Efficient Implementation of Lattice-based Cryptography for Embedded Devices

Tim Güneysu, Tobias Oder
Ruhr-University Bochum

16th IMA International Conference on Cryptography and Coding

12.12.2017

Implementation on Embedded Devices

RUB

- What are the goals?
  - Throughput/latency
  - Code size/area
  - Power/energy

- Cross-disciplinary work and interaction between engineers and cryptographers required
  - Parameter selection and design decisions can make schemes more efficient but also weaker

Side-channel attacks

- Timing
  - Cache
  - Execution time
- Power, EM
  - Simple power analysis
  - Differential power analysis
  - Correlation-based
- Active attacks
  - Inducing faults

Lattice-based Cryptography

RUB

- 28 submissions to the NIST post-quantum project[1]
- Efficiency
- Scalability
- Versatility
  - Encryption
  - Digital signatures
  - Key exchange
  - Advanced constructions (IBE, FHE,…)

[1] https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf

Lattice Classes

Standard or random lattices

- Unstructured matrices
- Main Operation: matrix-vector multiplication

Lattice Classes

Standard or random lattices

- Unstructured matrices
- Main Operation: matrix-vector multiplication

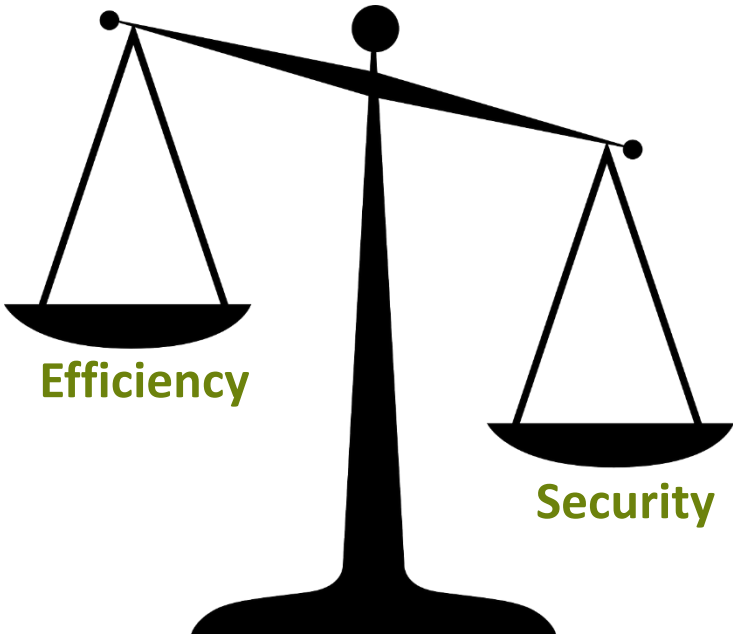
Ring or ideal lattices

- Smaller parameters
- Faster implementations
- Smaller implementations
- Main Operation: polynomial multiplication

But less trust in security due to structure!

Module Lattices

Idea: Find a trade-off between the advantages of both classes



Main operation: Matrix-vector multiplication

- But matrix elements are polynomials!

Schemes

RUB

Non-exhaustive list

	Encryption	Signature	Key Exchange
Standard Lattices	LWE Encrypt	TESLA Bai-Galbraith GPV	Frodo
Ideal Lattices	Ring-LWE Encrypt NTRU Encrypt	BLISS GLP Ring-TESLA	„A new hope“
Module Lattices	Kyber	Dilithium Dilithium-G	CCA2-secure Kyber

Schemes

RUB

Non-exhaustive list

	Encryption	Signature	Key Exchange
Standard Lattices	LWE Encrypt	TESLA Bai-Galbraith GPV	Frodo
Ideal Lattices	Ring-LWE Encrypt NTRU Encrypt	BLISS GLP Ring-TESLA	„A new hope“
Module Lattices	Kyber	Dilithium Dilithium-G	CCA2-secure Kyber

Schemes

RUB

Non-exhaustive list

	Encryption	Signature	Key Exchange
Standard Lattices	LWE Encrypt	TESLA Bai-Galbraith GPV	Frodo
Ideal Lattices	Ring-LWE Encrypt NTRU Encrypt	BLISS GLP Ring-TESLA	„A new hope“
Module Lattices	Kyber	Dilithium Dilithium-G	CCA2-secure Kyber

CCA2-Security

RUB

- Plain Ring-LWE encryption is only secure against chosen-plaintext attackers (CPA)
- Many use cases require security against chosen-ciphertext attackers (CCA)
  - Attacker has access to a decryption oracle
- Generic Fujisaki-Okamoto transform
  - Assumes negligible decryption error
  - Tweak by Targhi and Unruh for post-quantum security
  - Expensive re-encryption in decryption

Masking Ring-LWE

RUB

Masking = Protection against power analysis

Components to be masked in CCA2-secure Ring-LWE

- PRNG/Hash
- NTT
- Sampler
- Encoding/Decoding

Implementation

RUB

See our implementation: ia.cr/2016/1109 together with Tobias Schneider, Thomas Pöppelmann, and Tim Güneysu

- New masking scheme combined with CCA2-security
- Practical evaluation
  - Performance
  - Memory
  - Side-channel experiments
- Target platform ARM-Cortex-M4

Masked CCA2-secure Ring-LWE

- Dimension n = 1024
- Modulus q = 12289
- Standard deviation ς = 2
- 233 bits of PQ security

Operation	Cycle Counts	
	Unmasked	Masked
Key Generation	2,669,559	-
CCA2-secured Encryption	4,176,684	-
CCA2-secured Decryption	4,416,918	25,334,493
CPA-RLWE Encryption	3,910,871	19,315,432
CPA-RLWE Decryption	163,887	550,038
Shake-128	87,738	201,997
NTT	83,906	-
INTT	104,010	-
Uniform Sampling (TRNG)	60,014	-
SampleNoisePoly (PRNG)	1,142,448	6,031,463
PRNG (64 bytes)	88,778	202,454

Masked CCA2-secure Ring-LWE

- Dimension n = 1024
- Modulus q = 12289
- Standard deviation ς = 2
- 233 bits of PQ security

Operation	Cycle Counts	
	Unmasked	Masked
Key Generation	2,669,559	-
CCA2-secured Encryption	4,176,684	-
CCA2-secured Decryption	4,416,918	25,334,493
CPA-RLWE Encryption	3,910,871	19,315,432
CPA-RLWE Decryption	163,887	550,038
Shake-128	87,738	201,997
NTT	83,906	-
INTT	104,010	-
Uniform Sampling (TRNG)	60,014	-
SampleNoisePoly (PRNG)	1,142,448	6,031,463
PRNG (64 bytes)	88,778	202,454

Masked CCA2-secure Ring-LWE

- Dimension n = 1024
- Modulus q = 12289
- Standard deviation ς = 2
- 233 bits of PQ security

Operation	Cycle Counts	
	Unmasked	Masked
Key Generation	2,669,559	-
CCA2-secured Encryption	4,176,684	-
CCA2-secured Decryption	4,416,918	25,334,493
CPA-RLWE Encryption	3,910,871	19,315,432
CPA-RLWE Decryption	163,887	550,038
Shake-128	87,738	201,997
NTT	83,906	-
INTT	104,010	-
Uniform Sampling (TRNG)	60,014	-
SampleNoisePoly (PRNG)	1,142,448	6,031,463
PRNG (64 bytes)	88,778	202,454

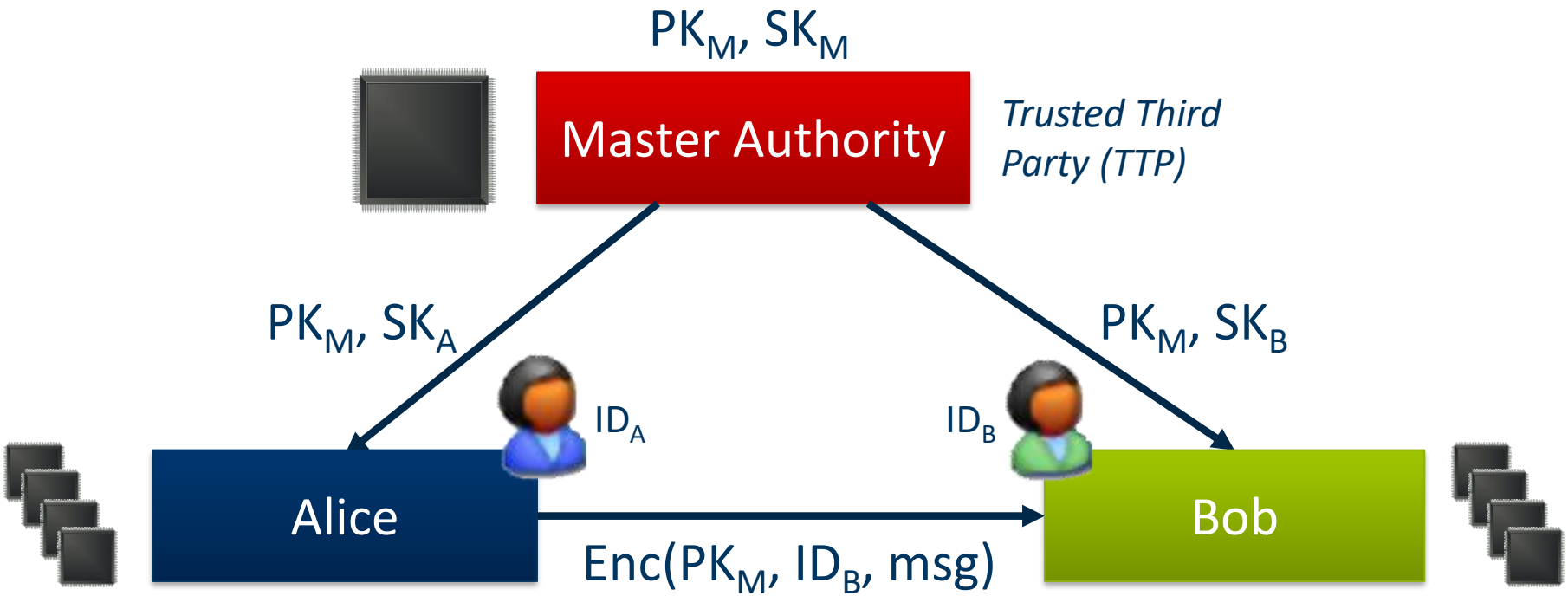
Masked CCA2-secure Ring-LWE

- Dimension n = 1024
- Modulus q = 12289
- Standard deviation ς = 2
- 233 bits of PQ security

Operation	Cycle Counts	
	Unmasked	Masked
Key Generation	2,669,559	-
CCA2-secured Encryption	4,176,684	-
CCA2-secured Decryption	4,416,918	25,334,493
CPA-RLWE Encryption	3,910,871	19,315,432
CPA-RLWE Decryption	163,887	550,038
Shake-128	87,738	201,997
NTT	83,906	-
INTT	104,010	-
Uniform Sampling (TRNG)	60,014	-
SampleNoisePoly (PRNG)	1,142,448	6,031,463
PRNG (64 bytes)	88,778	202,454

Identity-based Encryption (IBE)

- **Demand** for advanced security services (e.g., smart environments)
- **Concept**: Extend asymmetric encryption scheme based on public identifier ID_X (e.g., given name, MAC, e-mail address, etc.)



IBE Implementation

- Implementation of encryption and decryption of [DPL14] feasible on embedded devices

- Key generation memory-wise and computationally expensive

[DPL14] Efficient Identity-Based Encryption over NTRU Lattices, Léo Ducas, Thomas Prest, Vadim Lyubashevsky, ASIACRYPT 2014

IBE Implementation

- Implementation of encryption and decryption of [DPL14] feasible on embedded devices
- Key generation memory-wise and computationally expensive
- Cortex-M4 microcontroller
  - Enc/Dec: 6/2 ms
- Spartan6 FPGA
  - Enc/Dec: 80/54 µs

[DPL14] Efficient Identity-Based Encryption over NTRU Lattices, Léo Ducas, Thomas Prest, and Vadim Lyubashevsky, ASIACRYPT 2014

Conclusion

Lattice-based cryptography is practical on embedded devices!

But consider limited resources

Future Work

- Side-channel security
- Efficient IBE key generation
- More cryptanalysis

RUB

Thank You For Your Attention!

hgi Horst Görtz Institut für IT-Sicherheit