A silent competition for ultra-fast public key cryptography

Presented by

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

Raising the awareness:

There is an ongoing silent competition for ultra-fast public key primitives

NTNU
Innovation and Creativity

What is a loud cryptographic competition?

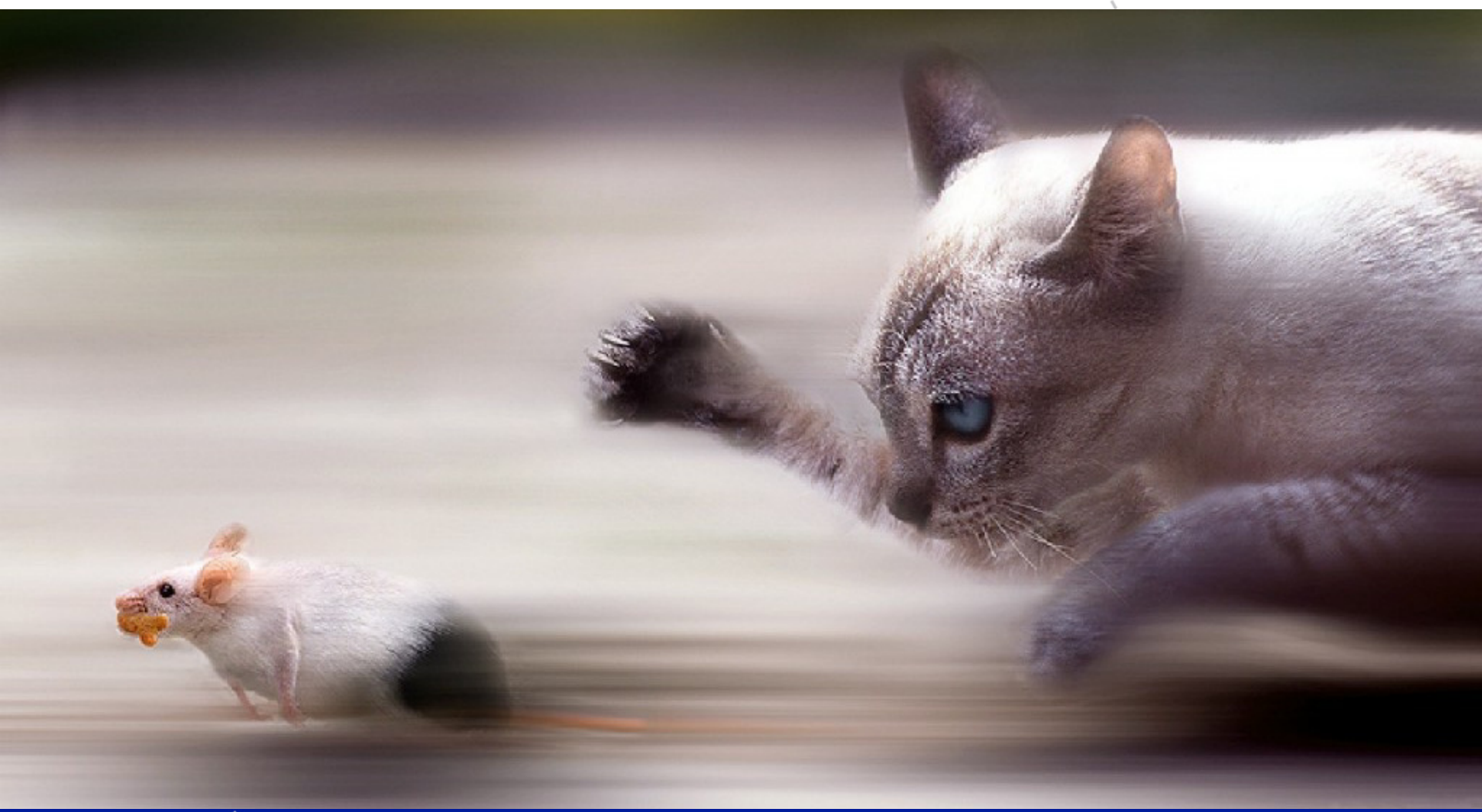
NTNU
Innovation and Creativity

SHA-3 competition before the NIST announcement for the finalists

SHA-3 competition before the NIST announcement for the finalists

What does it mean: Ultra-fast public key primitives?

Search Google images for: ultra fast



Search Google images for: ultra fast

NTNU
Innovation and Creativity

Search Google images for: ultra fast

Look at SUPERCOP for Measurements of public-key signature systems

NTNU
Innovation and Creativity

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

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

So, what does it mean: Ultra-fast public key primitives?

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

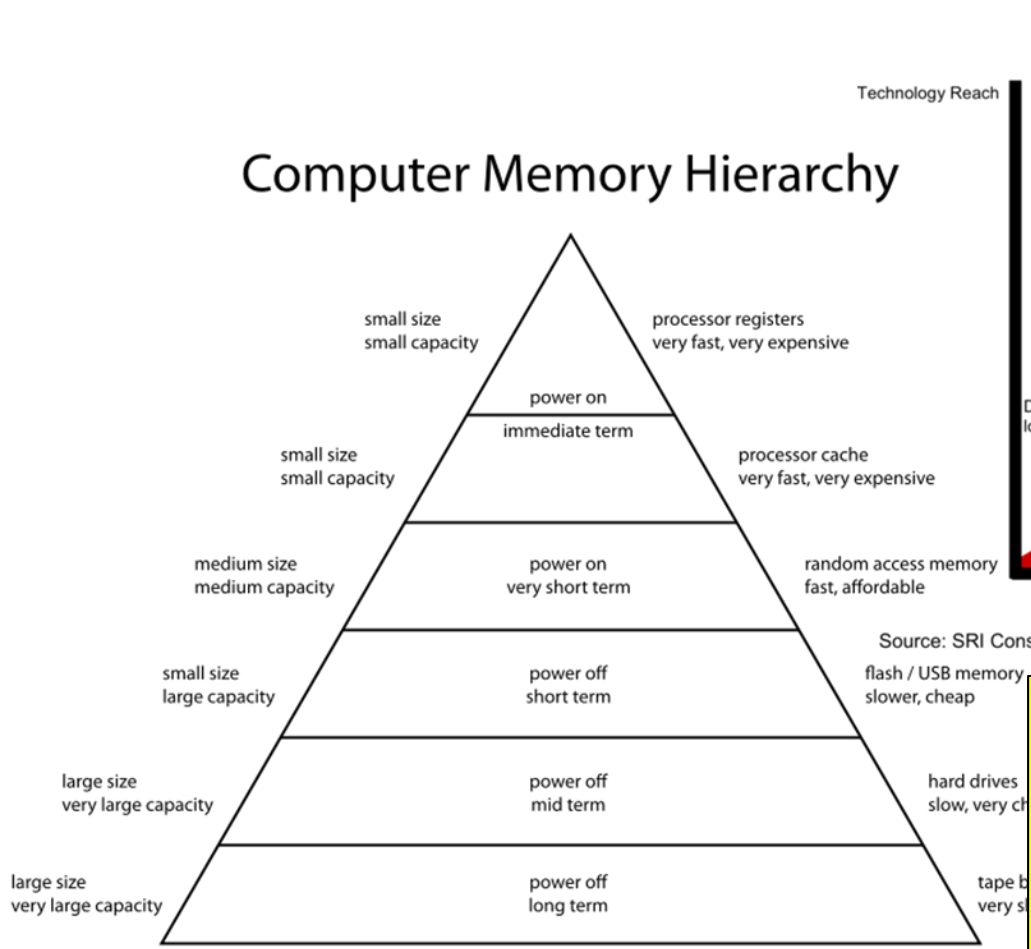
Cycles to sign 59 bytes			
quartile	median	quartile	system
1283164	1297996	1306580	ecdonaldp192
1324288	1337120	1343664	ecdonaldp256
1360532	1371852	1380548	donald2048
1625044	1637744	1655040	ronald1024
1657112	1665588	1679752	ecdonaldk163
2785164	2796580	2817992	ecdonaldp384
3904204	3922324	3953112	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

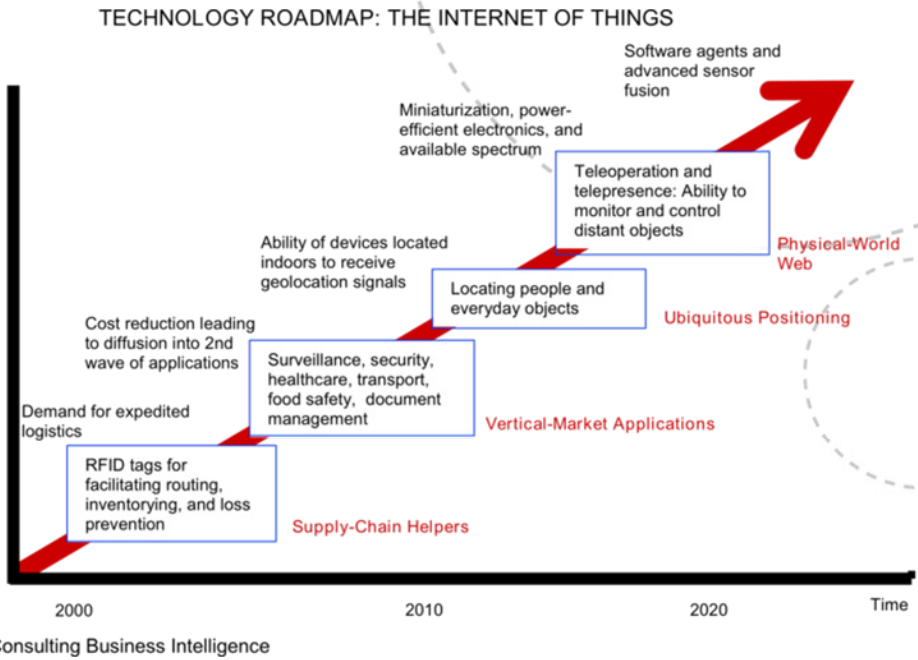
New designs vs RSA or ECC
10, 100, 1000, 5000 times faster

NTNU
Innovation and Creativity

Why we should be interested about ultra-fast public key crypto?

Why we should be interested about ultra-fast public key crypto?





Because they fit nice with the scalability of the future Internet of Things, where billions of petabytes will have to be processed, authenticated, digitally signed, …

Advertisement!

Beside MQQ-SIG, soon expect to see:

- MQQ-SIG with smaller public keys,
- MQQ-ENC (encryption),
- MQQ-ID (Identification schemes),
- MQQ-IBE (first Multivariate Quadratic Identity Based Encryption scheme).

- Cryptographers: Please look at them and try to break them!

NTNU
Innovation and Creativity

Thank you for your attention!

NTNU
Innovation and Creativity