CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Secure Connected Devices

PROFESSOR MÁIRE O'NEILL
Regius Chair in Electronics and Computer Engineering,
Director, CSIT
Director, Research Institute in Secure Hardware & Embedded Systems (RISE)

QUEEN'S UNIVERSITY BELFAST

Secure Connected Devices

- **Trusted Hardware**
  - PUF-based authentication
  - Hardware Trojan Detection
  - Side Channel Analysis
  - Security & Approximate Computing
  - Deep Learning in HW Security
- **Advanced Crypto Architectures**
  - Post-quantum crypto architectures
  - Hybrid quantum/PQC designs
  - Homomorphic Encryption, IBE, ABE
  - Password Authenticated Key Exchange

SCD Research Team

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Academic Staff

Prof Máire O'Neill

Dr Ayesha Khalid (SL)

Dr Ciara Rafferty (SL)

Dr Chongyan Gu (SL)

Dr Arnab Kumar Biswas

Dr Indranil Ghosh Ray

Dr Anh-Tuan Hoang

Research Staff

Shichao Yu

Jack Miskelly

Malik Imran

Aditya Japa

Ziying Ni

Gor Piliposyan

PhD students

Ryan Bevin

An Troung To

Yuhang Hao

Mark Kennaway

Zain Shabbir

Niall Canavan

Adam Farren

Robert Moore

Ziying Ni

Tuan Dung Pham

Post-quantum Cryptography & Hybrid Quantum/PQC Designs

QUEEN'S UNIVERSITY BELFAST

Why PQC?

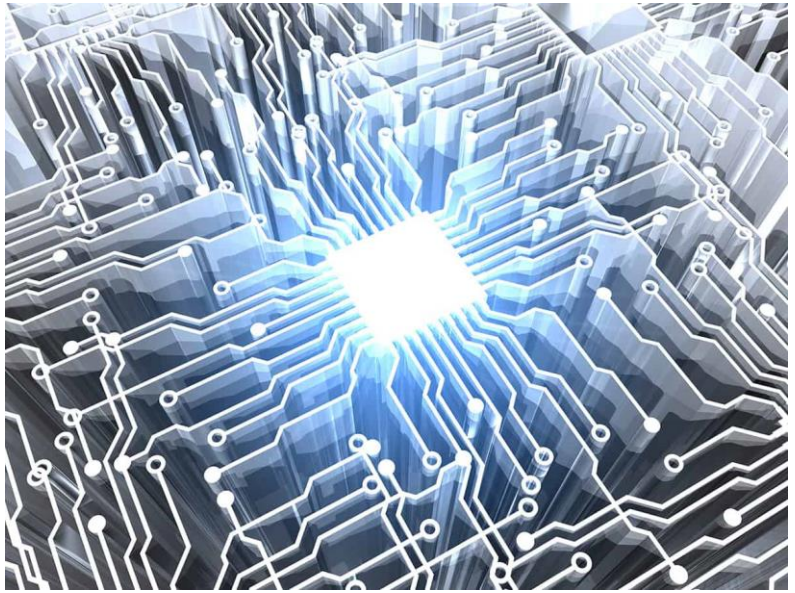
“There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031.”

–Dr. Michele Mosca, U. of Waterloo

What happens if/when quantum computers become a reality?

Commonly used public-key cryptographic algorithms (based on integer factorization and discrete log problem) such as:

RSA, DSA, Diffie-Hellman Key Exchange, ECC, ECDSA will **no longer be secure** due to Shor’s algorithm.



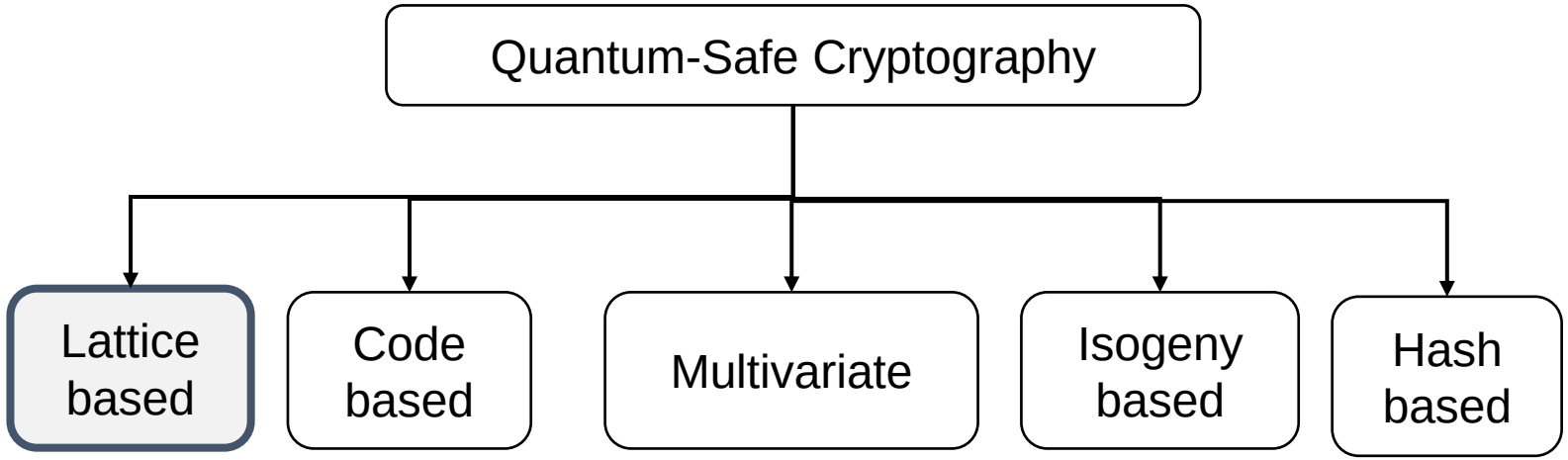
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Quantum-safe or Post-quantum cryptography (PQC)

Cryptosystems from classical problems that are secure today, **and** should remain secure even after practical quantum computing becomes a reality

Quantum-Safe Cryptography



Lattice-based cryptography is flourishing:

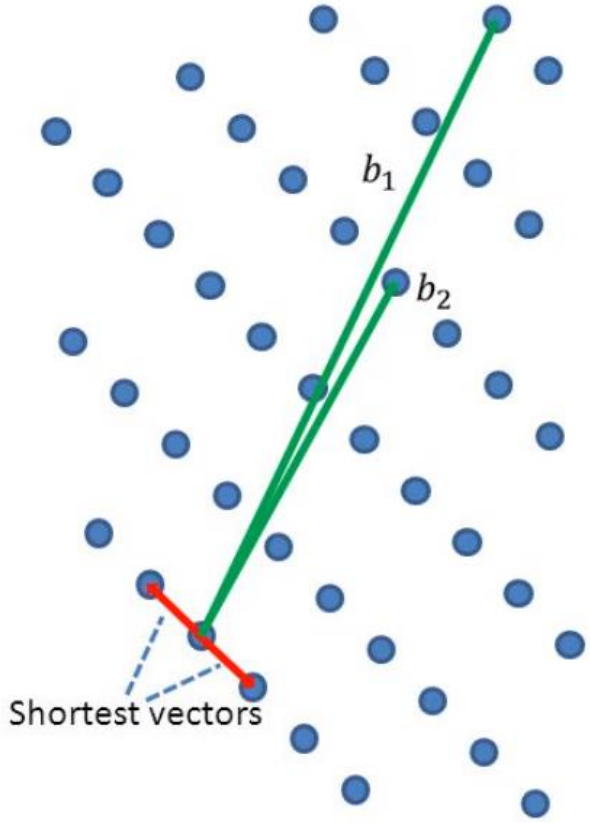
- IBM offering *quantum safe TLS option in IBM cloud*
- AWS offer hybrid post-quantum TLS with Kyber
- Google using PQC (NTRU-HRSS)

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Lattice-based cryptography (LBC)

- LBC is based on shortest vector/closest vector problems
- LBC encryption and digital signature schemes already practical & efficient, i.e. can match/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*



Lattice Based Cryptography

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Currently two popular lattice-based problems for cryptography are the **Learning With Error (LWE)** problem and **Ring-LWE problem**

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 $\boldsymbol{b} \equiv \boldsymbol{As} + \boldsymbol{e}\ mod\ q$

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

EU H2020 SAFEcrypto Project

Jan 2015 - Dec 2018

SAFEcrypto (Secure Architectures for Future Emerging Cryptography)
- 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 on **lattice-based cryptography**
- Solutions for Satellite Communications, Municipal Data Analytics & IoT

www.safecrypto.eu

Queen's University Belfast
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES
THALES
HWCommunications Ltd
creating the next generation of solutions
IBM
Inria INVENTEURS DU MONDE NUMÉRIQUE
DELL EMC
RUHR UNIVERSITÄT BOCHUM
RUB
Università della Svizzera italiana

Summary

Practical HW & SW Implementations of lattice-based schemes delivered:

Signatures: BLISS, Ring-TESLA, Dilithium, Falcon

Encryption/KEM: Standard LWE, RLWE Encryption, Frodo, New Hope, Kyber

Advanced Primitives: Lattice-based AKE, Lattice-based IBE

Designed novel methodologies for **SW And HW countermeasures for LBC** implementations

- masked RLWE ARM implementation (*resource-constrained SW*)
- Constant-time LBC primitives (*high-performance SW)*
- masked RLWE FPGA implementation (*high-performance HW*)
- Constant-time samplers and fault attack countermeasures (*high-performance & resource constrained HW)*

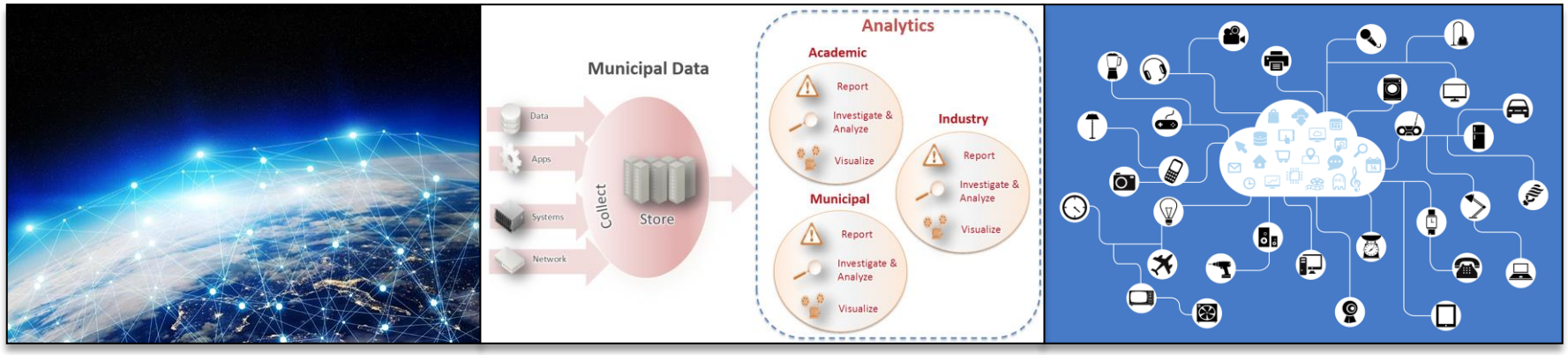
A KMIP client supporting LBC keys was **developed & integrated within Dell EMC's Key Trust Platform (KTP)**

SAFE crypto

Summary

SAFEcrypto outputs demonstrate that ***Lattice-based cryptography can meet the requirements of real world scenarios***.

Smart Tag Systems



Satellite Communications

Municipal Data Analytics

Quantum/Post-Quantum Projects

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

QUANTUM COMMUNICATIONS HUB

UKRI Engineering and Physical Sciences Research Council

TOSHIBA

- Investigation of efficient **PQC KEM & digital signature** HW designs
- Exploration of **hybrid PQC/QKD designs**
- **Security assessment** of devices, systems, and hybrid systems

PQC Implementation Considerations

QUEEN'S UNIVERSITY BELFAST

PQC Implementation considerations

- Algorithmic security
- Physical security
  - Side-channels & timing analysis
- Performance optimisations (area, time)
- Tailored platform optimisations
- Hybrid QKD+PQC

FPGA Acceleration for PQC

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

- PQC algorithms typically have **larger parameter sizes** (Public key, private key, cipher text, signature sizes etc.) in comparison.

Lattice based
Round 4
Digital Signature
(sizes in bytes)

Candidate	Claimed Security	Public key	Private key	Signature
Dilithium	Level 2	1 312	2 528	2 420
	Level 3	1 952	4 000	3 293
	Level 5	2 592	4 864	4 595
FALCON-512	Level 1	897	7 553	666
FALCON-1024	Level 5	1 793	13 953	1 280

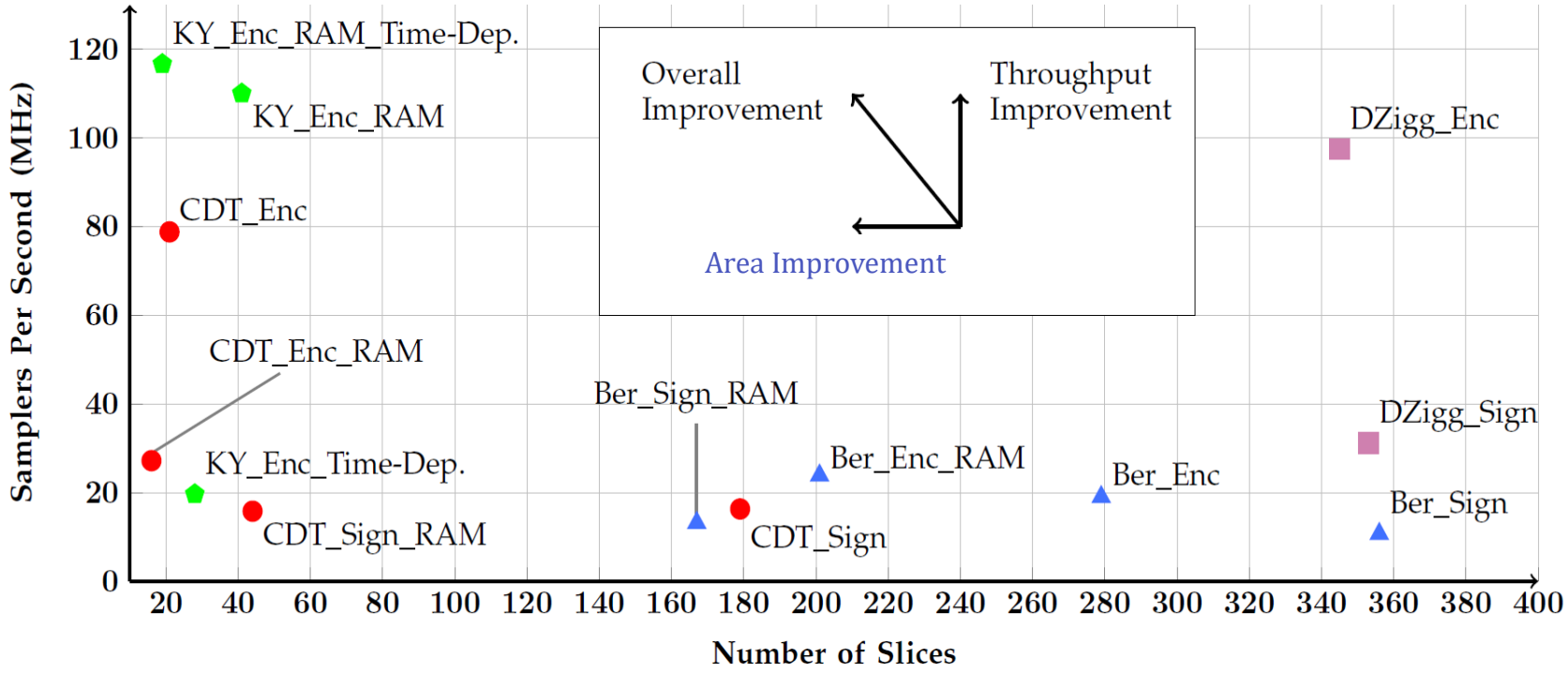
- In reconfigurable logic this incurs
  - Larger communication bandwidth
  - Larger internal storage

Error Sampling Evaluation in Hardware

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

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



Efficient Soft-Core Multiplier for PQC Digital Signatures *accepted to ISCAS'24*

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

- 5x5 finite field Multiplier for PQC digital signatures such as QR-UOV, MAYO, MQOM
- Significant area reductions (30% reduced compared to Vivado mult, ~50% reduced to state-of-the-art when integrated into matrix-vector architecture

TABLE I
RESULTS IMPLEMENTED ON FPGA (XILINX VIRTEX-7)

	Size	LUT	CPD *ns*	Power *mW*	ADP	PDP	APDP
PM	**5 × 5**	**16**	**2.59**	**0.61**	**41.44**	**1.58**	**25.28**
PFFM	**5 × 5**	**27**	**2.28**	**1.31**	**61.56**	**2.98**	**80.46**
Vivado [23]	5 × 5	23	2.32	0.72	53.36	1.67	38.42
M1 [15]	4 × 4	12	2.15	0.50	25.8	1.09	13.08
	5 × 5	21		-	-	-	-
	6 × 6	24	3.09	0.86	74.16	2.67	64.08
M2* [18]	4 × 4	24	3.84	0.52	92.16	2.00	48
	6 × 6	49	5.10	1.34	249.9	6.87	336.6
M3 [21]	4 × 4	12	2.02	0.56	24.72	1.13	13.56
	5 × 5	23	-	-	-		
	6 × 6	26	2.93	0.93	76.18	2.72	70.84
M4 [22]	5 × 5	13	-	-	-	-	-

*M2 results are taken from [15]. [18] lacks results for these sizes.

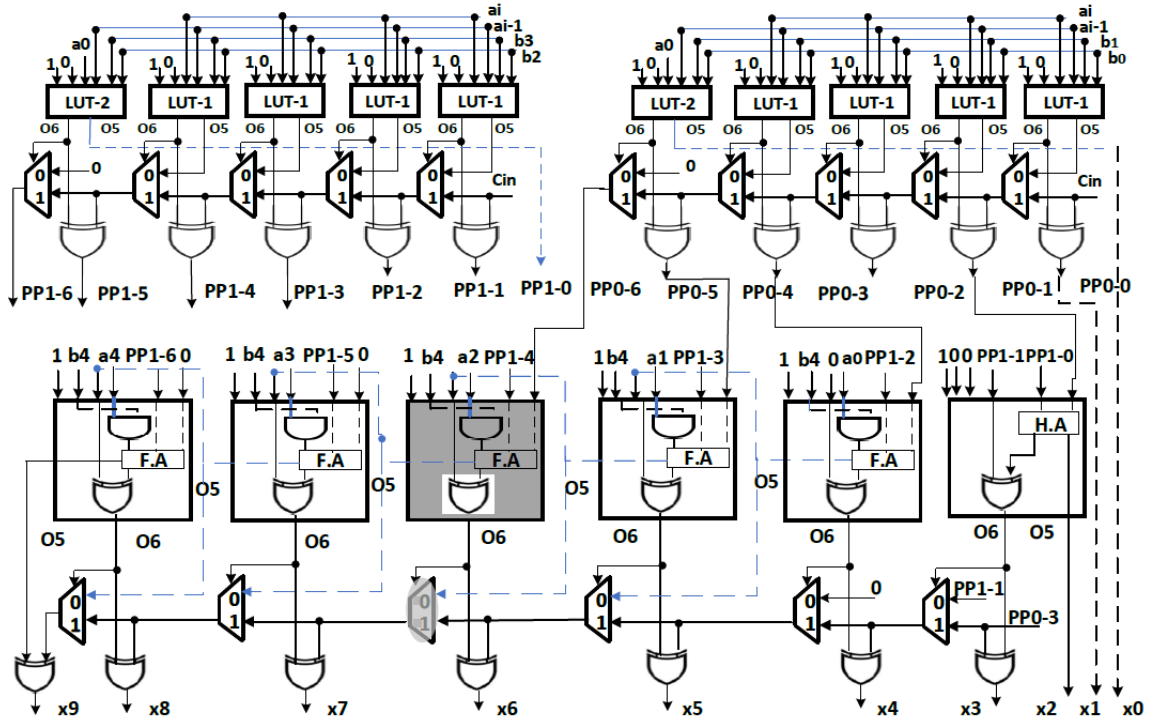


Fig. 2. Proposed 5 × 5 multiplier hardware architecture

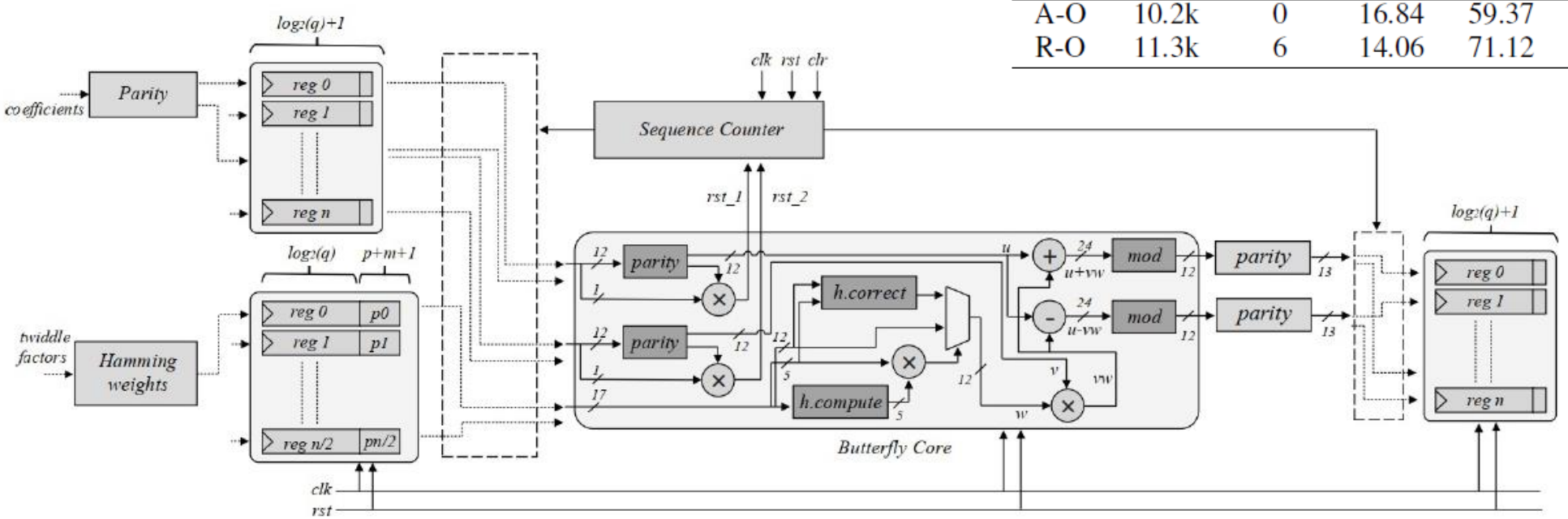
Error-Resistant NTT architectures for CRYSTALS-Kyber *VLSI-SoC '23*

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

- Error detection and mitigation for NTT in Kyber on FPGA, via hamming codes and parity bits to detect and correct SEUs.
- Area overhead of approx. 29%

TABLE I
RESULTS IMPLEMENTED ON FPGA (VIRTEX-7)

	#LUT	#DSP	Time *ns*	Freq. *MHz*	TP *Mbps*	TP/A *TP/kL*	%+A
Basic Architecture							
A-O	7.9k	0	16.57	60.32	206.82	26.17	-
R-O	7.8k	6	13.86	72.11	247.26	31.69	-
Hamming codes							
A-O	9.2k	0	16.34	61.17	209.75	22.79	16.4
R-O	9.3k	6	13.59	73.54	252.17	27.11	19.2
Hamming codes + Parity bits							
A-O	10.2k	0	16.84	59.37	203.71	19.97	10.8
R-O	11.3k	6	14.06	71.12	243.86	21.58	21.5



Hybrid PQC-QKD (MUCKLE++)

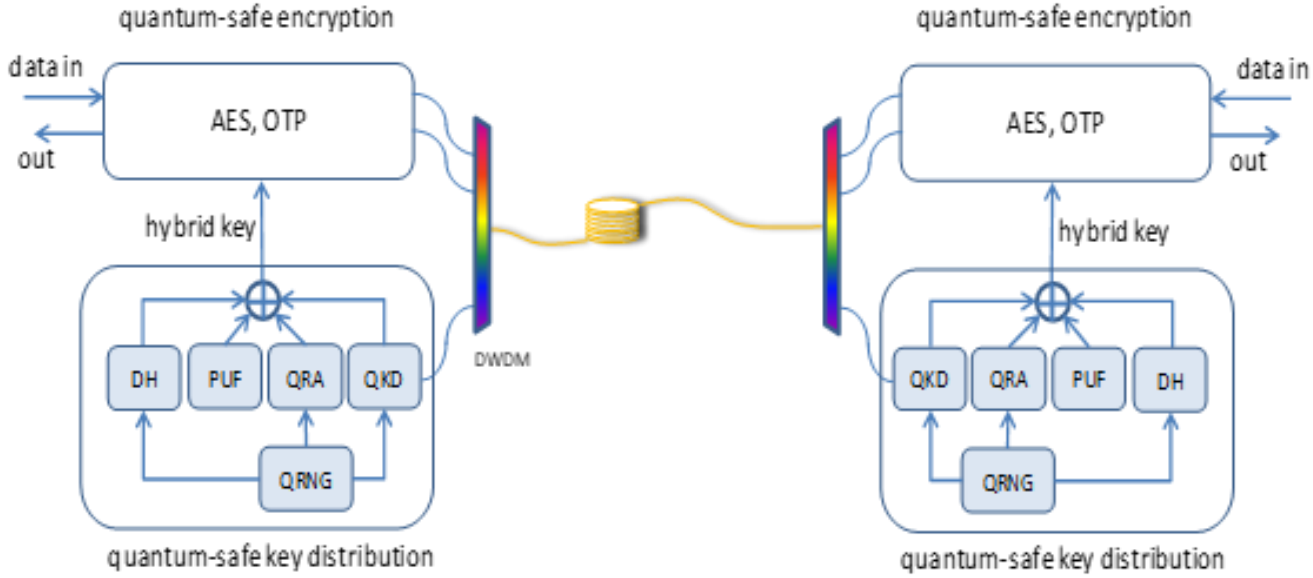
accepted to Journal of Advanced Quantum Technologies

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

- As part of the Toshiba-led ISCF project **AQuaSec**, we investigated the integration of classical and post-quantum cryptography on a Toshiba platform

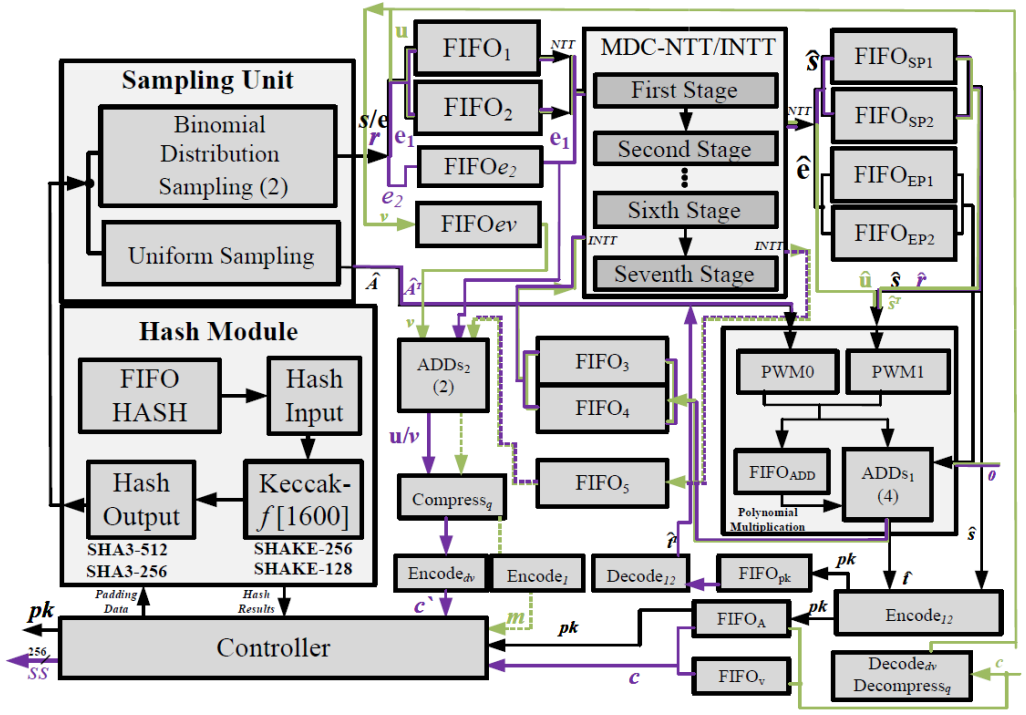
- Hybrid design combining QRA and QKD
  - PUF integration enabling Pre-Shared Key
  - Hardware-software integration for acceleration

AQuaSeC



High-Performance Kyber Accelerator

IEEE Transactions on Computers, Vol. 72 (12), Dec 2023



Implemented on FPGA Artix-7 XC7A200

- Security Level 1:
- Total time (KeyGen+Enc+Dec) = 22.6µs
- Security Level 3:
- Total time (KeyGen+Enc+Dec) = 34.1µs
- Security Level 5:
- Total time (KeyGen+Enc+Dec) = 49µs

25-51% speed-up over state-of-the-art
50-75% reduction in DSPs at comparable security levels

- Exploits architectural parallelisation via optimal inter-module and intra-module pipelining
- Utilises a fully pipelined Radix 2 Multipath Delay Commutator (MDC)-NTT Core and the hardware for NTT and INTT is shared.

Bistream Fault Injection Attack on Kyber

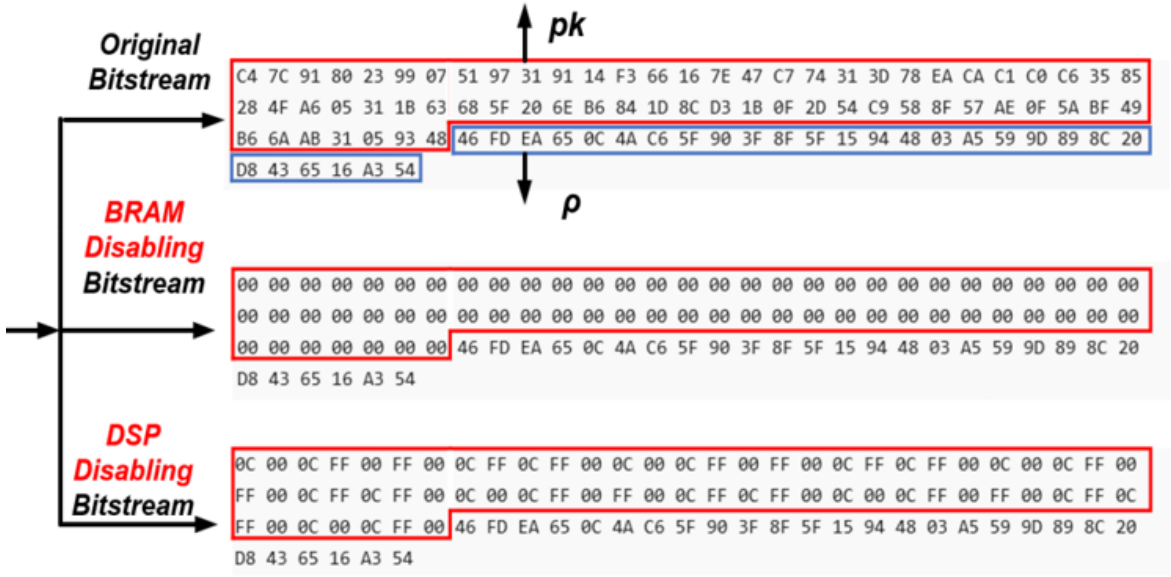
accepted DATE 2024

- First malicious bitstream modification attack on Kyber FPGA design on Artix-7
- Consider 4 attacks: (1) disabling BRAM; (2) disabling DSPs; (3) zeroing NTT ROM; and (4) tampering with sampler results
- It is possible to reduce complexity of polynomial mult operations or enable direct secret key or message recovery

TABLE I

COMPLEXITY OF pk/ct UNDER FOUR ATTACK METHODS AND WHETHER EVE AND ALICE COULD RECOVER MESSAGE m

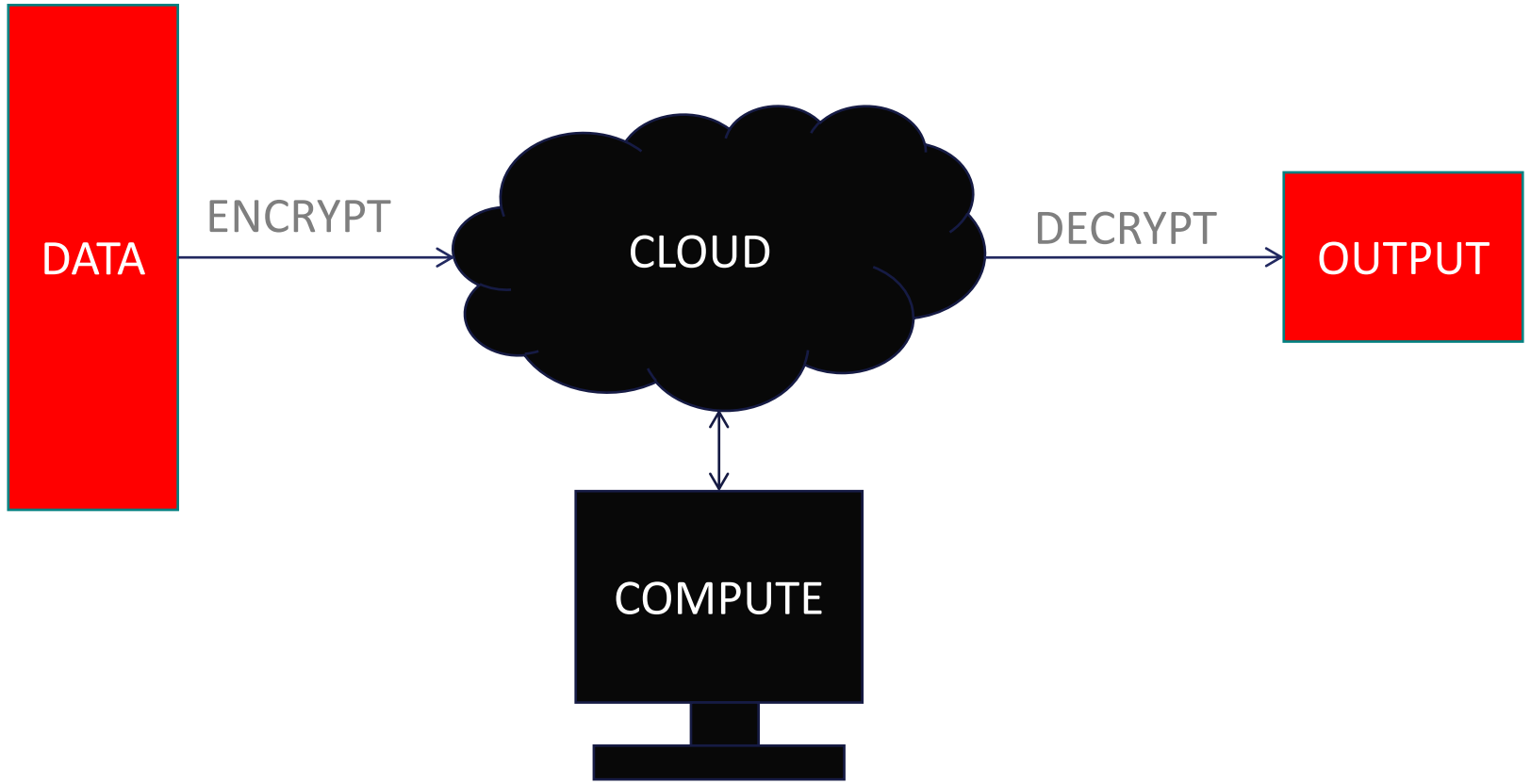
Attack Methods	KeyGen			KeyEncaps.			Bits
	pk	m(Eve)	m(Alice)	ct	m(Eve)	m(Alice)	
BRAM	Weak	✓	✓	Weak	✓	✓	540
DSP	Weak	✓	✓	Weak	✓	✓	240
NTT ROM	Strong	✓	×	Strong	✓	✓	1,163
CBD2	Strong	✓	✓	Strong	✓	✓	768



Homomorphic Encryption

QUEEN'S UNIVERSITY BELFAST

Cloud computing with FHE



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

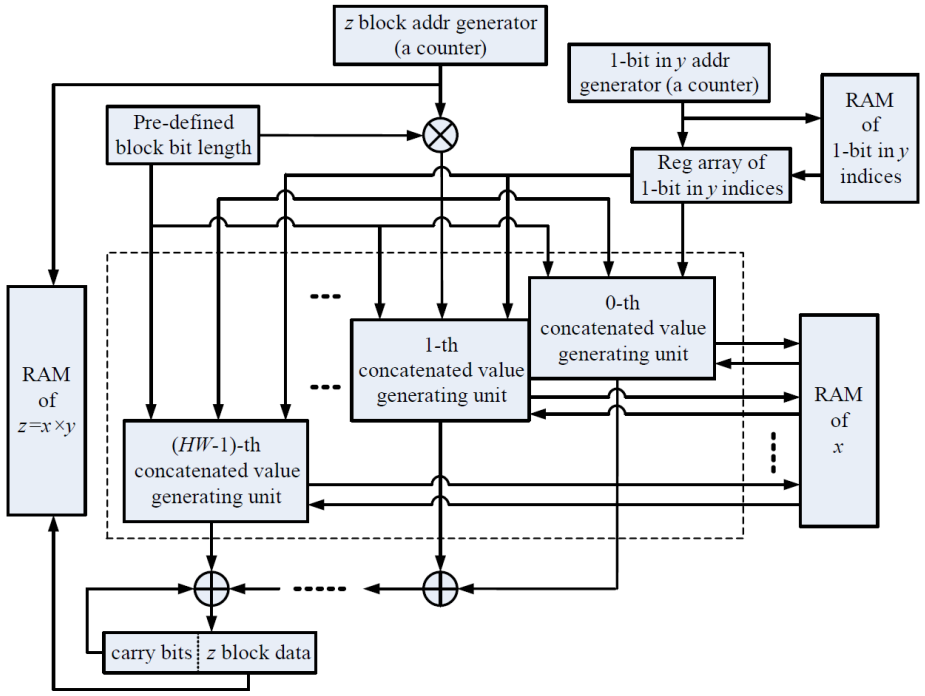
High-speed FHE over the integers

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

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



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

High-speed FHE over the integers

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

CSIT 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!

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

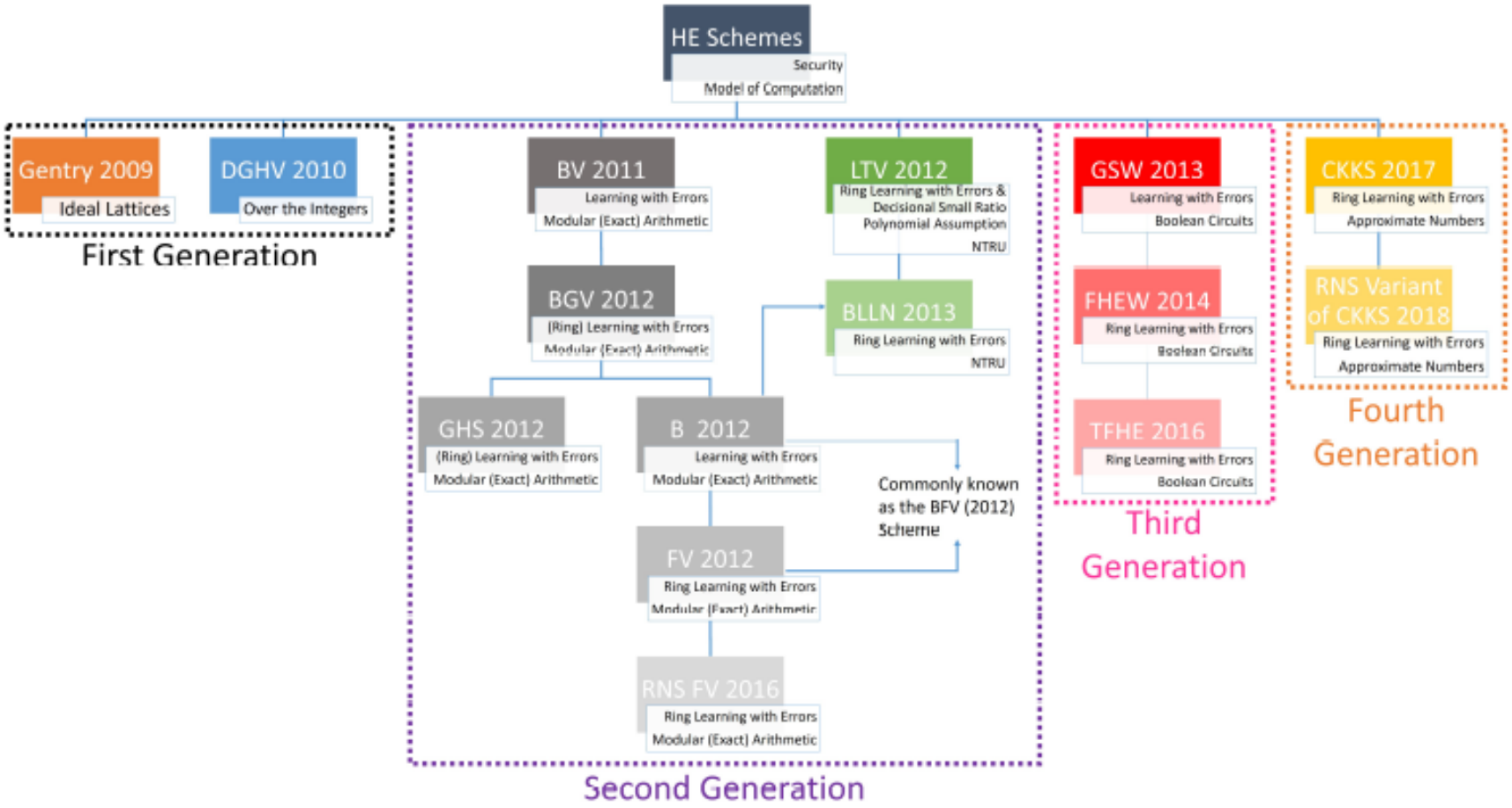
Challenges for FHE

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

CHALLENGE: What is the most suitable application for homomorphic encryption?

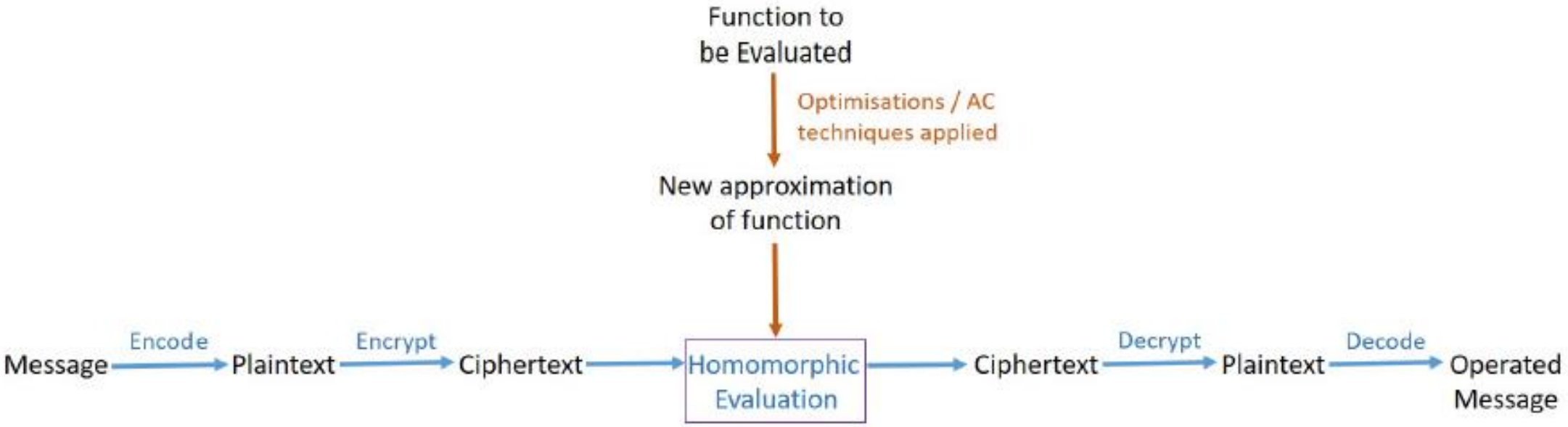
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Homomorphic Encryption Developments



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Where to accelerate/approximate HE?



Can we accelerate/approximate FHE further?

- CKKS – Homomorphic Encryption using approximate arithmetic
  - Certain applications trade off accuracy with energy efficiency and performance

- Approximating approximate FHE: Investigating the use of approximate computing to further accelerate HE
  - Task skipping
  - Loop perforation
  - Depth reduction

Results show speed up of 12-45% over HE without approx. computing – *with a cost of reduced accuracy**

**Accelerating Homomorphic Encryption using Approximate Computing Techniques, Shabnam Khanna, Ciara Rafferty, SECRYPT 2020*

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

RESULTS

Homomorphic Evaluation of Function	Degree	log Q_l	Total Time	Amortized Time	% speed-up	Average error from actual
Logistic Function						
Without Optimisation (1), inputs 0-1	9	280	0.274354 s	33 μs	N/A	1.52×10^{-7}
Without Optimisation (1), inputs > 1	9	280	0.275538 s	34 μs	N/A	3.55×10^{29}
Task Skipping Approach 1 (3)	7	240	0.144749 s	18 μs	45.5 %	2.08×10^{-6}
Task Skipping Approach 2 (5)	9	280	0.234501 s	29 μs	12.1 %	0.11979
Task Skipping Approach 3 (7)	9	280	0.235498 s	29 μs	12.1 %	3.55×10^{29}
Depth Reduction (11)	7	240	0.145621 s	18 μs	45.5 %	6.18×10^{-4}
Task Skipping Approach 2 with Depth Reduction (14)	7	240	0.114206 s	14 μs	57.6 %	0.12041
Task Skipping Approach 3 with Depth Reduction (14)	7	240	0.114705 s	14 μs	57.6%	3.55×10^{29}
Exponential Function						
Without Optimisation (2), inputs 0-1	8	280	0.495471 s	60 μs	N/A	0.333321
Without Optimisation (2), inputs ≥ 1	9	280	0.495397 s	60 μs	N/A	5.59×10^{25}
Task Skipping Approach 1 (4)	7	240	0.316672 s	39 μs	35 %	0.08334
Task Skipping Approach 2 (6)	8	280	0.38291 s	47 μs	21.6 %	0.70835
Task Skipping Approach 3 (8)	8	280	0.384384 s	47 μs	21.6 %	5.59×10^{25}
Depth Reduction (10)	7	240	0.318610 s	39 μs	35 %	2.42×10^{-5}
Task Skipping Approach 2 with Depth Reduction (13)	7	240	0.228299 s	28 μs	53.3 %	0.70833
Task Skipping Approach 3 with Depth Reduction (13)	7	240	0.227856 s	28 μs	53.3 %	5.59×10^{25}

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Privacy-Preserving Data Analytics


MACHINE LEARNING


PREDICTIONS


HEALTH DATA


STATISTICS


BIG DATA

Can we carry out analytics on data without leaking personally identifiable information?

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Data Analytics and Homomorphic Encryption

Machine learning for Financial Services

- ML pipeline with HE*
- Logistic regression model
- Predictions performed on encrypted financial data
- Shows promise in terms of accuracy and performance

*Towards a Homomorphic Machine Learning Big Data Pipeline for the Financial Services Sector, O Masters, H Hunt, E Steffinlongo, J Crawford, F Bergamaschi, M Dela Rosa, C Quini, C Alves, F de Souza, D Goncalves Ferreira, IACR ePrint Archive 2019

CryptoNets (2016)[1]

- Research by Microsoft and Princeton
- Adapted Neural Networks to encrypted data
- Use a large ML dataset (MNIST)
- CryptoNets achieves "***99% accuracy and can make more than 51000 predictions per hour on a single PC***"

- Need to use polynomial functions within HE-enabled NNs
- Approximate non-polynomial functions (i.e. ReLU, sigmoid function)

1 https://www.microsoft.com/en-us/research/wp-content/uploads/2016/04/CryptonetsTechReport.pdf

Approximate Homomorphic Pre-processing for CNNs

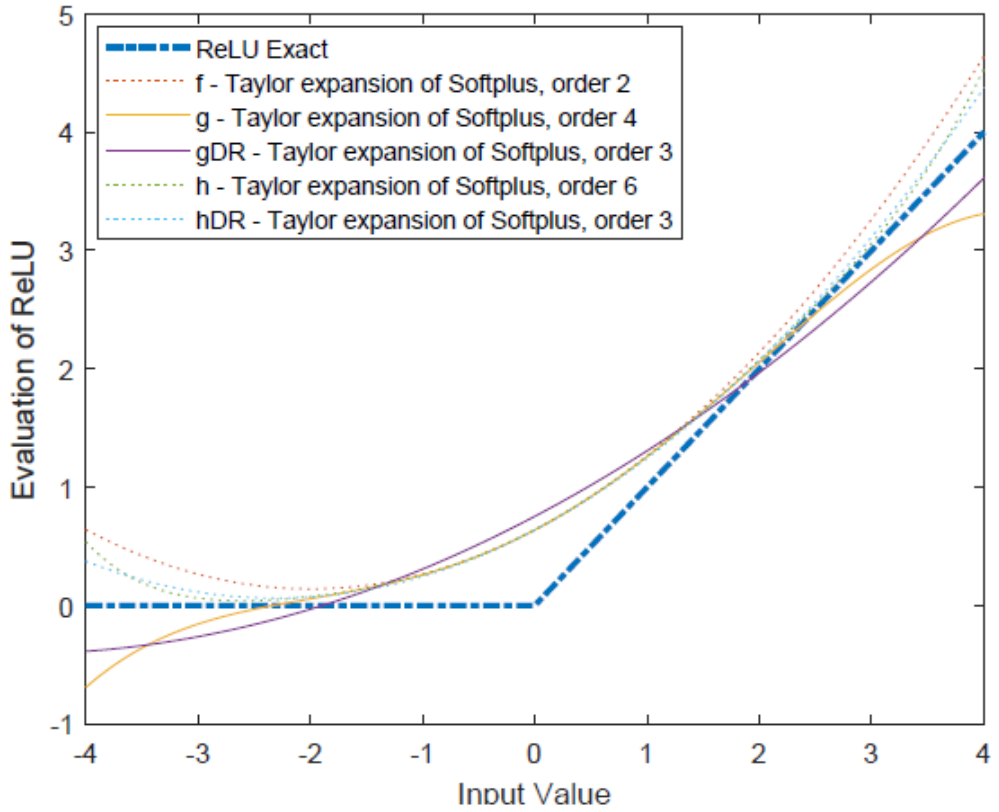


Fig. 5.2 The various Taylor expansions of Softplus, along with the exact ReLU function and the depth reduced approximations.

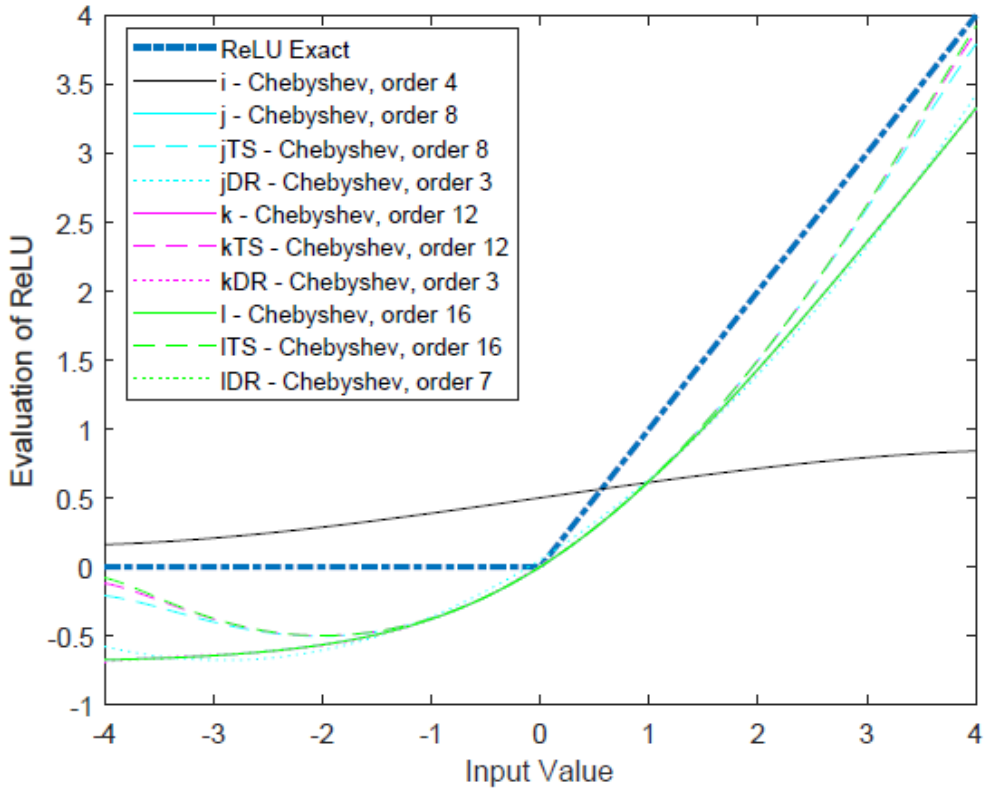


Fig. 5.3 The Chebyshev polynomial approximations, along with the exact ReLU function and the task-skipped and depth reduced approximations

**Approximate Homomorphic Pre-processing for CNNs, Shabnam Khanna, Ciara Rafferty, SECRYPT 2023*

Approximate Homomorphic Pre-processing for CNNs

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

	ReLU Exact	Chebyshev 16 No Change [-255,255]	Chebyshev 16 Task Skipping [-255,255]	Chebyshev 16 Depth Reduction (x^3) [-4,4]
Classification Accuracy (HE Plaintext)	99.14%	99.06%	99.18%	99.34%
Validation Accuracy	98.57%	97.37%	97.18%	98.55%
Validation Loss	4.51%	9.00%	9.03%	54.7%
Run-time (μs)(Train)	170.3	400.2	201.8	198.0
Run-time (s) (Test, HE backend, Plaintext)	0.3333	0.8155	0.3713	0.3749
% Speed-up (Train)	N/A	N/A	50%	51%
% Speed-up (Test, HE backend, Plaintext)	N/A	N/A	54%	54%

Table 5.3 Table showing classification accuracy and run-time of the various ReLU approximations (average over 20 runs), based on the Chebyshev order 16 approximation, applied to the CryptoNets CNN implemented in nGraph-HE.

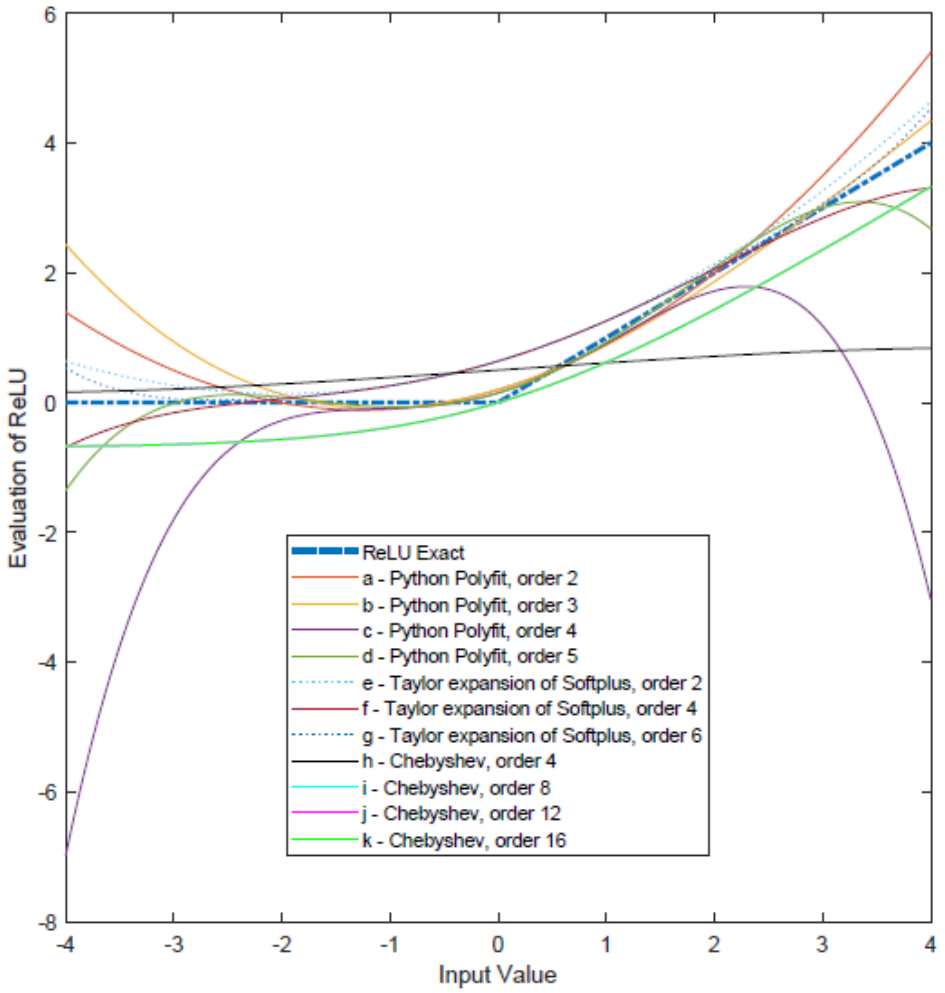


Fig. 5.4 All eleven original polynomial approximations of the ReLU function

**Approximate Homomorphic Pre-processing for CNNs, Shabnam Khanna, Ciara Rafferty, SECRYPT 2023*

PAKE (Password Authenticated Key Exchange) Authentication Protocols

Precomputation safety

After server compromise, if attacker can retrieve client's password from the saved information in a dictionary size computation, it is not precomputation safe.

All symmetric PAKEs are trivally vulnerable to precomputation attack.

Target is to design asymmetric PAKE (aPAKE) which is precomputation safe, free from PKI and implementable.

Research Summary

Major standards bodies including **IEEE, ISO/IEC** and the **IETF** have worked towards standardizing PAKE schemes, with mixed results.

IETF selected OPAQUE (Eurocrypt 2019) as world's first precomputation safe aPAKE, however it pointed out **several important questions against OPAQUE which remained unaddressed and which stops OPAQUE from being used commercially.**

Main problem of OPAQUE - dependency on an abstract primitive - H2C

1. **Though OPAQUE is theoretically precomputation safe, however it critically relies on hash-to-curve (H2C). As of June 2021 (more than one year after the selection process was finished), the H2C ID remains a draft (draft-irtf-cfrg-hash-to-curve) and is not implementable.**
2. **H2C offers, with non-negligible probability, points in less secure smaller subgroup instead of prime order group which is needed for security of OPAQUE.**

What we propose

We design world's first asymmetric PAKE which is

1. **Precomputation safe,**
2. **Free from H2C,**
3. **Public key infrastructure (PKI) free,**
4. **Easy to implement with existing libraries (GMP, GNU etc)**
5. **Based on state-of-the-art CDH assumption.**

Market

- **All email services (Google, Yahoo!, AOL, etc.)**
- **Online shopping portals (Amazon, Ebay, etc.)**
- **Social Media Applications (Facebook, Twitter, Linkedin etc.)**
- **Cloud services (Dropbox, AWS, Google, Microsoft, etc.)**
- **All Other Client-Server Applications**

What we look for

Partnership **Spinout**

Patenting **Commercialize**

Thank you