Practical Implementation of Lattice-based cryptography

Adrian Waller

Thales UK

This project has received funding from the European Union H2020 research and innovation programme under grant agreement No 644729

SAFEcrypto Project

4-year H2020 project: Jan 2015 - Dec 2018

SAFEcrypto provides a new generation of practical, robust and physically secure post-quantum cryptographic solutions that ensure long-term security for future ICT systems, services and applications.

Focus is on **lattice-based cryptography** and solutions demonstrated for:

1. Satellite communications
2. Municipal Data Analytics
3. IoT

Queen's University Belfast
CSIT Centre for Secure Information Technologies
THALES
HWCommunications Cyber Security and Resilience
IBM
Inria Inventeurs du monde numérique
DELL EMC
Ruhr Universität Bochum RUB
Università della Svizzera italiana

Quantum-Safe Cryptography

Lattice-based Cryptography (LBC) emerging as a promising PQ candidate

- LBC encryption and digital signatures already practical & efficient
  - NTRUEncrypt exists since 1996 with no significant attacks to date
  - LBC schemes can match and outperform ECDSA/RSA schemes
- Underlying operations can be implemented efficiently
- Allows for other constructions/applications beyond encryption/signatures - Identity based encryption, Attribute-based encryption, Fully homomorphic encryption

Family	Signature	Encryption/ KEM	Total
Lattice-based	5	23	28
Code-based	3	17	20
Multivariate	8	2	10
Hash-based	3	0	3
Isogeny-based	0	1	1
Other	2	5	7
Total	21	48	69

strongSwan

SAFEcrypto

Lattice Based Cryptographic Building Blocks

- **Matrix vector multiplication** for standard lattices
- **Polynomial multiplication** for ideal lattices
- **Error Sampling**
  - Bernoulli sampling
  - Cumulative Distribution Table (CDT) sampling
  - Knuth-Yao sampling
  - Ziggurat sampling
  - Micciancio-Walter Gaussian Sampler
  - …

Challenges for Practical LBC Implementations

- Need to be as efficient and versatile as classical Public Key systems, such as RSA and ECC
- Embedded devices are constrained
  - No large memories
  - Limited computational power
- Choice of parameters is crucial - long-term/QC-security
  - Larger Parameters directly affects performance
  - Scalability
- Choice of Sampler
  - Different choice for signatures Vs encryption
  - Different choice for high speed Vs compact design
- Need to consider vulnerability to Side Channel Analysis

Practical Implementation of Basic Primitives

This project has received funding from the European Union H2020 research and innovation programme under grant agreement No 644729

Lattice-based Encryption on FPGA

- LWE (Standard) Vs Ring-LWE (Ideal) Encryption
  - Standard LBC shown to be practical – 1272 Ops/sec on Spartan 6 FPGA

Operation and Algorithm	Device	LUT/FF/SLICE	BRAM/ DSP	MHz	Cycles	Ops/s
LWE Encrypt ($\lambda = 128$)	S6LX45	6152/4804/1866	73/1	125	98304	1272
LWE Encrypt ($\lambda = 64$)	S6LX45	6078/4676/1811	73/1	125	98304	1272
LWE Decrypt	S6LX45	63/58/32	13/1	144	32768	4395
RLWE Encrypt (Pöppelmann & Güneysu (PG), 2014)*	S6LX16	4121/3513/-	14/1	160	6861	23321
RLWE Decrypt (PG 2014)*	S6LX16	4121/3513/-	14/1	160	4404	36331
RLWE Encrypt (PG 2014)*	V6LX75T	4549/3624/1506	12/1	262	6861	38187
RLWE Decrypt (PG 2014)*	V6LX75T	4549/3624/1506	12/1	262	4404	59492
RLWE Encrypt (PG 2014)	S6LX9	282/238/95	2/1	144	136212	1057
RLWE Decrypt (PG 2014)	S6LX9	94/87/32	1/1	189	66338	2849
RLWE Encrypt (Roy et al, 2014)*	V6LX75T	1349/860/-	2/1	313	6300	49751
RLWE Decrypt (Roy et al, 2014)*	V6LX75T	1349/860/-	2/1	313	2800	109890

Frodo KEM Implementation on ARM

FrodoKEM (standard lattices) has a number of design options:

- FrodoKEM-640 (~ AES-128 security) – **total execution time of 836ms**
- FrodoKEM-976 (~ AES-192 security) – total execution time of 1.84s

PRNG implemented using AES and cSHAKE

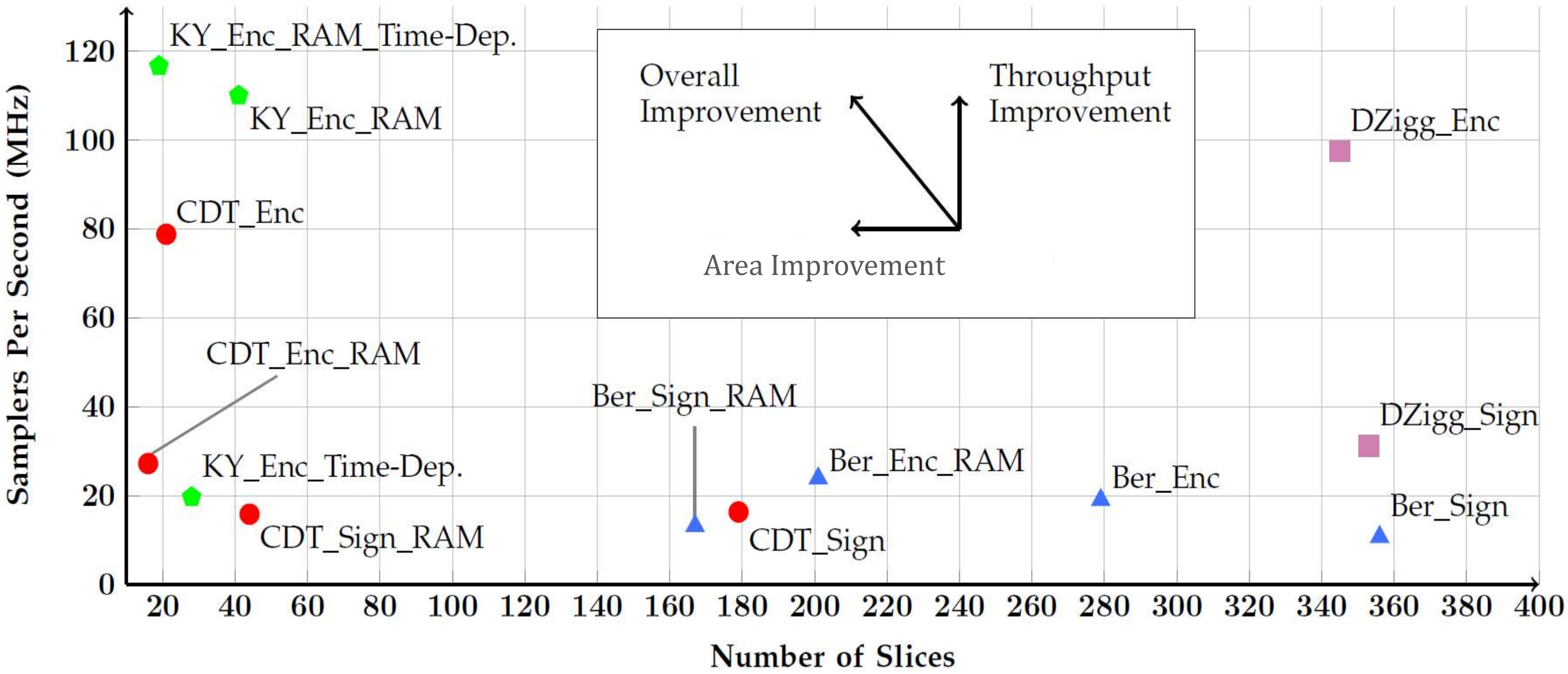
Implementation	Platform	Security Level	Cycle counts
FrodoKEM-640-AES	Cortex-M4	128 bits	140,398,055
FrodoKEM-976-AES	Cortex-M4	192 bits	315,600,317
FrodoKEM-640-cSHAKE	Cortex-M4	128 bits	310,131,435
FrodoKEM-976-cSHAKE	Cortex-M4	192 bits	695,001,098
FrodoKEM-640-cSHAKE [pqm]	Cortex-M4	128 bits	318,037,129
KyberNIST-768 [pqm]	Cortex-M4	192 bits	4,224,704
NewHopeUSENIX-1024 [AJS16]	Cortex-M4	255 bits	2,561,438
ECDH scalar multiplication [DHH+15]	Cortex-M0	pre-quantum	3,589,850

Cycle counts for ARM Cortex-M4 implementations (at 168 MHz)

Error Sampling Evaluation in Hardware

Error Sampling is a key component in LBC - major bottleneck in practice

- *Comprehensive evaluation of Discrete Gaussian Samplers* - offers recommendations on most appropriate sampler to use for encryption, authentication, high-speed applications etc..
- Proposed *independent-time hardware designs* of a range of samplers offering security against side-channel timing attacks

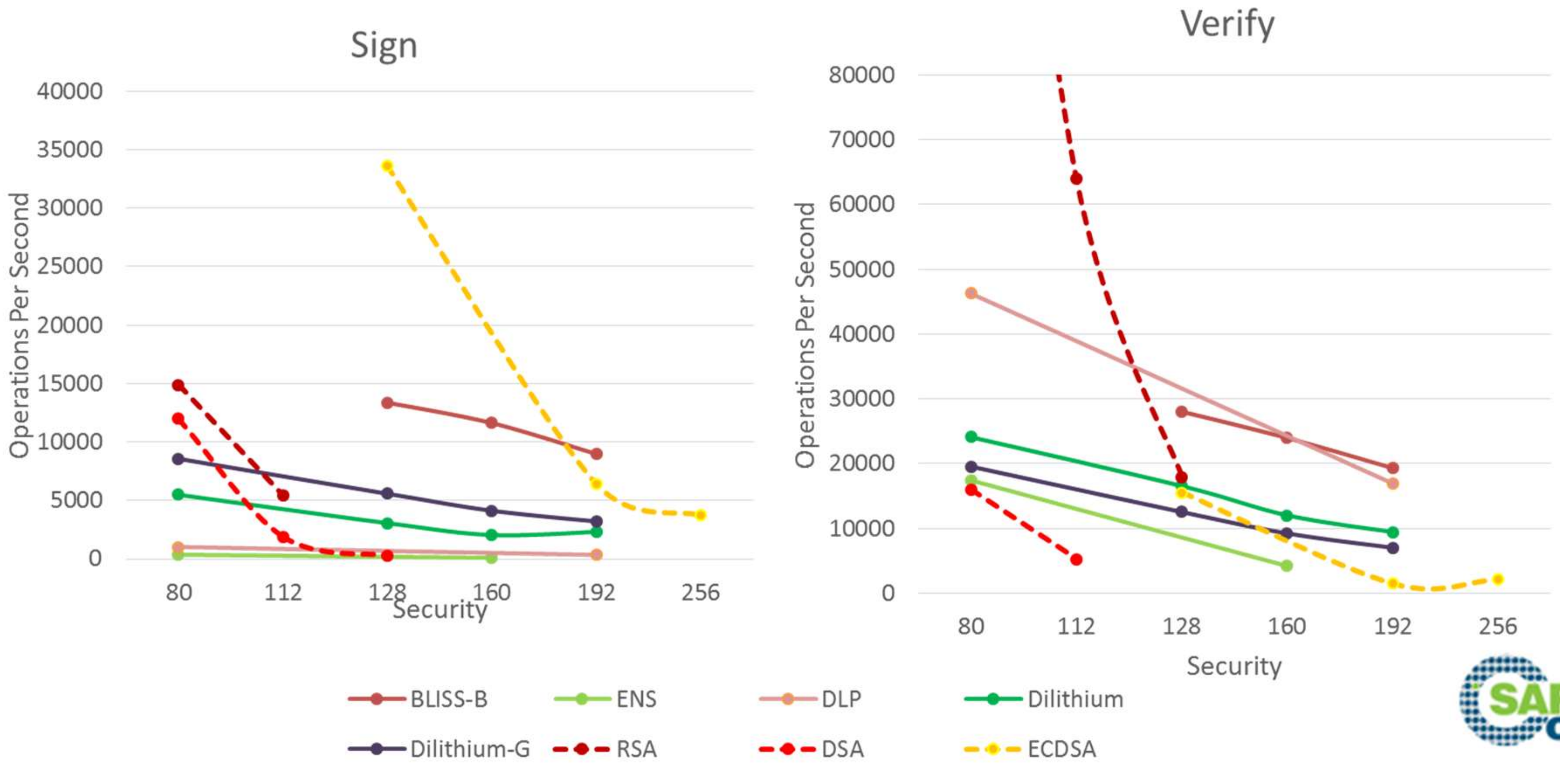


libsafecrypto: https://github.com/safecrypto/libsafecrypto

Open source software library enabling the development of lattice-based crypto solutions for commercial applications. Currently supports:

- **Signatures:** BLISS-B, Dilithium, Dilithium-G, Ring-TESLA, DLP, ENS
- **Encryption:** RLWE, Kyber
- **KEM:** ENS, Kyber

Digital Signatures: Classical vs LBC Signatures (Intel Core i7 6700 3.4 GHz)

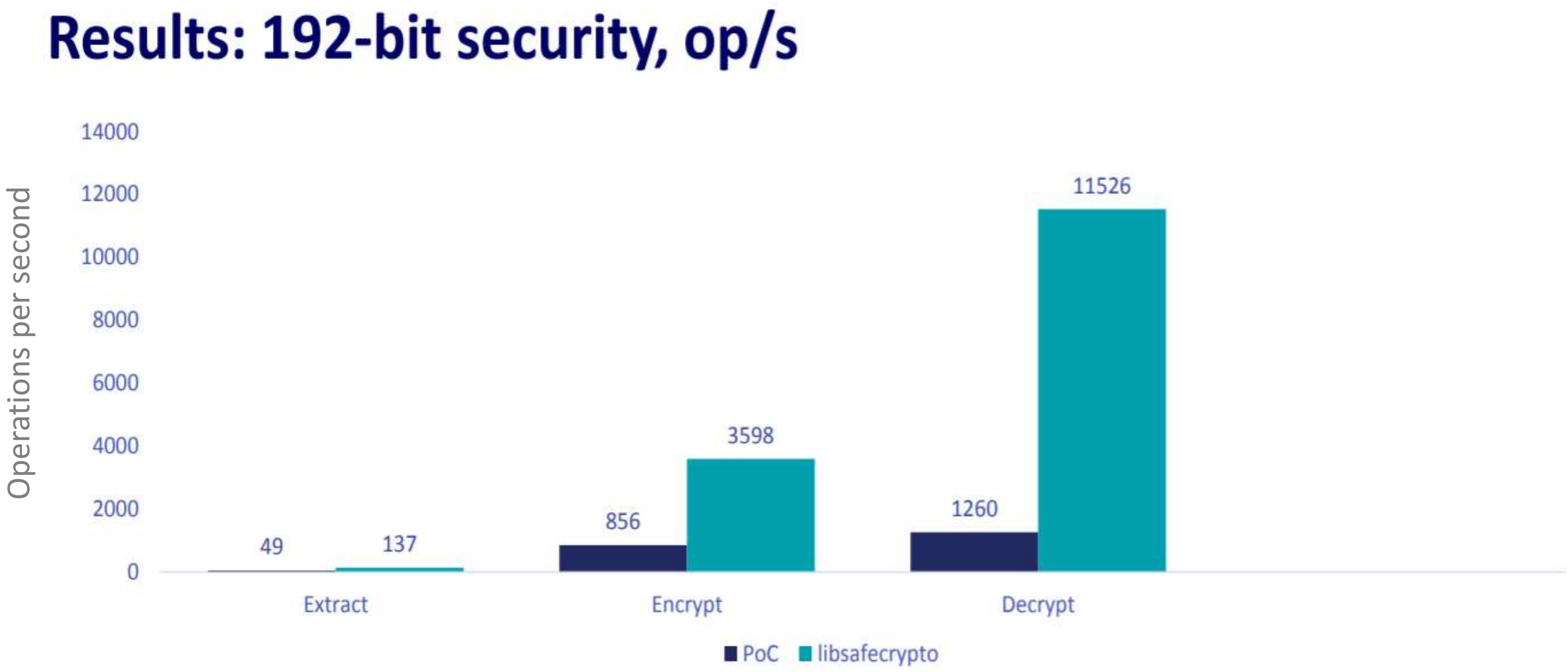


Practical Implementation of Advanced Primitives

This project has received funding from the European Union H2020 research and innovation programme under grant agreement No 644729

Practical lattice-based Identity-Based Encryption

First ANSI C Implementation of DLP-IBE Scheme[1]
(Intel Core i7 6700 3.4 GHz)



1. Ducas, L., Lyubashevsky, V., Prest, T.: Efficient identity-based encryption over NTRU lattices, pp. 22-41. Advances in Cryptology ASIACRYPT 2014, Springer

Practical lattice-based Identity-Based Encryption

Implementation of DLP-IBE Scheme on ARM Cortex-M

Operation/cycles	(512/16813057) Cortex-M0	(512/16813057) Cortex-M4	(1024/134348801) Cortex-M0	(1024/134348801) Cortex-M4
Encryption	3,297,380	972,744	6,202,910	1,719,444
Decryption	1,155,000	318,539	2,171,000	557,015

80 bit security: 5.8ms per enc operation (Cortex-M4)

- Results are 2 orders of magnitude faster than pairing-based IBE implementations
- **Results highlight that IBE is practical for IoT devices**

SAFEcrypto

Side Channel Analysis (SCA) attacks

NIST Post-quantum Cryptography standardisation

In addition to **security**, candidates need to consider **practicality**:

1. Investigation of resistance to physical attacks
2. Development of Side Channel Attack (SCA) countermeasures

“Schemes that can be made resistant to side-channel attack **at minimal cost are more desirable** than those whose performance is severely hampered by any attempt to resist side-channel attacks”[1]

Physical security vulnerabilities of Lattice based constructions are *understudied*

1. http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-forproposals-final-dec-2016.pdf

SCA in the context of Lattice Based Cryptography

Side Channel Analysis (SCA) can be used to extract the secret key from electronic devices using power, EM, timing analysis, acoustics

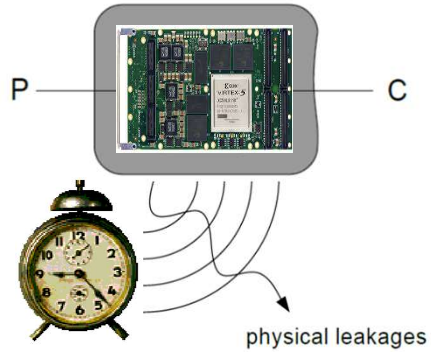
- SCA attacks and their countermeasures are an established field
  - *Why re-invent the wheel?*

- The underlying components of lattice-based schemes are *different compared to* today's prevalent symmetric/asymmetric cryptographic schemes

Timing Attacks on LBC

Timing attacks exploit the **differences in execution time** to perform an operation, e.g.,

- Different execution delays of different instructions, conditional branches
- Data fetch times due to cache memory hit/miss, attacks called *Cache attacks*



Attacks reported on lattice-based schemes target

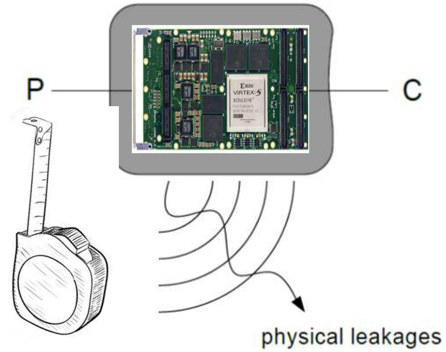
- Different number of calls to Hash function during decryption[1] (NTRU)
- Different cache access patterns in CDT and Bernoulli sampler implementations (BLISS)[2]
- Attacking the shuffled Gaussian samples via a cache attack[3] (BLISS)

1. J H Silverman, W Whyte. Timing attacks on NTRUEncrypt via variation in the number of hash calls. CT-RSA, Springer, 208–224, 2007.
2. L G Bruinderink, A Hülsing, T Lange, Y Yarom. Flush, Gauss, and Reload–a cache attack on the BLISS lattice-based signature, CHES 2016, Springer, 323–345.
3. P Pessl. Analyzing the shuffling side-channel countermeasure for lattice-based signatures. INDOCRYPT 2016, Springer, 153–170

Power Analysis Attacks on LBC

Power analysis attacks extract secret information by **correlating power leakage of a device and the secret values processed** during the algorithm execution.

- Simple Power Analysis (SPA)
- Differential power analysis (DPA)
- First order DPA, Higher order DPA



Attacks reported on lattice-based schemes target

- DIV instruction duration in ARM Cortex-M4 microcontrollers depends on the processed value[1] (RLWE)
- Difference in the hamming distance information, generated during the computation of the convolution product[2] (NTRU)

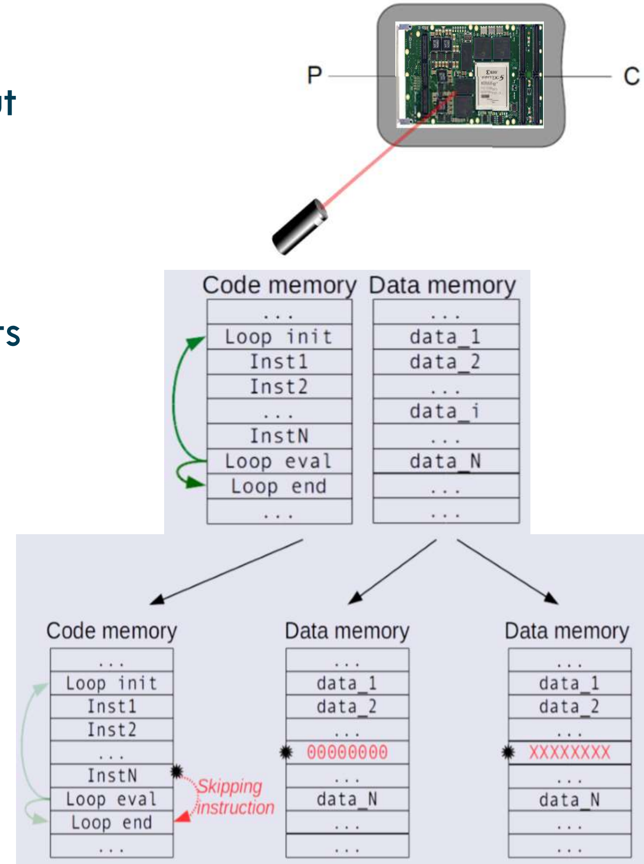
1. R Primas, P Pessl, S Mangard. 2017. Single-Trace Side-Channel Attacks on Masked Lattice-Based Encryption. CHES 2017, Springer, 513–533.
2. M-K Lee, J E Song, D Choi, D-G Han. 2010. Countermeasures against power analysis attacks for the NTRU public key cryptosystem. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 93, 1 (2010), 153–163

Fault Attacks on LBC

- **Fault attack** involves maliciously injecting an error into a device computing cryptographic operations
  - *Exploit the faulty behavior* to gather information about the secret key

- **How**: varying the supply voltage, system clock speed, ambient temperatures. Expensive and highly precise faults injected using dedicated laser beams

- **Effects:** faults shown to induce effects such as
  - changing the values of internal registers, e.g., **zeroing**
  - incorrect branching of the program, e.g., **randomization**
  - skipping of program instructions, e.g., **loop abort**



Fault Attacks on LBC

Fault attacks reported on lattice-based schemes

- Fault injection attacks have been applied to NTRU-Encrypt[1] & NTRU-Sign[2]
- A full recovery of the secret key value is possible by early loop termination of the random commitment vector and the Gaussian sample generation (BLISS,GLP,TESLA, GPV)[3]
- BLISS, ringTESLA and GLP signatures found to be vulnerable to[4]:
  - zeroing faults during the signing and verification,
  - skipping faults during the key generation and verification

1. A. A Kamal, A M Youssef. 2011. Fault analysis of the NTRUEncrypt cryptosystem. IEICE transactions on fundamentals of electronics, communications and computer sciences 94, 4, 1156–1158, 2011
2. A. A Kamal, A M Youssef. 2012. Fault analysis of the NTRUSign digital signature scheme. Cryptography and Communications 4, 131–144, 2012.
3. T Espitau, P-A Fouque, B Gérard, M Tibouchi, Loop-abort faults on lattice-based Fiat-Shamir and hash-and-sign signatures. SAC 2016, Springer, 140–158.
4. N Bindel, J Buchmann, J Krämer. Lattice-based signature schemes and their sensitivity to fault attacks. FDTC 2016, pp. 63–77.

SAFEcrypto

Practical Case Studies

This project has received funding from the European Union H2020 research and innovation programme under grant agreement No 644729

THALES

Satellite Communications Case Study

Thales have integrated SAFEcrypto implementations of QS algorithms into StrongSwan

- IPsec relies on Diffie-Hellman (or its Elliptic Curve variant) for key agreement and on ECDSA or RSA for authentication, when setting up secure channels using the IKEv2 protocol

Thales UK have implemented:

- IKEv2 using algorithms submitted to the NIST competition with SAFEcrypto contributions: Kyber and Dilithium
  - Using Software (ground) and FPGA (space-qualified)
- Analysed their suitability in terms of performance, memory usage and message sizes
- Demonstrated using simulated communications between ground and satellites
- Hybrid Kyber and ECDH
  - draft-tjhai-ipsecme-hybrid-qske-ikev2-01

Lessons learnt

- No issues in meeting application requirements
- Hybrid approach is attractive for risk averse customers

KMIP for solution deployments

Dell EMC have investigated generation and management of QS keys in its KMIP (Key Management Interoperability Protocol) supported key management offerings.

- KMIP is widely used standard used in many systems including embedded systems to enable interoperability across vendors for management and distribution of cryptographic keys.

Dell EMC contributions have included:

- Liaising with KMIP committee on standardisation approaches
- Integrating SAFEcrypto library into Key Trust Platform product
- Demonstration in a municipal data analytics use case
  - Secure collection of environmental sensor data for the purpose of informing policy decision making
  - Quantum safe digital signature algorithms applied on application layer data

Lessons learnt

- KMIP requires only a few changes to support QS
- No issues in meeting application requirements

HWCommunications
Cyber Security and Resilience

Integrating QS into tinydtls

HW Comms is integrating SAFEcrypto implementations of QS algorithms into IoT smart tag sensors.

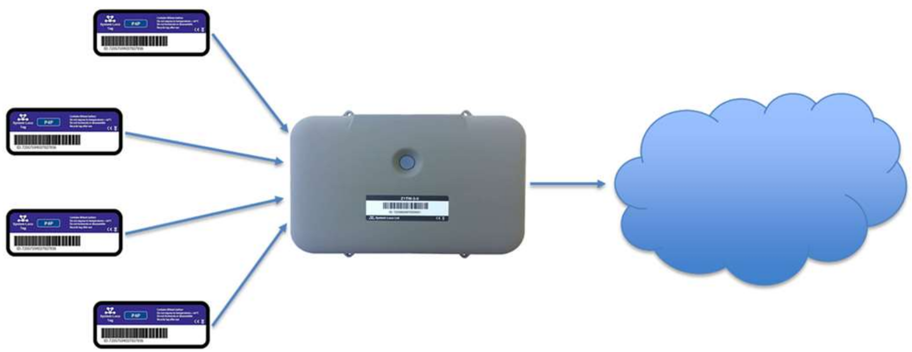
- tinydtls - a light-weight implementation of the DTLS protocol that can be used in devices with tight memory constraints aimed at IoT devices

The implementation includes the following:

- Quantum Secure DTLS handshaking with Kyber and Dilithium
- Legacy support for ECDH and Pre-Shared Keys remains
- Support for QS constrained application protocol (CoAP) with libcoap and modified tinydtls
- QS Identity Based Encryption (DLP-IBE) implemented on smart tags

Lessons learnt

- No issues in meeting application requirements
- Even IBE possible on constrained devices
  - ARM Cortex-M0/M4

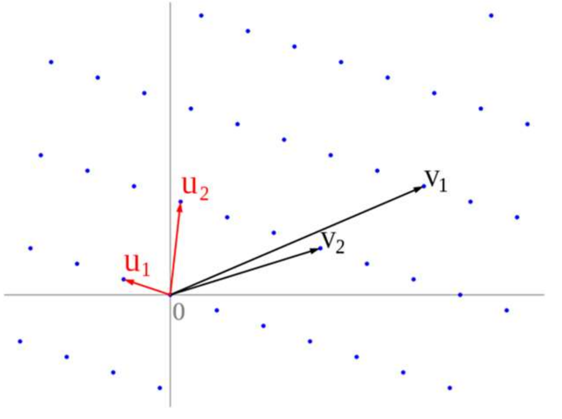


Conclusions

- Lattice-based cryptosystems are a **promising Post-Quantum cryptography solution** for long-term security applications

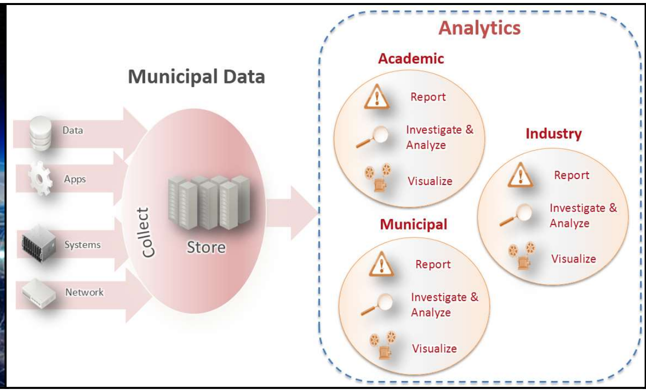
- LBC **offers versatility** in the range of cryptosystems it can support

- **Practical Implementations of lattice-based schemes** possible:
  - Standard LWE, RLWE Encryption
  - Frodo KEM
  - Dilithium, Kyber, RingTESLA, BLISS-B
  - Lattice-based AKE
  - Lattice-based IBE



Conclusions

- Important to **consider SCA countermeasures appropriate to LBC** and their effect on performance.
- SAFEcrypto outputs demonstrate that ***Lattice-based cryptography can meet the requirements of real world scenarios***.

Project Deliverables and Publications can be found at www.safecrypto.eu