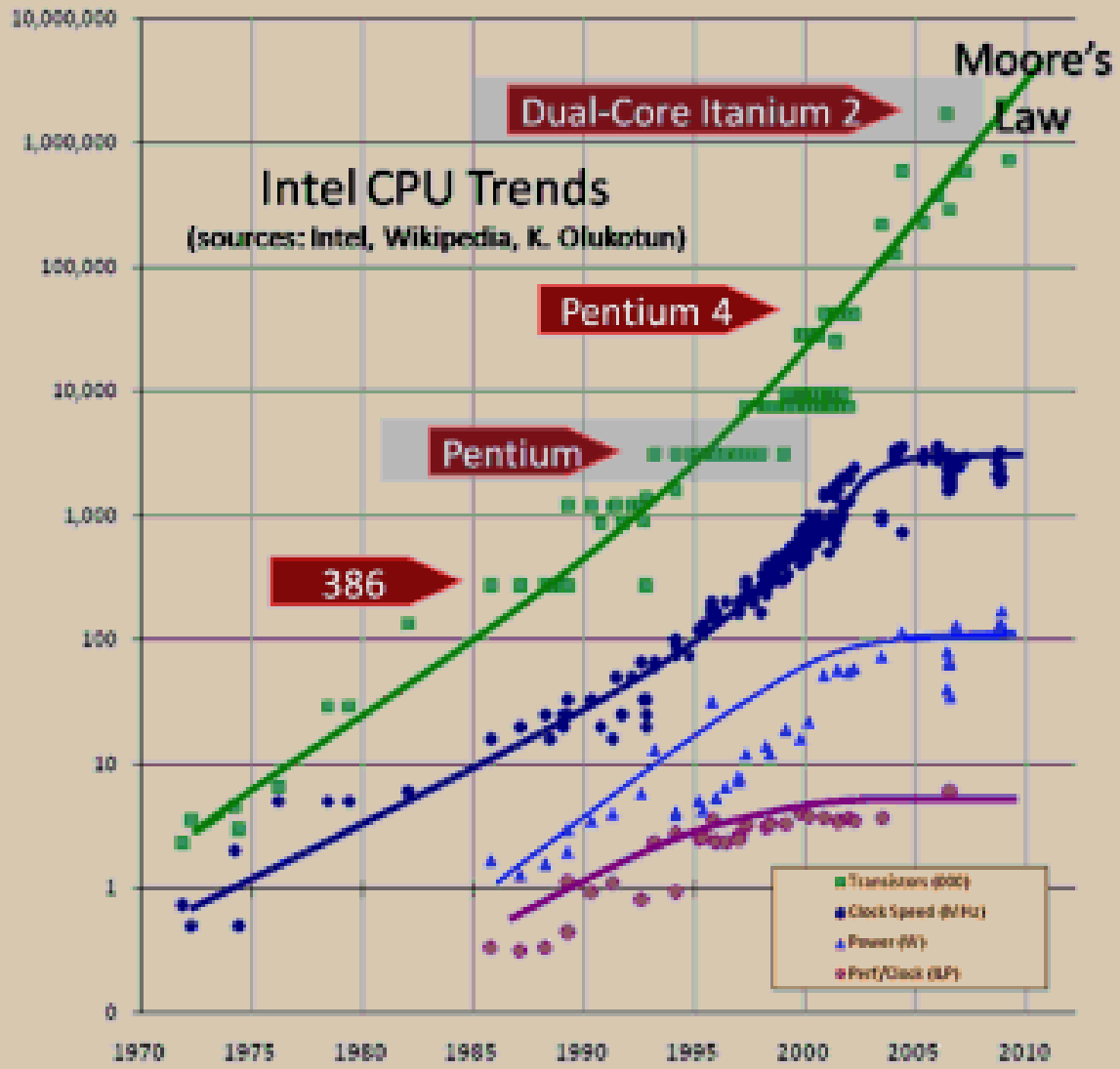

16-Core SPARC T3
Six-Core Core i7
Six-Core Xeon 7400
10-Core Xeon Westmere-EX
Dual-Core Itanium 2
8-core POWER7
Quad-core z196
AMD K10
Quad-Core Itanium Tukwila
8-Core Xeon Nehalem-EX
POWER6
Itanium 2 with 9MB cache
Six-Core Opteron 2400
AMD K10
Core i7 (Quad)
Core 2 Duo
Cell
Itanium 2
AMD K8
Barton
Atom
Pentium 4
2000
2011



Intel CPU Introductions (graph updated August 2009; article text Herb Sutter, Dr. Dobb's Journal, 30(3), March 2005)

NTNU
Innovation and Creativity

Each Year We Get ~~Faster~~ More Processors



Historically:
Boost single-stream performance via more complex chips.

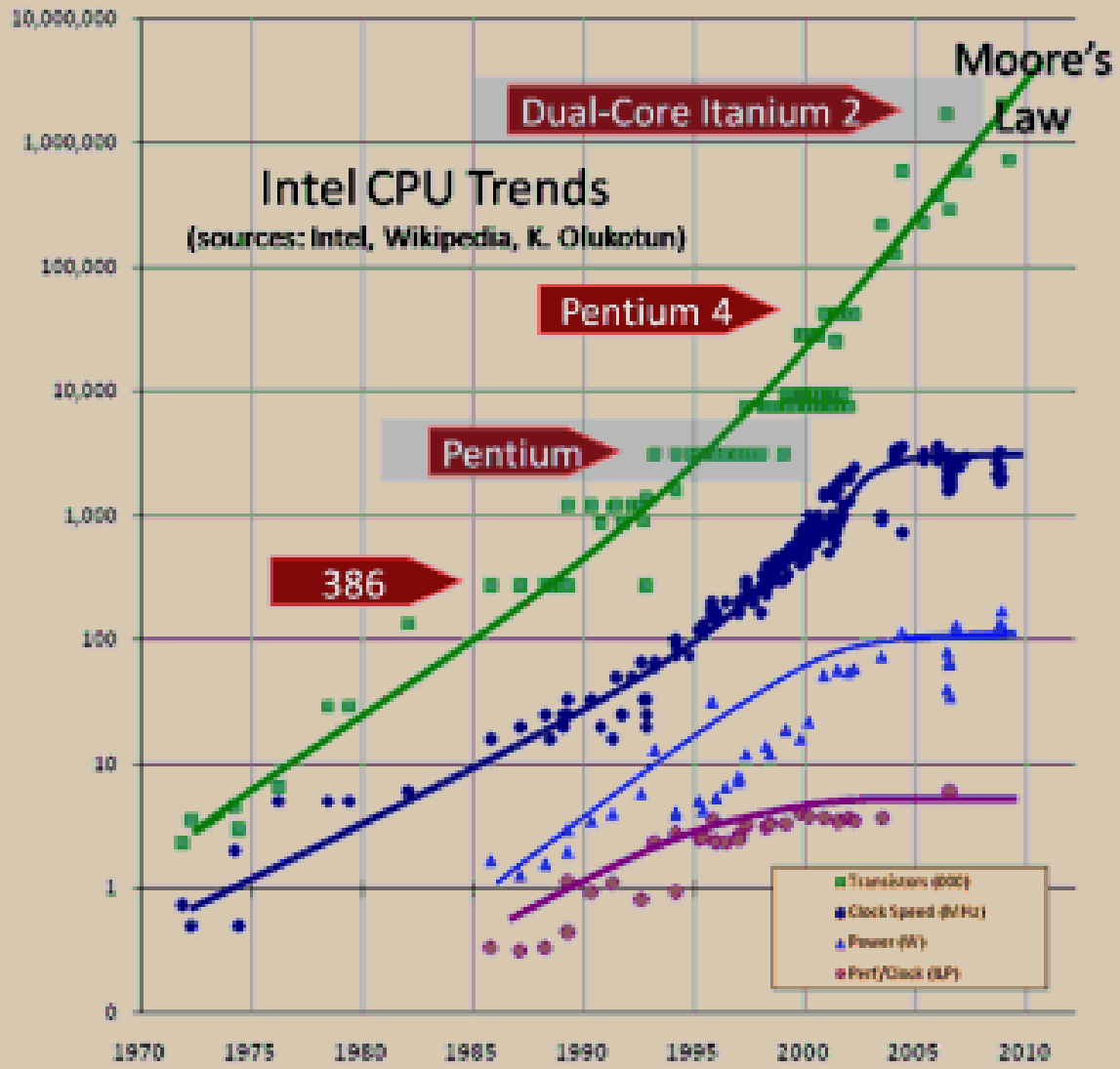
Now:
Deliver more cores per chip (+ GPU, NIC, SoC).

The free lunch is over for today's sequential apps and many concurrent apps. We need killer apps with lots of latent parallelism.

Graph and comments from article by Herb Sutter, Dr. Dobb's Journal, 30(3), March 2005)

NTNU
Innovation and Creativity

Each Year We Get ~~Faster~~ More Processors



Historically:
Boost single-stream performance via more complex chips.

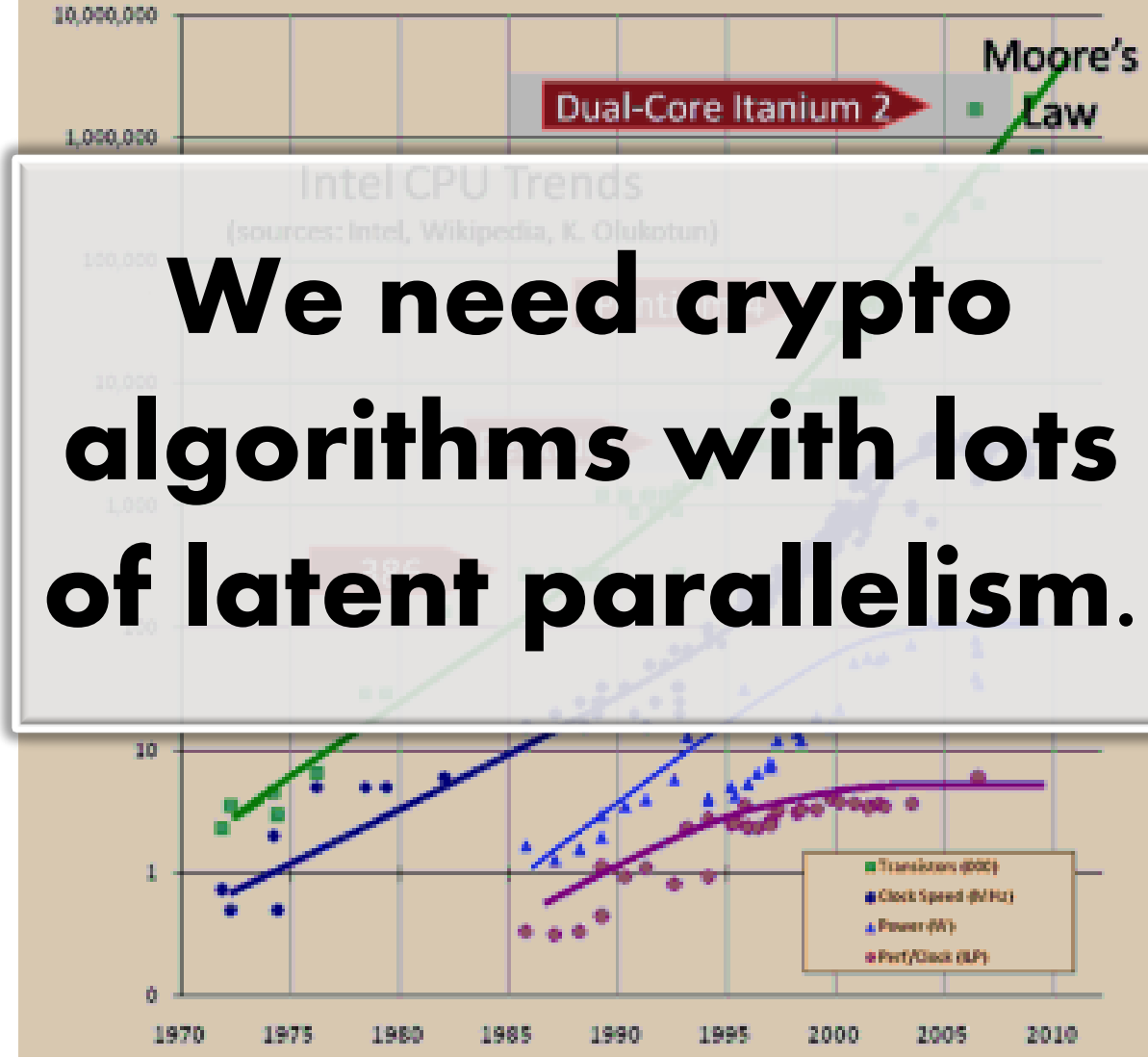
Now:
Deliver more cores per chip (+ GPU, NIC, SoC).

The free lunch is over for today's sequential apps and many concurrent apps. We need killer apps with lots of latent parallelism.

Graph and comments from article by Herb Sutter, Dr. Dobb's Journal, 30(3), March 2005)

NTNU
Innovation and Creativity

Each Year We Get ~~Faster~~ More Processors



Historically:
Boost single-stream performance via more complex chips.

Now:
Deliver more cores per chip (+ GPU, NIC, SoC).

The free lunch is over for today's sequential apps and many concurrent apps. We need killer apps with lots of latent parallelism.

We need crypto algorithms with lots of latent parallelism.

Graph and comments from article by Herb Sutter, Dr. Dobb's Journal, 30(3), March 2005)

NTNU
Innovation and Creativity

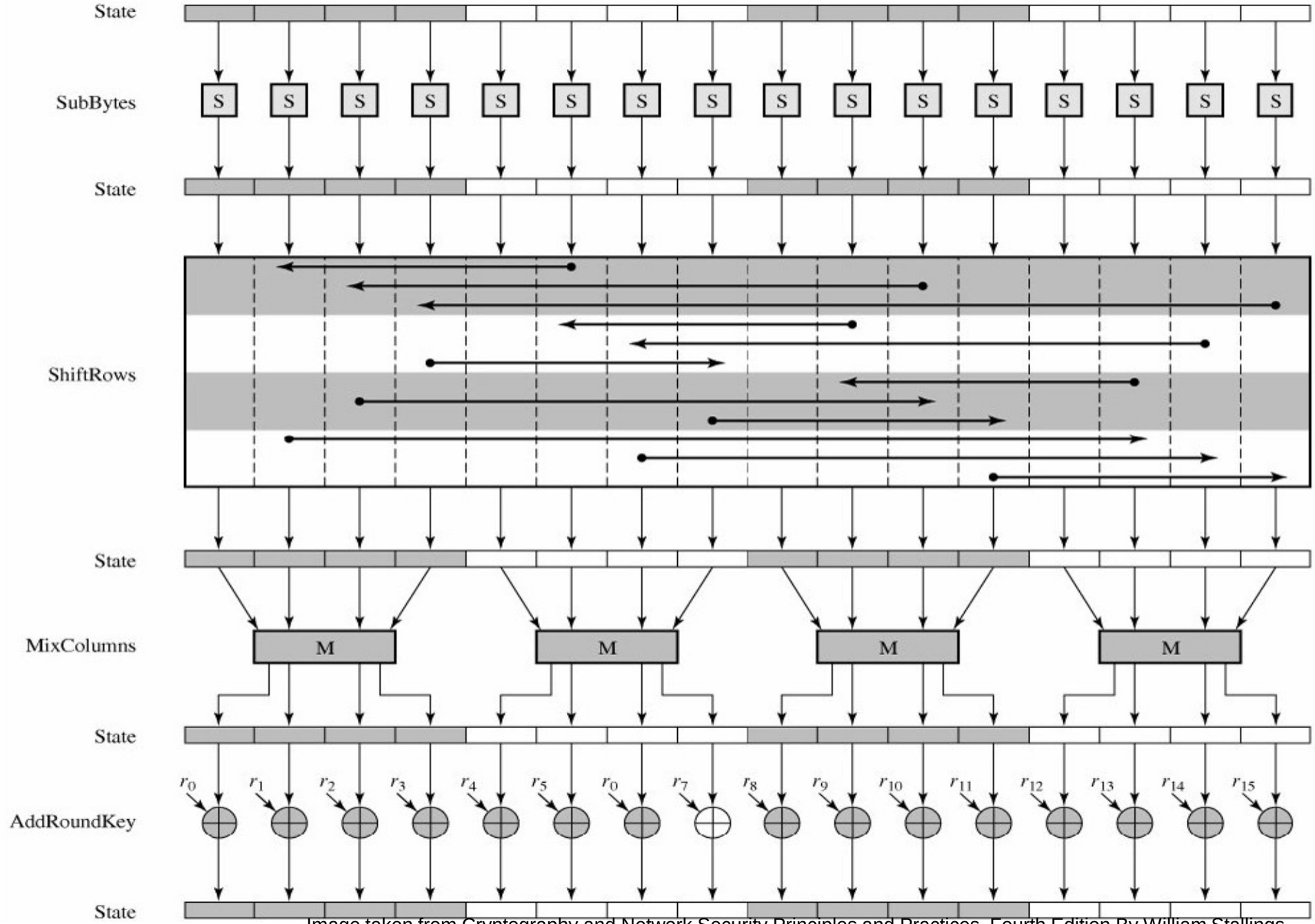


Image taken from Cryptography and Network Security Principles and Practices, Fourth Edition By William Stallings

The parallelism of one AES round (10, 12 or 14 rounds)

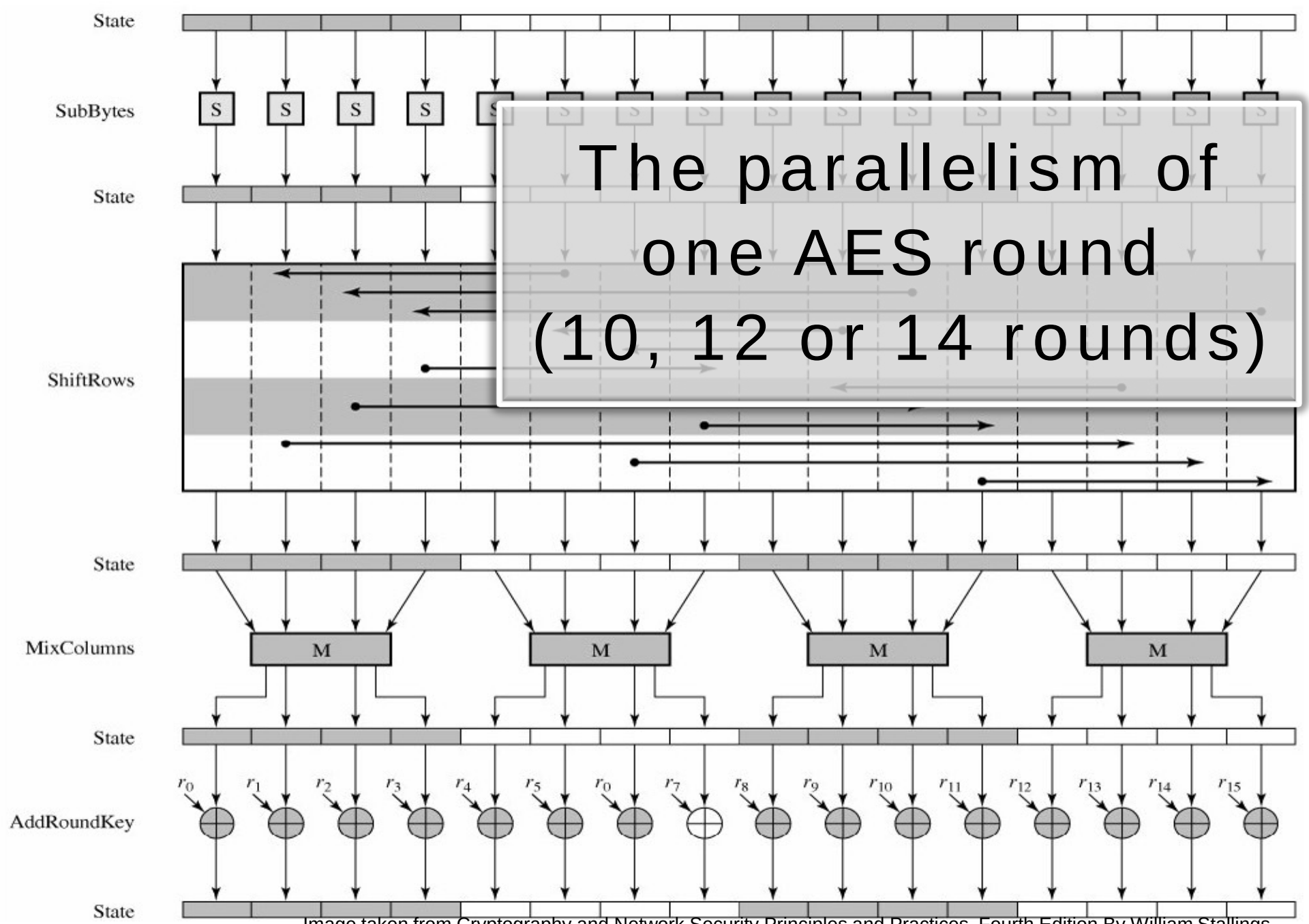
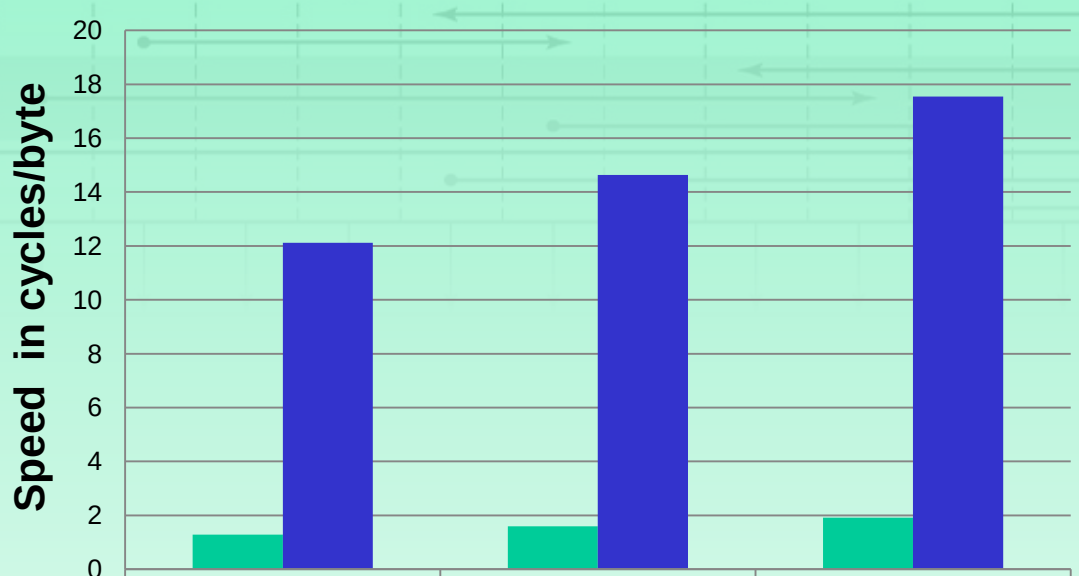


Image taken from Cryptography and Network Security Principles and Practices, Fourth Edition By William Stallings

The parallelism of one AES round

Gains with AES-NI instructions in the new Intel CPUs
SUPERCOP [D. J. Bernstein and T. Lange, 22 Oct 2011**]**



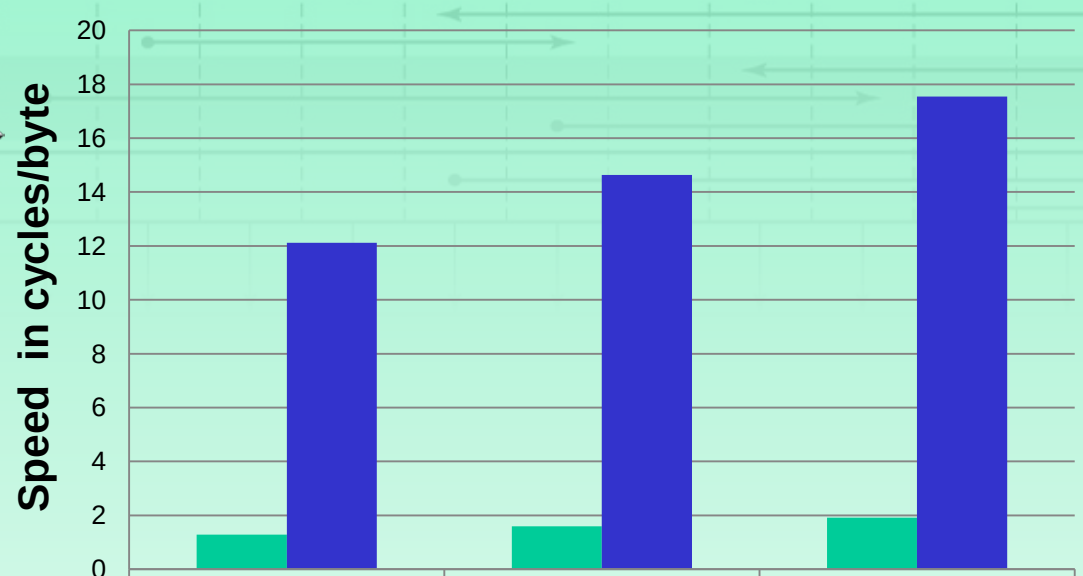
	AES128-CTR	AES192-CTR	AES256-CTR
Intel Core i7-2600K, Sandy Bridge 32nm (206a7); 2011	1.28	1.6	1.91
Intel Core 2 Duo E8400, 45nm (1067a); 2008	12.12	14.64	17.55

Image taken from Cryptography and Network Security Principles and Practices, Fourth Edition By William Stallings

The parallelism of one AES round

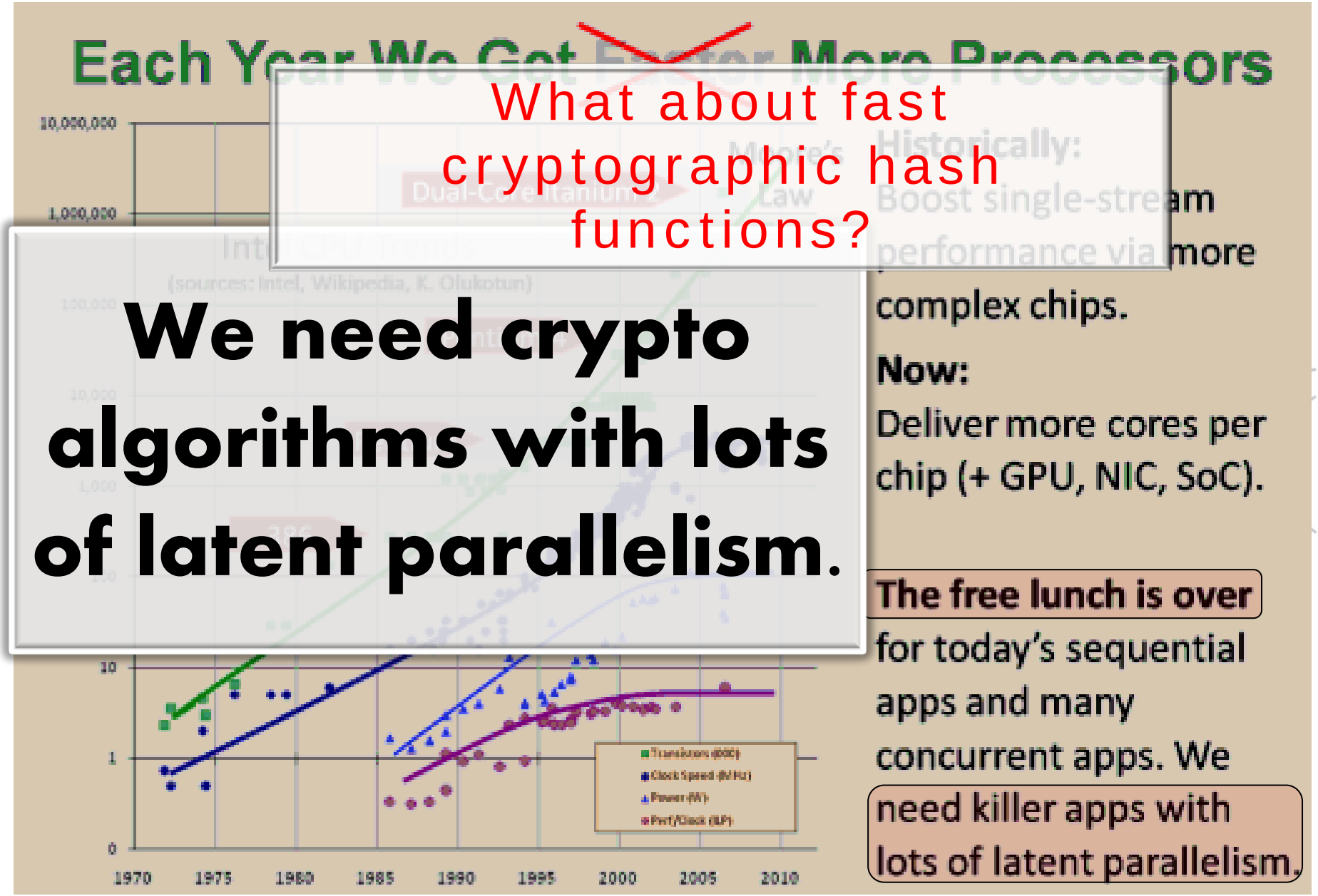
Gains with AES-NI instructions in the new Intel CPUs SUPERCOP [D. J. Bernstein and T. Lange, 22 Oct 2011]

Gains x 9



	AES128-CTR	AES192-CTR	AES256-CTR
Intel Core i7-2600K, Sandy Bridge 32nm (206a7); 2011	1.28	1.6	1.91
Intel Core 2 Duo E8400, 45nm (1067a); 2008	12.12	14.64	17.55

Image taken from Cryptography and Network Security Principles and Practices, Fourth Edition By William Stallings



What about fast cryptographic hash functions?

We need crypto algorithms with lots of latent parallelism.

Graph and comments from article by Herb Sutter, Dr. Dobb's Journal, 30(3), March 2005)

NTNU
Innovation and Creativity

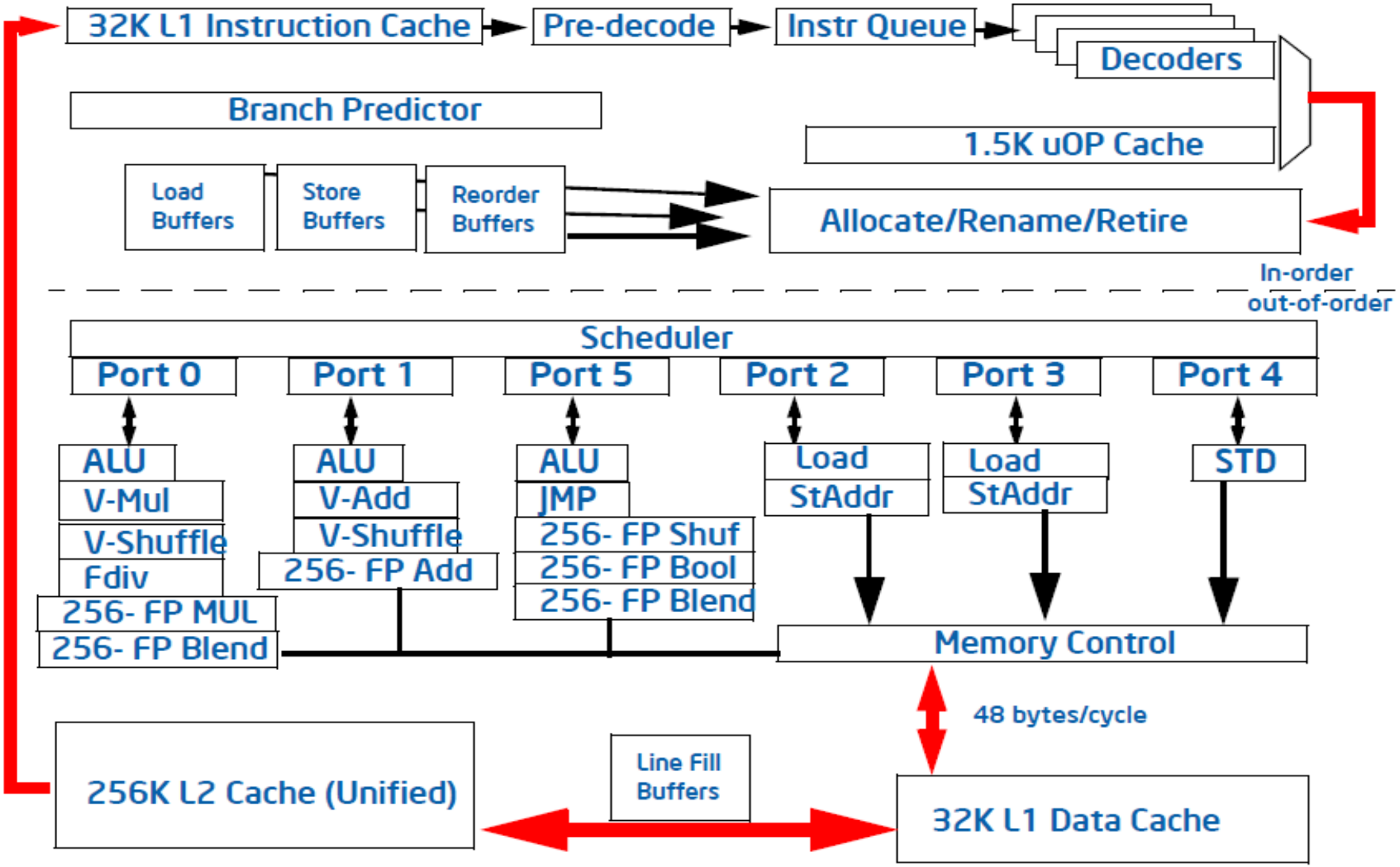


Figure 2-1. Intel microarchitecture code name Sandy Bridge Pipeline Functionality

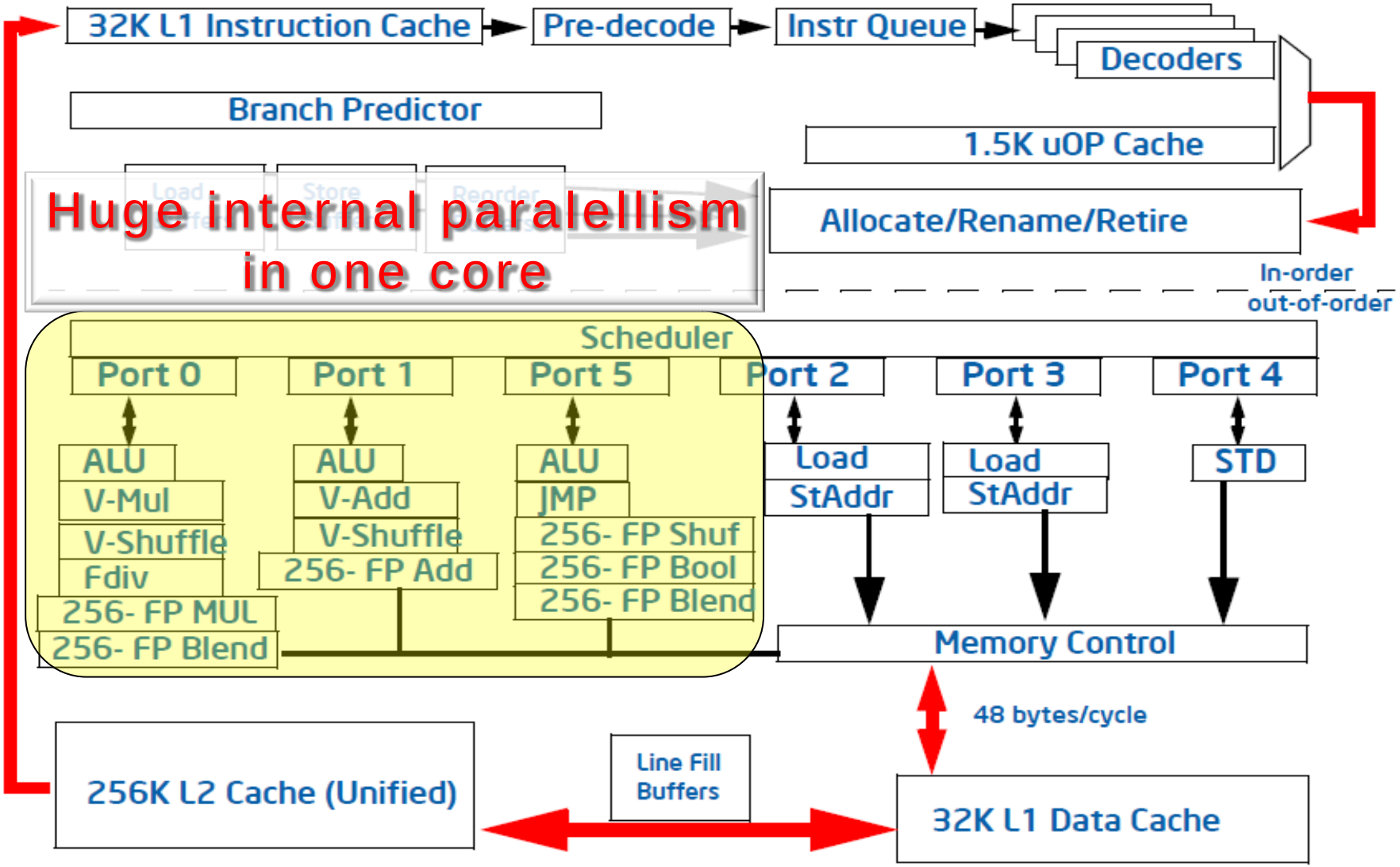


Figure 2-1. Intel microarchitecture code name Sandy Bridge Pipeline Functionality

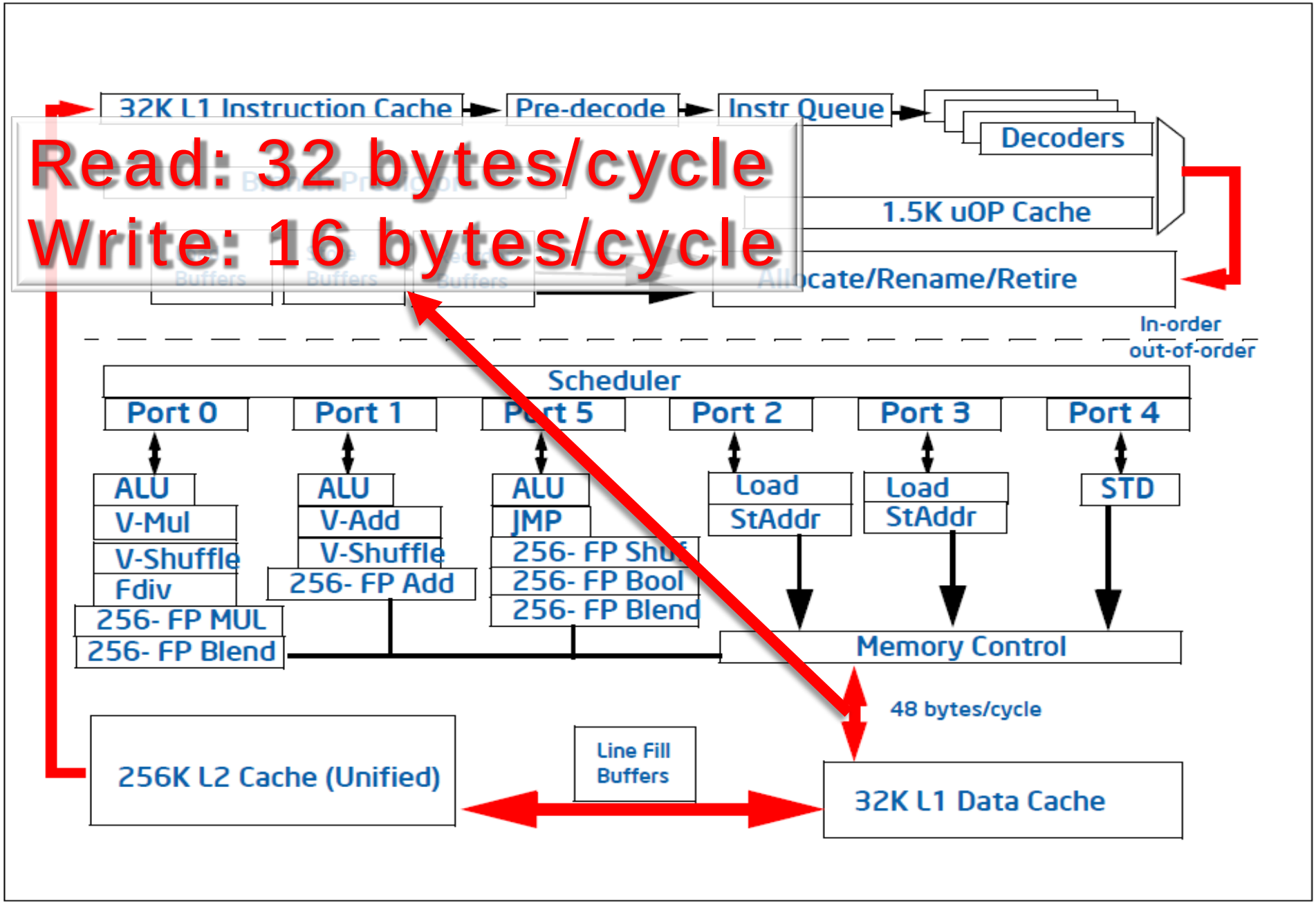


Figure 2-1. Intel microarchitecture code name Sandy Bridge Pipeline Functionality

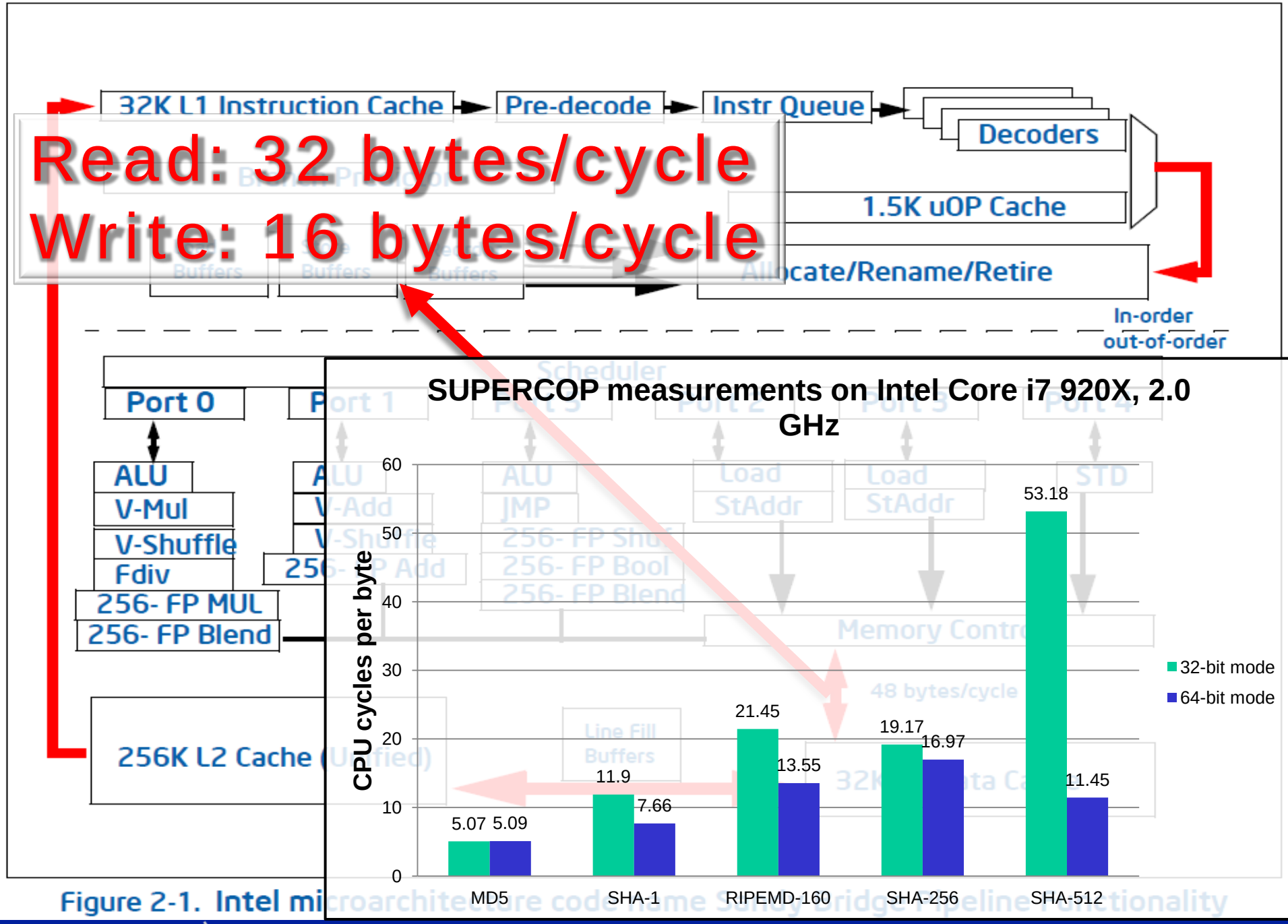


Figure 2-1. Intel microarchitecture code name Sandy Bridge Pipeline Functionality

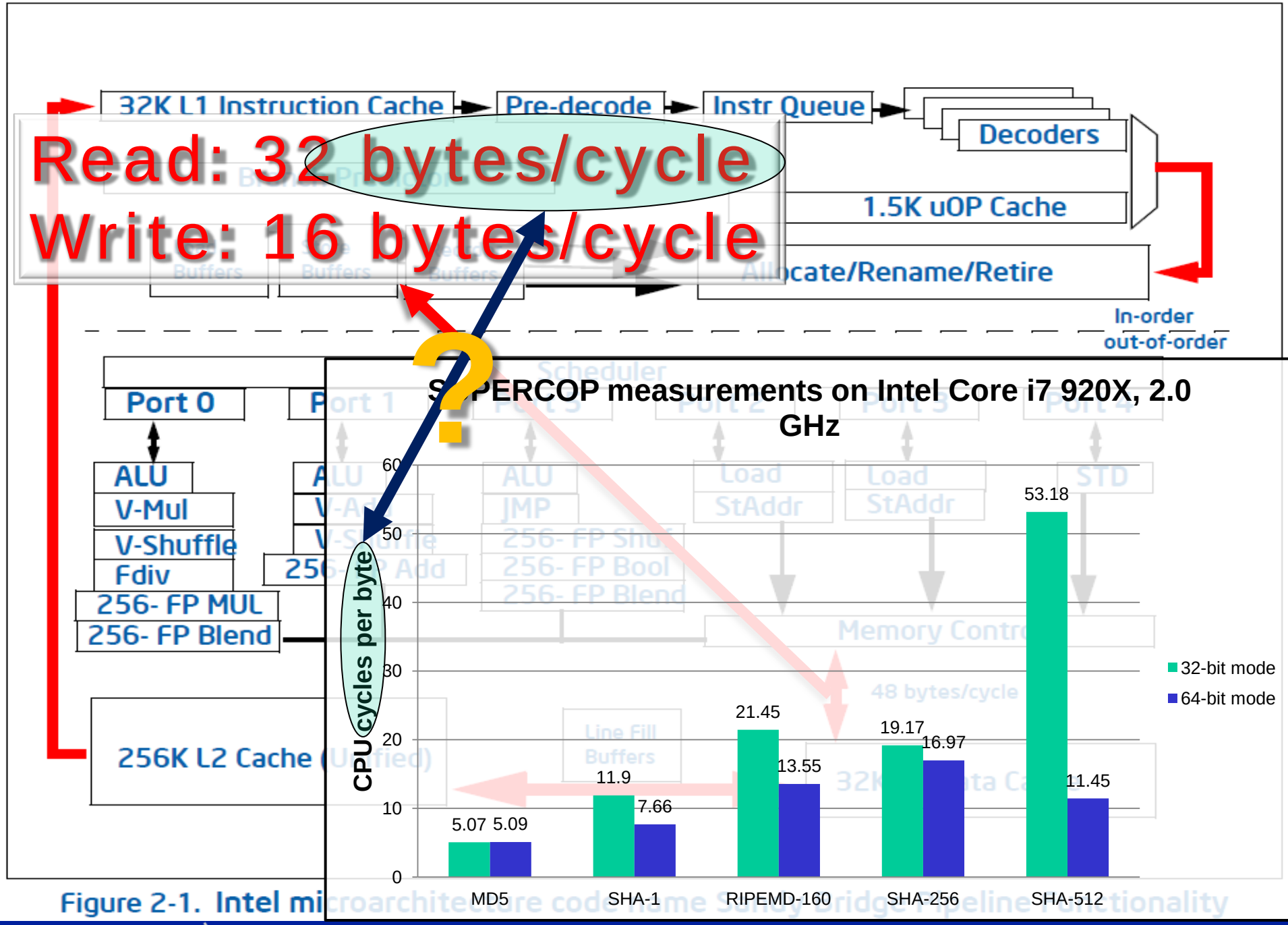


Figure 2-1. Intel microarchitecture code name Sandy Bridge Pipeline Functionality

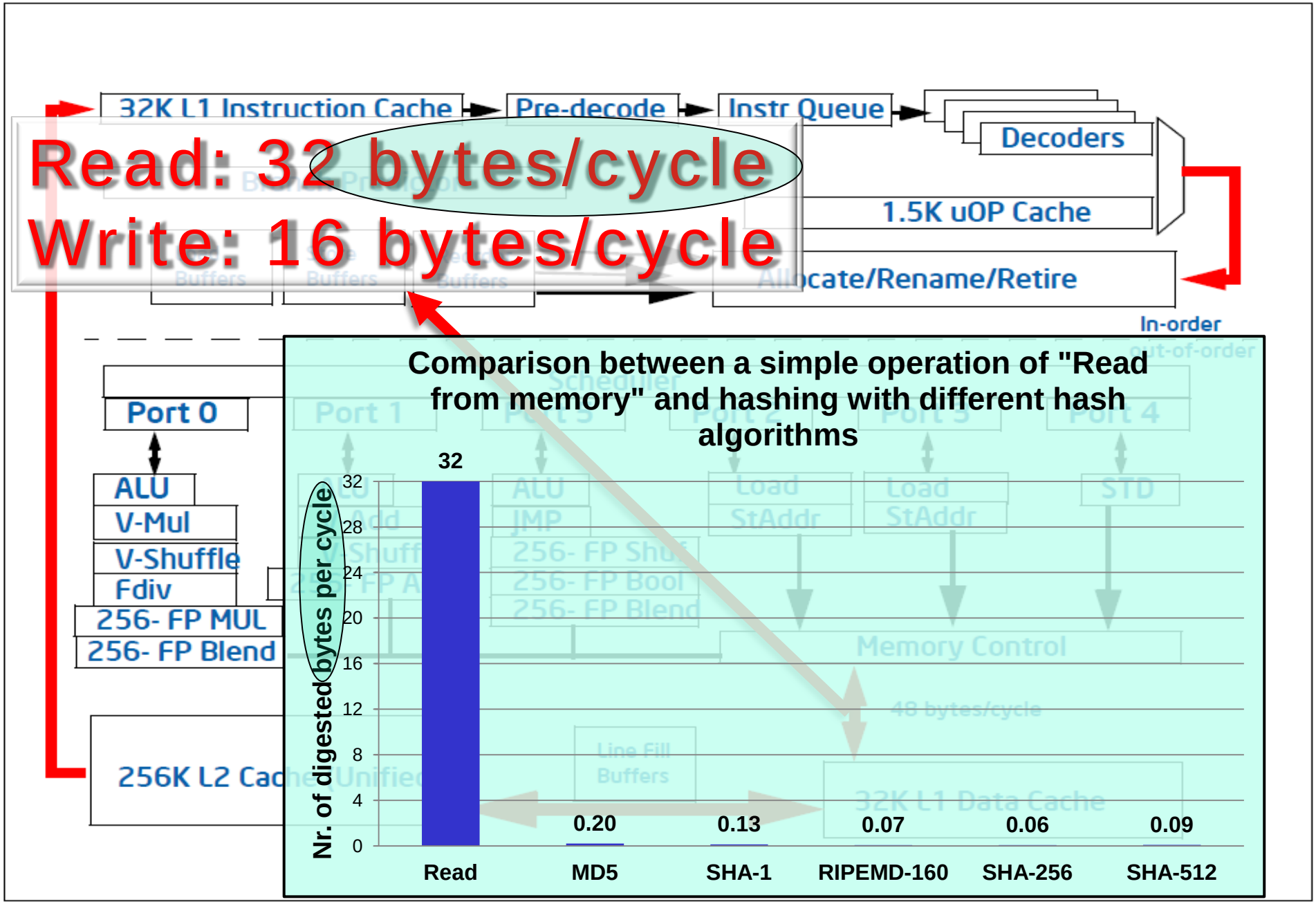


Figure 2-1. Intel microarchitecture code name Sandy Bridge Pipeline Functionality

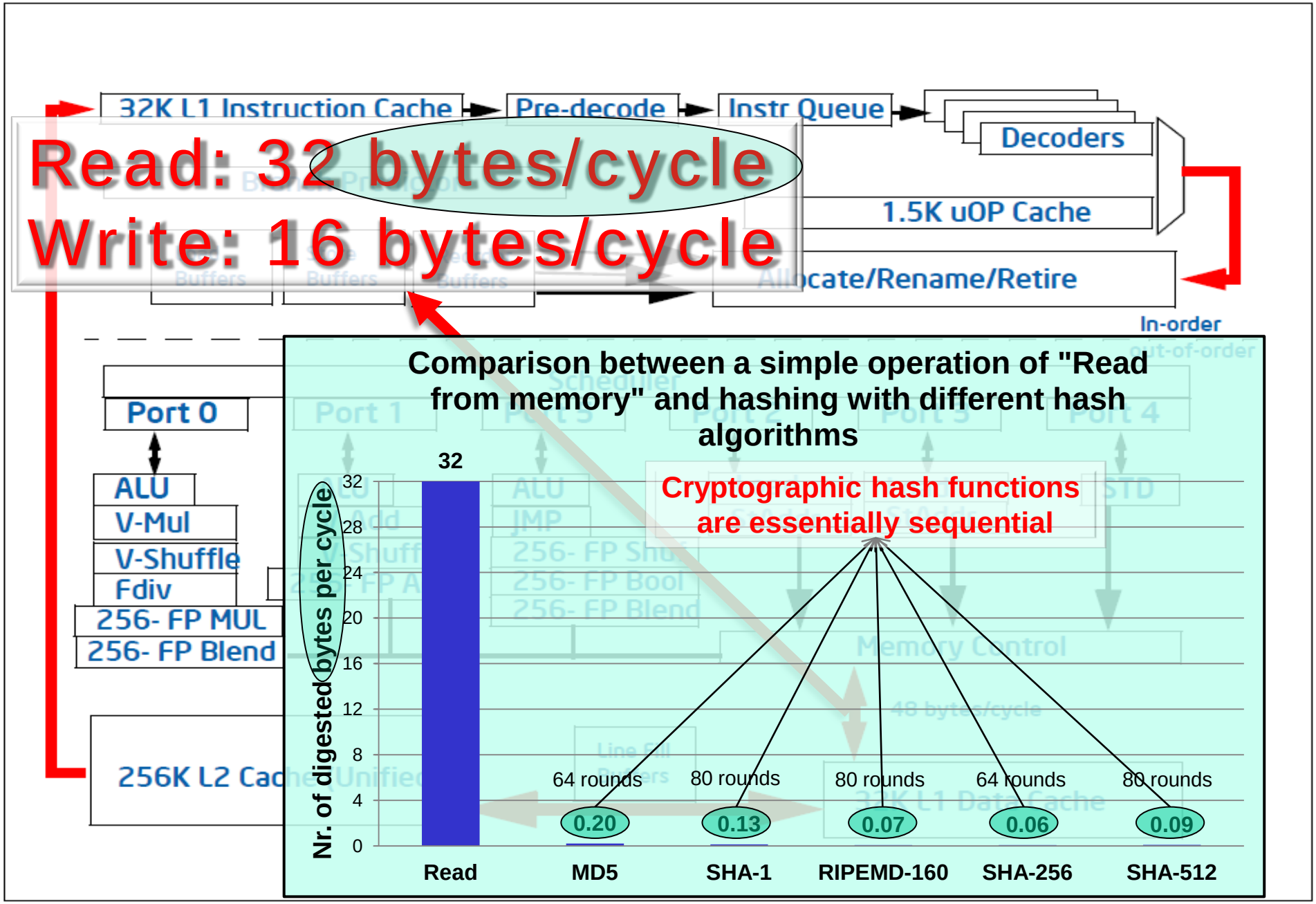
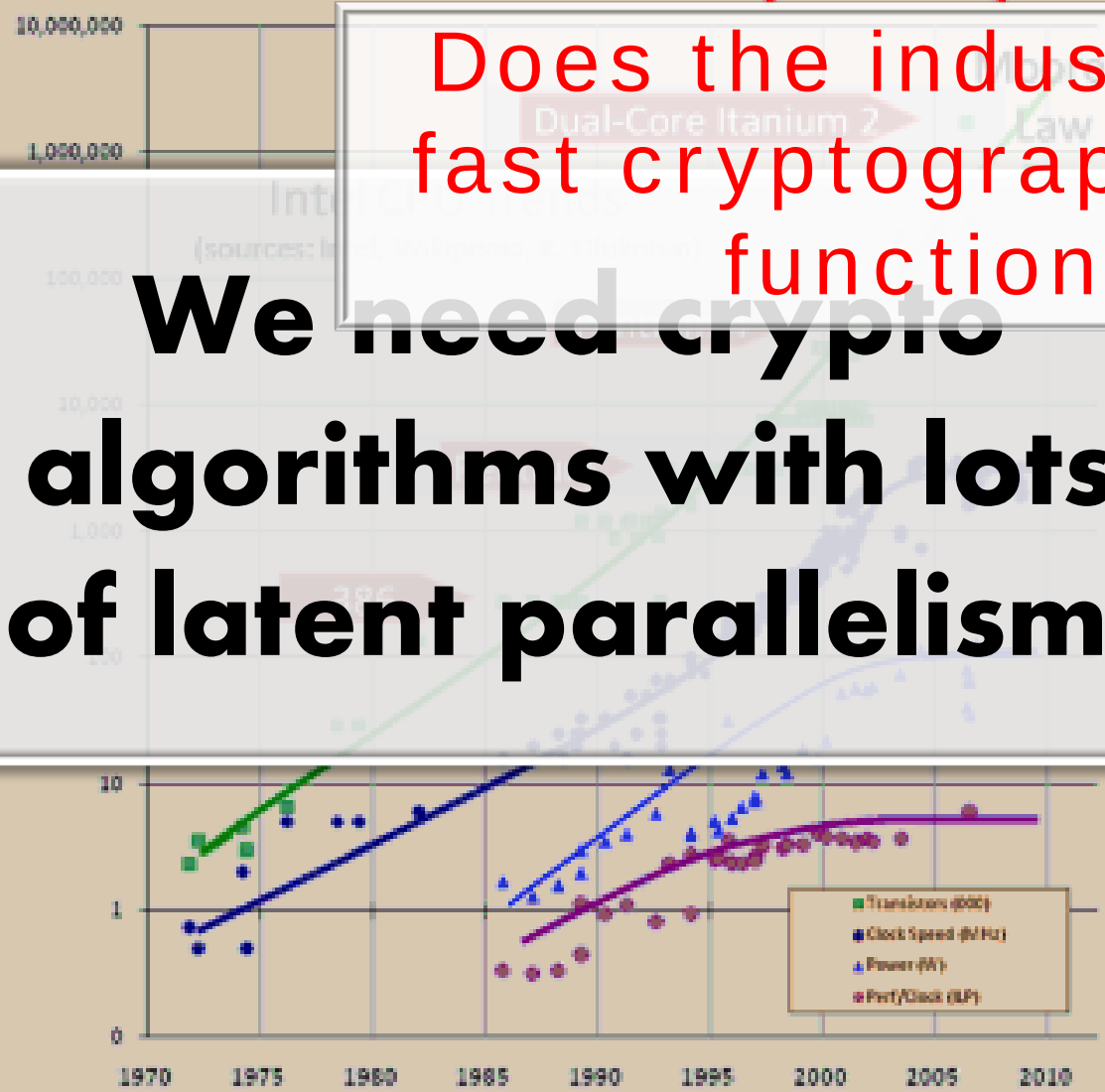


Figure 2-1. Intel microarchitecture code name Sandy Bridge Pipeline Functionality

Each Year We Get ~~Faster~~ More Processors

Does the industry need fast cryptographic hash functions?

We need crypto algorithms with lots of latent parallelism.



Boost single-stream performance via more complex chips.

Now:

Deliver more cores per chip (+ GPU, NIC, SoC).

The free lunch is over for today's sequential apps and many concurrent apps. We need killer apps with lots of latent parallelism.

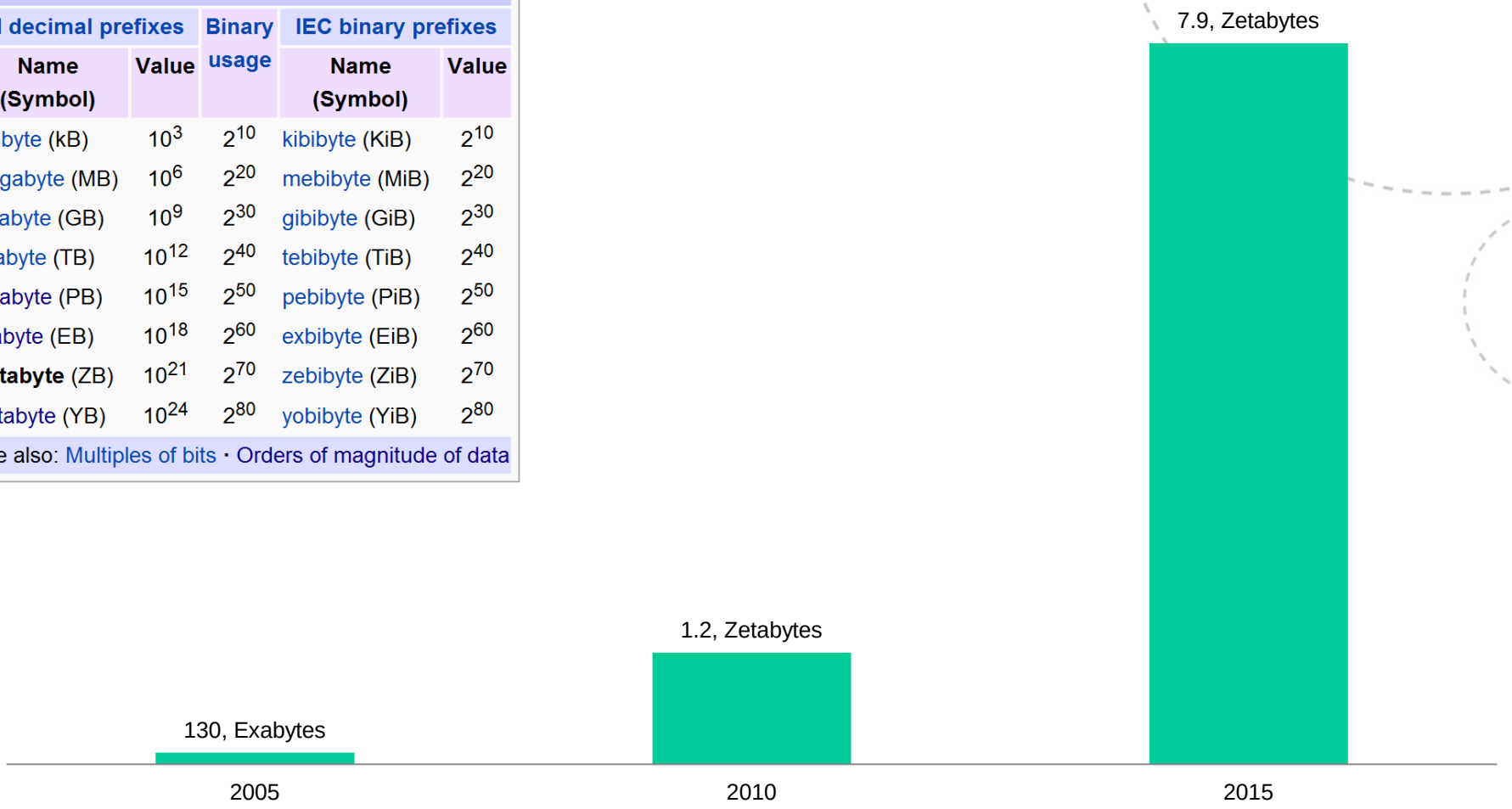
Graph and comments from article by Herb Sutter, Dr. Dobb's Journal, 30(3), March 2005)

NTNU
Innovation and Creativity

Total data storage in the world

Source: IDC's Digital Universe Study, sponsored by EMC, June 2011

Multiples of bytes				v · d · e
SI decimal prefixes		Binary usage	IEC binary prefixes	
Name (Symbol)	Value		Name (Symbol)	Value
kilobyte (kB)	10^3	2^{10}	kibibyte (KiB)	2^{10}
megabyte (MB)	10^6	2^{20}	mebibyte (MiB)	2^{20}
gigabyte (GB)	10^9	2^{30}	gibibyte (GiB)	2^{30}
terabyte (TB)	10^{12}	2^{40}	tebibyte (TiB)	2^{40}
petabyte (PB)	10^{15}	2^{50}	pebibyte (PiB)	2^{50}
exabyte (EB)	10^{18}	2^{60}	exbibyte (EiB)	2^{60}
zettabyte (ZB)	10^{21}	2^{70}	zebibyte (ZiB)	2^{70}
yottabyte (YB)	10^{24}	2^{80}	yobibyte (YiB)	2^{80}
See also: Multiples of bits · Orders of magnitude of data				



NTNU
Innovation and Creativity

OpenStack - open source software for building private and public clouds

OpenStack - open source software for building private and public clouds

July 2010

Nova: computer processing services

Swift: storage services

Use of cryptographic hash functions in OpenStack Object Storage

- Object Storage documentation on use of MD5
- *"Various hashing algorithms were tried. **SHA** offers better security, but the ring doesn't need to be cryptographically secure and SHA is slower. **Murmur** was much faster, but **MD5** was built-in and hash computation is a small percentage of the overall request handling time. In all, once it was decided the servers wouldn't be maintaining the rings themselves anyway and only doing hash lookups, MD5 was chosen for its general availability, good distribution and adequate speed."*

NTNU
Innovation and Creativity

- The Apache™ Hadoop™ project develops open-source software for reliable, scalable, distributed computing.
- The project includes these subprojects:
  - **Hadoop Common**: The common utilities that support the other Hadoop subprojects.
  - **Hadoop Distributed File System (HDFS™)**: A distributed file system that provides high-throughput access to application data.
  - **Hadoop MapReduce**: A software framework for distributed processing of large data sets on compute clusters.
- Default block size is 64MB, but frequently is 128MB or even more

Hadoop Distributed File System (HDFS™)

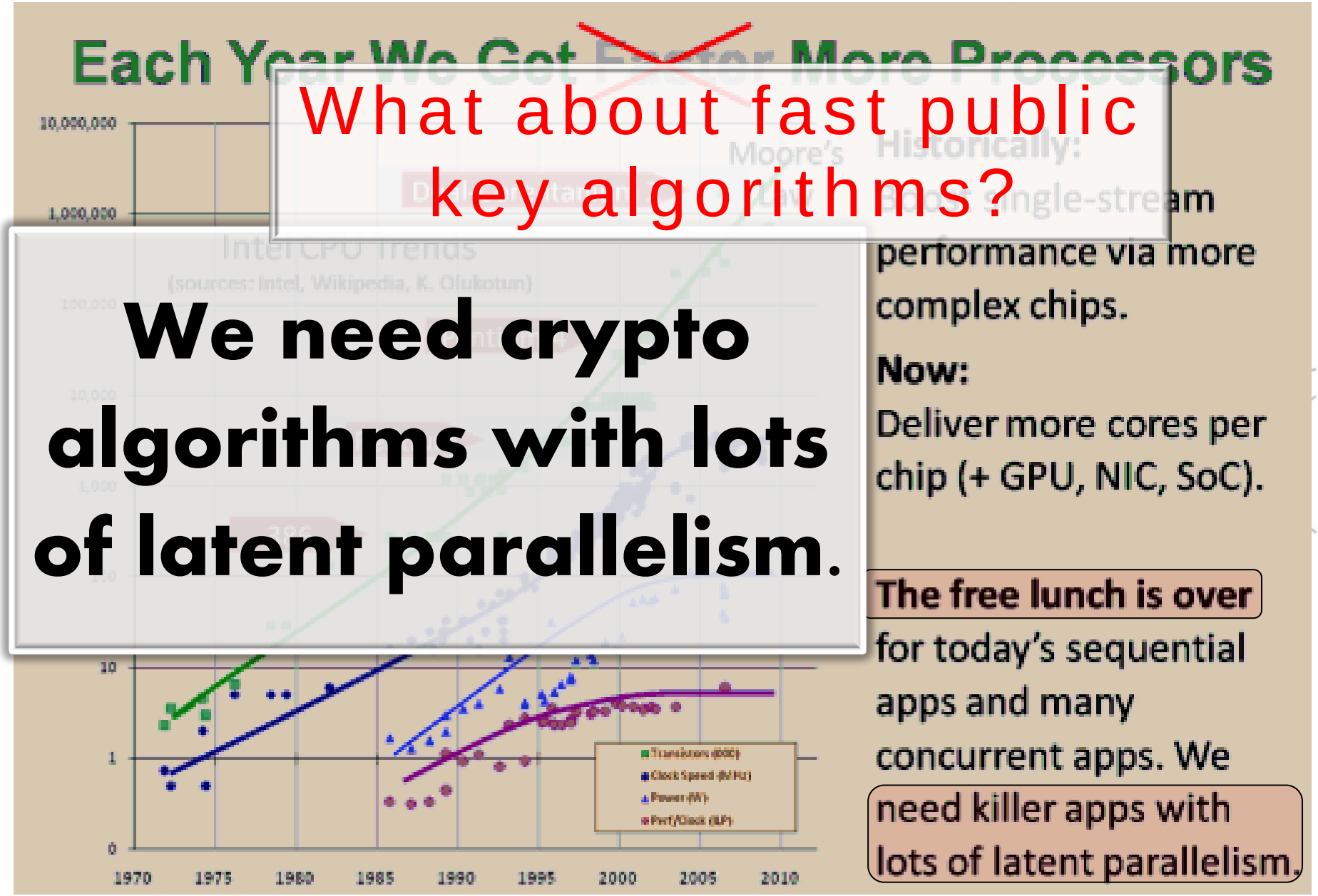
- Hadoop's internal Distributed hash-checksum mechanic:
  - Saving the **CRC32** of every 512 bytes (per block) and then doing a **MD5 hash** on that.
  - Then when the "getFileChecksum()" method is called, each block for a file sends its **MD5 hash** to a collector which are gathered together and a **MD5 hash** is calculated for all of the block hashes.

NTNU
Innovation and Creativity

The use of MD5 cryptographic hash function

- The same mistake as WEP designers did for the wireless security
- But it is understandable because programmers and engineers need fast digesting functions
- The big cloud computing projects that deal with thousands of petabytes would benefit a lot from a cryptographic hash function that is **significantly faster than MD5**

NTNU
Innovation and Creativity

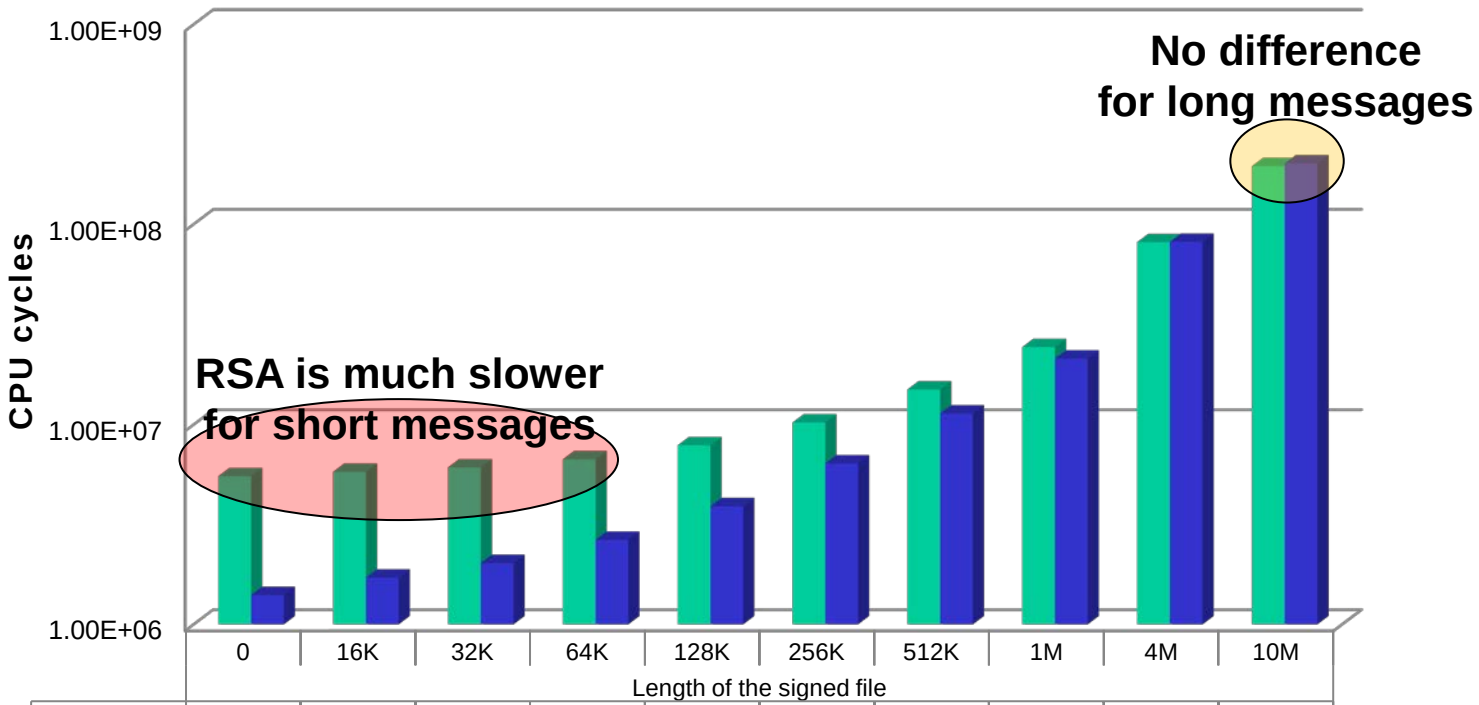


Graph and comments from article by Herb Sutter, Dr. Dobb's Journal, 30(3), March 2005)

NTNU
Innovation and Creativity

Operations in most popular public key algorithms are essentially sequential

Signing time (file size from 0 to 10M)

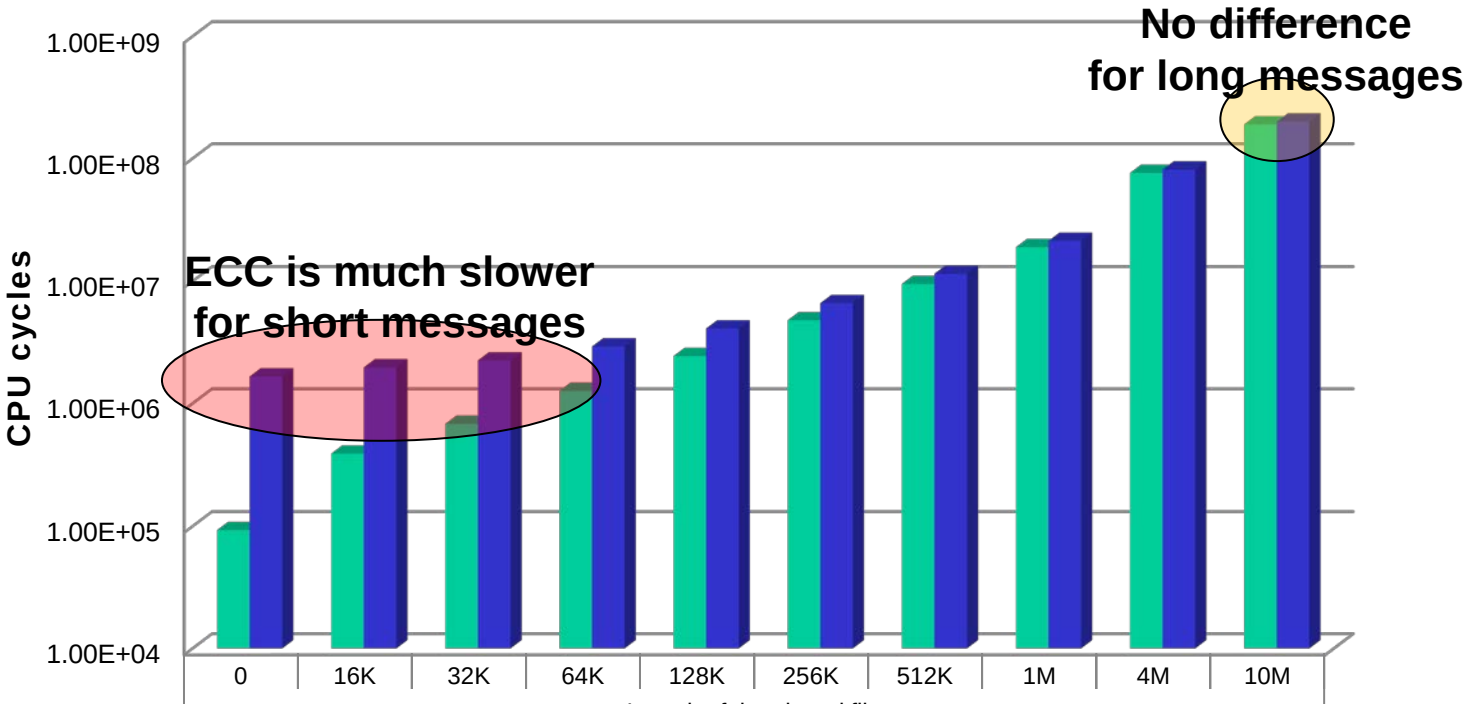


	0	16K	32K	64K	128K	256K	512K	1M	4M	10M
RSA1536	5.51E+06	5.80E+06	6.10E+06	6.70E+06	7.87E+06	1.02E+07	1.50E+07	2.44E+07	8.12E+07	1.95E+08
ECDSA192	1.40E+06	1.71E+06	2.03E+06	2.65E+06	3.90E+06	6.38E+06	1.14E+07	2.14E+07	8.16E+07	2.02E+08

NTNU
Innovation and Creativity

Operations in most popular public key algorithms are essentially sequential

Verification time (file size from 0 to 10M)

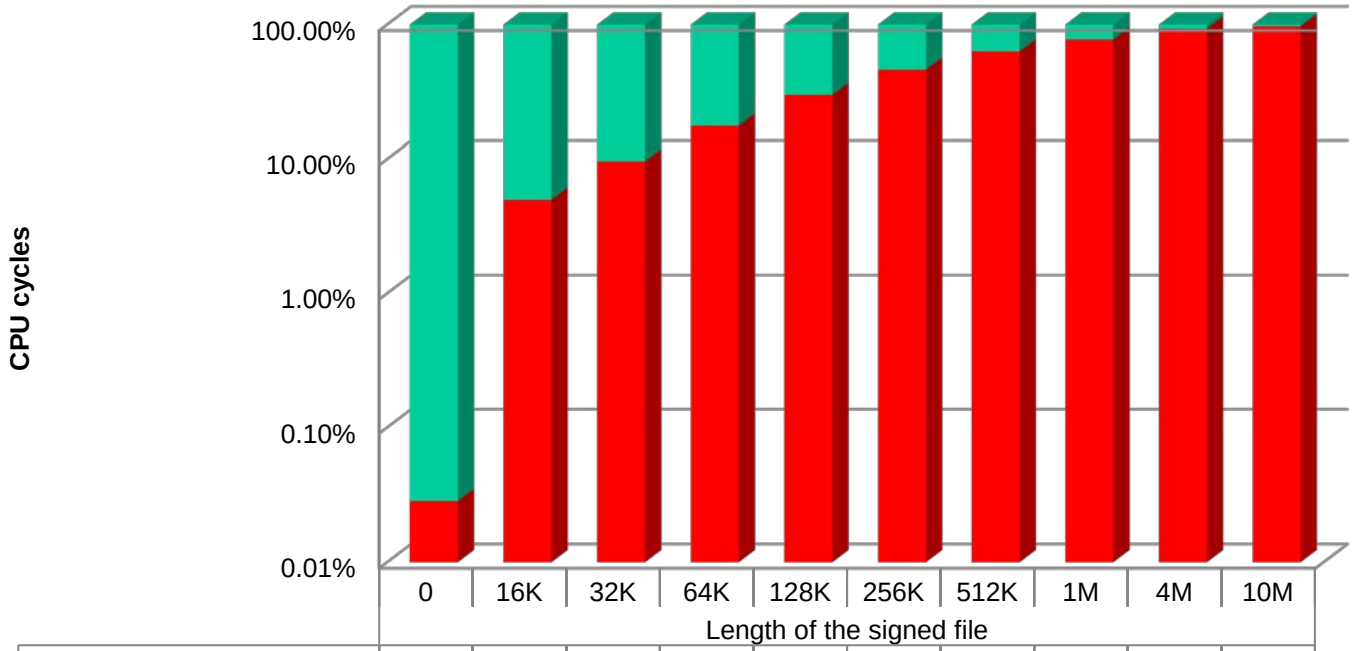


	0	16K	32K	64K	128K	256K	512K	1M	4M	10M
RSA1536	9.30E+04	3.88E+05	6.80E+05	1.27E+06	2.44E+06	4.79E+06	9.49E+06	1.90E+07	7.61E+07	1.90E+08
ECDSA192	1.66E+06	1.97E+06	2.25E+06	2.92E+06	4.10E+06	6.61E+06	1.15E+07	2.14E+07	8.10E+07	2.00E+08

NTNU
Innovation and Creativity

Digital signatures are composed of two cryptographic operations (hashing and public key operations that in this moment are essentially sequential)

Signing time with RSA1536 vs hashing time with SHA256

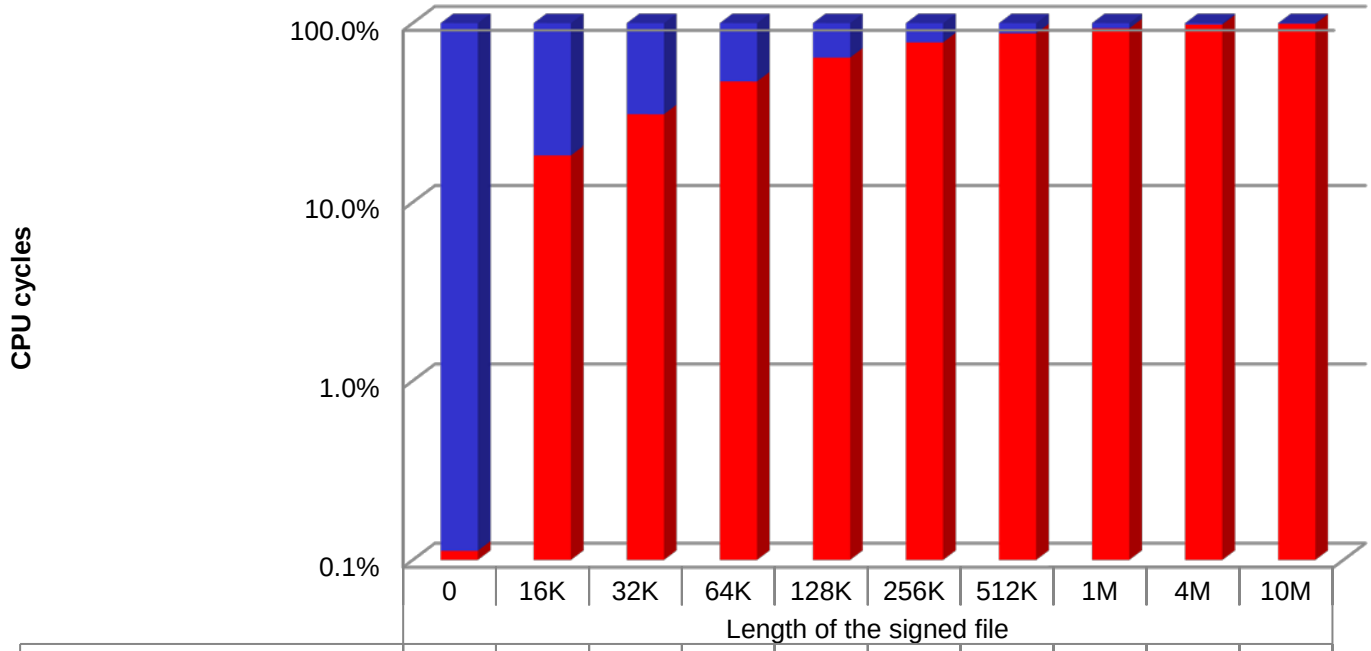


	0	16K	32K	64K	128K	256K	512K	1M	4M	10M
RSA1536 Signing	99.97%	95.0%	90.4%	82.3%	70.0%	53.8%	36.8%	22.6%	6.8%	2.8%
RSA1536 SHA256 Hashing	0.03%	5.0%	9.6%	17.7%	30.0%	46.2%	63.2%	77.4%	93.2%	97.2%

NTNU
Innovation and Creativity

Digital signatures are composed of two cryptographic operations (hashing and public key operations that in this moment are essentially sequential)

Signing time with ECDSA192 vs hashing time with SHA256



	0	16K	32K	64K	128K	256K	512K	1M	4M	10M
ECDSA192 Signing	99.9%	81.7%	69.1%	52.9%	35.9%	21.9%	12.3%	6.5%	1.7%	0.7%
ECDSA192 SHA256 Hashing	0.1%	18.3%	30.9%	47.1%	64.1%	78.1%	87.7%	93.5%	98.3%	99.3%

NTNU
Innovation and Creativity

Public key security recommendations vs reality

Security level	2^{80}	2^{96}	2^{112}	2^{128}	2^{192}	2^{256}
RSA/DSA	1024	1536	2048	3072	7680	15360
ECDSA	160	192	224	256	384	512

- A generally accepted position is that for the period 2010 - 2030, the minimum security level should be at least 112 bits, and beyond 2030 the minimum security level should be 128 bits.
- Still, a lot of organizations that use the public key cryptography are using security levels of 80 or 96 bits.

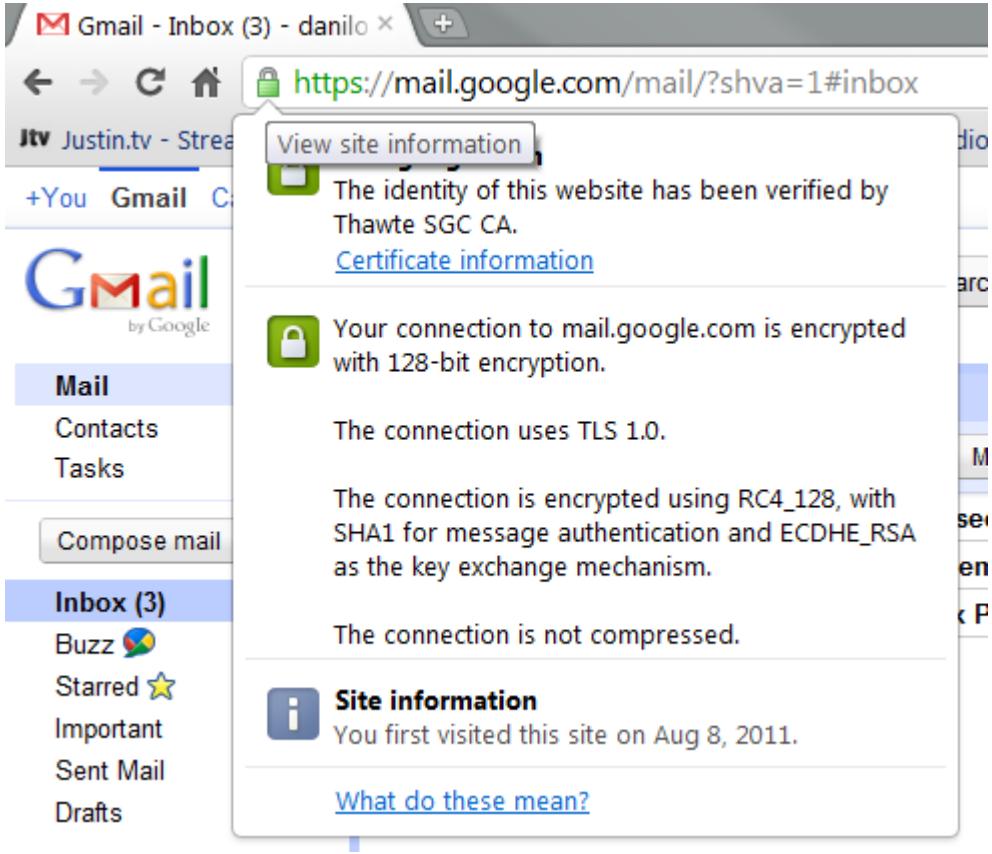
NTNU
Innovation and Creativity

Public key security recommendations vs reality

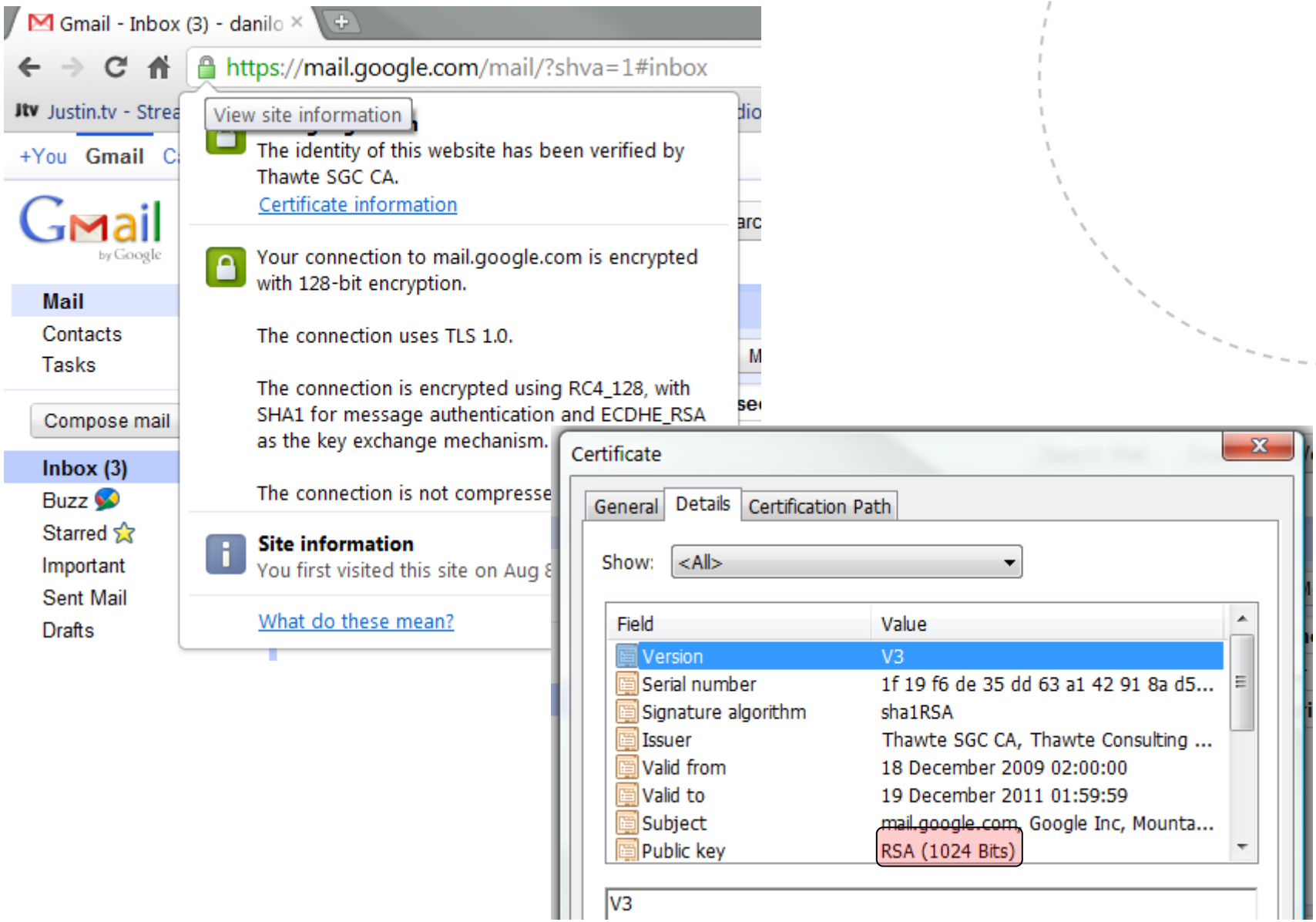
Security level	2^{80}	2^{96}	2^{112}	2^{128}	2^{192}	2^{256}
RSA/DSA	1024	1536	2048	3072	7680	15360
ECDSA	160	192	224	256	384	512

- A generally accepted position is that for the period 2010 - 2030, the minimum security level should be at least 112 bits, and beyond 2030 the minimum security level should be 128 bits.
- Still, a lot of organizations that use the public key cryptography are using security levels of 80 or 96 bits.

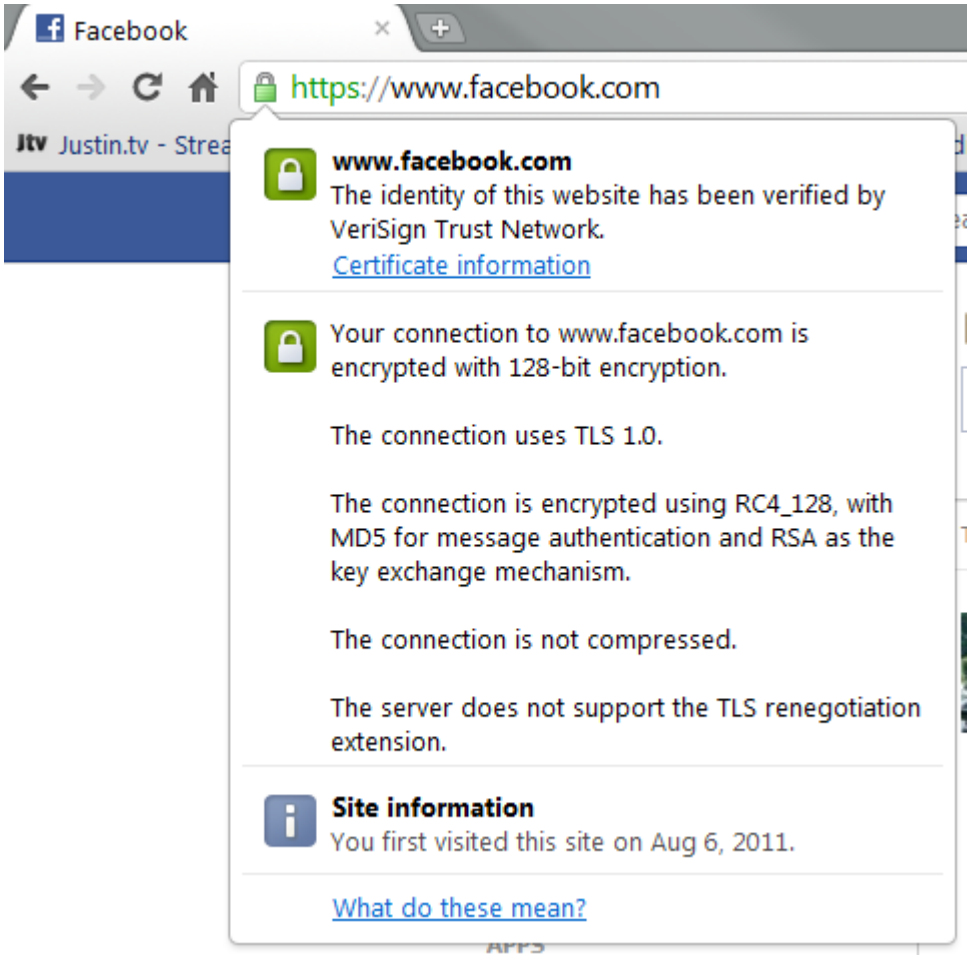
NTNU
Innovation and Creativity



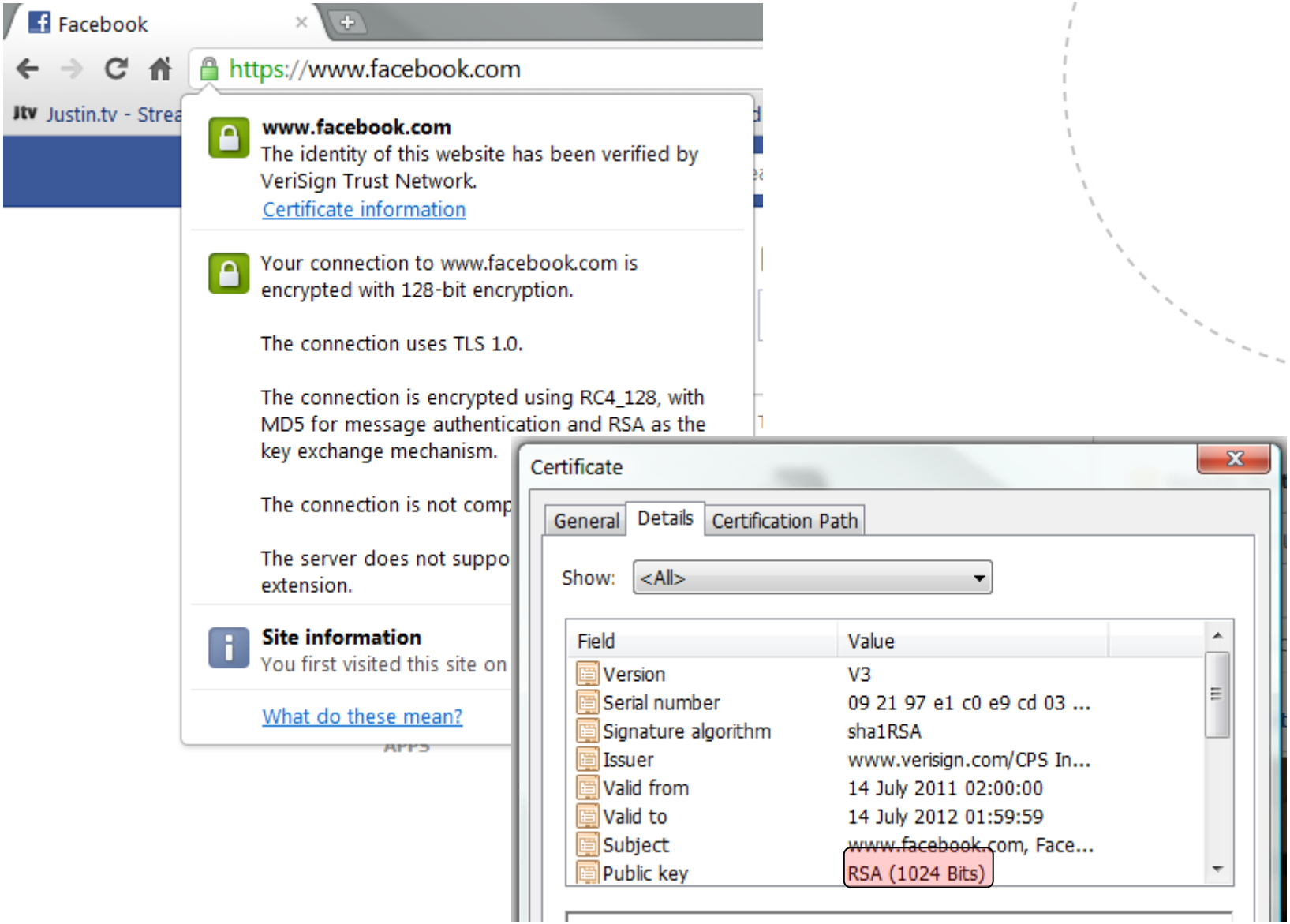
NTNU
Innovation and Creativity



NTNU
Innovation and Creativity

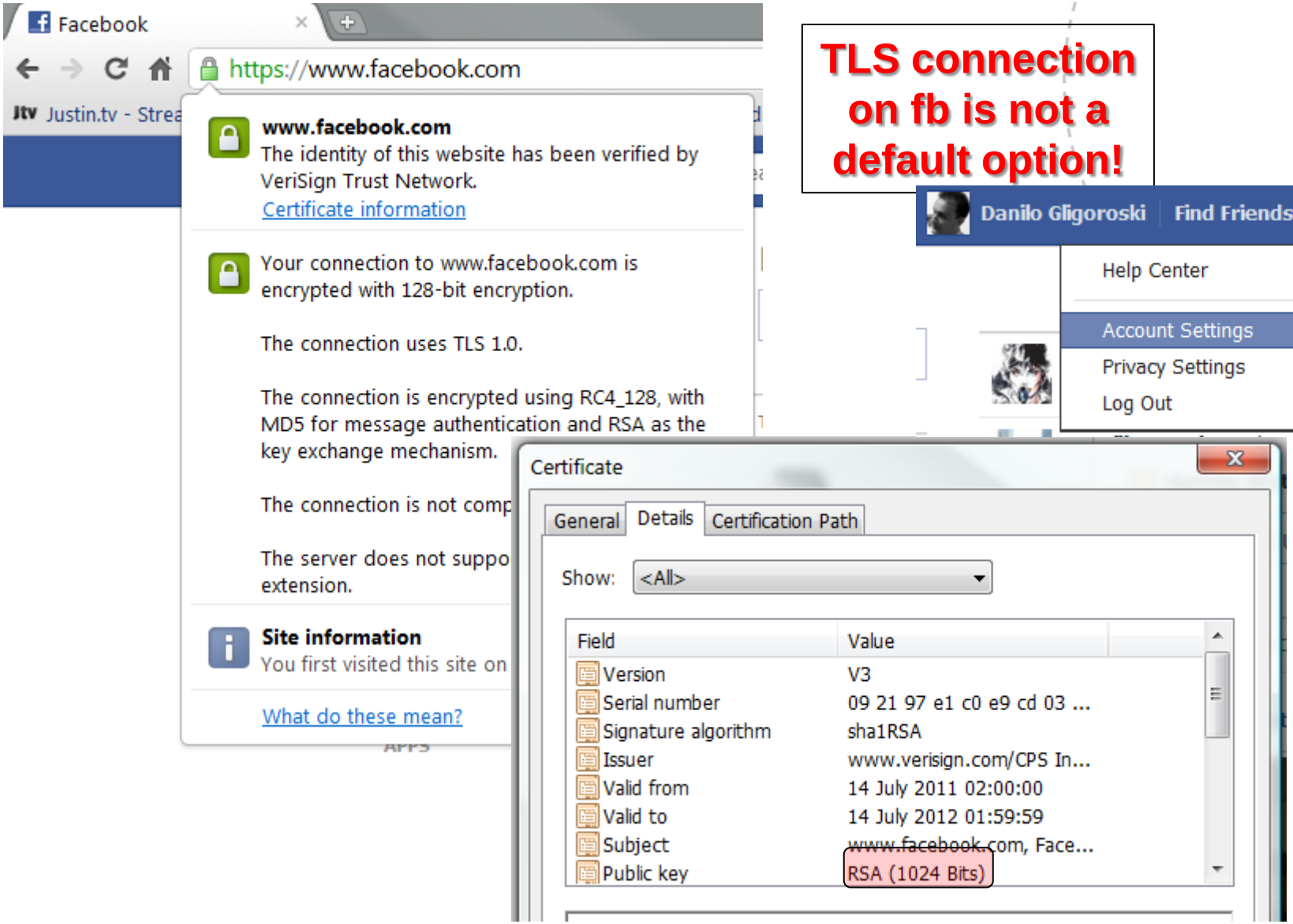


NTNU
Innovation and Creativity

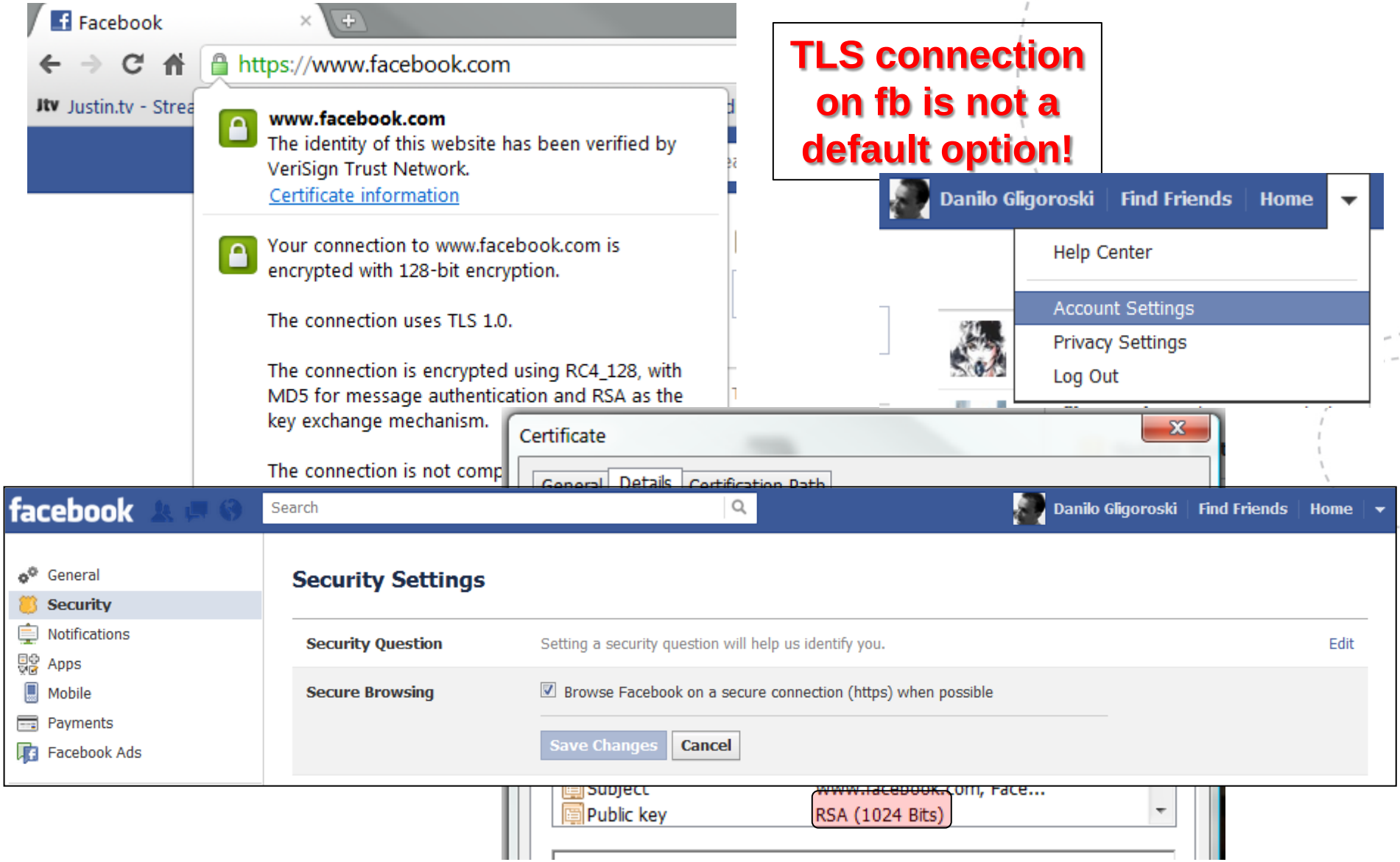


NTNU
Innovation and Creativity

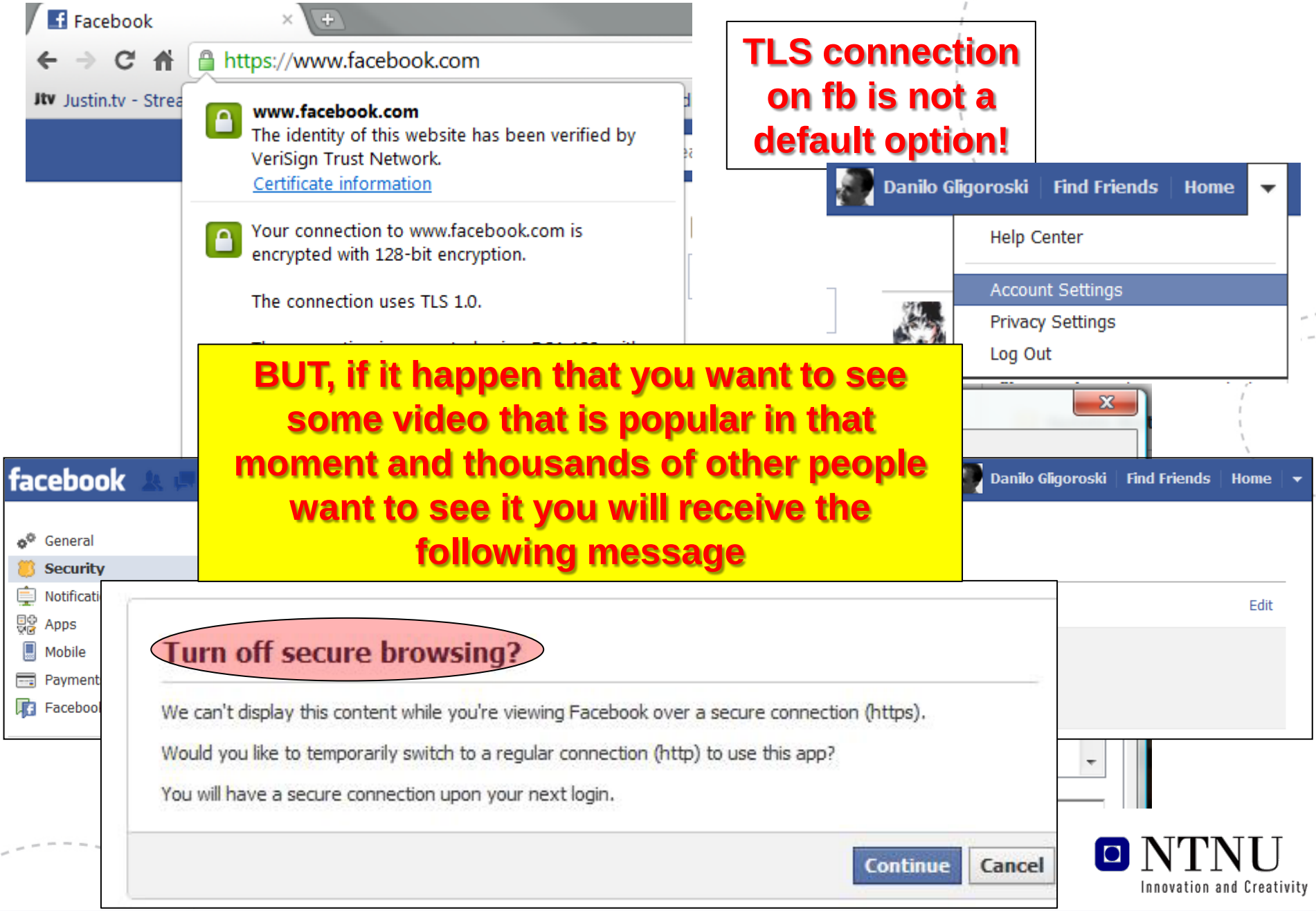
TLS connection on fb is not a default option!



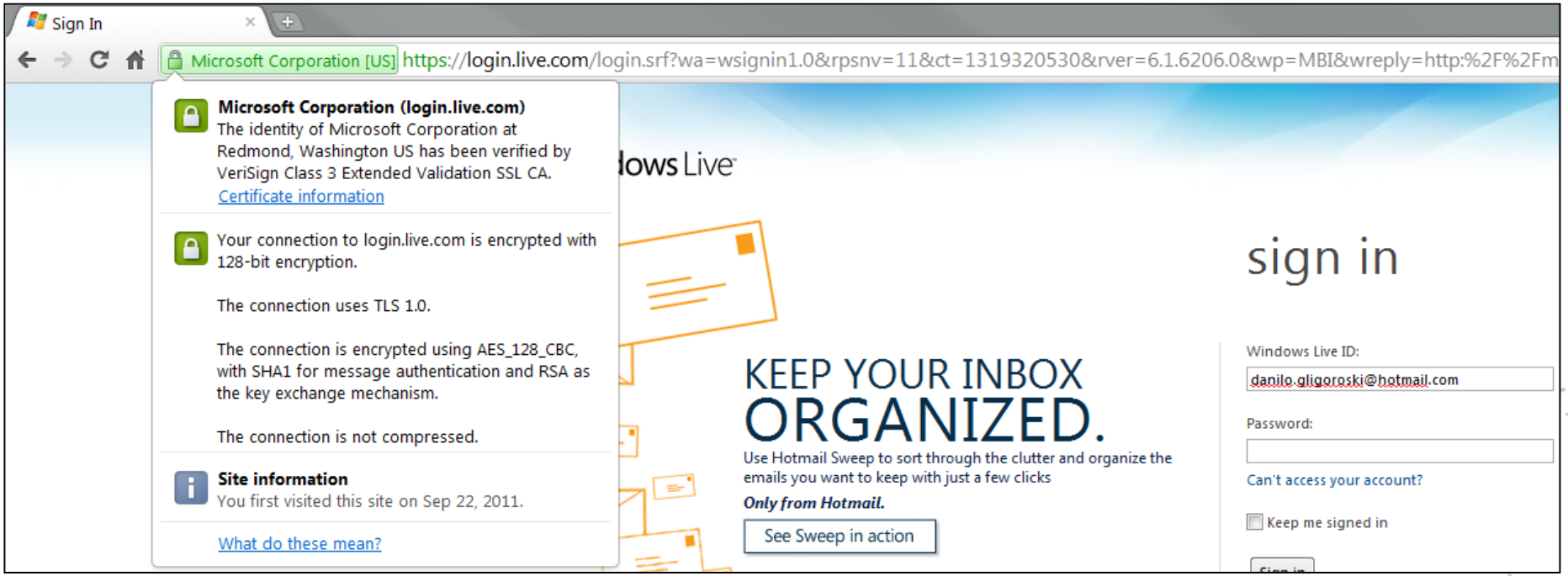
NTNU
Innovation and Creativity

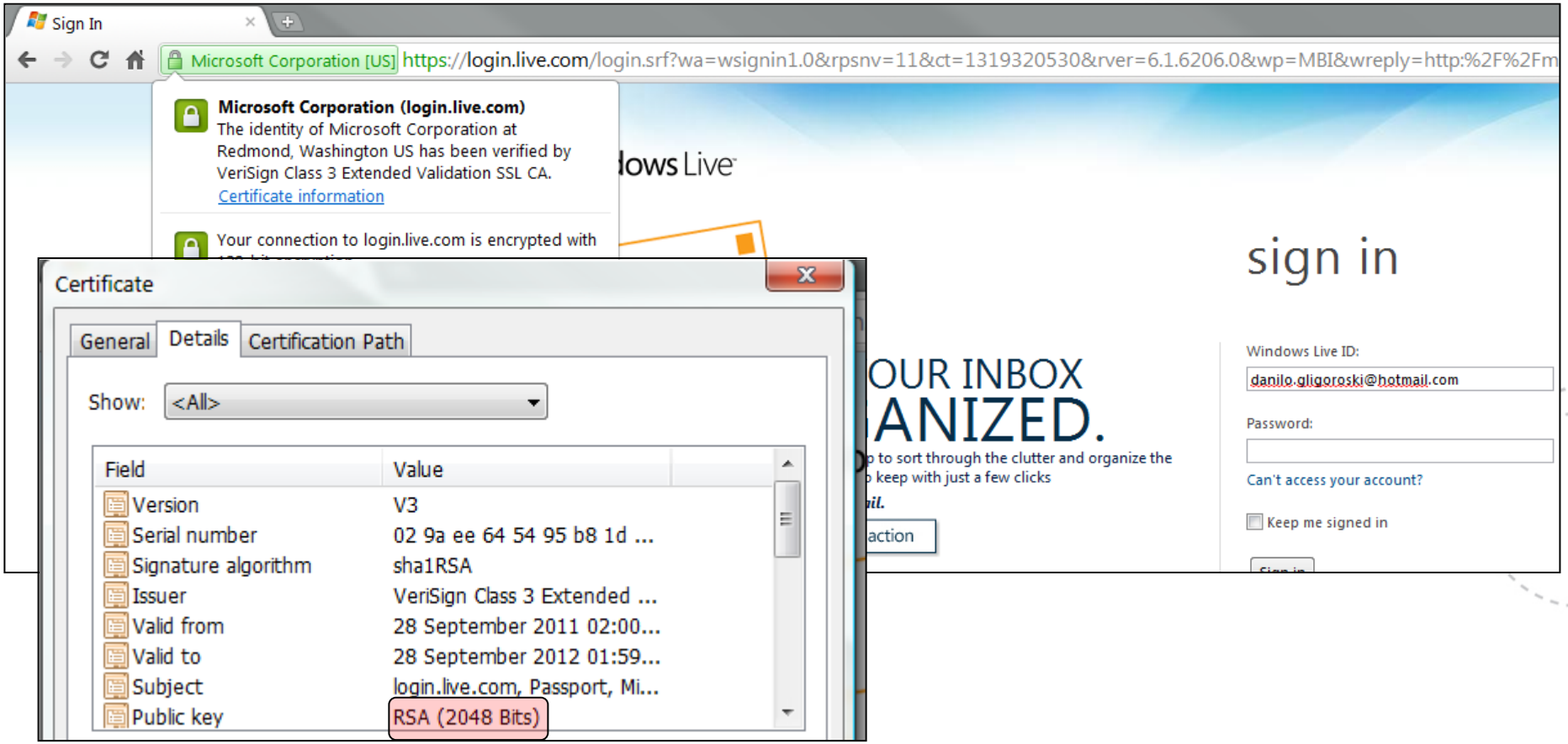


NTNU
Innovation and Creativity

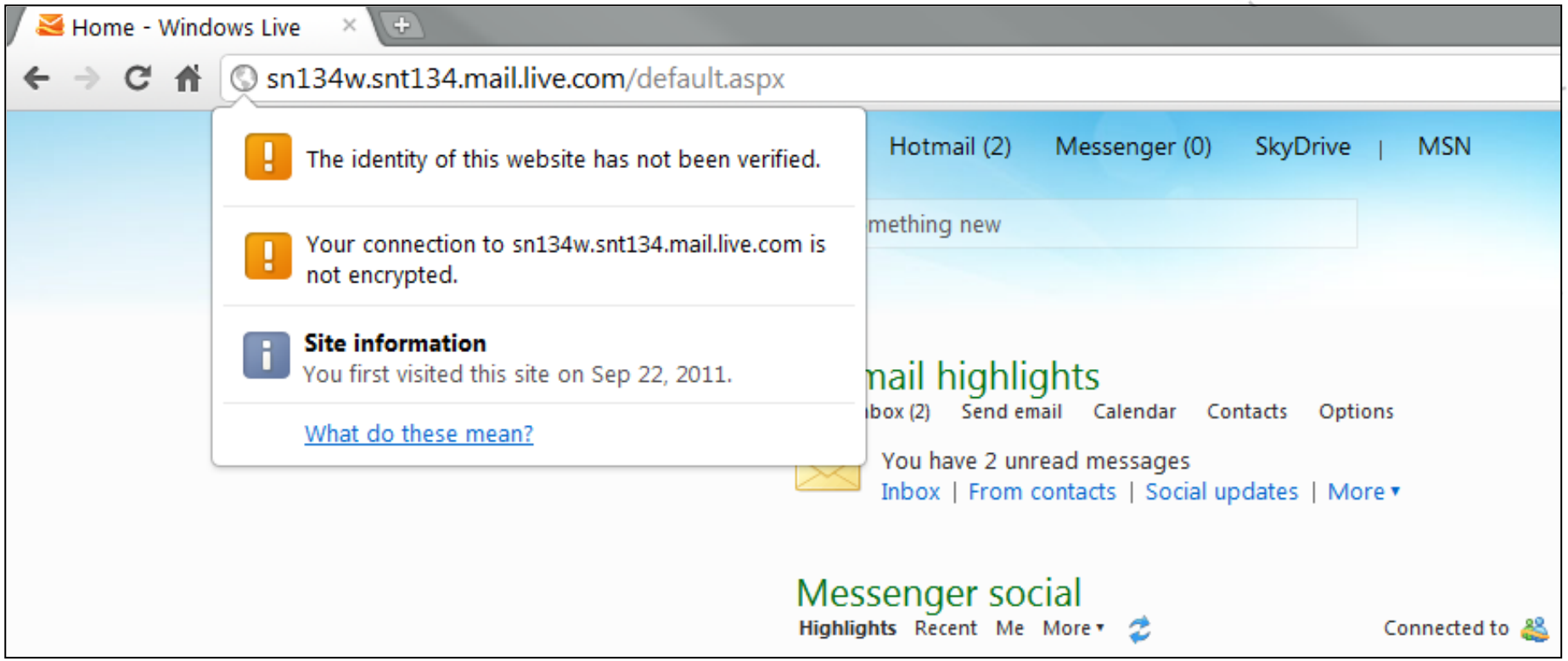


NTNU
Innovation and Creativity


Sign In
Microsoft Corporation [US]
https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1319320530&rver=6.1.6206.0&wp=MBI&wreply=http:%2F%2Fm
Microsoft Corporation (login.live.com)
The identity of Microsoft Corporation at Redmond, Washington US has been verified by VeriSign Class 3 Extended Validation SSL CA.
Certificate information
Your connection to login.live.com is encrypted with 128-bit encryption.
The connection uses TLS 1.0.
The connection is encrypted using AES_128_CBC, with SHA1 for message authentication and RSA as the key exchange mechanism.
The connection is not compressed.
Site information
You first visited this site on Sep 22, 2011.
What do these mean?
dows Live
KEEP YOUR INBOX
ORGANIZED.
Use Hotmail Sweep to sort through the clutter and organize the emails you want to keep with just a few clicks
Only from Hotmail.
See Sweep in action
sign in
Windows Live ID:
danilo.gligoroski@hotmail.com
Password:
Can't access your account?
Keep me signed in


Sign In
Microsoft Corporation [US]
https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1319320530&rver=6.1.6206.0&wp=MBI&wreply=http:%2F%2Fm
Microsoft Corporation (login.live.com)
The identity of Microsoft Corporation at Redmond, Washington US has been verified by VeriSign Class 3 Extended Validation SSL CA.
Certificate information
Your connection to login.live.com is encrypted with
Certificate
General
Details
Certification Path
Show: <All>
Field
Value
Version
V3
Serial number
02 9a ee 64 54 95 b8 1d ...
Signature algorithm
sha1RSA
Issuer
VeriSign Class 3 Extended ...
Valid from
28 September 2011 02:00...
Valid to
28 September 2012 01:59...
Subject
login.live.com, Passport, Mi...
Public key
RSA (2048 Bits)
sign in
Windows Live ID:
danilo.gligoroski@hotmail.com
Password:
Can't access your account?
Keep me signed in

BUT, after the successful user login, the TLS connection is gone



With millions (billions) of users and millions of petabytes that need to be securely digested, checked, authenticated, stored or transmitted, apparently we are hitting the wall of usability with some of the current crypto algorithms.

NTNU
Innovation and Creativity

We need cryptographic hash and public key algorithms that will be essentially parallel, and thus will be ultra fast on the current and future CPUs.

NTNU
Innovation and Creativity

Look at SUPERCOP for Measurements of public-key signature systems

Beside well established and trusted RSA, DSA and ECDSA

Primitive	Description
`donald512`	DSA signatures using a 512-bit prime
`donald1024`	DSA signatures using a 1024-bit prime
`donald2048`	DSA signatures using a 2048-bit prime
`ecdonaldb163`	ECDSA signatures using the standard NIST B-163 elliptic curve, a curve over a field of size 2^163
...	...
`ecdonaldp521`	ECDSA signatures using the standard NIST P-521 elliptic curve, a curve modulo the prime 2^521-1
`ronald512`	512-bit RSA signatures with message recovery
...	...
`ronald4096`	4096-bit RSA signatures with message recovery

NTNU
Innovation and Creativity

A lot of other designs

	Primitive	Description	Designers
1.	`3icp`	3-invertible cycle with minus and prefix	Jintai Ding Christopher Wolf Bo-Yin Yang
2.	`bls`	Boneh–Lynn–Shacham: Pairing-based short signatures	Michael Scott
3.	`ed25519`	EdDSA signatures using Curve25519	Daniel J. Bernstein Niels Duif Tanja Lange Peter Schwabe Bo-Yin Yang
4.	`hector`	Hyperelliptic Curve with Two-Rank One: Signatures using a genus-2 hyperelliptic curve of 2-rank 1 over a field of size 2^113	Peter Birkner Peter Schwabe
5.	`mqqsig160 – mqqsig256`	160 - 256 bit signatures based on Multivariate-Quadratic-Quasigroups	Danilo Gligoroski Rune Steinsmo Ødegard Rune Erlend Jensen Ludovic Perret Jean-Charles Fauge`re Svein Johan Knapskog Smile Markovski

NTNU
Innovation and Creativity

A lot of other designs

	Primitive	Description	Designers
6.	pflash1	C*- with a prefix over GF16 designed to match SFLASH	Jintai Ding Bo-Yin Yang
7.	rainbow	Rainbow multivariate-quadratic signatures	Jintai Ding Dieter Schmidt
8.	rainbow5640 & rainbow6440	Rainbow over GF31	Jintai Ding Bo-Yin Yang
9.	rainbowbinary16242020 & 256181212	Rainbow over GF16	Bo-Yin Yang
10.	rwb0fuz1024	1024-bit Rabin-Williams signatures with compression	Adam Langley (Google)
11.	sflashv2	SFLASHv2 multivariate-quadratic signatures	Louis Goubin Nicolas Courtois Thomas Icart
12.	tts6440	Rainbow over GF16	Bo-Yin Yang

amd64; Sandy Bridge (206a7); 2011 Intel Core i7-2600K; 4 x 3400MHz; threads; sandy0, supercop-20110708

Cycles to sign 59 bytes			
quartile	median	quartile	system
5028	5032	5040	mqqsig224
5044	5052	5060	mqqsig256
5564	5616	5652	mqqsig160
7424	7476	7520	mqqsig192
21348	21404	21488	rainbowbinary256181212
44772	44860	44944	tts6440
48176	48560	49004	rainbowbinary16242020
71984	72068	72280	ed25519
75628	75796	78076	rainbow5640
100872	101088	101264	sflashv2
128356	128516	132340	rainbow6440
233836	237392	240488	donald512
513472	525092	537420	ronald512
555784	562480	570192	donald1024
580932	582392	584072	rainbow
726780	734420	739864	ecdonaldp160
958388	968972	984668	ronald768
328804	995116	1704396	3icp
1149144	1156900	1165640	ecdonaldp224
708052	1208212	2203320	pflash1

Cycles to sign 59 bytes			
quartile	median	quartile	system
1283164	1297996	1306580	ecdonaldp192
1324288	1337120	1343664	ecdonaldp256
1360532	1371852	1380548	donald2048
1625044	1637744	1655040	ronald1024
1657112	1665588	1679752	ecdonaldk163
2765164	2796580	2817932	ecdonaldp384
3904204	3922324	3953112	ronald1536
5136420	5157552	5174616	ecdonaldk283
5605980	5629004	5642988	ecdonaldb283
5858976	5888580	5918352	ecdonaldp521
7677956	7725364	7787476	ronald2048
11096908	11127692	11162296	ecdonaldk409
12296128	12321440	12349988	ecdonaldb409
21587800	21683476	21818548	ronald3072
23877492	23920456	23994632	ecdonaldk571
26748216	26795812	26865356	ecdonaldb571
47030164	47083916	47179400	ronald4096

New designs vs RSA or ECC
10, 100, 1000, 5000 times faster

NTNU
Innovation and Creativity

ONE SLIDE of self-promotion

Multivariate Cryptography Projects under my supervision at NTNU

- MQQ (design in 2008, broken by Groebner bases)
- MQQ-SIG (design and SW implementation finished in 2011, HW implementation is ongoing, so far resistant against all known attacks, very fast, but huge public keys 125 – 512 KB)
- MQQ-SIG with smaller public keys (2 – 16 KB), (design is done in 2011, now in SW implementation phase)
- MQQ-SIG (narrowband subliminal channels, simple design, implementation still pending but very simple to implement on top of existing SW implementation – 2011, 2012)
- MQQ-ENC (encryption, design is done, now in SW implementation phase – 2011, 2012),
- MQQ-ID (Identification schemes, initial design in 2011),
- MQQ-IBE (first Multivariate Quadratic Identity Based Encryption scheme, initial design done in 2011).

- Security of MQQ crypto: Was and will be a matter of public scrutiny of the crypto community
- Efficiency: 1,000-10,000 times more efficient than currently most popular schemes
- All of MQQ crypto algorithms are PATENT-FREE

NTNU
Innovation and Creativity

“Cryptographic Contests”

- Positive experience of several previously conducted cryptographic contests (DES, AES, NESSIE, eSTREAM, SHA-3)
- Cryptographic community was
  - **galvanized,**
  - **motivated,**
  - **gained new knowledge, and**
  - **provided a huge amount of scientific feedback**
- There are technological and theoretical preconditions for design of new parallel and ultra fast cryptographic primitives for the emerging technologies

NTNU
Innovation and Creativity

“Cryptographic Contests”

- Benefits of being organizer of a cryptographic contest
  - Harvest the state of the art public knowledge of a vast and growing worldwide cryptographic community
  - In connection with industry and society, via the topics of the contests, influence the directions of the development of the cryptology
  - Get very qualitative and patent-free crypto designs
  - Get a massive public security scrutiny for free
- Benefits of participating in a cryptographic contest
  - Faster way to disseminate your crypto designs
  - Faster way to get feedback about your (crypto or crapto) design ☺
  - Chance to break other designs (make friends or enemies ☺)
  - Have a nice feeling that you are contributing for the safer future of the humanity ☺

NTNU
Innovation and Creativity

Instead of conclusions …

We propose to establish a regular mechanism "Cryptographic Contests" for addressing the cryptographic challenges for the emerging technologies

NTNU
Innovation and Creativity

Thank you for your attention!

NTNU
Innovation and Creativity