Selecting Secure Parameters for Lattice-based Cryptography

Markus Rückert and Michael Schneider
Technische Universität Darmstadt

TECHNISCHE UNIVERSITÄT DARMSTADT

Theory vs. Practice

TECHNISCHE UNIVERSITÄT DARMSTADT

Efficiency

$\tilde{\mathcal{O}}(n^2)$ bits

Theory vs. Practice

TECHNISCHE UNIVERSITÄT DARMSTADT

Efficiency

$\tilde{\mathcal{O}}(n^2)$ bits

vs.

n^2 bits

$10^6 n^2 (\log(n))^{100}$ bits

Theory vs. Practice

TECHNISCHE UNIVERSITÄT DARMSTADT

Efficiency

$\tilde{O}(n^2)$ bits

vs.

n^2 bits

$10^6 n^2 (\log(n))^{100}$ bits

Security

$X(n)$ is secure if $Y(f(n))$ is hard

Theory vs. Practice

TECHNISCHE UNIVERSITÄT DARMSTADT

Efficiency

$\tilde{O}(n^2)$ bits

vs.

n^2 bits

$10^6 n^2 (\log(n))^{100}$ bits

Security

$X(n)$ is secure if $Y(f(n))$ is hard

vs.

$X(200)$ is likely to be secure until the year 2030

Reductions for Modern Lattice Crypto

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Worst case SVP $\leq$ LWE $\leq$ Encryption

Reductions for Modern Lattice Crypto

TECHNISCHE
UNIVERSITÄT
DARMSTADT

$$\text{Worst case SVP} \leq \text{LWE} \leq \text{Encryption}$$
$$\text{Worst case SVP} \leq \text{SIS} \leq \text{Signatures}$$

Reductions for Modern Lattice Crypto

TECHNISCHE UNIVERSITÄT DARMSTADT

Worst case SVP $\leq$ LWE $\leq$ Encryption

Worst case SVP $\leq$ SIS $\leq$ Signatures

How hard is the worst-case of a problem?

Attacks

Sig $\rightarrow$ SIS

Reductions for Modern Lattice Crypto

TECHNISCHE UNIVERSITÄT DARMSTADT

Worst case SVP $\leq$ LWE $\leq$ Encryption

Worst case SVP $\leq$ SIS $\leq$ Signatures

How hard is the worst-case of a problem?

Attacks

Sig $\rightarrow$ SIS

Enc $\rightarrow$ LWE $\overset{\text{duality}}{\rightarrow}$ SIS

Outline for the Rump Session Talk

TECHNISCHE UNIVERSITÄT DARMSTADT

1. Analyze SIS (once and for all)
   - 1.1 Take SIS(n, m, q, β)
   - 1.2 Analyze influence of n, m, q, β
     - 1.2.1 Show that m is inconsequential
     - 1.2.2 Show that bigger q make the problem harder
     - 1.2.3 Show that bigger n make the problem harder
   - 1.3 Find hardness measure $\delta = \delta(n, m, q, \beta)$
   - 1.4 Run thousands of experiments
     - dimension m
     - worst-case dimension n
     - modulus q
     - norm bound β
   - 1.5 Draw conjectures
   - 1.6 Do not forget the milk!
2. Set up parameters for *hybrid encryption* and *hash-then-sign*
   - 2.1 Use Lenstra's Heuristic to estimate future security
   - 2.2 Employ a double Moore law to account for
     - new technology
     - new algorithms
3. Translate "forging" to SIS for signatures
4. Translate "distinguishing" to SIS for encryption

Main Conjectures

TECHNISCHE UNIVERSITÄT DARMSTADT

Conjecture 1

For every $n \in \mathbb{N}_{>0}$, constant $c \geq 2$, prime $q \geq n^c$, and $m > n\log_2(q)$, the best known approach to solve SIS with parameters (n, q, m, β) involves solving δ-HSVP in dimension $d = \sqrt{n\log(q)/\log(\zeta)}$ for $\zeta = \sqrt[m]{\beta/q^{n/m}} \leq \delta = \sqrt[d]{\beta/q^{n/d}}$.

Conjecture 2

For $\delta = \delta(n, m, q, \beta) \in (1, 1.015]$, attacking SIS with hardness δ takes at least $T(\delta) = 10^{-15}2^{-(\log_2(\delta)^{1.001})} + 0.005$ dollar-days.

What?

TECHNISCHE
UNIVERSITÄT
DARMSTADT

What?

TECHNISCHE UNIVERSITÄT DARMSTADT

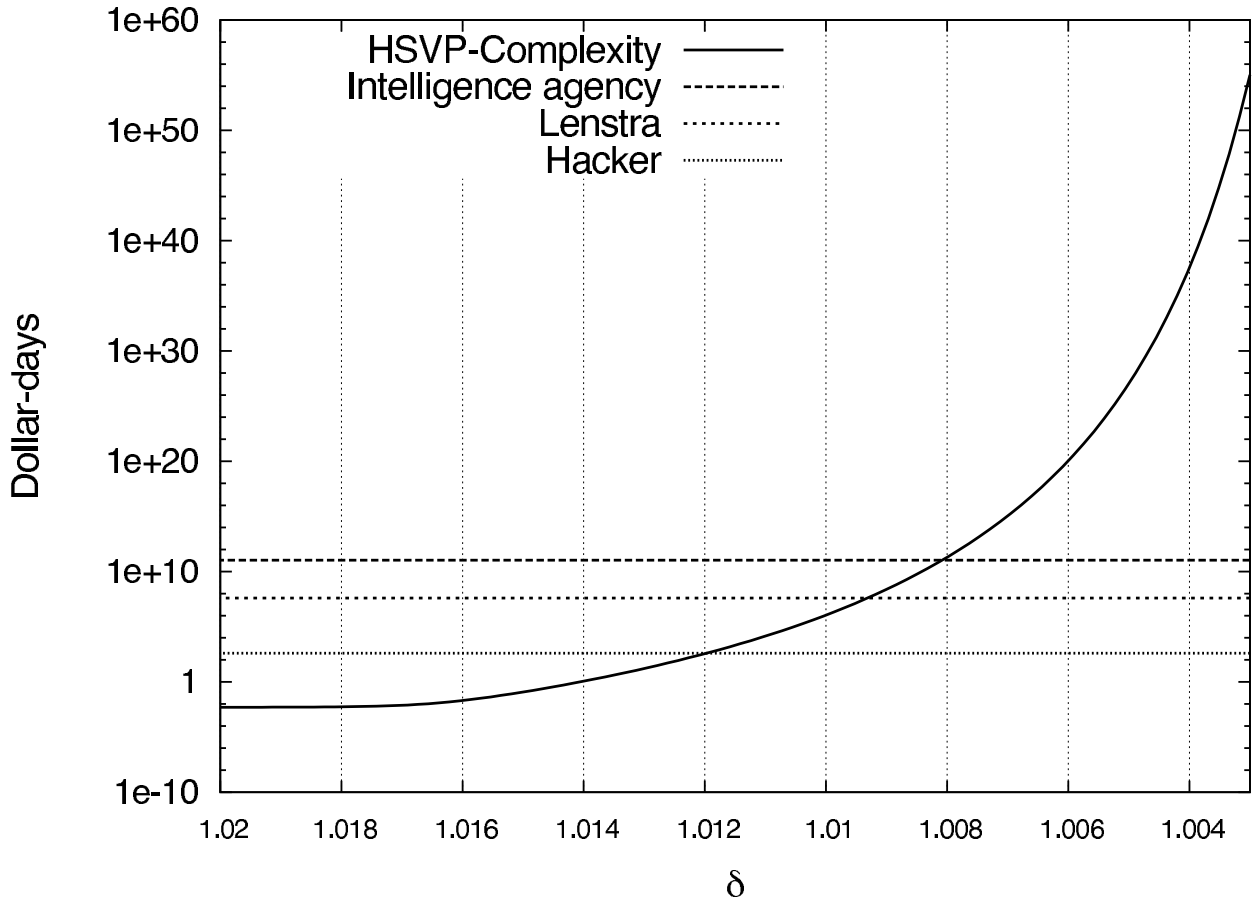


Figure: Attack effort (DD) in log-scale compared with typical attack capabilities.

Key Sizes for Encryption (Lenstra, year 2050)

TECHNISCHE UNIVERSITÄT DARMSTADT

Encryption of a 200 bit key.

Trapdoor-LWE for CCA (GPV, STOC 2008)

```
Ciphertext:    80 KB
Public Key:    30 MB
Secret Key:    50 MB
```

Key Sizes for Encryption (Lenstra, year 2050)

TECHNISCHE UNIVERSITÄT DARMSTADT

Encryption of a 200 bit key.

Trapdoor-LWE for CCA (GPV, STOC 2008)

```
Ciphertext:   80 KB
Public Key:   30 MB
Secret Key:   50 MB
```

Ring-LWE (LRP, EC 2010)

```
Ciphertext:  2 KB
Public Key:  1 KB
Secret Key:  1 KB
```

Key Sizes for Signatures (Lenstra, year 2050)

TECHNISCHE UNIVERSITÄT DARMSTADT

Signature of a 300 bit hash.

Bonsai-tree Signatures (CHKP, EC 2010)

```
Signature :    50 MB
Public Key:    40 GB
Secret Key:   150 MB
```

Key Sizes for Signatures (Lenstra, year 2050)

TECHNISCHE UNIVERSITÄT DARMSTADT

Signature of a 300 bit hash.

Bonsai-tree Signatures (CHKP, EC 2010)

```
Signature :   50 MB
Public Key:   40 GB
Secret Key:  150 MB
```

Lyubashevsky's ROM Signatures (Asiacrypt 2009)

```
Signature :   3 KB
Public Key:   3 KB
Secret Key:  13 KB
```

Smartcards?

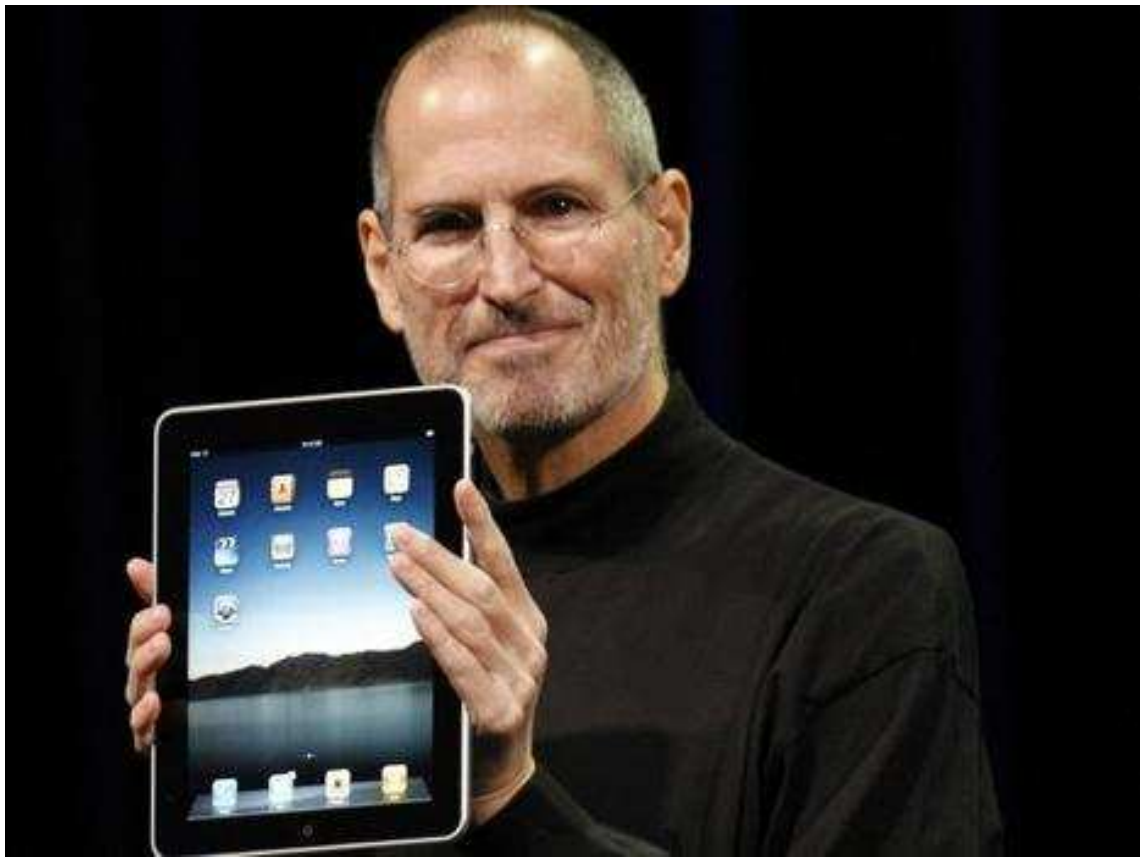
TECHNISCHE
UNIVERSITÄT
DARMSTADT

YES!

Smartcards?

TECHNISCHE UNIVERSITÄT DARMSTADT

YES!



Want to know more? It's on ePrint!

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Report 2010 / 137

Speaker for Rent

TECHNISCHE UNIVERSITÄT DARMSTADT

Rates (Euro)

R = (Duration of talk x Distance from DA) / (Acceptance rate)

Speaker for Rent

TECHNISCHE UNIVERSITÄT DARMSTADT

Rates (Euro)

R = (Duration of talk x Distance from DA) / (Acceptance rate)

also payable in cigarettes