**QUEEN'S
UNIVERSITY
BELFAST**

AxRLWE: A Multi-level Approximate Ring-LWE Co-processor for Lightweight IoT Applications

Kundi, D-S., Khalid, A., Bian, S., Wang, C., O'Neill, M., & Liu, W. (2021). AxRLWE: A Multi-level Approximate Ring-LWE Co-processor for Lightweight IoT Applications. *IEEE Internet of Things Journal*.
<https://doi.org/10.1109/JIOT.2021.3122276>

Published in:
IEEE Internet of Things Journal

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
[Link to publication record in Queen's University Belfast Research Portal](#)

Publisher rights
Copyright 2021, IEEE.
This work is made available online in accordance with the publisher's policies. Please refer to any applicable terms of use of the publisher.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

AxRLWE: A Multi-level Approximate Ring-LWE Co-processor for Lightweight IoT Applications

Dur-e-Shahwar Kundi *Member, IEEE*, Ayesha Khalid *Member, IEEE*, Song Bian *Member, IEEE*, Chenghua Wang, Máire O'Neill *Senior Member, IEEE* and Weiqiang Liu *Senior Member, IEEE*

Abstract—This work presents a multi-level approximation exploration undertaken on the Ring-Learning-with-Errors (R-LWE) based Public-key Cryptographic (PKC) schemes that belong to quantum-resilient cryptography algorithms. Among the various quantum-resilient cryptography schemes proposed in the currently running NIST's Post-quantum Cryptography (PQC) standardization plan, the lattice based LWE schemes have emerged as the most viable and preferred class for the IoT applications due to their compact area and memory footprint compared to other alternatives. However, compared to the classical schemes used today, R-LWE is much harder a challenge to fit on embedded IoT (end-node) devices, due to their stricter resource constraints (lower area, memory, energy budgets) as well as their limited computational capabilities. To the best of our knowledge, this is the first endeavour exploring the inherent approximate nature of LWE problem to undertake a multi-level Approximate R-LWE (AxRLWE) architecture with respective security estimates opt for lightweight IoT devices. Undertaking AxRLWE on Field Programmable Gate Arrays (FPGAs), we bench-marked a 64% area reduction cost compared to earlier accurate R-LWE designs at the cost of reduced quantum-security. With 45nm CMOS technology, AxRLWE was bench-marked to fit well within the same area-budget of lightweight ECC processor and consume a third of energy compared to special class of R-Binary LWE (R-BLWE) designs being proposed for an IoT, with better security level.

Index Terms—Approximate Computing (AxC), Lattice-Based Cryptography (LBC), Learning-with-Error (LWE), Ring-LWE (R-LWE), Internet of Things (IoTs)

I. INTRODUCTION

The impending realization of scalable quantum computers will have a significant impact on today's security. Quantum computers will be capable of executing Shor's algorithm, which can, in polynomial time, break the two hard mathematical problems, i.e., the integer factorization and discrete logarithm problems [1]. These problems make the basis of most of the Public-key Cryptographic (PKC) schemes that are used in today's security infrastructure (including RSA/ECC) to provide encryption and (authenticated) key exchange. Reacting to this urgency, much research is now being conducted into *quantum-resilient* or *Post-quantum* Cryptography (PQC). The

concern is rightly reflected by the stance of government agencies, including National Security Agency (NSA) and Communications-Electronics Security Group (CESG) [2]–[4]. The National Institute of Standards and Technology (NIST) announced a call requesting new quantum-resilient candidates to be considered for analysis, standardization and eventually industry adoption [5]. Various PQC schemes under consideration in the NIST standardization process are based on a diverse background of mathematical problems. What remains common however, is the fact that all of these quantum-resistant algorithms are much more complex than the currently deployed PKC techniques, i.e., larger key sizes, higher computational complexity, making them impractical for low-cost devices specially in the *Internet of Things* (IoT) scenario.

The IoT is growing at a phenomenal rate and has rightly revolutionized how we interact with the world today. The influence of IoT in our day to day activities is set to further increase with a projected 25 billion connected devices by 2020, according to Gartner [6], while Cisco states that by 2020, 50 billion devices will be network-connected [7]. The computational capabilities of these ubiquitous IoT devices depend on the layer in which they are deployed, i.e., server, edge or the end-nodes. The server/edge devices may benefit from embedded portable processors or configurable hardware platforms (i.e., Field Programmable Gate Arrays (FPGAs)). Whereas, the end-node entities are mostly very simple in design having limited area/power capabilities with recommendations of classical security-level to be at least 112-bits [8]. Ensuring security and privacy for an increasing number of these lightweight connected devices is a crucial concern for which the *quantum-safe* cryptographic family must cater for.

Out of the various PQC primitives, the lattices based family of cryptography offers the most viable and versatile solution for adaptation in the IoT device hierarchy [9]. Lattice problems have non-deterministic polynomial-time (NP) hardness with average-case to worst-case hardness and up-till now are resistant to attacks by the quantum computers. The *Learning-with Errors* (LWE) problem was first introduced in 2005 [10] that became the foundation of many Lattice-based schemes being submitted to the NIST PQC. However, this original LWE problem, based on the *Standard Lattices*, involves high computational and spatial cost restricting performance. To tackle that, LWE was modified to the Ring-LWE (R-LWE) problem by Lyubashevsky *et al.* in 2010 [11] based on *Ideal/Ring Lattices*. Light-weight R-LWE co-processors on FPGAs have been actively researched [12]–[16], proving their feasibility for the practical deployment on server/edge based IoT devices.

D.-S. Kundi*, C. Wang and W. Liu are with the School of Electronics and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China. E-mail: {dureshahwar, chwang, liuweiqiang}@nuaa.edu.cn
*She is also with National University of Sciences and Technology, Pakistan. Email: shahwar@pnec.nust.edu.pk

S. Bian is with the School of Cyber Science and Technology, Beihang University, Beijing, China. E-mail: sbian@buaa.edu.cn

A. Khalid and M. O'Neill are with the Centre for Secure Information Technologies, Queen's University Belfast, Belfast, U.K. E-mail: a.khalid@qub.ac.uk, m.oneill@ecit.qub.ac.uk

Very limited results for Very Large Scale Integration (VLSI) based Application Specific Integrated Circuit (ASIC) implementations of R-LWE, have been reported [17], [18]. An ASIC based custom hardware can not only provide higher speed performance but also a more compact design with lower power (as needed for portable applications). It is worth mentioning that the lightweight hardware implementation of ECC processor [19] requires only 20k GEs to 29.7k GEs for $GF(2^{163})$ to $GF(2^{233})$ (having respective classical-security levels of 80-bit to 112-bit), whereas, the R-LWE implementations reported in [17], [18] require much more, i.e., 776k GE and 106k GE respectively, because of the costly discrete Gaussian (DG) errors distribution and primarily polynomial multiplication.

In this context, a simple variant of R-LWE, called R-Binary LWE (R-BLWE) is presented by Buchmann *et al.* in 2016 [20] specially targeting an IoT. It used uniform binary error distribution instead of the expensive discrete Gaussian distribution, hence avoiding the multiplications. Several of their compact hardware implementations have been reported [21]–[24]. In terms of security, for lattice dimension of $n=256$ and modulus- $q=256$, R-BLWE has the reported classical/quantum-security estimates as 84/73-bits in 2017 in [21]. A more recent research reports even a lower security estimates for the same dimensional R-BLWE scheme, i.e., 64-bits (classical underestimates) [25]. The use of binary errors is one of the extreme simplification of R-LWE scheme to reach R-BLWE, resulting in degraded security that might not suits all applications.

Another promising approach is the use of Approximate Computing (AxC), exploiting the approximate nature of R-LWE scheme to reach even lower powered and compact designs, better suited to highly constrained IoT devices, at the cost of suitable security levels. In 2018 Bian *et al.* [26] utilized the conventional approximate Dynamic Range Unbiased Multiplier (DRUM) multiplier [27] for the polynomial multiplication in R-LWE scheme, they however did not undertake the effect on the overall scheme in terms of security degradation. Kundi *et al.* [28] also demonstrated the effect of approximation (via error truncation) to reach an area and power efficient approximate modular multiplier for R-LWE.

In view of the previous work done, it is easy to identify some research gaps in the context of approximation of R-LWE cryptosystem, when taken up to in ultra lightweight edge devices for IoT applications. None of the previously reported implementations present a multi-level approximation with associated resource saving and respective degraded security strength penalty, allowing the user to pick a design point best suited to his application resource budget and security appetite. The security analysis is either not taken up or only a single security level is presented. To fill in the gap, we present AxRLWE co-processor, that offers a multi-level trade-off between performance (cost, energy, latency etc.) and the quantum-security levels.

Contributions: We propose AxRLWE with multiple approximation levels for boosting the performance of R-LWE PKE on programmable FPGAs/ASICs in exchange of lowered resource usage and security estimates. Each level offers notable performance benefits and provides a knob to control

inaccuracy added to an execution. We demonstrate the effectiveness of the proposed techniques using elaborate place and route results on FPGAs and ASICs.

The main contributions of our work are given below

- We propose AxRLWE, a multi-level approximate Ring-Learning-with-Errors (R-LWE) cryptosystem along with a comparative security analysis. To the best of our knowledge, no earlier approximation effort on quantum-resistant schemes undertake multi-level approximation, providing various design points with resource vs. security trade-off.
- We analyze the effect of approximation on the security degradation enabling a user to pick a version best suited to his/her security/resource budget by providing updated quantum-security estimates via [29].
- All the AxRLWE designs were analyzed for resource consumption on both FPGA devices as well as 45nm CMOS technology library for bench-marking against the state-of-the-art accurate R-LWE as well as approximate implementations, i.e., binary R-LWE [21] and InvR-BLWE [21].
- AxRLWE conveniently excels by superior performance compared to reported accurate as well as binary R-LWE designs in terms of substantially low area/energy budgets.
- Our smallest AxRLWE supports quantum-security of 66-bit against the 62-bit of R-BLWE/InvRBLWE and requires only 9.0k GE.

The rest of the paper is organized as follows. Section II, provides the background knowledge about the R-LWE cryptosystem and the Approximate Computing (AxC). Meanwhile, Section III explains the design of our proposed approximate R-LWE (**AxRLWE**) along with the undertaken optimizations. The detailed analysis of the approximate R-LWE design is presented in Section IV whereas the implementation results and discussion are given in Section V. Finally, the Section VI presents the conclusions.

II. THE RING-LEARNING-WITH-ERRORS (R-LWE) CRYPTOSYSTEM

The R-LWE-based cryptosystems use *Ideal Lattices*, which correspond to ideals in the ring $\mathbb{Z}[x]/\langle f \rangle$, where f is an irreducible polynomial of degree n . For better efficiency and security the ring is often taken as $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ where n is a power-of-two integer and q is a prime modulus such that $q \equiv 1 \pmod{2n}$. Moreover, the procedures for the key generation, encryption, and decryption of R-LWE based PKE scheme are described as follows:

- 1) Key Generation ($a \leftarrow U$): Sampling $r_1, r_2 \leftarrow \chi_\sigma$; Calculate $p = r_1 - a \times r_2$, Public key: (a, p) ; Secret key: r_2
- 2) Encryption ($a, p, m \leftarrow \{0, 1\}$): Sampling $e_1, e_2, e_3 \leftarrow \chi_\sigma$; and Encode $\tilde{m} = \lfloor (q/2) \rfloor m$; and Calculate $c_1 = a \times e_1 + e_2$, $c_2 = p \times e_1 + e_3 + \tilde{m}$;
- 3) Decryption (c_1, c_2, r_2): Calculate $\tilde{m}' = c_1 \times r_2 + c_2$ and Convert $\tilde{m}'$ into $\{0, 1\}$ such that if $\tilde{m}' \in (\lfloor (3q/4) \rfloor, \lfloor (q/4) \rfloor)$ then $m = 0$ else $m = 1$.

All the operations are based on polynomials in the ring $\mathbb{R}_q$, U represents the uniform distribution and χ is a discrete Gaussian (DG) distribution with a standard deviation σ and mean $\mu = 0$ whereas ' $\times$ ', ' $+$ ' represent the modular multiplication and addition operations, respectively. For hardware implementation of R-LWE, the DG sampler and the modular polynomial multiplier are the main bottlenecks.

A. Polynomial Multiplication

The simplest method to carry out the modular polynomial multiplication and ideal for resource-constrained applications is the Schoolbook Algorithm. This method requires less hardware and supports any q contrary to its alternate Number Theoretic Transform (NTT) technique (that requires pre-computation, array reordering and post-computation and supports only $q \equiv 1 \pmod{2n}$). But, it has a quadratic complexity with $O(n^2)$ multiplications and $O(n^2 - 1)$ modulo additions/subtractions, that asymptotically make it more energy hungry for a battery operated IoT device.

The schoolbook polynomial multiplication algorithm is expressed as Eq. 1 [12]:

$$\begin{aligned} c(x) &= a(x) \cdot b(x) = \left[\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j x^{i+j} \right] \bmod (x^n + 1) \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (-1)^{\lfloor (i+j)/n \rfloor} a_i b_j x^{(i+j) \bmod n} \end{aligned} \quad (1)$$

Each coefficient is reduced modulo q and polynomial reduction modulo $x^n + 1$ is performed by using bit mask when n is power of two and $(-1)^{\lfloor (i+j)/n \rfloor}$ is 1 for $i + j < n$ and -1 for $i + j \geq 2n - 2$.

Hence, in this work the focus is to provide effective solutions utilizing schoolbook polynomial multiplication by exploring new implementation techniques such as Approximate Computing (AxC).

B. Approximate Computing (AxC)

The AxC [30] is a promising energy-efficient hardware technique that provides significant efficiency gains at the cost of permissible quality degradation. Right now, it has been employed in a number of error-tolerant applications such as image processing, multimedia signal processing, machine learning, pattern recognition etc., but not yet explored for the LWE cryptography. The motivation of this proposed work is further fueled by the fact that LWE problem is approximate in nature. For such ciphers, profiling and controlling errors is related to the correctness of the LWE scheme whereas the security depends on the lattice dimension and the standard deviation of DG distribution.

C. Discrete Gaussian (DG) Sampling

The Discrete Gaussian sampling is computed via different rejection sampling techniques that come with their own pros and cons [31]. The Cumulative Distribution Table (CDT)-based sampler is the simplest method of sampling that comprises of a pre-computed table of N discrete Gaussian cumulative distribution function (CDF) values each with ' λ ' bits of

precision and requires a large comparator with a binary search complexity of $\log_2(N)$ comparisons in order to generate a final sample of $\lceil \log_2 q \rceil$ -bit [32]. Whereas, the rejection sampling is a straight forward method that does not require any pre-computed data but it accept/reject a value with a probability equal to its probability in the target distribution. The problem with rejection sampling is that the probability of rejection is a function of modulus- q as $(1 - q/2^{\lceil \log_2 q \rceil})$ and its improvement may require samples with larger width of $\lceil \log_2 kq \rceil$ -bit and the MR module to convert back to $\log_2 q$ -bit. Both of these result in large overhead and are inappropriate solutions for the resource-constrained applications.

D. Parameter-set

Normally the R-LWE based PKE is parameterized by (n, q, χ, σ) where n defines the lattice dimensions, q is the prime modulus and σ represents the standard deviation of the distribution χ . The selected parameter-set for the R-LWE from [33] is summarized in Table I, based on the q , $\lceil \log_2 q \rceil$ provides the length of the operands (in bits) for the multiplier as well as the error sampler.

The R-LWE version as summarized in Table I provides a medium security level [33], [34] (roughly equivalent to AES-128, NIST PQC security level-1) being sufficient for low-weight IoT end-node devices.

TABLE I
R-LWE PARAMETER INSTANTIATIONS.

n	q	σ	$\lceil \log_2 q \rceil$	Security Level
256	7681	4.51	13	106-bits Classical [34]

III. PROPOSED APPROXIMATE R-LWE (AxRLWE)

In this section, we present the architectural details of our proposed Approximate R-LWE (AxRLWE) cryptosystem, designed specially for the IoT end node devices by keeping in mind their resource budget and security requirements. The AxRLWE comprises of design of an Approximate Modular Multiplier (AxMM) and a Binomial sampler.

A. Approximate Modular Multiplier (AxMM)

If we analyzed the R-LWE PKE scheme, the hardware of schoolbook based polynomial multiplication generally depends on the modulus- q where the width of the inputs; multiplier and multiplicand are calculated as $\lceil \log_2 q \rceil$ -bit that results in a $\lceil \log_2 q \rceil \times \lceil \log_2 q \rceil$ -bit multiplier as shown in Fig. 1. The multiplier input options are a (public parameter being sampled from uniform distribution and smaller than the modulus- q), p (public key) and c_1 (cipher text) whereas the multiplicand input options are r_2 and e_1 , both are sampled from the DG distribution with standard deviation σ . After the multiplication, the final result of $(2 \cdot \lceil \log_2 q \rceil)$ -bit is reduced back to $\lceil \log_2 q \rceil$ -bit with the help of Modular Reduction (MR) unit (mostly employed Barrett's reduction algorithm [35]).

It is observed that the multiplicand for the polynomial multiplication always come from the DG distribution having a

Fig. 1. Schoolbook based modular polynomial multiplication.

bell-shaped curve, symmetric at both sides of the μ . The $\mu - k\sigma$ and $q - \mu - k\sigma$; where $k=1,2,3...$ represents the positive and negative values respectively (in case of LWE with modulus- q). This fact has been exploited by many researchers to utilize the Signed-Magnitude Representation (SMR) for the Gaussian data instead of using a conventional unsigned representation [16], [36]. The modular polynomial multiplication with these negative values can easily be realized as follows: $a \times (-b) \bmod q = q - [a \times b \bmod q]$.

Hence, this translates the width of multiplicand input from $\log_2 q$ -bit to $1_{sign} + \lceil \log_2 7\sigma \rceil$ -bit, where 7σ represents the maximum preferable tail-cut bound for the distribution [13], [31]. So, for $\sigma=4.51$ it results in 6-bit signed number instead of 13-bit unsigned accommodating the maximum value upto $\pm 31 (\pm 7\sigma)$. Whereas, the signed bit will not be utilized during the modular multiplication operation. However, if we further analyzed the distribution of error w.r.t to their percentage as shown in Fig. 2. The 99.7% of values that lies within interval $[\mu - 3\sigma, \mu + 3\sigma]$ of Gaussian distribution are of 4-bit (± 13.35) whereas in the next interval, only 0.2% of values are of 5-bit that hardly represents a single value out of $n=256$ samples. So, in hardware the width of multiplicand can be reduced to 4-bit by truncating the MSB[5] of $\lceil \log_2 7\sigma \rceil$ -bit without having significant effect on the security of the R-LWE scheme. We called it the first level of approximation, i.e., $L = 1$.

Fig. 2. Discrete Gaussian (DG) distribution $\sigma=4.51$.

To make the hardware of R-LWE scheme more suitable for IoT end-node devices, we further explore the operand truncation strategy of approximate computing (AxC) technique based on the approximate nature of LWE scheme as well as motivation from the R-BLWE scheme with binary errors [21]. The second level of approximation, i.e. $L = 2, 3$ represents the rounding of Gaussian samples from higher range to the smaller one by truncating $\lceil \log_2 7\sigma \rceil$ to even lower width to support the smaller errors. This enables us to further reduce the hardware of original multiplier to $\lceil \log_2 q \rceil \times \lceil \log_2 7\sigma \rceil - L$ based on the $L = 1, 2, 3$ as summarized in Table II. The $L = 1$ represents only the first level of approximation based on the DG distribution while $L = 2, 3$ includes the second level of optimization in addition to the first. Hence, selecting $L = 3$ will result in 13×2 multiplier in comparison to an original 13×13 multiplier and hence will greatly reduced the hardware cost for an IoT end-node device.

TABLE II
EFFECT OF APPROXIMATION ON MULTIPLICAND'S WIDTH.

Approx. Level (L)	Original width* $\lceil \log_2 q \rceil \times \lceil \log_2 q \rceil$	SMR* $\lceil \log_2 q \rceil \times \lceil \log_2 7\sigma \rceil$	This work $\lceil \log_2 q \rceil \times (\lceil \log_2 7\sigma \rceil - L)$
1	13×13	13×5	13×4
2	—	—	13×3
3	—	—	13×2

* $q=7681, \sigma=4.51$

For the polynomial multiplication, the resulting hardware of our proposed Approximate Modular Multiplier (AxMM) is shown in Fig. 3 (a) and its deployment for the R-LWE decryption phase is shown in Fig. 3 (b). The 2-bit L will specify the selection of LSB range of multiplicand, on the basis of the level of approximation. All the input values are delivered to the AxRLWE cryptoprocessor through the input modules while the output is accessed serially when the *done* signal becomes '1'.

B. Binomial Sampler

For the implementation of DG sampling, we explore an approximation to normal Gaussian distribution strategy via binomial distribution, which is not yet fully investigated by the previous R-LWE designs. The binomial sampling enables an easier and low-cost sampling, in comparison to the most widely used CDT and rejection sampling techniques (as mentioned in Section II-C).

The hardware architecture of our proposed binomial sampler is shown in Fig. 3 (a), it calculates the hamming weight of two k -bit random samples (from Trivium PRNG) as given by (2), being approximated on the basis of standard deviation σ (as $k \approx \sigma^2$) and is configured to generate $1_{sign} + \lceil \log_2 7\sigma \rceil$ -bit error samples.

$$\text{output} = \sum_{i=0}^k a_i - \sum_{i=0}^k b_i \quad (2)$$

Furthermore, this approximation works well for $\sigma < 5$ with negligible effects on the security because of characteristics of DG distribution. That is why most of NIST PQC candidates employed it instead of Gaussian distribution, i.e., NewHope [37], CRYSTALS-Kyber [38] etc.

IV. ANALYSIS

It is believed that the higher level of approximations, i.e., $L = 2, 3$ may affect the correctness criteria of a R-LWE scheme as well as reducing the security. Hence, this section provides the detailed evaluation of the undertaken hardware optimization on the correctness criteria of a R-LWE scheme as well as its implication on the security. Because, we are approximating the errors, it may vary the standard deviation of DG distribution, i.e., σ . So, in this section we first calculate the resulting σ for the higher level of approximation, i.e., $L = 2, 3$ and then presents the analysis regarding the decryption failure probability (as correctness criteria) as well as the achievable security estimates w.r.t the resulting σ .

Fig. 3. (a) The proposed hardware of Approximate Modular Multiplier (AxMM) and binomial sampler, (b) Lightweight architecture of AxRLWE for decryption phase.

A. Effect on the Standard Deviation (σ)

By increasing the level of approximation L basically decreases the width of the multiplicand that in-turn reduces the range of the error samples being drawn from the DG distribution. For $L=1$, the multiplicand width is $\lceil \log_2 7\sigma \rceil - L = 4$ with $\sigma=4.51$ (as shown in Table II) and the supported range of error samples is between $[-15, +15]$. Similarly, for $L=2$, it is reduced to 3-bit and will have the range of error samples in $[-7, +7]$, the values greater than this range are converted back to 3-bit. It means the probability density function $P(x)$ of DG distribution will change. The new σ is calculated through $\lceil \log_2 7\sigma_{new} \rceil = \lceil \log_2 7\sigma \rceil - L$ as well as adjusted (to cover the specified range of error samples) with the help of a plot. The resulting σ w.r.t $L=2$ and 3 is calculated as 2.66 and 1.24 respectively, as shown in Fig. 4, where the probability of '0' sample for $\sigma=2.66$ increases from 8.85% to 15.00% and for $\sigma=1.24$ increases from 8.85% to 32.17%.

Fig. 4. Effect of approximation level (L) on the σ .

B. Decryption Failure Probability (δ)

During the decryption phase, the final $\bar{m}'$ translates to:

$$\begin{aligned} c_1 r_2 + c_2 &= e_2 r_2 + e_1 r_1 + e_3 + \lfloor q/2 \rfloor m \\ &= \langle e, r \rangle + \lfloor q/2 \rfloor m \end{aligned} \quad (3)$$

The decryption will fail if error threshold of decoder, i.e., $\langle e, r \rangle > \lfloor q/4 \rfloor$. This per-symbol error probability is denoted by δ , that depends on σ according to Lemma 3.1 [39].

Lemma 3.1 (correctness criteria): *the error probability per symbol (over the choice of secret key) is bounded from above by any desired $\delta > 0$, as long as*

$$(\sigma\sqrt{2\pi})^2 \leq \frac{\sqrt{2\pi}}{c} \cdot \frac{t}{\sqrt{2n \cdot \ln(2/\delta)}} \quad (4)$$

where $t = \lfloor \frac{q}{4} \rfloor$ and $c \geq 1$ is a constant; for $n=256$, $c=1.25$ [39].

Using (4) the δ improves to 10^{-3} for the $\sigma=2.66$ and 10^{-4} for the $\sigma=1.24$, whereas, was 10^{-2} for the $\sigma=4.51$. Hence, it is evident from the above that decreasing the σ will improve the decryption failure probability (δ) of the scheme, as stated in [12] and the same is proved in Table 1 of [33]. Afterwards, it became the motivation for the PQC candidates choosing error distribution with smaller σ 's, resulting in improved values of δ [37]. But, reduced σ may effect the security of the R-LWE scheme.

C. Security Estimates

The Security estimates of LWE/R-LWE against different σ is obtained from the LWE hardness estimator [40] that is available at [29]. R-LWE parameters are kept as mentioned in the Table I ($\sigma = 4.51$) for $L = 1$, while for $L = 2, 3$ a lowered $\sigma = 2.66, 1.24$ is instead taken. The importance our proposed technique is that the lattice dimensions, i.e., $n = 256$ will not change, mainly contributes towards the security and energy consumption.

The LWE hardness estimator provides the concrete security estimates against the following three lattice based problems depending upon the Shortest Vector Problem (SVP) oracle being utilized based on the classical/quantum enumeration or sieving algorithms (the reader is referred to [40], [41] for the complete algorithmic details).

- 1) The **unique SVP (uSVP)** that is reduced from the bounded distance decoding (BDD) problem.
- 2) The **Decoding (Dec) problem** using Babai's nearest plane algorithm [42].
- 3) The **dual-lattice (Dual) attack problem** under the BKZ 2.0 cost model [43].

TABLE III
SECURITY ESTIMATES UNDER BKZ 2.0 COST MODEL USING QUANTUM SIEVING ALGORITHMS.

(σ, L)	$uSVP$	Dec	$Dual$
(4.51, 1)*	91.2	111.2	125.3
(2.66, 2)*	78.7	92.5	101.4
(1.24, 3)*	66.0	74.6	77.9
R-BLWE [21] **	62.0	70.1	68.0
InvRBLWE [22] **			

* $n=256$, $q=7681$, ** $n=256$, $q=256$

The Block-wise Korkine-Zolotarev (BKZ) is a lattice reduction algorithm first introduced in [44], to solve the hardness of average-case lattice problem (i.e., LWE), which is the foundation of many LBC schemes. The evaluated security estimates against the $uSVP$, dec and $dual$ attacks w.r.t the different L and corresponding σ are provided in Table III, using quantum sieving algorithms. Under the same settings, we also evaluates the latest quantum-security level of R-BLWE [21] and InvRBLWE [22] (the preferred option for IoT resource-constrained devices). The highlighted values are the final achieved quantum-security levels. The lowest level supported by our AxRLWE is 66-bits at $L = 3$ (having 2-bit signed-error samples) whereas the R-BLWE [21] and InvRBLWE [22] have 62-bits quantum-security level (having 1-bit uniform binary error distribution; $\{0, 1\}$ as well as reduced modulus- q , i.e., 256).

Furthermore, it is observed from the LWE hardness estimator that decreasing the modulus- q will improve the quantum-

TABLE IV
AXRLWE COMPARISON WITH EARLIER FPGA BASED IMPLEMENTATIONS.

Design	Device	Process	LUT/Slices/DSP*/BRAM*	Equiv. Slices	Freq. (MHz)	Thr. (Kbps)	Area Savings(%) L1,L2,L3	Throughput per Slice, TPS (Kbps/S)
R-LWE [15]	Kintex-7	Enc	1098/337/1/0	440	288	560.9	47 ~ 53	1.27
		Dec	609/182/1/0	285		1121.81	35 ~ 43	3.93
R-LWE [16]	Kintex-7	Enc	898/303/1/1.5	579	305	1119.84	60 ~ 64	1.93
		Dec	635/194/1/0.5	354	303	2255.49	48 ~ 55	6.37
R-BLWE [21]	Spartan-6	Dec	57/19/0/2	159	135	525.25	-16 ~ -1	3.3
AxRLWE (L=1)	Kintex-7	Enc	706/230/0/0	230		615.23		2.67
		Dec	592/185/0/0	185	315	1230.47		6.65
AxRLWE (L=2)	Kintex-7	Enc	658/220/0/0	220		625.00		2.84
		Dec	566/176/0/0	176	320	1250.00		7.10
AxRLWE (L=3)	Kintex-7	Enc	643/206/0/0	206		625.00		3.03
		Dec	546/160/0/0	160	320	1250.00		7.81

*Equivalent (Equiv.) Slices: DSP $\approx$ 102.4 Slices and 18K BRAM $\approx$ 116.2 Slices [16]

security level. As in case of R-BLWE/InvRBLWE, with $q=256$ and binary errors, the degradation in security level is not that much w.r.t other security parameters but the only shortcoming is that it does not supports the DG error distribution. Hence, keeping the original R-LWE scheme with DG error distribution and changing the modulus- q from 7681 to 4093 (as that of [39]) or 3329 (as in [33]) with same lattice dimensions (i.e., $n=256$), the quantum-security level will increase to 70-bits/72-bits contrary to 66-bits in the case for $\sigma=1.24$ ($L = 3$). Moreover, this will also reduce the memory/register requirements as well as the key sizes. In addition, selecting the modulus- q as power of 2 i.e., 4096 instead of 4093 [45], will further eliminate the need of MR circuitry, same as that of R-BLWE/InvRBLWE schemes. It is stated that a modulus- q not necessarily a prime, has negligible effects on the security level [45] and we also evaluate the effect through the LWE hardness estimator, which comes out to be same as 70-bits. Hence, there is always a trade-off between the security and the correctness of the R-LWE scheme. Decreasing the σ , improves the decryption failure probability (as (4)) but decreases the security of the scheme. In contrast, larger modulus- q has a better success probability of key reconciliations but reduced the security level.

Finally, we noted that the above design optimization widely applies to cryptographic constructions based on many variants of LWE. For example, CRYSTALS-Kyber [38] and SABER [46], which are the final-round candidates for the NIST post-quantum key exchange standardization process, are based on the module versions of the LWE and learning with rounding (LWR) problems, respectively. We point out that the basic arithmetic operands in both CRYSTALS-Kyber and SABER are polynomials, and that such polynomials share the same n and similar q as that in Table I, i.e., $q=3329$ and $q=2^{13}$, respectively. Therefore, we can easily leverage the instantiated parameters and hardware architectures for the acceleration of standard post-quantum key exchange on IoT devices.

V. IMPLEMENTATION RESULTS AND DISCUSSIONS:

All the AxRLWE designs were manually implemented and tested in Verilog HDL and synthesized using *Xilinx Vivado 2018.3 Suite* on Xilinx Kintex-7 FPGA devices as well as Synopsys *Design Compiler* (DC) with VLSI *Nangate Open-Cell 45nm* slow process technology library. For FPGA device,

each design was profiled for area and maximum frequency and results are reported after Post-place & Route (Post-PAR) verification. Whereas, for ASICs, the area results are reported as μm^2 as well as the number of Gate Equivalent (GE) in terms of 2-input NAND and the synthesis was targeted for area minimization (with the max area constraint set to 0) while power consumption was estimated by Synopsys *Prime Time* based on gate level netlist switching activity by back annotation.

Table IV provides the hardware results of our proposed AxRLWE design on FPGA for $L = 1, 2, 3$. The proposed designs are implemented utilizing only the LUTs and Slices while for the comparison with the designs [15], [16], [21] having DSP and BRAM blocks, a column of Equivalent (Equiv.) Slices is provided based on the estimates in [16]. Finally, hardware efficiency of FPGA designs are benchmarked using the Throughput-per-Slice (TPS) metric.

As expected, an increase in approximation reduces the area resources along with a relative increase in the TPS. Our proposed AxRLWE designs ($L1, L2, L3$) result in an area saving of 48 ~ 53% compared to the naive and accurate implementation of R-LWE [15] having a 13×13 -bit multiplier whereas an area saving of 60 ~ 64% from an optimized R-LWE design [16] having two 13×5 -bit multipliers accommodated into a single DSP. This trick in [16] halves up the latency ($n^2/2$), doubling throughput, i.e., 1119.84 Kbps (Enc) and 2255.49 Kbps (Dec). For lightweight IoT devices, high throughput performance may not be a design goal and is often an over-kill. Hence, compared to the exact reported designs, the AxRLWE designs provide an area saving of up to $\approx 64\%$, at the cost of lowered security level, that is acceptable for lightweight IoT devices. Comparing our proposed AxRLWE co-processor designs with R-BLWE [21] (a special class of R-LWE having binary errors and power of 2 modulus- q , requiring no modular reduction unit), our AxRLWE $L = 3$ implementation with 2-bit error-samples has better security estimates of 66-bits compared to 62-bits [21] (refer Table III) while utilizing same area resources for the Decryption, i.e., 160 Slices with 58% higher throughput performance. Moreover, it is evident from the Table IV that our proposed designs have higher TPS for both Enc/Dec, compared to the previously reported R-LWE and R-BLWE designs. Hence, provide a balanced solution w.r.t area and performance as well as the security.

Table V gives the hardware results of AxRLWE on ASIC, highlighting the resource and performance outcomes for the decryption phase only as that of R-BLWE [21] and InvRBLWE [22] designs. For the fair comparison, we re-coded the existing R-LWE based FPGA designs [15], [16] with respective single 13×13 -bit and 13×5 -bit multiplier and synthesized using Synopsys DC with same technology library. The Power @33.3MHz operating frequency gives a sum of dynamic and static power for a fair comparative analysis of AxRLWE with the available variant of R-LWE design, i.e., InvRBLWE [22], whereas the latency for all the energy calculations is n^2 cycles based on the lattice dimension of $n = 256$. Similarly, it is apparent from the Table V, as the approximation level increases for our AxRLWE, there is a substantial area saving that follows from $L = 1$ to $L = 3$. Unlike the other reported implementations, AxRLWE provides a range of approximations to let the user pick the one as per his performance/security requirements having fixed lattice dimensions. Comparing AxRLWE ($L = 3$) having 66-bits quantum-security with InvRBLWE [22] having 62-bits (ref. Table III), our design not only consumes lower power at @33.3MHz operating frequency but also has $\approx 3 \times$ lower energy consumption with 131nJ compared to the 355nJ, hence suitable for energy harvesting IoT devices. Moreover, all of our AxRLWE designs fit within the same area budget of 20k GE as that of lightweight ECC co-processor [19] and have better quantum-security estimates.

VI. CONCLUSIONS

This work explores approximate computing for Ring-Learning-with-Errors (R-LWE) based Post-quantum Cryptographic (PQC), by taking advantage of its inherent approximate nature. The proposed Approximate R-LWE (AxRLWE) co-processor design is novel in terms of the multi-level approximation that it carries along with a thorough security analysis for each approximation level under the setting of same lattice dimensions. It allows the user to pick the right version as suited best according to his security appetite and resource budget. AxRLWE designs when taken up on comparable FPGAs provides up to $\approx 64\%$ area saving compared to the accurate R-LWE at the cost of degraded equivalent security levels fit for the lightweight IoT devices. Comparing AxRLWE on CMOS, our proposed designs are with in the Gate Equivalent (GE) budget of the earlier lightweight ECC processor. Further, our design was able to provide substantial power savings with

about $\approx 3 \times$ lowered energy consumption against the binary R-LWE scheme with similar security. Our results show that approximation has the potential to bring the PQC within the tight area/energy budgets available in embedded IoT (edge) devices.

ACKNOWLEDGEMENT

This work is supported by grants from the National Natural Science Foundation of China (62022041 and 61871216) and the Engineering and Physical Sciences Research Council of U.K. (EP/N508664/- CSIT2).

REFERENCES

- [1] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.
- [2] CNSS, "Use of public standards for the secure sharing of information among national security systems," Committee on National Security Systems: CNSS Advisory Memorandum, Information Assurance 02-15, July 2015.
- [3] CESG, "Quantum key distribution: A CESG white paper," February 2016. [Online]. Available: <https://www.cesg.gov.uk/white-papers/quantum-key-distribution>
- [4] National Security Agency, "Commercial national security algorithm suite," August 2015. [Online]. Available: <https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm>
- [5] D. Moody, "Post-quantum cryptography: NIST's plan for the future," Talk given at PQCrypto Conference, February 2016. [Online]. Available: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf
- [6] V. M. J. Rivera and R. Gartner, "4.9 billion connected 'things' will be in use in 2015," *The Washington Post*, Feb 2016. [Online]. Available: <http://www.gartner.com/newsroom/id/2905717>
- [7] Cisco, "Internet of things (IoT)," *The Washington Post*, July 2015. [Online]. Available: <http://www.cisco.com/web/solutions/trends/iot/portfolio.html>
- [8] K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, "Report on lightweight cryptography," National Institute of Standards and Technology (NIST), Tech. Rep. NISTIR 8114, Mar. 2017. [Online]. Available: <https://doi.org/10.6028/NIST.IR.8114>
- [9] A. Khalid, S. McCarthy, M. O'Neill, and W. Liu, "Lattice-based cryptography for IoT in a quantum world: Are we ready?" in *Proc. IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI)*, 2019, pp. 194–199.
- [10] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proc. 37th Annual ACM Symposium on Theory of Computing (STOC)*, May 2005, pp. 84–93.
- [11] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and Learning with Errors over rings," in *Advances in Cryptology – EUROCRYPT*, H. Gilbert, Ed. Springer Berlin Heidelberg, 2010, pp. 1–23.
- [12] T. Pöppelmann and T. Güneysu, "Towards efficient arithmetic for lattice-based cryptography on reconfigurable hardware," in *Proc. International Conference on Cryptology and Information Security in Latin America*, 2012, pp. 139–158.
- [13] —, "Towards practical lattice-based public-key encryption on reconfigurable hardware," in *Proc. International Conference on Selected Areas in Cryptography*, 2013, pp. 68–85.
- [14] —, "Area optimization of lightweight lattice-based encryption on reconfigurable hardware," in *Proc. IEEE International Symposium on Circuits and Systems (ISCAS)*, 2014, pp. 2796–2799.
- [15] S. Fan, W. Liu, J. Howe, A. Khalid, and M. O'Neill, "Lightweight hardware implementation of R-LWE lattice-based cryptography," in *Proc. IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, 2018, pp. 403–406.
- [16] W. Liu, S. Fan, A. Khalid, C. Rafferty, and M. O'Neill, "Optimized schoolbook polynomial multiplication for compact lattice-based cryptography on FPGA," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2019.
- [17] S. Song, W. Tang, T. Chen, and Z. Zhang, "LEIA: A 2.05mm² 140mw lattice encryption instruction accelerator in 40nm cmos," in *Proc. IEEE Custom Integrated Circuits Conference (CICC)*, 2018, pp. 1–4.

TABLE V

AXRLWE COMPARISON WITH ASIC BASED IMPLEMENTATIONS ON 45NM TECHNOLOGY LIBRARY (DECRYPTION).

Design	Area* (μm^2)	(GE)	Freq. (MHz)	Power (mW)	Energy (nJ)
R-LWE [15]	33k	41.4k	100	1.16	760
R-LWE [16]	22k	27.6k	110	0.88	524
InvRBLWE [22]	6k	7.6k	33.3	0.18	355
ECC [19] **	—	20k	6.81	1.12k	130k
AxRLWE (L=1)	17k	21.6k	116	0.60	339
AxRLWE (L=2)	11k	13.9k	122	0.39	210
AxRLWE (L=3)	7.2k	9.0k	125	0.25	131

* 1 GE= NAND2 = 0.798 μm^2 , ** 65nm, GF(2¹⁶³)

- [18] U. Banerjee, T. S. Ukyab, and A. P. Chandrakasan, "Sapphire: A configurable crypto-processor for post-quantum lattice-based protocols," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 4, pp. 17–61, 2019.
- [19] R. Salarifard, S. Bayat-Sarmadi, and H. Mosanaei-Boorani, "A low-latency and low-complexity point-multiplication in ECC," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 65, no. 9, pp. 2869–2877, 2018.
- [20] J. Buchmann, F. Göpfert, T. Güneysu, T. Oder, and T. Pöppelmann, "High-performance and lightweight lattice-based public-key encryption," in *Proc. 2nd ACM International Workshop on IoT Privacy, Trust, and Security (IoTPTS'16)*, 2016, p. 2–9.
- [21] A. Aysu, M. Orshansky, and M. Tiwari, "Binary Ring-LWE hardware with power side-channel countermeasures," in *Proc. Design, Automation & Test in Europe Conference Exhibition (DATE)*, 2018, pp. 1253–1258.
- [22] S. Ebrahimi, S. Bayat-Sarmadi, and H. Mosanaei-Boorani, "Post-quantum cryptoprocessors optimized for edge and resource-constrained devices in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5500–5507, 2019.
- [23] J. Xie, K. Basu, K. Gaj, and U. Guin, "Special session: The recent advance in hardware implementation of post-quantum cryptography," in *Proc. of 38th VLSI Test Symposium (VTS)*, San Diego, CA, USA, 2020, pp. 1–10.
- [24] S. Ebrahimi and S. Bayat-Sarmadi, "Lightweight and fault-resilient implementations of binary Ring-LWE for IoT devices," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6970–6978, 2020.
- [25] R. Player, "Parameter selection in lattice-based cryptography," Ph.D. dissertation, Royal Holloway, University of London, 2018.
- [26] S. Bian, M. Hiromoto, and T. Sato, "DWE: Decrypting Learning with Errors with errors," in *Proc. 55th ACM/ESDA/IEEE Design Automation Conference (DAC)*, June 2018, pp. 1–6.
- [27] S. Hashemi, R. I. Bahar, and S. Reda, "DRUM: A dynamic range unbiased multiplier for approximate applications," in *Proc. IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Nov 2015, pp. 418–425.
- [28] D.-S. Kundi, S. Bian, A. Khalid, C. Wang, M. O'Neill, and W. Liu, "AxMM: Area and power efficient approximate modular multiplier for R-LWE cryptosystem," in *Proc. IEEE International Symposium on Circuits and Systems (ISCAS)*, 2020, pp. 1–5.
- [29] M. Albrecht, "Estimator for the bit security of LWE instances," 2015. [Online]. Available: <https://bitbucket.org/malb/lwe-estimator>
- [30] H. Jiang, C. Liu, L. Liu, F. Lombardi, and J. Han, "A review, classification, and comparative evaluation of approximate arithmetic circuits," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 13, no. 4, pp. 60:1–60:34, 2017.
- [31] J. Howe, A. Khalid, C. Rafferty, F. Regazzoni, and M. O'Neill, "On practical discrete Gaussian samplers for lattice-based cryptography," *IEEE Transactions on Computers*, vol. 67, no. 3, pp. 322–334, 2016.
- [32] A. Khalid, J. Howe, C. Rafferty, F. Regazzoni, and M. O'Neill, "Compact, scalable, and efficient discrete Gaussian samplers for lattice-based cryptography," in *Proc. IEEE International Symposium on Circuits and Systems (ISCAS)*, 2018, pp. 1–5.
- [33] N. Göttert, T. Feller, M. Schneider, J. Buchmann, and S. Huss, "On the design of hardware building blocks for modern lattice-based encryption schemes," in *Cryptographic Hardware and Embedded Systems (CHES)*. Springer Berlin Heidelberg, 2012, pp. 512–529.
- [34] T. Pöppelmann, "Efficient implementation of ideal lattice-based cryptography," Ph.D. dissertation, Ruhr-University Bochum, Germany, June 2015.
- [35] P. Barrett, "Implementing the Rivest Shamir and Adleman Public Key Encryption algorithm on a standard Digital Signal Processor," in *Proc. Advances in Cryptology – CRYPTO*. Springer Berlin Heidelberg, 1987, pp. 311–323.
- [36] Y. Zhang, C. Wang, D.-S. Kundi, A. Khalid, M. O'Neill, and W. Liu, "An efficient and parallel R-LWE cryptoprocessor," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 5, pp. 886–890, 2020.
- [37] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange - a New Hope," *Cryptology ePrint Archive*, Report 2015/1092, 2015, <https://eprint.iacr.org/2015/1092>.
- [38] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Kyber algorithm specifications and supporting documentation," *NIST PQC Round*, vol. 2, p. 4, 2019.
- [39] R. Lindner and C. Peikert, "Better key sizes (and attacks) for LWE-based encryption," in *Topics in Cryptology – CT-RSA*, A. Kiayias, Ed. Springer Berlin Heidelberg, 2011, pp. 319–339.
- [40] M. R. Albrecht, R. Player, and S. Scott, "On the concrete hardness of Learning with Errors," *Journal of Mathematical Cryptology*, vol. 9, no. 3, pp. 169–203, 2015. [Online]. Available: <https://doi.org/10.1515/jmc-2015-0016>
- [41] T. Wunderer, "On the security of lattice-based cryptography against lattice reduction and hybrid attacks," Ph.D. dissertation, Technical University of Darmstadt, Germany, August 2018.
- [42] L. Babai, "On lovász' lattice reduction and the nearest lattice point problem," *Combinatorica*, vol. 6, no. 1, pp. 1–13, 1986.
- [43] Y. Chen and P. Q. Nguyen, "BKZ 2.0: Better lattice security estimates," in *Advances in Cryptology – ASIACRYPT*. Springer Berlin Heidelberg, 2011, pp. 1–20.
- [44] C.-P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," *Mathematical Programming*, vol. 66, no. 1, pp. 181–199, 1994.
- [45] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé, "Classical hardness of Learning with Errors," in *Proc. 45th Annual ACM Symposium on Theory of Computing (STOC)*, 2013, pp. 575–584.
- [46] J.-P. D'Anvers, A. Karmakar, S. S. Roy, and F. Vercauteren, "Saber: Module-LWR based key exchange, CPAs-secure encryption and CCA-secure KEM," in *International Conference on Cryptology in Africa*. Springer, 2018, pp. 282–305.

member of Technical Committee of CASCOM and IEEE Circuits and Systems Society.

DAAD Scholarship Award for her Ph.D. studies at RWTH Aachen, Germany. She is a member of VSA Technical Committee of IEEE Circuits and Systems Society.

members/reviewers for top international conferences/journals across different fields of studies, including AAAI, ASP-DAC, Journal of Cryptology, and ACM TODAES. He is a member of IEEE and IPSJ.

Dur-e-Shahwar Kundi is currently a Post-doc Fellow at College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China under the scheme of China Postdoctoral Science Foundation 2019. She received her M.Sc. and Ph.D. degree in Electrical Engineering from National University of Sciences and Technology (NUST), Karachi, Pakistan, in 2010 and 2016 respectively. Her research interests include hardware security, cryptographic engineering and reconfigurable computing. She is a

Ayesha Khalid is currently a Lecturer with Queen's University of Belfast, Belfast, U.K. She received her the B.E. degree in Computer Systems Engineering from the National University of Sciences and Technology (NUST), Pakistan, and the M.S. degree in Electrical Engineering from the Center for Advanced Studies in Engineering (CASE), University of Engineering and Technology, UET-Taxila. Her research interests include lattice-based cryptography, embedded systems security, side channel attacks, and cryptographic hardware. She was a recipient of the

Song Bian Song Bian received B.S. from University of Wisconsin-Madison in 2014. He received M.S. and Ph.D. from Kyoto University in 2017 and 2019, respectively. He is currently an associate professor at Beihang University. His main areas of interest include applied cryptography, secure multi-party computation and domain-specific hardware accelerators. He was a research fellow of the Japan Society for the Promotion of Science from 2017 to 2019, and an assistant professor at Kyoto University from 2019 to 2021. He served as technical committee

Chenghua Wang received the B.Sc. and M.Sc. degrees from Southeast University, Nanjing, China, in 1984 and 1987, respectively. In 1987, he joined the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics (NUAA), where he became a full Professor in 2001. He has published 6 books and over 100 technical papers in journals and conference proceedings. He is the recipient of more than ten teaching and research awards at the provincial and ministerial level. His current research interests include testing

of integrated circuits and systems for communications.

Máire O'Neill is currently a Regius Professor in Electronics and Computer Engineering, Acting Director of Institute of Electronics, Communications and Information Technology (ECIT) and Director of UK Research Institute in Secure Hardware and Embedded Systems (RISE). She obtained an M.Eng. with distinction and a Ph.D. in Electrical and Electronic Engineering from Queen's University Belfast (QUB) in 1999 and 2002 respectively. She has received numerous awards for her research to date which include 2014 UK Royal Academy of Engineering Silver Medal, Women's Engineering Society (WES) prize at 2006 IET Young Woman Engineer of Year awards and named as British Female Inventor of the Year in 2007. She has authored two research books and has over 190 international peer-reviewed conference and journal publications. She is Associate Editor for IEEE ToC and IEEE TETC and Guest Editor for several journals, including the IET Information Security (2005) launch issue and a special issue on 'Cryptography in the coming decade' in ACM Trans. on Embedded Computing (2015). She has been a technical program committee member for many international conferences, including DAC, CHES, DATE, SOCC, ISCAS, IET ISSC and RFIDSec. She is a Fellow of Royal Academy of Engineering, Fellow of the Irish Academy of Engineering, and Member of Royal Irish Academy.

engineering Silver Medal, Women's Engineering Society (WES) prize at 2006 IET Young Woman Engineer of Year awards and named as British Female Inventor of the Year in 2007. She has authored two research books and has over 190 international peer-reviewed conference and journal publications. She is Associate Editor for IEEE ToC and IEEE TETC and Guest Editor for several journals, including the IET Information Security (2005) launch issue and a special issue on 'Cryptography in the coming decade' in ACM Trans. on Embedded Computing (2015). She has been a technical program committee member for many international conferences, including DAC, CHES, DATE, SOCC, ISCAS, IET ISSC and RFIDSec. She is a Fellow of Royal Academy of Engineering, Fellow of the Irish Academy of Engineering, and Member of Royal Irish Academy.

Weiqiang Liu (M'12-SM'15) received the B.Sc. degree in Information Engineering from Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China and the Ph.D. degree in Electronic Engineering from the Queen's University Belfast (QUB), Belfast, UK, in 2006 and 2012, respectively. In Dec. 2013, he joined the College of Electronic and Information Engineering, NUAA, where he is currently a Professor and the Vice Dean of the college. He has published one research book by Artech House and over 100 leading journal and

conference papers. His paper was selected as the Highlight Paper of IEEE TCAS-I in the 2021 January Issue and the Feature Paper of IEEE TC in the 2017 December issue. He has been awarded the prestigious Excellent Young Scholar Award by National Natural Science Foundation of China in 2020. He serves as the Associate Editors for IEEE Transactions on Circuits and System I: Regular Papers (2020.1-2021.12), IEEE Transactions on Emerging Topics in Computing (2019.5-2021.4) and IEEE Transactions on Computers (2015.5-2019.4), an Steering Committee Member of IEEE Transactions on VLSI Systems (2021.1-2022.12). He is the program co-chair of IEEE ARITH 2020, and also technical program committee members for ARITH, DATE, ASAP, ISCAS, ASP-DAC, ISVLSI, GLSVLSI, SiPS, NANOARCH, AICAS and ICONIP. He is a member of CASCOS and VSA Technical Committee of IEEE Circuits and Systems Society. His research interests include approximate computing, hardware security and VLSI design for digital signal processing and cryptography.