Flush, Gauss, and Reload
A Cache Attack on the BLISS Lattice-Based Signature Scheme

Leon Groot Bruinderink, Andreas Hülsing, Tanja Lange, Yuval Yarom

Peaks in Dutch Cyber Security Research

NWO Netherlands Organisation for Scientific Reseai

dcypher

IBM

Flush, Gauss, and Reload

A Cache Attack on the BLISS Lattice-Based Signature Scheme

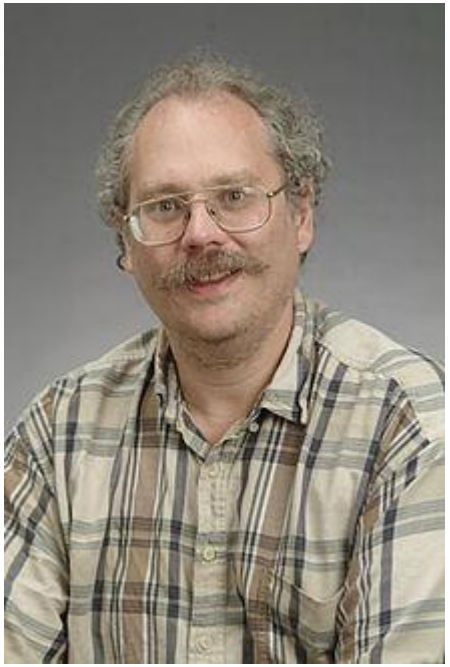
Leon Groot Bruinderink (TU/e),
Andreas Hülsing (TU/e), Tanja Lange (TU/e),
Yuval Yarom (University of Adelaide & NICTA)

(Public-key) cryptography is ubiquitous

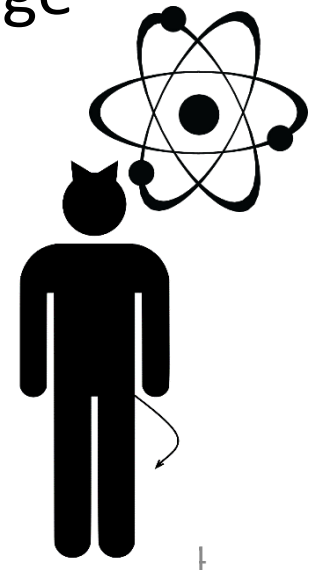
- Code signing (Signatures)
  - Software updates
  - Software distribution
  - Mobile code

- Communication security (Signatures, PKE / KEX)
  - TLS, SSH, IPSec, ...
  - eCommerce, online banking, eGovernment, ...
  - Private online communication

The quantum threat



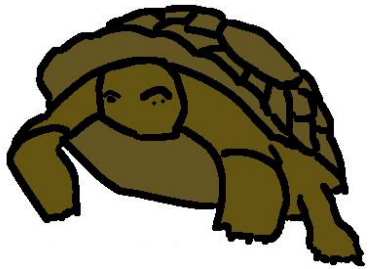
- Scalable quantum-computers can efficiently break today‘s public-key cryptography
- Predictions for first QC range from 20 years to never
- Risc assessment



Post-quantum cryptography

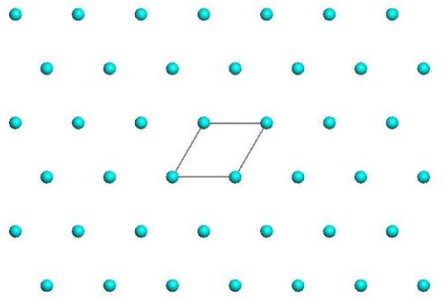
- Cryptography conjectured to withstand attacks with (scalable) quantum computers
- Different areas: Hash-based, code-based, multivariate, isogeny-based and lattice-based cryptography
- Transition in US planned within next 10 years (NSA & NIST)

PQCRYPTO
ICT-645622



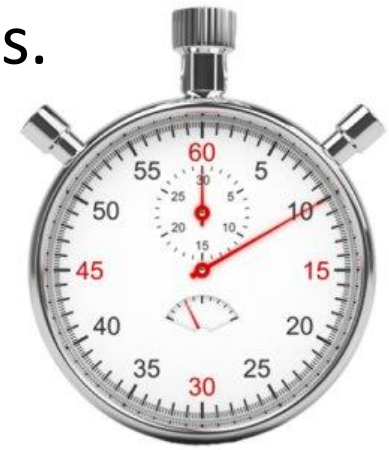
Lattice-based cryptography

- Based on problems from lattice theory: (approximate) shortest vector problem / closest vector problem
- Post-quantum candidate
- Efficient constructions for signatures and key-exchange are known
- Solid formal security arguments
- Fast implementations
- First field tests by Google



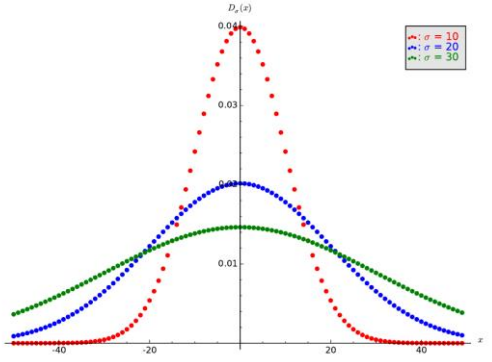
Side-channels

- Implementations might leak secret information through
  - timing,
  - cache-access patterns,
  - electro-magnetic radiation,
  - power consumption...
- Not covered by standard security models.



Discrete Gaussians

- Basic building block in lattice-based cryptography.
- Used to “hide” secret.
- Unknown how to implement efficiently in constant time. (But also unknown how to exploit)



BLISS (Ducas, Durmus, Lepoint, Lyubashevsky, CRYPTO 2013)

- „Bimodal lattice signature scheme“
- Most advanced lattice-based signature scheme
- Open-source implementation in StrongSwan library.

BLISS signature

$$Sig = (\vec{z}, \vec{c}), \vec{c} = H(msg || \dots);$$

$$\vec{z} = \vec{y} + (-1)^b S\vec{c}$$

Random bit

Discrete Gaussian vector

Secret key

Challenges

- Found side-channels only leak partial information about $\vec{y}$
- Information is noisy
- Only one trace per $\vec{y}$

Results

- Side-channel attack on BLISS (full break).
- Practical cache attack on both samplers implemented by designers.
- First algorithm to “un-hide” secret key given side-channel information for Gaussian noise.
- Can compute secret key after < 5000 signatures.

Paper in proceedings of CHES 2016
Full version available at IACR eprint archive

http://eprint.iacr.org/2016/300

Thank you!

Questions?