Post-quantum cryptography – long-term confidentiality and integrity for communication

Tanja Lange

Coding Theory and Cryptology

Ei/Ψ

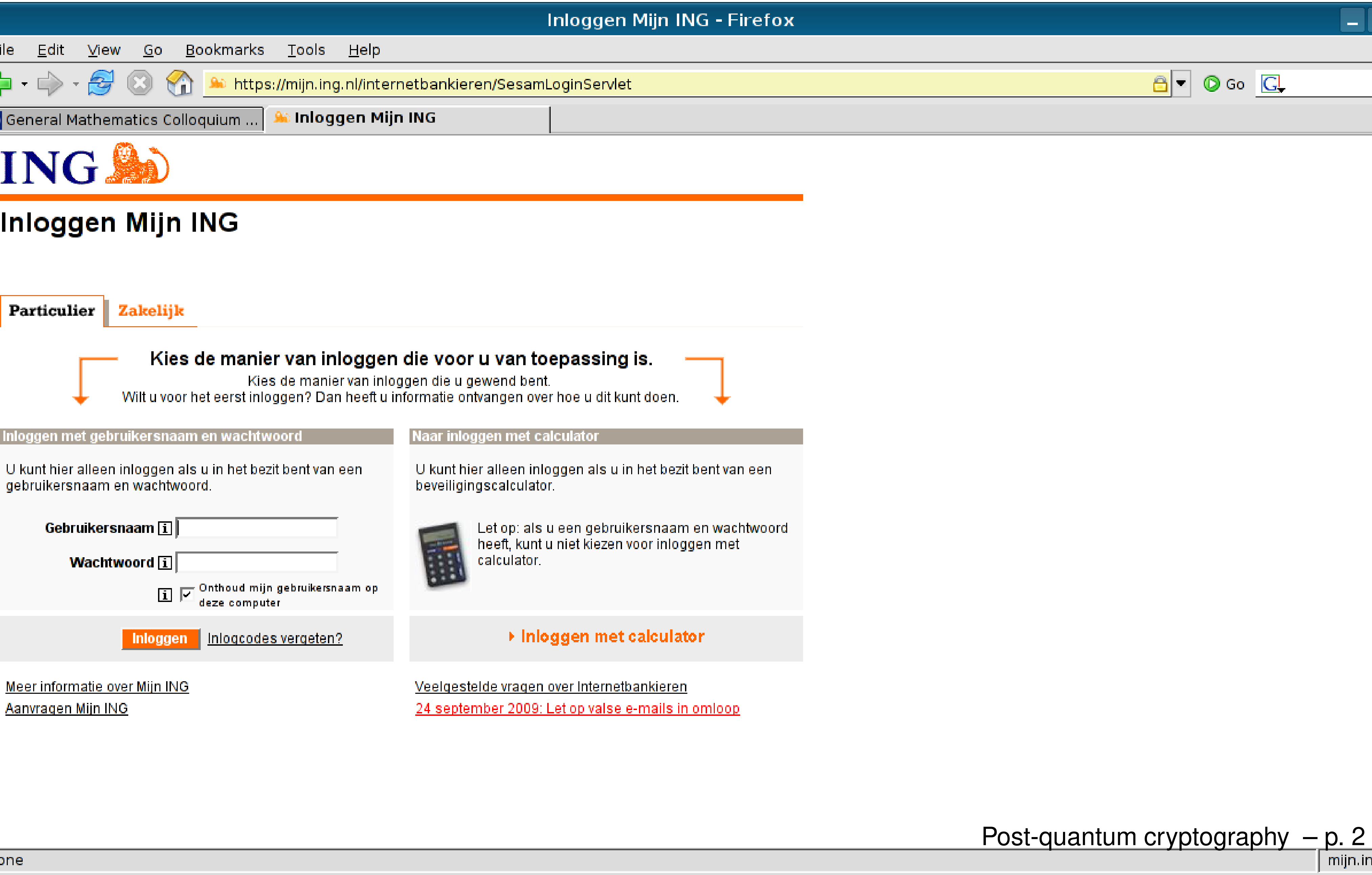
Department of Mathematics and Computer Science

Technische Universiteit Eindhoven

tanja@hyperelliptic.org

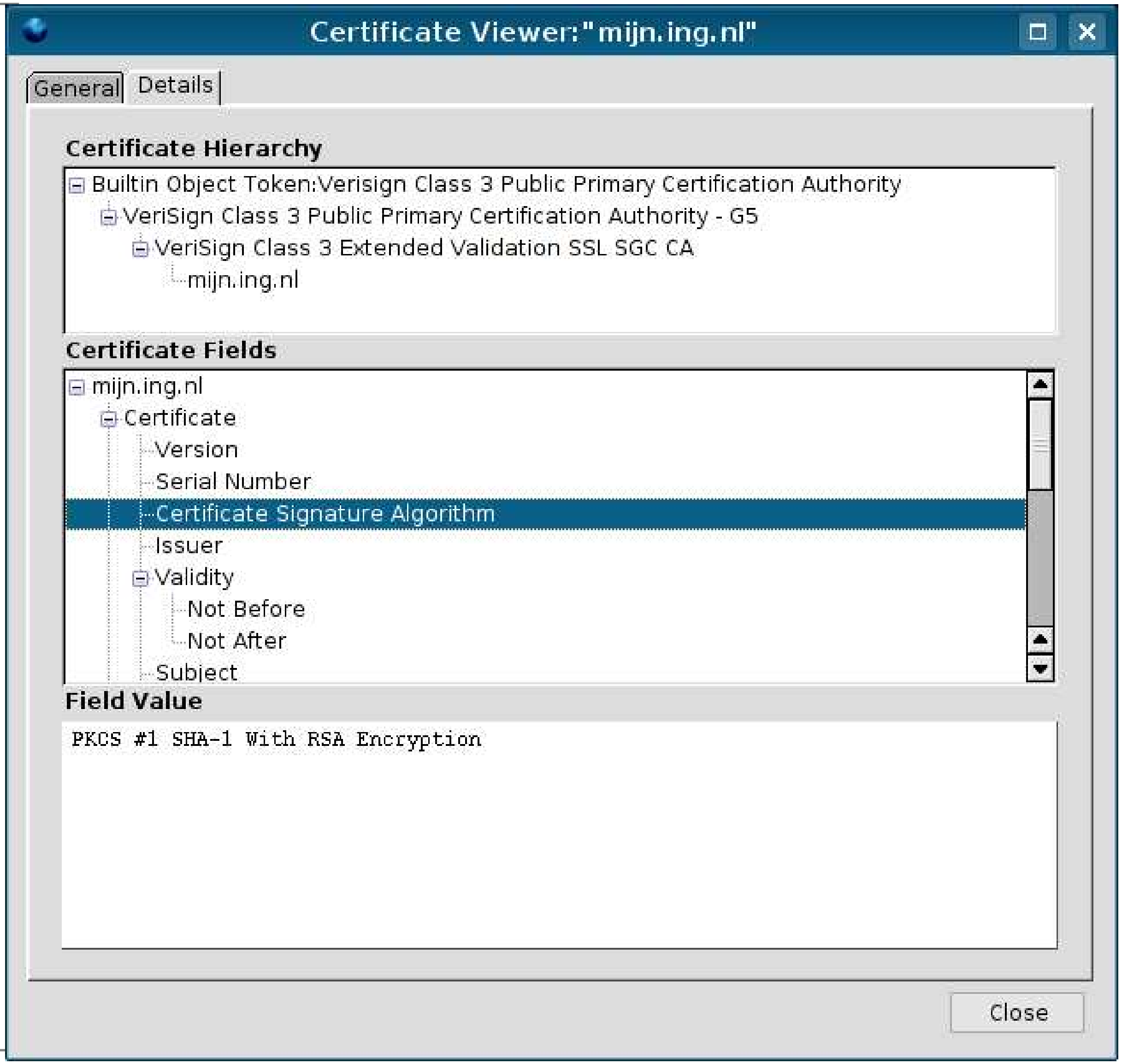
06.11.2012

Real-world use I



Real-world use II

Real-world use III



Subject's Public Key

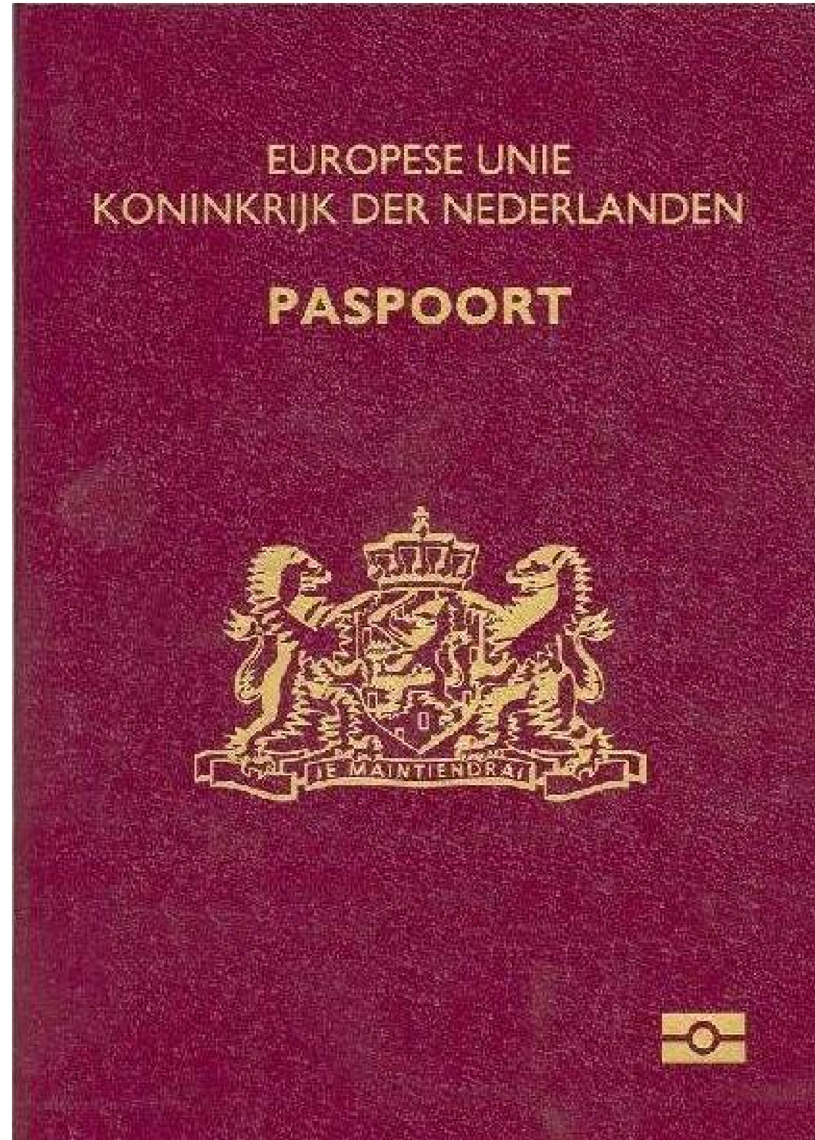
```
30 81 89 02 81 81 00 cc d1 35 c6 8f f6 d9 e9 1f
0b a6 a8 b7 53 4d 8d 21 69 11 16 8e 50 2c c2 34
f4 9e 9e 41 d7 74 47 20 a8 71 0e a1 58 31 67 87
5e d5 31 9b 44 dd 12 74 53 8b 34 c1 d9 a7 b0 5e
27 b5 e8 d1 9c c3 7c 73 bd 6a 61 e4 75 7a e2 fd
6f 7c ca e4 48 05 97 e0 1f 4a 99 9e 29 53 78 fd
65 6d 77 78 9f 9e 63 fc 05 71 18 90 a4 c2 19 97
73 e3 17 a8 ff 15 cd 0a 68 d8 43 aa 6c c5 b3 75
58 31 42 d9 e5 8b 5f 02 03 01 00 01
```

These numbers represent a 1024 bit modulus $n = p \cdot q$, with primes p and q which is used in the RSA cryptosystem. RSA secures the connection to `https://www.ing.nl`.

Anybody knowing p and q can impersonate the bank but, luckily, factoring integers of this type is hard.

Real-world use IV

- Electronic passport contains signature to guarantee authenticity.
- This uses the discrete logarithm problem on elliptic curves over finite fields as hardness assumption.
- Public-key cryptography is a nice playground for number theorists, algebraic geometers, . . . and is necessary to achieve confidentiality and integrity.



Threat of quantum computers

Shor's algorithm makes polynomial time:

- integer factorization
- DLP in finite fields
- DLP on elliptic curves
- DLP in general class groups

Grover's algorithm brings faster simultaneous search in data

- some security loss in symmetric crypto (block and stream ciphers)
- some security loss in hash functions (massive for VSH)

Compensate for Grover by $\approx$ doubling key size.

Threat of quantum computers

Shor's algorithm makes polynomial time:

- integer factorization
- DLP in finite fields
- DLP on elliptic curves
- DLP in general class groups

Grover's algorithm brings faster simultaneous search in data

- some security loss in symmetric crypto (block and stream ciphers)
- some security loss in hash functions (massive for VSH)

Compensate for Grover by $\approx$ doubling key size.

Sorry,
no picture
available
quite yet.

. . . but 15 years from now . . .

Large quantum computers might be reality. Then

- RSA is broken.
- DH key exchange is broken.
- DSA is broken.
- XTR is broken.
- ECDSA is broken.
- ECC is broken.
- HECC is broken.

. . . but 15 years from now . . .

Large quantum computers might be reality. Then

- RSA is broken.
- DH key exchange is broken.
- DSA is broken.
- XTR is broken.
- ECDSA is broken.
- ECC is broken.
- HECC is broken.
- all public-key cryptosystems

…but 15 years from now …

Large quantum computers might be reality. Then

- RSA is broken.
- DH key exchange is broken.
- DSA is broken.
- XTR is broken.
- ECDSA is broken.
- ECC is broken.
- HECC is broken.
- all public-key cryptosystems are broken?

…but 15 years from now …

Large quantum computers might be reality. Then

- RSA is broken.
- DH key exchange is broken.
- DSA is broken.
- XTR is broken.
- ECDSA is broken.
- ECC is broken.
- HECC is broken.
- all public-key cryptosystems are broken?
- Actually there are a few more public-key cryptosystems.

The “survivors”

Public-key encryption (confidentiality):

- Lattice-based cryptography (e.g. NTRU)
- Code-based cryptography (e.g. McEliece, Niederreiter)

Public-key signatures (integrity):

- Multivariate-quadratic-equations cryptography (e.g. HFE$^-$)
- Hash based cryptography (e.g. Merkle’s hash-trees signatures)

For these systems no efficient usage of Shor’s algorithm is known. Grover’s algorithm has to be taken into account when choosing key sizes.
Some more possibilities with less confidence.

Why care about this now?

15 years might seem a long time. But

- There is no guarantee that it takes at least 15 years.
- Long-term confidential documents (e.g. health records, state secrets) become readable once quantum computers are available.
- Electronic signatures on long-term commitments (e.g. last wishes, contracts) can be forged once quantum computers are available.
- Nobody will inform you if a secret agency made a breakthrough in constructing a quantum computer.
- The systems mentioned before remain secure – but need better study of parameters, faster implementations, and better embedding into protocols.

Post-quantum cryptography

- Cryptographic systems that run on conventional computers, are secure against attacks with conventional computers, and remain secure under attacks with quantum computers are called post-quantum cryptosystems.
- Post-quantum cryptography deals with
  - the design of such systems;
  - cryptanalysis of such systems;
  - the analysis of suitable parameters depending on different threat models;
  - design of protocols using the secure primitives.
- Could potentially develop cryptosystems for quantum computers – but there won't be a market too soon.

The END

The END

Thanks!