MQQ – A Public Key Block Cipher

Presented by Danilo Gligoroski

Department of Telematics, Faculty of Information Technology, Mathematics and Electrical Engineering,

The Norwegian University of Science and Technology (NTNU), O.S.Bragstads plass 2E, N-7491 Trondheim,

Name MQQ comes from

Multivariate Quadratic Quasigroup

• **Developers** Danilo Gligoroski Smile Markovski and Svein Johan Knapskog	• **Implementers** Danilo Gligoroski (in C) Mohamed El-Hadedy (in VHDL)

- **References and links**

[1] D. Gligoroski, S. Markovski and S. J. Knapskog, “Multivariate Quadratic Trapdoor Functions Based on Multivariate Quadratic Quasigroups”, Proceedings of MATH '08, Cambridge, Massachusetts, 2008.

[2] D. Gligoroski, S. Markovski and S. J. Knapskog, “Public Key Block Cipher Based on Multivariate Quadratic Quasigroups”,Cryptology ePrint Archive, Report 2008/320, http://eprint.iacr.org/

[3] M. El-Hadedy, D. Gligoroski and S. J. Knapskog, “High Performance Implementation of a Public Key Block Cipher - MQQ, for FPGA Platforms”, Cryptology ePrint Archive, Report 2008/339, http://eprint.iacr.org/

Properties of MQQ

1. MQQ is Multivariate Quadratic trapdoor function based on theory of quasigroups and quasigroup string transformations;
2. A deterministic one-to-one mapping;
3. There is no message expansion;
4. It has one parameter n (140, 160, 180, …) - the bit length of the encrypted block;
5. Its conjectured security level when $n \geq 140$ bits is $2^{n/2}$;
6. Its encryption speed is comparable to the speed of other multivariate quadratic PKCs;
7. Its decryption/signature speed is as a typical symmetric block cipher;
8. MQQ is a Public Key Block Cipher.

NTNU
Innovation and Creativity

Multivariate Quadratic Quasigroups

- Crucial observation that led to the new public key algorithm
  - Multivariate Quadratic Quasigroups
    - There are quasigroups of order 2^d, that when represented in their Algebraic Normal Form, they are Multivariate Quadratic

Example

*	0	1	2	3	4	5	6	7
0	3	2	6	7	1	0	4	5
1	5	3	7	1	0	6	2	4
2	0	6	3	5	4	2	7	1
3	6	7	2	3	5	4	1	0
4	7	1	4	2	3	5	0	6
5	1	0	5	4	2	3	6	7
6	4	5	1	0	6	7	3	2
7	2	4	0	6	7	1	5	3

\	0	1	2	3	4	5	6	7
0	5	4	1	0	6	7	2	3
1	4	3	6	1	7	0	5	2
2	0	7	5	2	4	3	1	6
3	7	6	2	3	5	4	0	1
4	6	1	3	4	2	5	7	0
5	1	0	4	5	3	2	6	7
6	3	2	7	6	0	1	4	5
7	2	5	0	7	1	6	3	4

$$*_{vv}(x_1,x_2,x_3,x_4,x_5,x_6) = \begin{bmatrix} x_1+x_3+x_1x_4+x_2x_4+x_3x_4+x_5+x_1x_5+x_2x_5+x_3x_5+x_1x_6+x_2x_6+x_3x_6 \\ 1+x_2+x_3+x_4+x_1x_4+x_2x_4+x_3x_4+x_1x_5+x_2x_5+x_3x_5+x_1x_6+x_2x_6+x_3x_6 \\ 1+x_2+x_3x_4+x_5+x_3x_5+x_6+x_1x_6+x_2x_6+x_3x_6 \end{bmatrix}^T$$

$$\backslash_{vv}(x_1,x_2,x_3,x_4,x_5,x_6) = \begin{bmatrix} 1+x_2+x_1x_3+x_2x_3+x_1x_4+x_2x_4+x_1x_3x_4+x_2x_3x_4+x_5+x_3x_5+x_1x_3x_5+x_2x_3x_5+ \\ +x_1x_6+x_2x_6+x_3x_6 \\ \hline x_1+x_1x_3+x_2x_3+x_4+x_1x_4+x_2x_4+x_1x_3x_4+x_2x_3x_4+x_3x_5+x_1x_3x_5+x_2x_3x_5+x_1x_6+ \\ +x_2x_6+x_3x_6 \\ \hline 1+x_1+x_2+x_3+x_4+x_1x_4+x_2x_4+x_1x_5+x_2x_5+x_6 \end{bmatrix}^T$$

Conjectured strength of MQQ

n	140	160	180	200
Complexity of Grobner basis attacks	2^{87}	2^{99}	2^{112}	2^{125}
Strength of our MQQ PKC	2^{70}	2^{80}	2^{90}	2^{100}

Table 8: Complexity of the Gröbner basis attacks for different number of variables n and the strength of MQQ against Gröbner basis attacks.

NTNU
Innovation and Creativity

C implementation of MQQ

Algorithm name	Encrypt (cycles)	Decrypt (cycles)	Sign (cycles)	Verify (cycles)
DSA signatures using a 1024-bit prime	N/A	N/A	1,041,400	1,246,312
ECDSA signatures using NIST B-163 elliptic curve	N/A	N/A	2,147,128	4,220,480
1024-bit RSA, 17 bits public exponent	119,800	2,952,752	2,938,632	98,712
160–bit MQQ, one processor	140,485	10,705	10,309	140,209
160–bit MQQ, two processors	80,105	6,212	6,155	79,903

Software speeds (in number of cycles) of several most popular public key algorithms on Intel Core 2 Duo processor in 64-bit mode of operation.
DSA, ECDSA and RSA numbers are taken from eBATS: ECRYPT Benchmarking of Asymmetric Systems

NTNU
Innovation and Creativity

VHDL (FPGA) implementation of MQQ

Algorithm name	1024-bit RSA, encrypt/decrypt	160–bit MQQ, encrypt/decrypt	128–bit AES, encrypt/decrypt
FPGA type	Virtex-5, XC5VLX30-3	Virtex-5, XC5VFX70T-2	Virtex-5
Frequency	251 MHz	276.7 / 249.4 MHz	325 MHz
Throughput	40 Kbps	44.27 Gbps / 399.04 Mbps	3.78 Gbps

VHDL (FPGA) implementation of MQQ

Algorithm name	1024-bit RSA, encrypt/decrypt	160–bit MQQ, encrypt/decrypt	128–bit AES, encrypt/decrypt
FPGA type	Virtex-5, XC5VLX30-3	Virtex-5, XC5VFX70T-2	Virtex-5
Frequency	251 MHz	276.7 / 249.4 MHz	325 MHz
Throughput	40 Kbps	44.27 Gbps / 399.04 Mbps	3.78 Gbps

Compared to 1024-bit RSA,160-bit MQQ is more than 17,000 times faster in encryption and more than 10,000 times faster in decryption.

NTNU
Innovation and Creativity

Classification according to parallelization properties of the public key algorithms

Essentially sequential

- Diffie-Hellman
- RSA
- ECC

Highly parallelizable (multivariate polynomials)

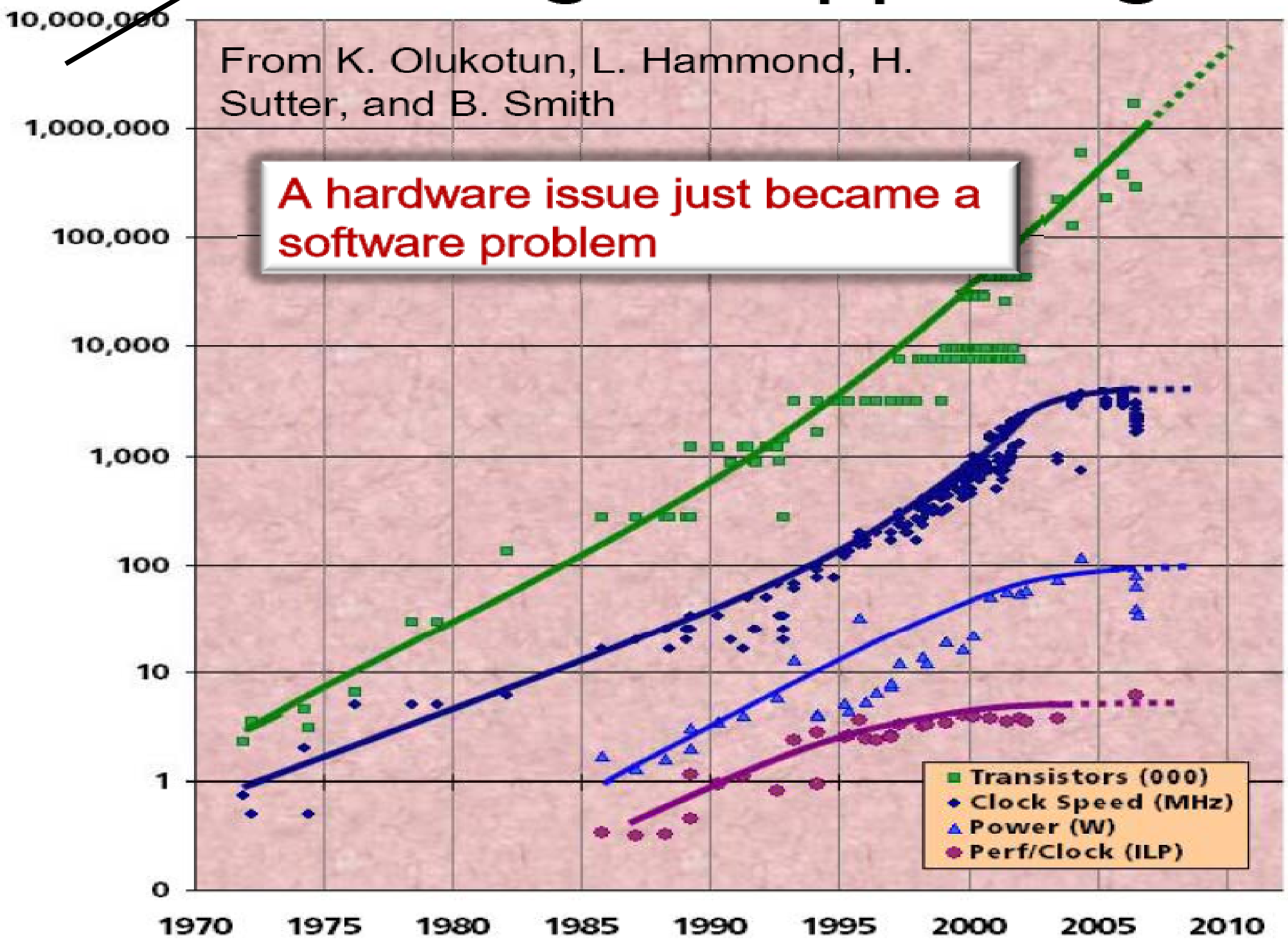
- HFE
- UOV
- MQQ
- NTRU

Perspectives of public key algorithms based on multivariate polynomials

A Slide from Jack Dongarra's presentation at SIAM 2008 annual meeting (July 2008)

ICL UT

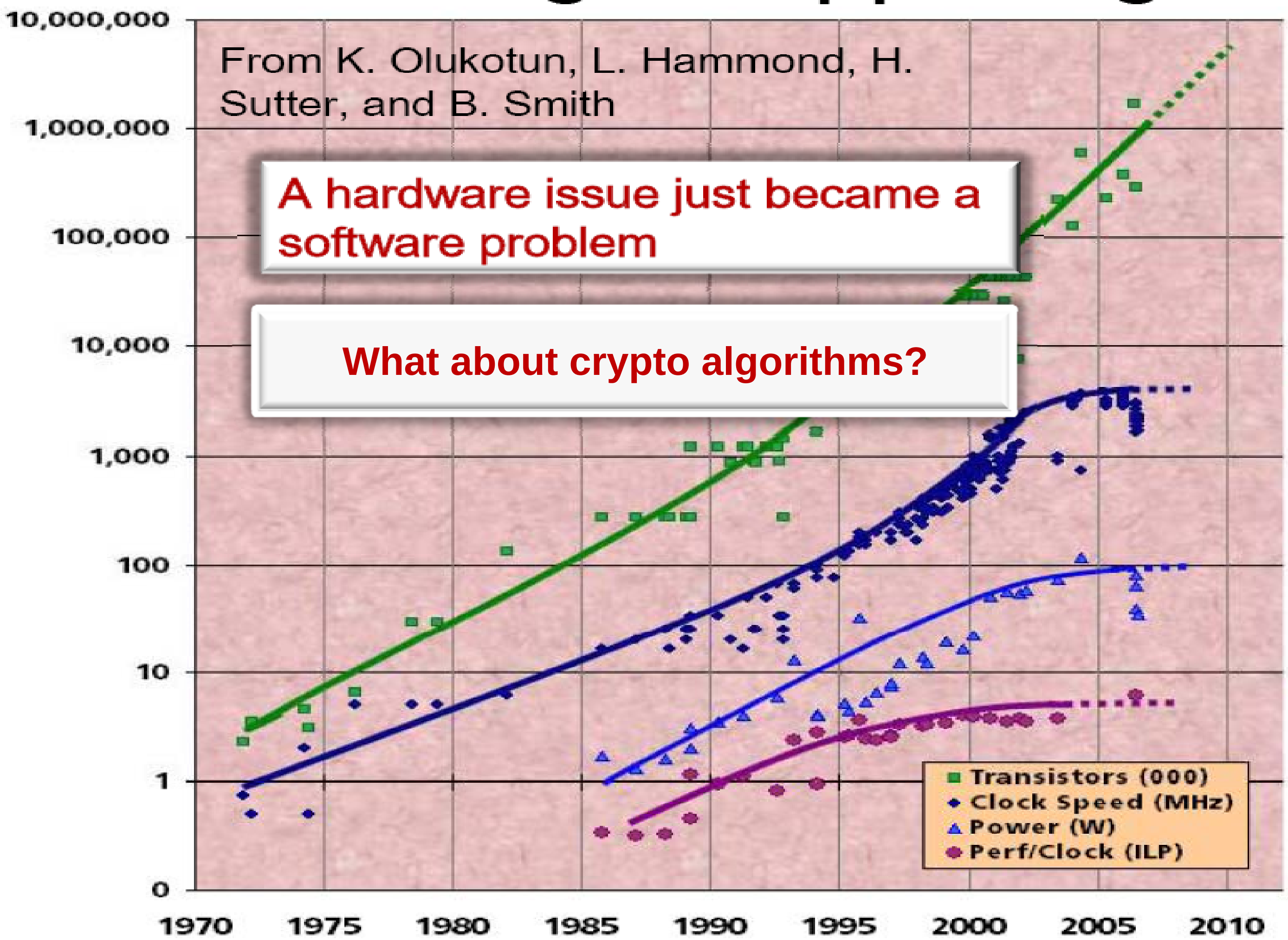
Something's Happening Here...



- In the "old days" it was: each year processors would become faster
- Today the clock speed is fixed or getting slower
- Things are still doubling every 18 -24 months
- Moore's Law reinterpretated.
  - Number of cores double every 18-24 months

Perspectives of public key algorithms based on multivariate polynomials

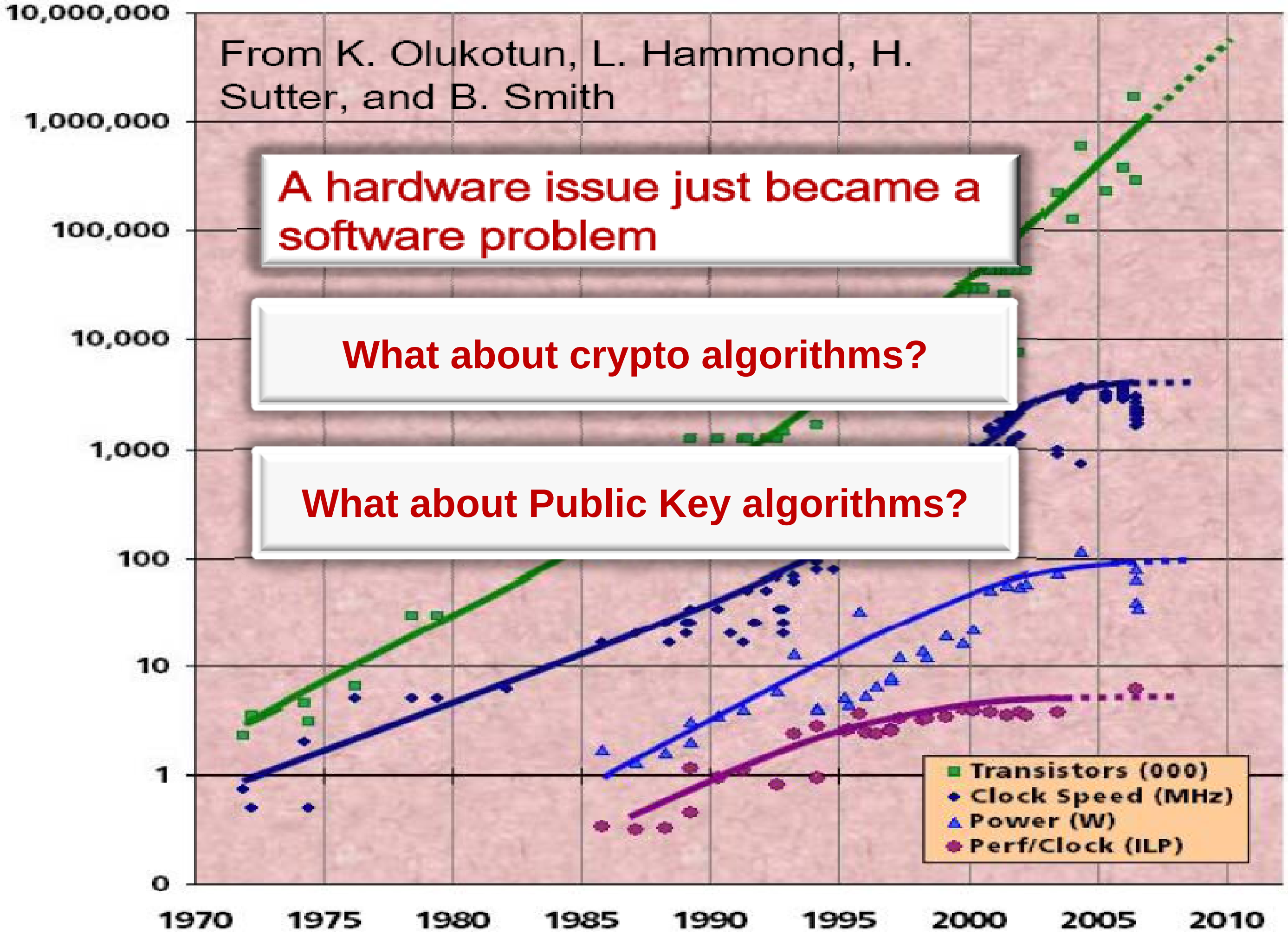
Something's Happening Here...



- In the "old days" it was: each year processors would become faster
- Today the clock speed is fixed or getting slower
- Things are still doubling every 18 -24 months
- Moore's Law reinterpretated.
  - Number of cores double every 18-24 months

Perspectives of public key algorithms based on multivariate polynomials

Something's Happening Here...



- In the "old days" it was: each year processors would become faster
- Today the clock speed is fixed or getting slower
- Things are still doubling every 18 -24 months
- Moore's Law reinterpretated.
  - Number of cores double every 18-24 months

Thank you for your attention!