The Queen's Anniversary Prizes For Higher and Further Education 2015

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Accelerating lattice-based and homomorphic encryption with optimised hardware designs

Dr Ciara Rafferty

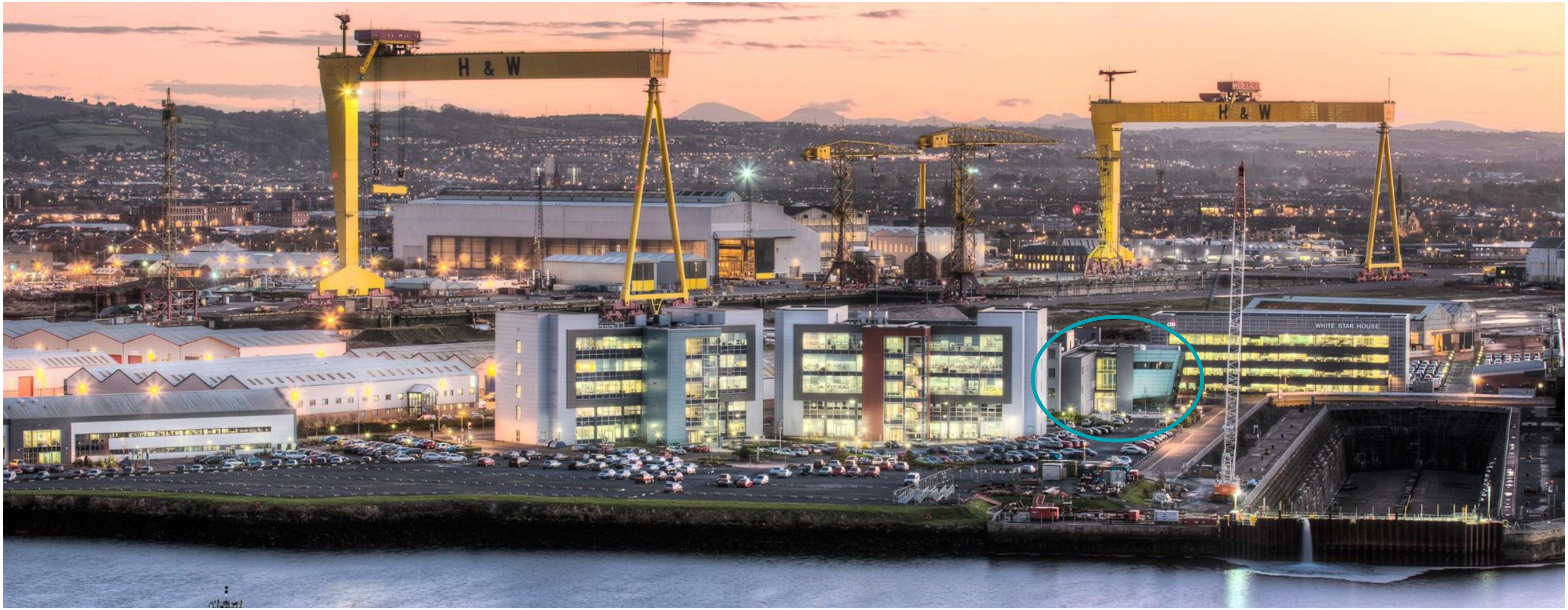
15 January 2018

Overview

1. Introduction
2. SAFEcrypto project overview
3. Hardware design considerations
4. Example: FHE
5. Example: LWE v RLWE
6. Future research directions

1. Introduction

CENTRE FOR SECURE INFORMATION TECHNOLOGIES



DSS Group

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Academics

Professor Máire O’Neill

Dr Ciara Rafferty

Currently recruiting - 2 posts

Post-doctoral Researchers

Dr Ayesha Khalid

Dr Chongyan Gu

Visiting Researchers

Dr Dooho Choo,
Principal Researcher, ETRI

Engineers

Gavin McWilliams (Director of Engineering)

Dr Neil Hanley (Senior Engineer)

Dr Neil Smyth (Senior Engineer)

Dr Philip Hodgers (Senior Engineer)

PhD Students

Richard Gilmore

Emma McLarnon

Sarah McCarthy

Seamus Brannigan

Shichao Yu

Jack Miskelly

2. SAFEcrypto overview

Rationale

What happens if/when quantum computers become a reality ?

Commonly used Public-key encryption algorithms
(based on integer factorisation and discrete log problem) such as:

RSA, DSA, DHKE, EC, ECDSA

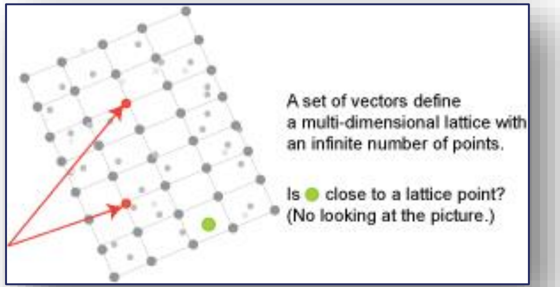
will be vulnerable to Shor's algorithm and ***will no longer be secure***.

Symmetric algorithms appear to be secure against quantum computers (and Grover's algorithm) by simply increasing the associated key sizes.

Quantum-Safe Cryptography

Post-Quantum Cryptography: aims to build cryptosystems from classical problems for which there is no known way to recast the problem in a quantum framework.

- **Code-based cryptography**:
  hard problem based on error correcting codes
- **Hash-based signature schemes**:
  based on properties of preimage and collision resistance
- **Multivariate-quadratic signature schemes**:
  based on solving multivariate quadratic equations in a finite field
- **Isogeny-based cryptography:**
  based on homomorphisms between elliptic curves
- **Lattice-based cryptography:**
  based on shortest vector/closest vector problems



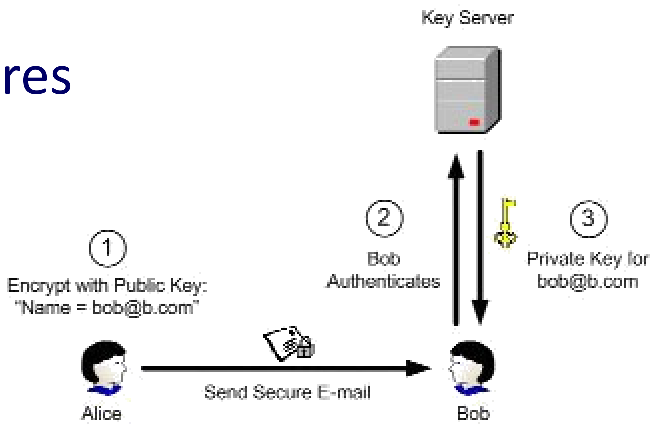
Quantum-Safe Cryptography

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

- LBC encryption and digital signatures already practical & efficient
  - NTRUEncrypt exists since 1996 with no significant attacks to date
  - Recent LBC signatures schemes shown to outperform RSA sig schemes

- Underlying operations can be implemented efficiently

- Allows for other constructions/applications beyond encryption/signatures
  - Identity based encryption (IBE)
  - Attribute-based encryption (ABE)
  - Fully homomorphic encryption (FHE)



CENTRE FOR SECURE INFORMATION TECHNOLOGIES

NATIONAL SECURITY AGENCY | CENTRAL SECURITY SERVICE

Defending Our Nation. Securing The Future.

HOME | ABOUT NSA | ACADEMIA | BUSINESS | CAREERS | INFORMATION ASSURANCE | RESEARCH | PUBLIC INFORMATION | CIVIL LIBERTIES

Information Assurance

- About IA at NSA
- IA Client and Partner Support
- IA News
- IA Events
- IA Mitigation Guidance
- IA Academic Outreach
- IA Business and Research
- IA Programs
  - Commercial Solutions for Classified Program

Home > Information Assurance > Programs > NSA Suite B Cryptography

SEARCH

Cryptography Today

In the current global environment, rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms and secure protocol standards are vital tools that contribute to our national security and help address the ubiquitous need for secure, interoperable communications.

Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to quantum resistant algorithms.

August 2015

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Quantum-safe Cryptography

US NIST - Call for Quantum-Resistant Cryptographic Algorithms (Aug 2016) for new public-key cryptography standards. *Draft standards expected in 6-8 years*

In addition to **theoretical algorithm proposals**, candidates need to consider **practicality**:

- Hardware & software architectures of quantum-resistant candidates
- Investigation of resistance to physical attacks
- Development of Side Channel Attack (SCA) countermeasures

Standardisation efforts also underway by ETSI and ISO/IEC groups (*CSIT actively involved in these)*

Round 1: NIST Submission Summary

Type	Signatures	KEM/Encryption	Overall
Lattice-based	4	24	28
Code-based	5	19	24
Multi-variate	7	6	13
Hash-based	4	-	4
Other	3	10	13
Total	23	59	82

**Table from ASIACRYPT talk 2017 by Dustin Moody*

SAFEcrypto: Secure Architectures of Future Emerging cryptography

Professor Máire O'Neill

Queen's University Belfast

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

CSIT is a Research Centre of the ECIT Institute

SAFEcrypto Project:

€3.8M 4-year H2020 project – commenced Jan 2015

SAFEcrypto will provide 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. Public-safety communications systems
3. Municipal Data Analytics

SAFEcrypto Project: Objectives

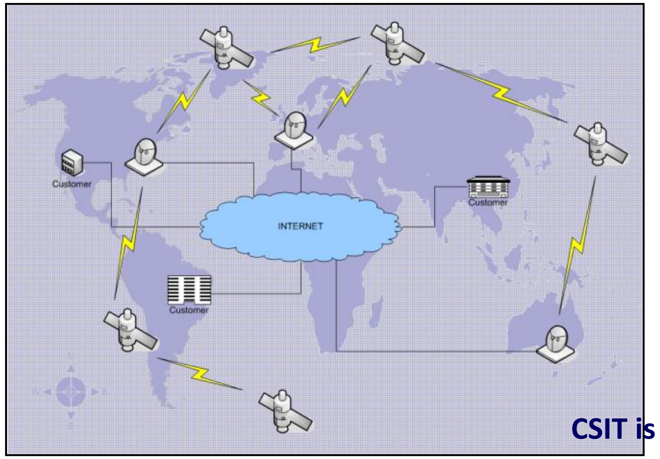
1. Investigate practicality of LBC primitives (digital signatures, authentication, IBE and ABE) to determine their fit-for-purpose in real-world applications
2. Design and implement hardware & software architectures of LBC primitives that will fulfill the needs of a wide range of applications
3. Investigate the physical security of the LBC implementations to protect against leakage of sensitive information via side channel and fault attacks
4. Evaluate LBC in current secure comms protocols, such as TLS, IPSec
5. Deliver *proof-of-concept demonstrators* of LBC primitives applied to 3 case-studies:
    - Satellite Communications
    - Public Safety Communication
    - Municipal Data Analytics

1. Satellite Communications

Security and key management vital within satellite systems

- Currently: - systems owned and operated by one organisation
  - symmetric key crypto exclusively used

- In future: - Repurposing of satellites and sharing of infrastructure
  - Number of space-based entities, missions & number/ variety of end users will increase
  - *Public key cryptography will be used*



- Given the longevity of satellite systems, public key solutions needs to withstand attacks for 10-40 years

  => ideal case study for post-quantum cryptography

2. Public Safety Communications

- Traditionally public safety comms relied on security of bespoke systems and closed networks.

- Future systems seeking to use COTS technology.

- LTE identified as a potential network layer solution
  - The browser application WebRTC may be used (*uses DTLS protocol*)

www.qinetiq.com

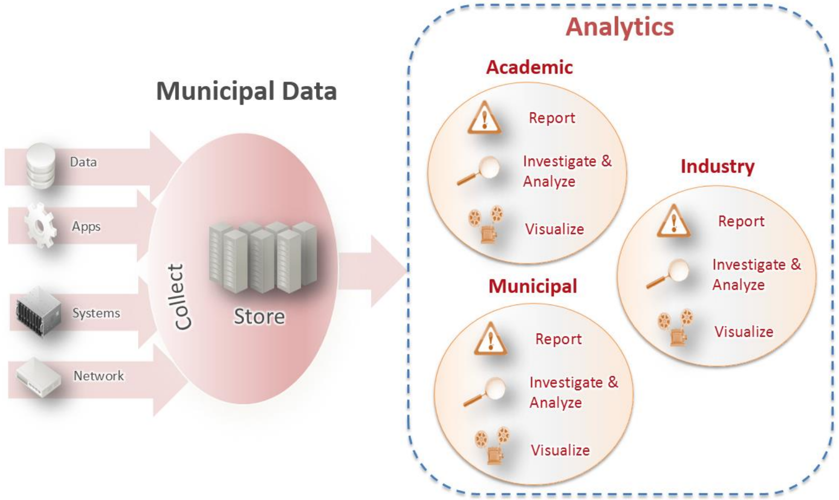
- Public safety comms technology may not be refreshed for up to 30 years…

  => need to provide long term security assurances e.g via post quantum cryptography

3. Municipal data analytics

- Significant benefits possible through collaborative analytics of large government-owned data sets;
- Needs appropriate management of accessibility & privacy of the info
- *Group key management* a key requirement

Need for long-term protection of personal & sensitive info within data sets



SAFEcrypto will provide:

- LBC key management approaches
  to manage access to data through group keys, broadcast keys, etc.
- A practical lattice-based IBE scheme *(potentially ABE)*

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
  - Parameters tend to be larger than classic PK schemes
  - Directly affects performance
  - Scalability

- (Understudied) Side channel vulnerabilities
  - Weaknesses in sampling
  - Emerging fault attacks…

Lattice Based Cryptographic Building Blocks

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

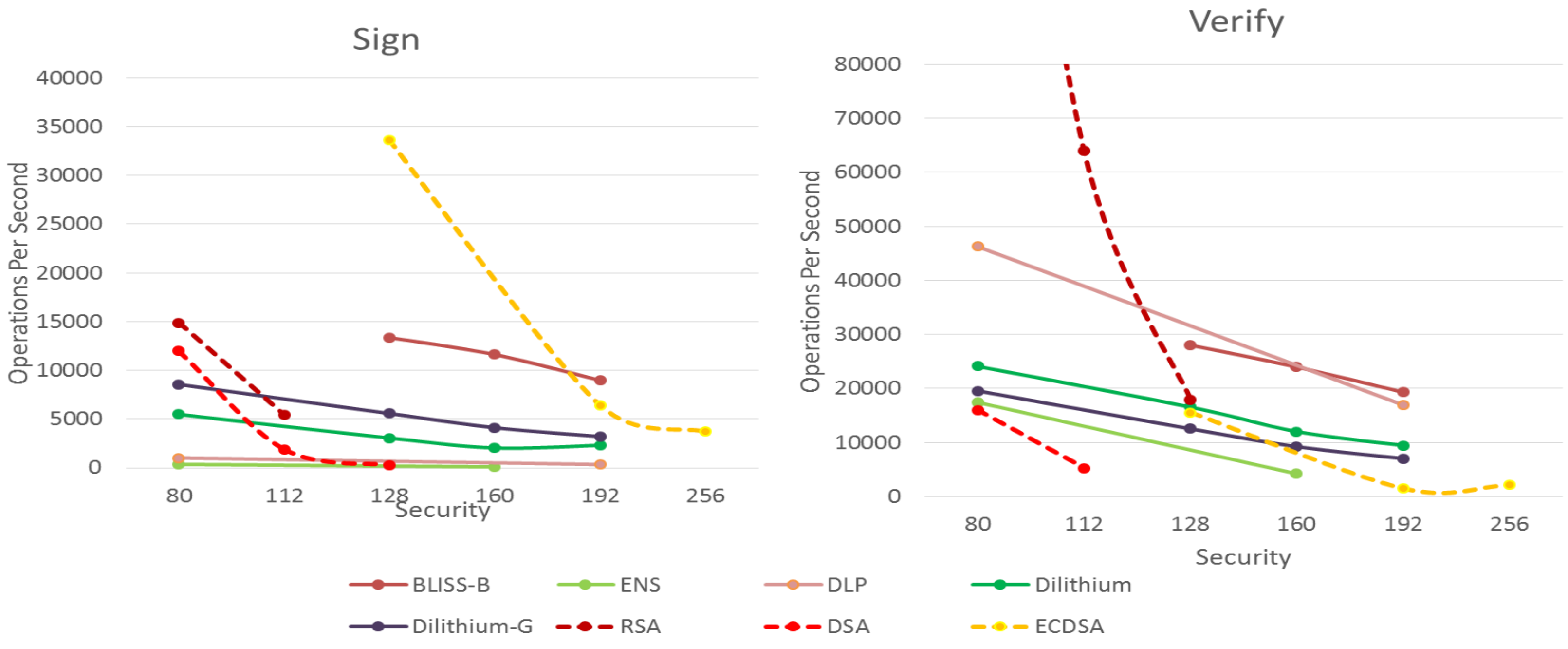
Outputs

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

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

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

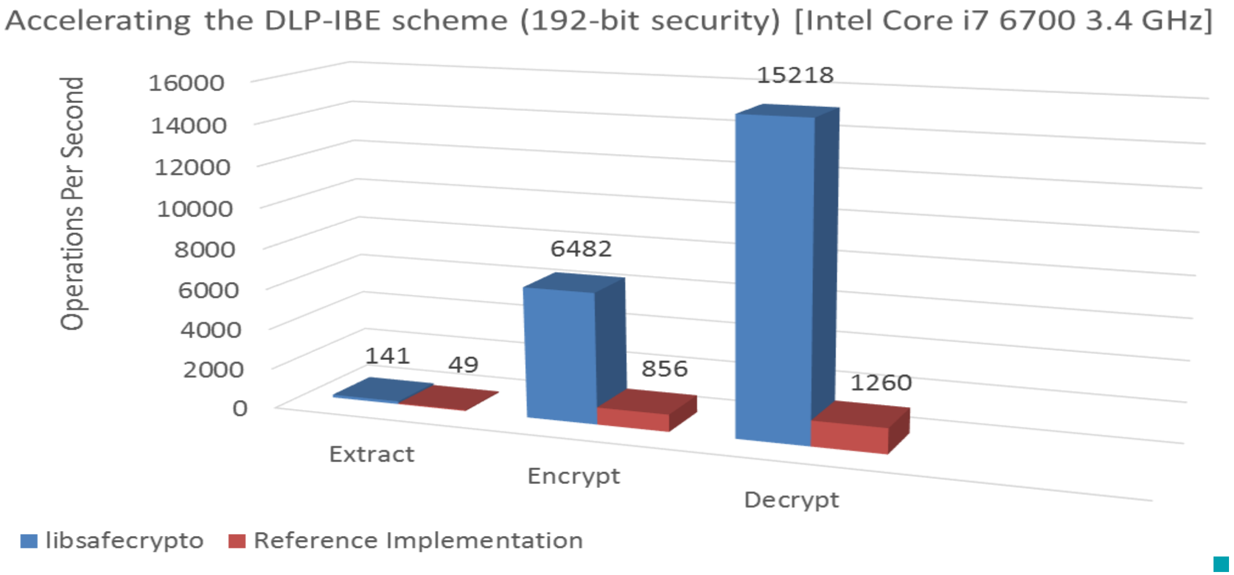
Digital Signatures: Classical vs LBC Signatures
(Intel Core i7 6700 3.4 GHz)



Outputs

Practical Identity-Based Encryption over NTRU Lattices

- First ANSI C Implementation of DLP-IBE Scheme



- ARM Cortex-M0/M4

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

* Sarah McCarthy, Neil Smyth, Elizabeth O'Sullivan, *"A Practical Implementation of Identity-based encryption over NTRU lattices" IMACC2017;*
** Tim Güneysu, Tobias Oder, "Towards lightweight IBE for the post-quantum-secure Internet of things", ISQED 2017*

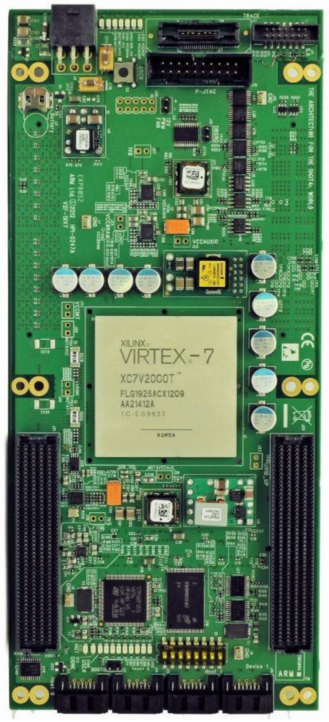
Future Plans

- Proof-of-concept ASIC designs
- Design and **implementation of physically secure** HW/SW LBC schemes
- **Proof of concept demonstrators** for the 3 case studies will generate quantum-safe solutions for a range of commonly used protocols, e.g. IKEv2, TLS, DTLS, KMIP
  - Applicable across many more use cases than those considered in SAFEcrypto
- Actively contribute to **current global initiatives**:
  - ETSI QSC Industry Specification Group
  - US NIST competition for Quantum-safe public-key candidates

3. Hardware design considerations

Hardware design goals

- High speed
- High throughput
- Low area / lightweight
- Low power / green
- Flexibility
- Reusability
- Security v implementation costs…



Hardware designs are highly dependant on the application and associated requirements

Target Platform

Field Programmable Gate Arrays (FPGAs)	Application Specific Integrated Circuits (ASICs)
• Flexible, reprogrammable designs • Fast turn-around time • Cost-effective, particularly for prototyping • Simpler to design	• Bespoke, fully customisable circuit designs • Highly optimised, low area designs possible • Slow turn-around time • Costly - suitable for large production volumes

Physical security

Several physical attack vectors:	Associated countermeasures:
• Power analysis • Timing analysis • Electromagnetic resonance • Fault attacks…	• Avoid conditional branches or loops bounded by secret value • Constant time implementations • Inclusion of dummy operations • Shuffling of operations • Masking • Physical active shields or anti-tampering countermeasures on device…

- Even if we are not considering hardware designs, we need to consider physical security

** For more information on physical security of Lattice-based Cryptography, see the following deliverable available on the SAFEcrypto website: "State-of-the-Art in Physical Side-channel Attacks and Resistant Technologies"*

Other considerations

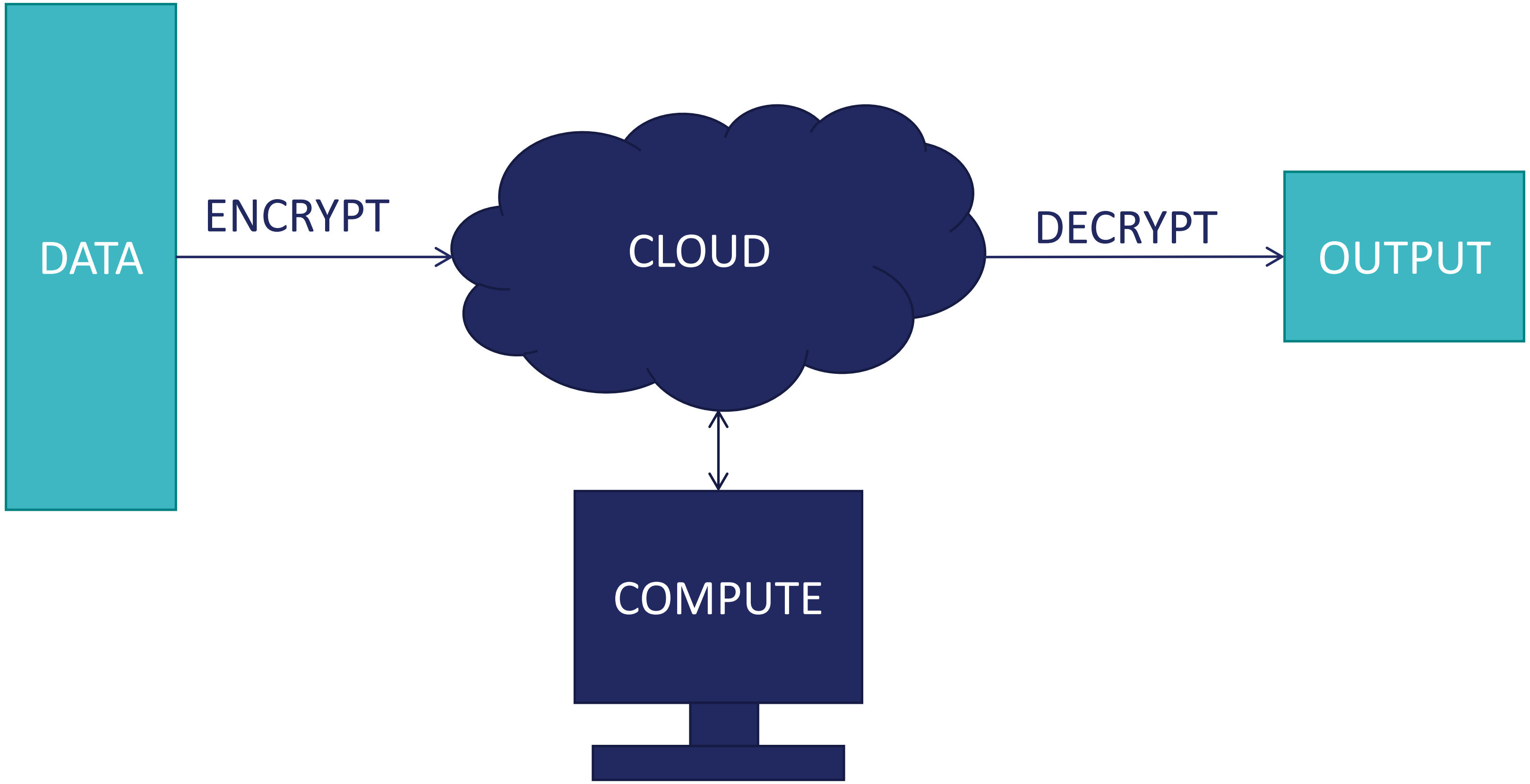
- Physical size:
  - Bit lengths of inputs, outputs, etc.
  - Memory requirements

- Minimisation of costly operations:
  - Divisions
  - Multiplications
  - Modular reductions

- Parallelism

4. Example: FHE

FHE Summary



Fully Homomorphic Encryption enables computation on encrypted data without the use of a decryption key

Motivation for FHE/SHE

- FHE allows computation on ciphertexts without the decryption key

- Introduced in 2009 by Craig Gentry
- Applications include:
  - Secure cloud computing
  - Multi-party computation

- Several theoretical developments since 2009, but FHE remains **highly unpractical**

Challenges for FHE

- Theoretical optimisations
- Parameter selection
- Implementation bottlenecks:
  - Multiplication
  - Modular reduction
- Memory challenges

FHE over the integers

$$C = m + 2r + 2\sum_{i=1}^{\theta} b_i x_i \, mod \, x_0$$

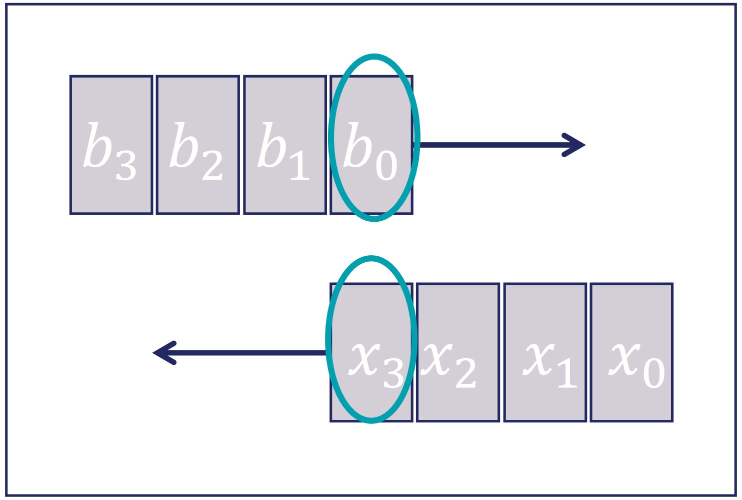
Parameter sizes	Bit-length of b_i	Bit-length of x_i or x_0	θ
Toy	936	150,000	158
Small	1476	830,000	572
Medium	2016	4,200,000	2110
Large	2556	19,350,000	7659

Coron et al., Public Key Compression and Modulus Switching for FHE over the Integers, EUROCRYPT 2012

Our Approach

1. Optimised **large multiplier architecture** for FPGA
2. Analysis of suitable **moduli** for modular reduction and NTT multiplication
3. Hardware architectures of **modular reduction techniques**
4. Hardware architecture of the **encryption** primitive of FHE over the integers
5. Combination of algorithmic and hardware optimisations to improve performance

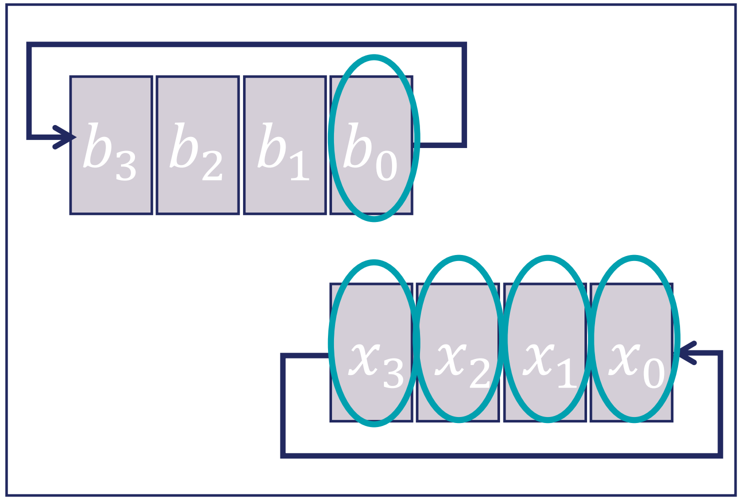
Comba multiplication



	DSP0	DSP1	DSP2	DSP3
1.	b_0x_3			
2.	b_1x_3	b_0x_2		
3.	b_2x_3	b_1x_2	b_0x_1	
4.	b_3x_3	b_2x_2	b_1x_1	b_0x_0
5.	b_3x_2	b_2x_1	b_1x_0	
6.	b_3x_1	b_2x_0		
7.	b_3x_0			

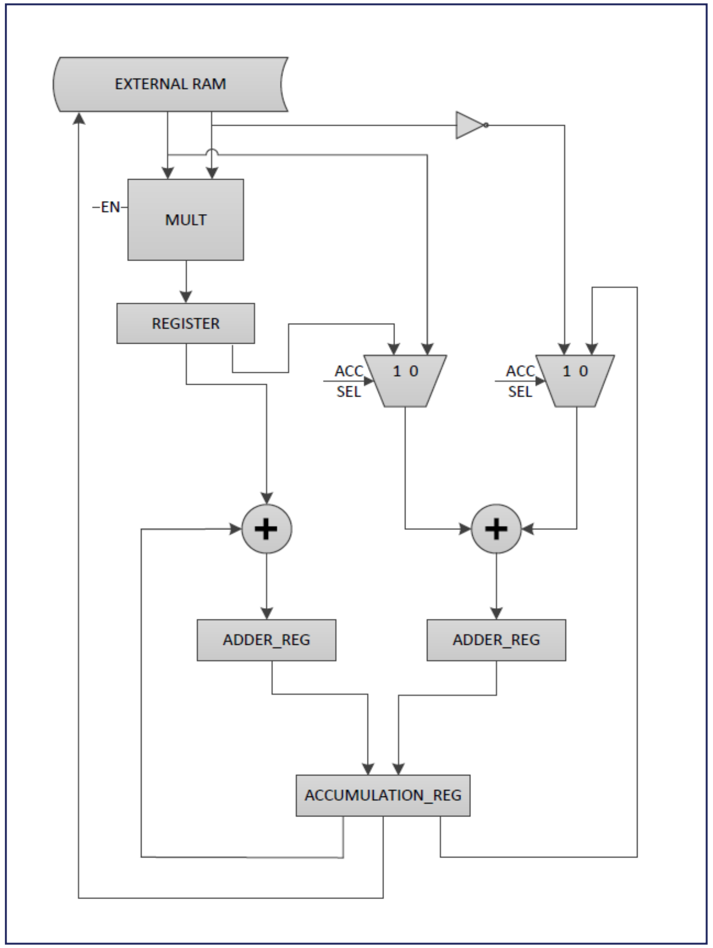
T. Güneysu, *"Utilizing Hardware Cores of Modern FPGA Devices for High-Performance Cryptography"*, J. Cryptographic Engineering

Comba multiplication

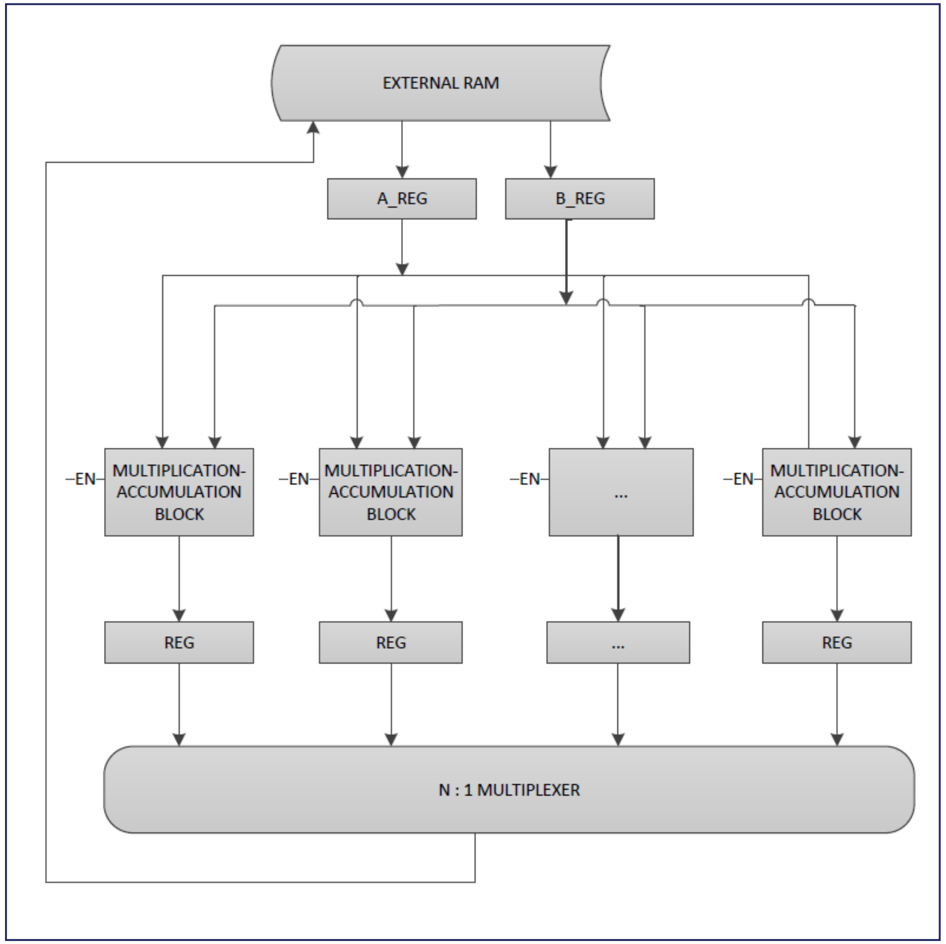


	DSP0	DSP1	DSP2	DSP3
1.	b_0x_3	b_0x_2	b_0x_1	b_0x_0
2.	b_1x_2	b_1x_1	b_1x_0	b_1x_3
3.	b_2x_1	b_2x_0	b_2x_3	b_2x_2
4.	b_3x_0	b_3x_3	b_3x_2	b_3x_1

Proposed Architectures



Low-area design



High-speed design

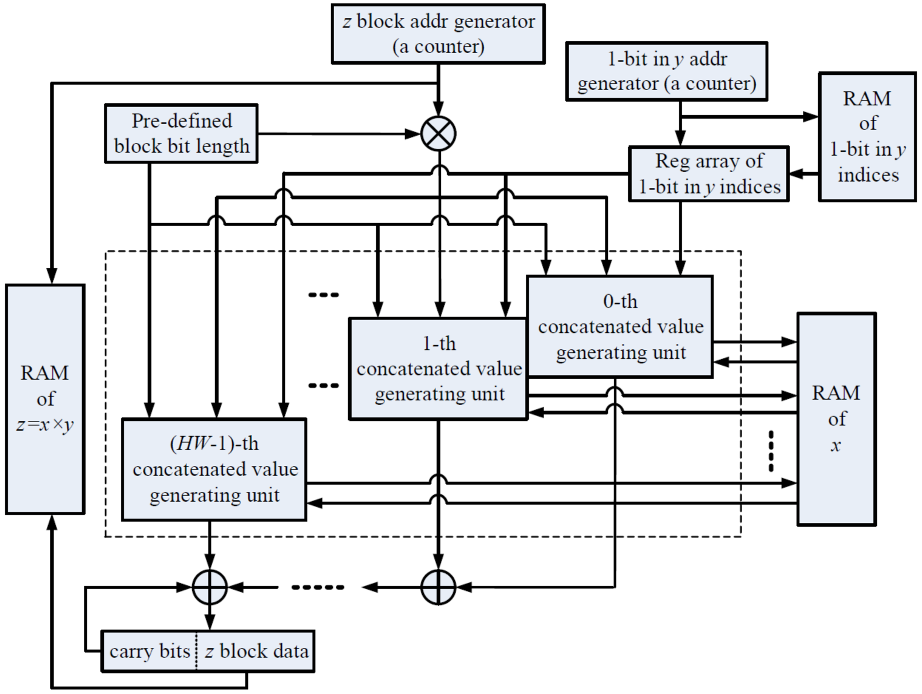
High-speed FHE over the integers

$$C = m + 2r + 2\sum_{i=1}^{\theta} b_i x_i \bmod x_0$$

Parameter sizes	Bit-length of b_i	Bit-length of x_i or x_0	θ
Toy	936	150,000	158
Small	1476	830,000	572
Medium	2016	4,200,000	2110
Large	2556	19,350,000	7659

b_i can be taken to be a Low Hamming Weight (LHW) integer with max HW of 15

Proposed LHW Multiplier Architecture



High-speed FHE over the integers

Coron et al., Public Key Compression and Modulus Switching for FHE over the Integers, EUROCRYPT 2012

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

THALES

Average timings of various implementations of integer based FHE encryption

Design	Toy	Small	Medium	Large
LHW design	0.0006s	0.011s	0.198s	3.317s
Low-latency design	0.00336s	0.05566s	0.9990s	16.595s
Prior FFT design (WAHC14)	0.000739s	0.0132s	0.4772s	7.994s
Comba design – high speed (SiPS14)	0.006s	0.114s	2.018s	32.744s
Benchmark software design	0.05s	1.0s	21s	7min 15s

Achieves 1-bit encryption in 3.3 secs - **x131 speed-up** for large parameter size

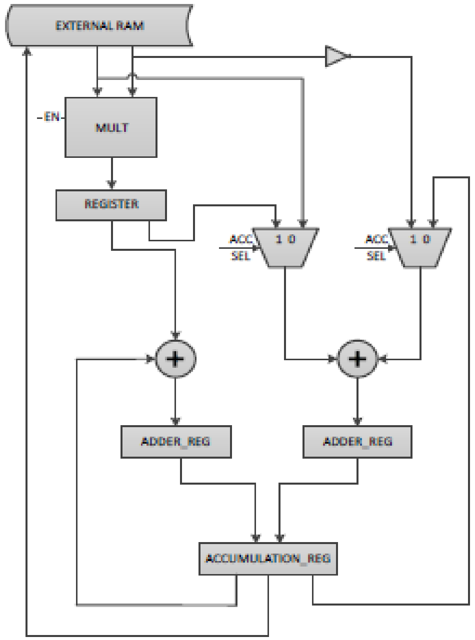
Still not practical!

FHE Results Summary

- Hardware acceleration of vital importance to achieve **practical** performance levels

- Novel **hardware** architectures of FHE encryption step with Comba multiplier and NTT+LHW multiplier

- Speed up factors of **up to 130** are achieved for a hardware design of the encryption step



Low-area architecture of FHE Encryption

"Optimised Multiplication Architectures for Accelerating Fully Homomorphic Encryption", by Xiaolin Cao, Ciara Moore, Máire O'Neill, Elizabeth O'Sullivan, Neil Hanley, IEEE Trans. On Computers 2016

5. Example: LWE

Standard v Ring LWE

LWE problem: find a secret key **s**, given access to $(\boldsymbol{A}, \boldsymbol{b}) \in \mathbb{Z}_q^{n \times n} \times \mathbb{Z}_q^n$, where $\boldsymbol{b} \equiv \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \bmod q$

Standard-LWE	Ring-LWE
Large key sizes required (size N^2)	**Reduced key sizes** can be used due to ideal lattice assumption (size N)
Matrix-vector multiplications required	**Reduces computations** to polynomial multiplication, allowing use of fast NTT multiplication
Security is based on the LWE problem	Security is based on the LWE problem with **an additional security assumption** to use an ideal lattice structure

Approach

- Consider standard LWE encryption to evaluate its practicality as an alternative option to ring LWE
- Goal is long term security
- Selection of standard LWE is application dependent
- First evaluation of standard LWE on hardware
- Spartan-6 FPGA targeted, balance area and performance

LWE Encryption Scheme *(Lindner & Peikert 2011)*

$n = 256,$
$q = 4093,$
$\sigma = 3.33,$

Medium parameter set

KEY GENERATION:

- $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times n}$
- $\boldsymbol{R_1}, \boldsymbol{R_2} \leftarrow D_\sigma^{n \times l}$
- $\boldsymbol{P} \equiv \boldsymbol{R_1} - \boldsymbol{A} \cdot \boldsymbol{R_2} \bmod q$

ENCRYPTION:

- $\boldsymbol{e_1}, \boldsymbol{e_2}, \boldsymbol{e_3} \leftarrow D_\sigma^n \times D_\sigma^n \times D_\sigma^l$
- $\bar{\boldsymbol{m}} = encode(\boldsymbol{m})$
- $c_1 \equiv e_1^t \boldsymbol{A} + e_2^t \bmod q;$
- $c_2 \equiv e_1^t \boldsymbol{A} + e_3^t + \bar{\boldsymbol{m}}^t \bmod q$

DECRYPTION:

- $\boldsymbol{m} = decode(\boldsymbol{c_1^t} \boldsymbol{R}_2 + \boldsymbol{c_2^t})$

Architecture of standard LWE encryption

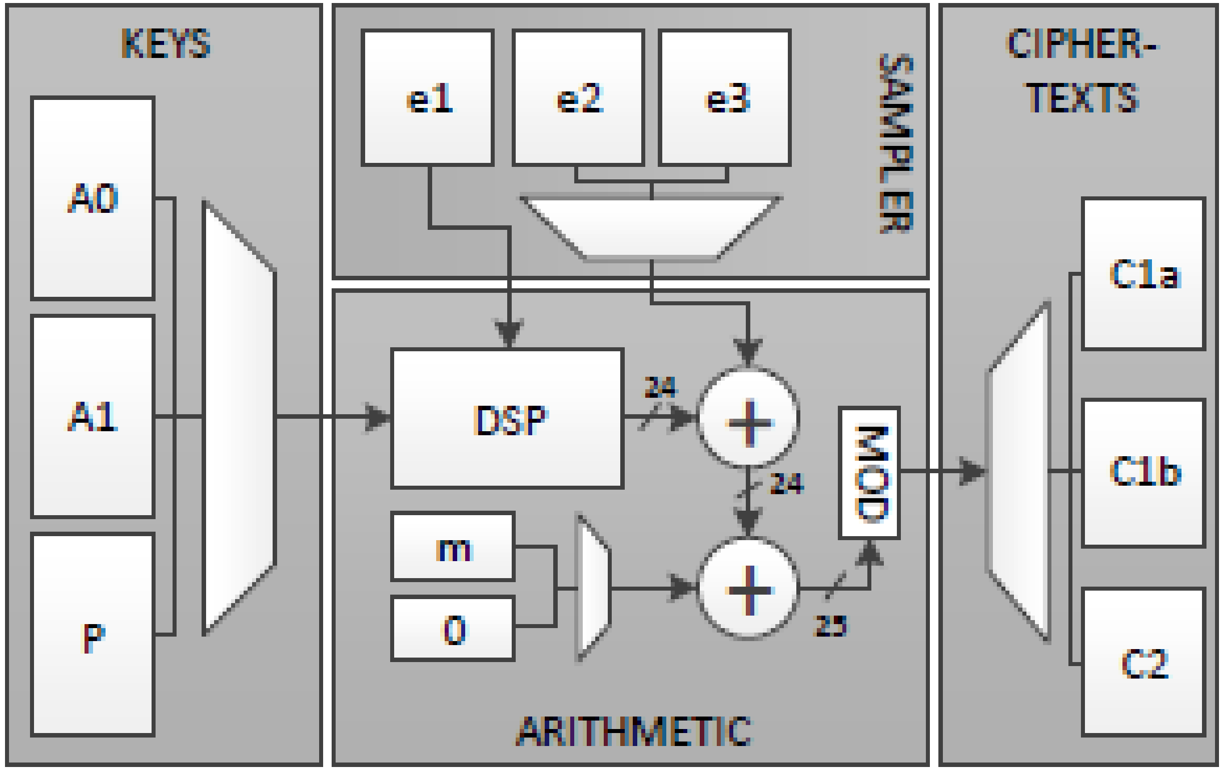


Figure 1: High level architecture of LWE encryption scheme. Lengths are 12 bits unless otherwise stated.

Architecture of standard LWE encryption

KEY GENERATION:

- $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times n}$
- $\boldsymbol{R_1}, \boldsymbol{R_2} \leftarrow D_\sigma^{n \times l}$
- $\boldsymbol{P} \equiv \boldsymbol{R_1} - \boldsymbol{A} \cdot \boldsymbol{R_2} \; mod \; q$

ENCRYPTION:

- $\boldsymbol{e_1}, \boldsymbol{e_2}, \boldsymbol{e_3} \leftarrow D_\sigma^n \times D_\sigma^n \times D_\sigma^l$
- $\bar{\boldsymbol{m}} = encode(\boldsymbol{m})$
- $c_1 \equiv e_1^t \boldsymbol{A} + e_2^t \; mod \; q;$
- $c_2 \equiv e_1^t \boldsymbol{P} + e_3^t + \bar{\boldsymbol{m}}^t \; mod \; q$

DECRYPTION:

- $\boldsymbol{m} = decode(\boldsymbol{c_1^t} \boldsymbol{R_2} + \boldsymbol{c_2^t})$

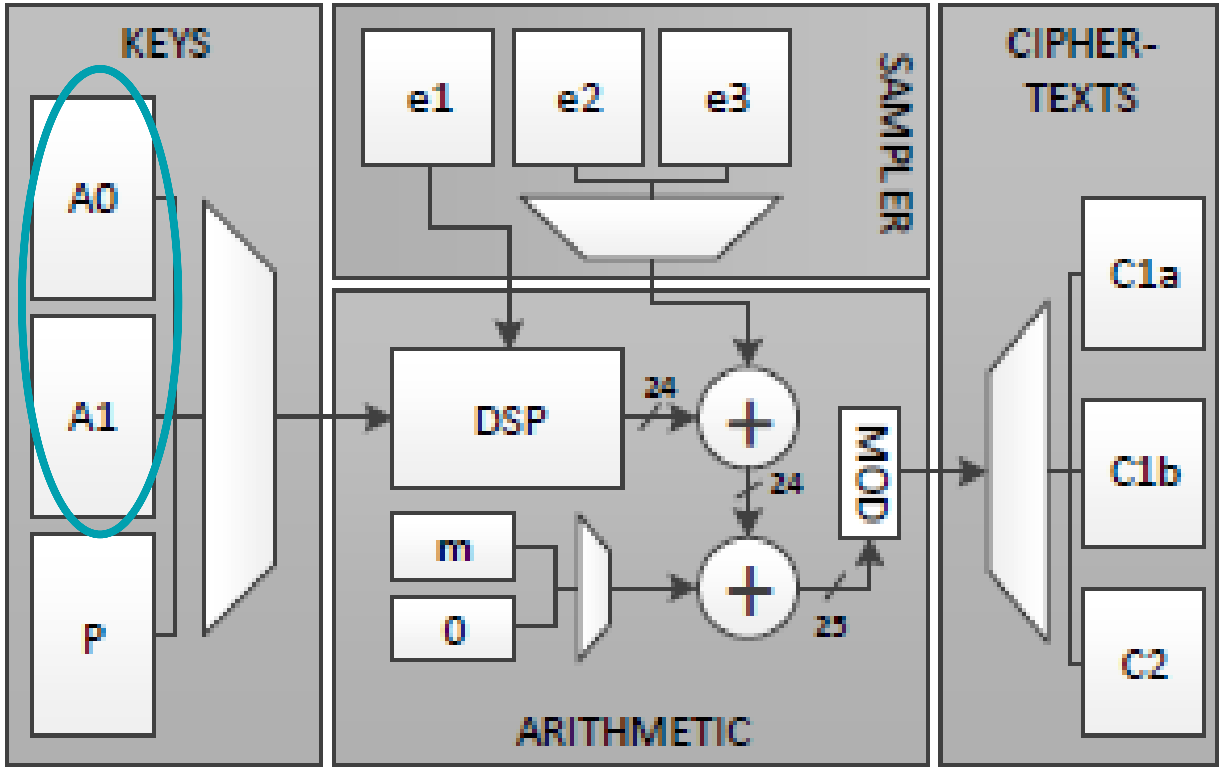


Figure 1: High level architecture of LWE encryption scheme. Lengths are 12 bits unless otherwise stated.

Architecture of standard LWE encryption

Algorithm 2 Encryption($\mathbf{A}_0, \mathbf{A}_1, \mathbf{P}, \mathbf{m} \in \{0,1\}^\ell$)

for $i = 0$ to $n-1$ **do**
  $\mathbf{e}_1(i) \leftarrow D_\sigma^n$ $\Longleftarrow$ Computed on-the-fly after first encryption.
end for
for $k = 0$ to 2 **do** $\Longleftarrow$ i.e., $\mathbf{A}_0$, $\mathbf{A}_1$, or $\mathbf{P}$.
  $SUM = 0$
  if $k \in \{0,1\}$ **then**
    for $j = 0$ to $\ell - 1$ **do**
      $e \leftarrow D_\sigma$ $\Longleftarrow$ Computed in parallel to MAC operations.
      for $i = 0$ to $n-1$ **do**
        $SUM := SUM + \mathbf{e}_1(i) \times \mathbf{A}_k(i,j) \mod q$
      end for
      $\mathbf{c}_i(j) = SUM + e \mod q$
    end for
  else
    for $j = 0$ to $\ell - 1$ **do**
      $e \leftarrow D_\sigma$
      for $i = 0$ to $n-1$ **do**
        $SUM := SUM + \mathbf{e}_1(i) \times \mathbf{P}(i,j) \mod q$
      end for
      $\mathbf{c}_i(j) = SUM + e + \bar{\mathbf{m}}(j) \mod q$
    end for
  end if
end for

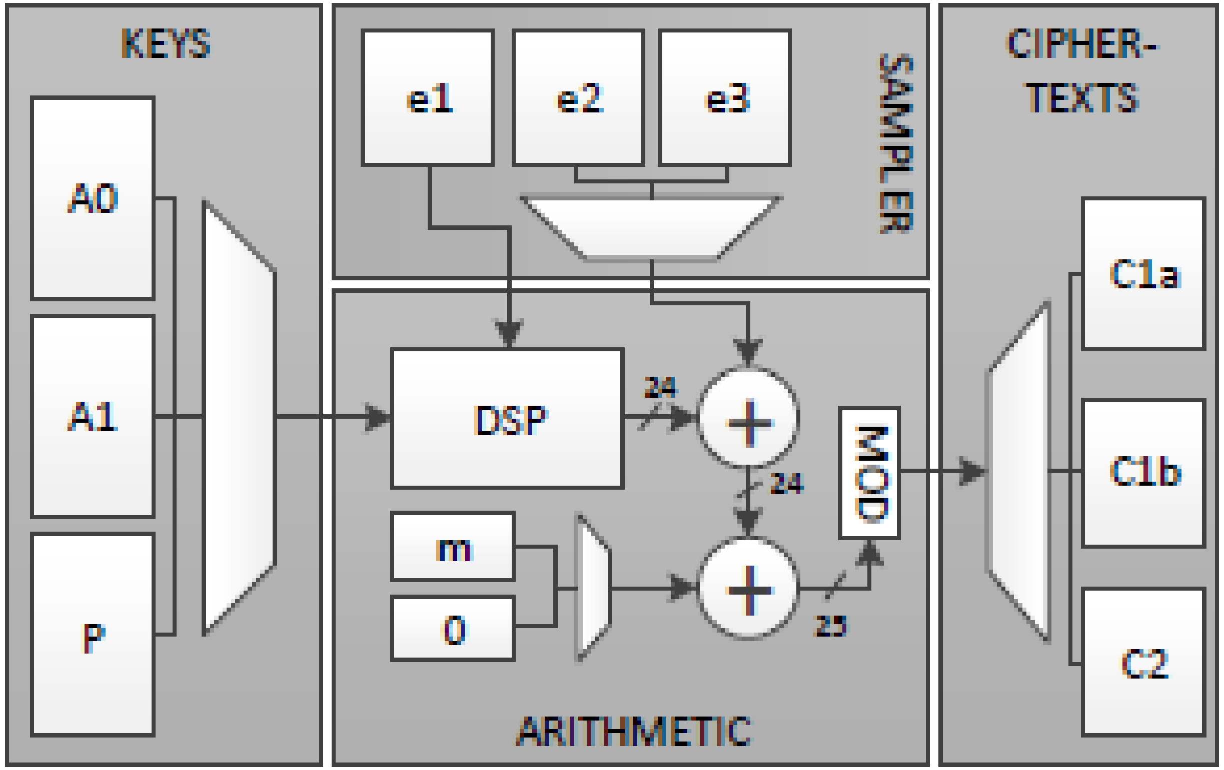
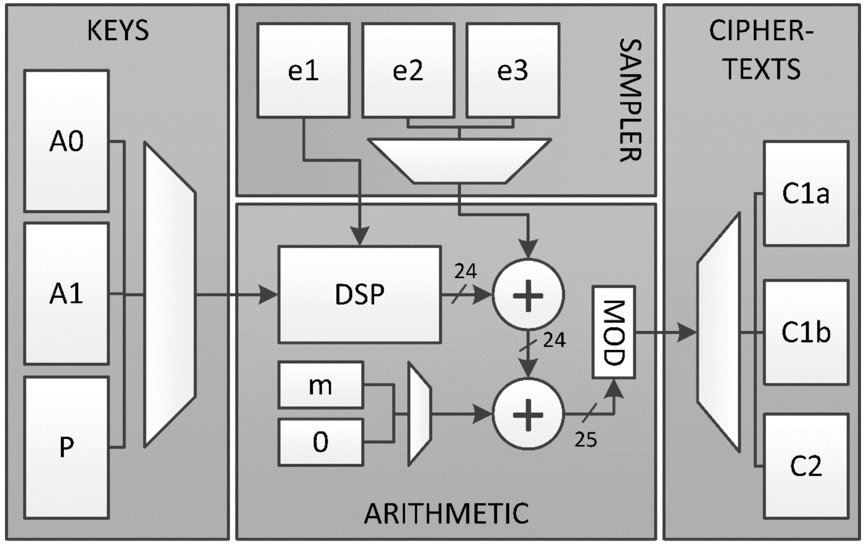


Figure 1: High level architecture of LWE encryption scheme. Lengths are 12 bits unless otherwise stated.

Lattice-based Encryption over Standard Lattices in Hardware

- First standard LWE encryption design on hardware (Spartan 6 FPGA)
- FPGA DSP slice targeted for multiplication-accumulation
- Bernoulli sampler used for discrete Gaussian Sampling
- Both encryption and decryption fit comfortably on FPGA



Performance results: 1272 encryptions per second and 4395 decryptions per second

* *Co-Authored with James Howe, Máire O'Neill, Francesco Regazzoni, Tim Güneysu and Kevin Beeden and published in the Proceedings of the 53rd Annual Design Automation Conference (**DAC**), 2016*

Comparison & Results

Encryption over standard lattices on a Spartan 6 – LX45 FPGA, compares well with RLWE

Operation/Algorithm	Device	LUT/FF/SLICE	BRAM/DSP	MHz	Cycles	Ops/s
LWE Encrypt (λ=128)	S6LX45	6152/4804/1866	73/1	125	98304	1272
LWE Encrypt (λ=64)		6078/4676/1811	73/1	125	98304	1272
LWE Decrypt		63/58/32	13/1	144	32768	4395
RLWE Encrypt (Göttert et al, 2012)	V6LX240T	298016/-/143396	-/-	-	-	-
RLWE Decrypt (Göttert et al, 2012)		124158/-/65174	-/-	-	-	-
RLWE Encrypt (Pöppelmann & Güneysu, 2013)	S6LX16	4121/3513/-	14/1	160	6861	23321
RLWE Decrypt (Pöppelmann & Güneysu, 2013)		4121/3513/-	14/1	160	4404	36331
RLWE Encrypt (Pöppelmann & Güneysu, 2013)	V6LX75T	4549/3624/1506	12/1	262	6861	38187
RLWE Decrypt (Pöppelmann & Güneysu, 2013)		4549/3624/1506	12/1	262	4404	36331
RLWE Encrypt (Pöppelmann & Güneysu, 2014)	S6LX9	282/238/95	2/1	144	136212	1057
RLWE Decrypt (Pöppelmann & Güneysu, 2014)		94/87/32	1/1	189	66338	2849
RLWE Encrypt (Roy et al, 2013)	V6LX75T	1349/860/-	2/1	313	6300	49751
RLWE Decrypt (Roy et al, 2013)		1349/860/-	2/1	313	2800	109890

Key Takeaways

- Consider Standard LWE as a viable alternative
- Recommended for applications requiring long term security assurance
- Further research required to improve performance

6. Future Research

What’s next?

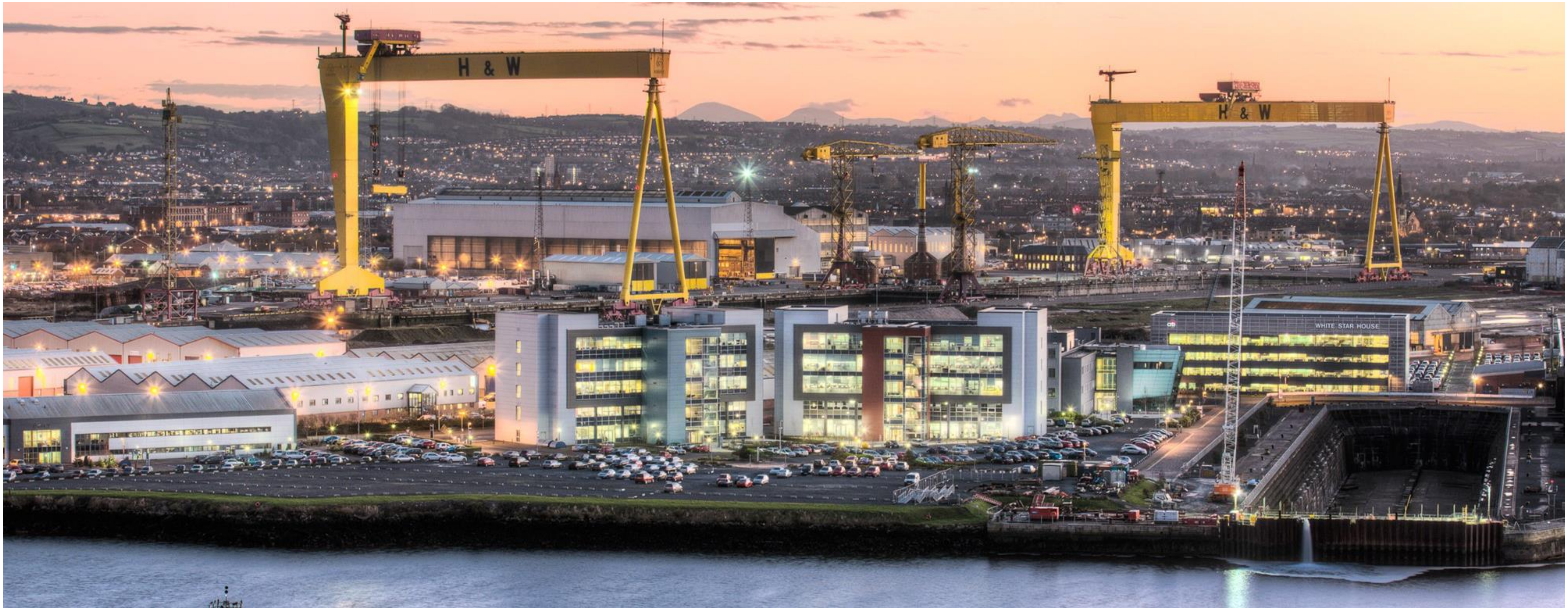
- NIST competition…
- Evaluations…
- SAFEcrypto library release

Conclusions

- Practicality is important
- Hardware designs can make a difference
- Algorithmic optimisations of the most importance
- Team effort
- Collaboration essential

Thank you for listening!

CENTRE FOR SECURE INFORMATION TECHNOLOGIES



Questions? c.m.rafferty@qub.ac.uk