Sapphire: A Configurable Crypto-Processor for Post-Quantum Lattice-based Protocols (Extended Version)

Utsav Banerjee, Tenzin S. Ukyab and Anantha P. Chandrakasan
Massachusetts Institute of Technology, Cambridge, MA, USA

Abstract. Public key cryptography protocols, such as RSA and elliptic curve cryptography, will be rendered insecure by Shor’s algorithm when large-scale quantum computers are built. Cryptographers are working on quantum-resistant algorithms, and lattice-based cryptography has emerged as a prime candidate. However, high computational complexity of these algorithms makes it challenging to implement lattice-based protocols on low-power embedded devices. To address this challenge, we present Sapphire – a lattice cryptography processor with configurable parameters. Efficient sampling, with a SHA-3-based PRNG, provides two orders of magnitude energy savings; a single-port RAM-based number theoretic transform memory architecture is proposed, which provides 124k-gate area savings; while a low-power modular arithmetic unit accelerates polynomial computations. Our test chip was fabricated in TSMC 40nm low-power CMOS process, with the Sapphire cryptographic core occupying 0.28 mm$^2$ area consisting of 106k logic gates and 40.25 KB SRAM. Sapphire can be programmed with custom instructions for polynomial arithmetic and sampling, and it is coupled with a low-power RISC-V micro-processor to demonstrate NIST Round 2 lattice-based CCA-secure key encapsulation and signature protocols Frodo, NewHope, qTESLA, CRYSTALS-Kyber and CRYSTALS-Dilithium, achieving up to an order of magnitude improvement in performance and energy-efficiency compared to state-of-the-art hardware implementations. All key building blocks of Sapphire are constant-time and secure against timing and simple power analysis side-channel attacks. We also discuss how masking-based DPA countermeasures can be implemented on the Sapphire core without any changes to the hardware.

Keywords: Lattice-based Cryptography · LWE · Ring-LWE · Module-LWE · post-quantum · NIST Round 2 · Number Theoretic Transform · Sampling · energy-efficient · low-power · constant-time · side-channel security · ASIC · hardware implementation

1 Introduction

Modern public key cryptography relies on hard mathematical problems such as integer factorization, discrete logarithms over finite fields and discrete logarithms over elliptic curve groups. However, these problems can be solved by a large-scale quantum computer in polynomial time using Shor’s algorithm [1], thus making today’s public key protocols like RSA and ECC vulnerable to quantum attacks. Given the rapid advancement in quantum computing technology over the past few years, cryptographers are developing quantum-secure public key algorithms to protect today’s data from tomorrow’s threats. Lattice-based cryptography is considered one of the most promising candidates for post-quantum cryptographic protocols because of its extensive security analysis as well as small public key and signature sizes.

The National Institute of Standards and Technology (NIST) formally initiated the process of standardizing post-quantum cryptography in 2016 [2]. The first round of candidates were announced in late 2017, with lattice-based cryptography accounting for 48% of the public-key encryption and key encapsulation (PKE/KEM) schemes and 25% of the signature schemes. In early 2019, the candidates moving on to the second round were announced [3], and lattice-based cryptography accounts for 53% (9 out of 17) and 33% (3 out of 9) of the candidates for PKE/KEM and signature schemes respectively. The theoretical foundation of several of these lattice-based protocols lies in the learning with errors (LWE) problem [4] and its variants such as Ring-LWE [5] and Module-LWE [6], and the hardness of LWE has been well-studied in the presence of both classical and quantum adversaries [7, 8]. This has been accompanied...
by several software and hardware implementations [9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20] of LWE and Ring-LWE-based public key encryption and key encapsulation protocols, each supporting specific lattice parameters chosen for increased performance and efficiency. Existing lattice-based cryptography implementations, both in software and hardware, have been thoroughly surveyed in [21]. Most of the hardware implementations focus on FPGA demonstration in order to support reconfigurability of lattice parameters, which is especially important for a fast evolving field like lattice-based cryptography, while existing ASIC implementations either lack configurability or have power and area overheads. Some of the key challenges of implementing lattice-based cryptography in ASICs have been discussed in [22], and this work presents a solution using a combination of architectural and algorithmic techniques.

**Our contributions:** In this work, we present Sapphire – a configurable lattice cryptography processor – which combines low-power modular arithmetic, area-efficient memory architecture and fast sampling techniques to achieve high energy-efficiency and low cycle count, ideal for securing low-power embedded systems. The key technical aspects of our work are as follows:

1. A low-power modular arithmetic core, with configurable prime modulus, is used to accelerate polynomial arithmetic operations; a pseudo-configurable modular multiplier is also implemented, which provides up to 3× improvement in energy-efficiency.
2. A single-port SRAM-based number theoretic transform (NTT) memory architecture provides 124k-gate area savings without any loss in performance or energy-efficiency.
3. An efficient Keccak core is combined with fast sampling techniques to speed up polynomial sampling, while supporting a wide variety of discrete distribution parameters.
4. These efficient hardware building blocks are integrated together with an instruction memory and decoder to build our crypto-processor, which can be programmed with custom instructions for polynomial sampling and arithmetic.
5. The Sapphire crypto-processor is coupled with an efficient RISC-V micro-processor to demonstrate several NIST Round 2 lattice-based key encapsulation and signature protocols such as Frodo [23], NewHope [24], qTESLA [25], CRYSTALS-Kyber [26] and CRYSTALS-Dilithium [27], achieving more than an order of magnitude improvement in performance and energy-efficiency compared to state-of-the-art assembly-optimized software and hardware implementations.
6. All the key building blocks, such as NTT, polynomial arithmetic and binomial sampling, are constant-time and secure against timing and simple power analysis attacks. While our baseline protocol implementations are not secure against differential power analysis attacks, we discuss how our crypto-processor can be programmed to implement masking-based countermeasures.
7. Our ASIC implementation was fabricated in the TSMC 40nm low-power CMOS process, and all protocol-level demonstrations and side-channel measurements were conducted on our test chip.

The rest of the paper is organized as follows: Section 2 provides a brief mathematical background on LWE and associated computations; in Section 3, we present our implementation of energy-efficient modular arithmetic along with an area-efficient NTT memory architecture; in Section 4, we describe our discrete distribution sampler accelerated by a low-power SHA-3 core; Section 5 describes the overall chip architecture; Section 6 presents detailed measurement results obtained from evaluating lattice-based protocols on our test chip, comparison with state-of-the-art software and hardware implementations as well as side-channel analysis; a summary of our key conclusions along with future research directions are discussed in Section 7.

This is an extended version of our CHES 2019 paper [28] with additional design information, implementation of Frodo-1344 and preliminary side-channel leakage analysis. Also, several appendices have been added at the end of the paper to provide supplementary data.

The specifications of CRYSTALS-Kyber were modified in NIST Round 2 after our CHES paper was originally submitted. So, the rest of this paper (excluding Appendix K) describes our implementation of Kyber-v1 based on the initial specification with \( q = 7681 \). In Appendix K, we have now added our implementation results of Kyber-v2 based on the updated specification with \( q = 3329 \).
2 Background

In this section, we provide a brief introduction to LWE, Ring-LWE and Module-LWE along with the associated computations. We use bold lower-case symbols to denote vectors and bold upper-case symbols to denote matrices. The symbol $\lg$ is used to denote all logarithms with base 2. The set of all integers is denoted as $\mathbb{Z}$ and the quotient ring of integers modulo $q$ is denoted as $\mathbb{Z}_q$. For two $n$-dimensional vectors $a$ and $b$, their inner product is written as $\langle a, b \rangle = \sum_{i=0}^{n-1} a_i \cdot b_i$. The concatenation of two vectors $a$ and $b$ is written as $a \| b$.

2.1 LWE and Related Lattice Problems

The Learning with Errors (LWE) problem [4] acts as the foundation for several modern lattice-based cryptography schemes. The LWE problem states that given a polynomial number of samples of the form $(a, \langle a, s \rangle + e)$, it is difficult to determine secret vector $s \in \mathbb{Z}_q^n$, where vector $a \in \mathbb{Z}_q^n$ is sampled uniformly at random and error $e$ is sampled from the appropriate error distribution $\chi$. Examples of secure LWE parameters are $(n, q) = (640, 2^{15})$, $(n, q) = (976, 2^{16})$ and $(n, q) = (1344, 2^{16})$ for Frodo [23].

LWE-based cryptosystems involve large matrix operations which are computationally expensive and also result in large key sizes. To solve this problem, the Ring-LWE problem [5] was proposed, which uses ideal lattices. Let $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$ be the ring of polynomials where $n$ is power of 2. The Ring-LWE problem states that given samples of the form $(a, a \cdot s + e)$, it is difficult to determine the secret polynomial $s \in \mathbb{R}_q$, where the polynomial $a \in \mathcal{R}_q$ is sampled uniformly at random and the coefficients of the error polynomial $e$ are small samples from the error distribution $\chi$. Examples of secure Ring-LWE parameters are $(n, q) = (512, 12289)$ and $(n, q) = (1024, 12289)$ for NewHope [24].

Module-LWE [6] provides a middle ground between LWE and Ring-LWE. By using module lattices, it reduces the algebraic structure present in Ring-LWE and increases security while not compromising too much on the computational efficiency. The Module-LWE problem states that given samples of the form $(a, a^2 s + e)$, it is difficult to determine the secret vector $s \in \mathbb{R}_q^n$, where the vector $a \in \mathcal{R}_q^k$ is sampled uniformly at random and the coefficients of the error polynomial $e$ are small samples from the error distribution $\chi$. Examples of secure Module-LWE parameters are $(n, k, q) = (256, 2, 7681)$, $(n, k, q) = (256, 3, 7681)$ and $(n, k, q) = (256, 4, 7681)$ for CRYSTALS-Kyber-v1 [26].

2.2 Number Theoretic Transform

While the protocols based on standard lattices (LWE) involve matrix-vector operations modulo $q$, all the arithmetic is performed in the ring of polynomials $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$ when working with ideal and module lattices. There are several efficient algorithms for polynomial multiplication [29], and the Number Theoretic Transform (NTT) is one such technique widely used in lattice-based cryptography.

The NTT is a generalization of the well-known Fast Fourier Transform (FFT) where all the arithmetic is performed in a finite field instead of complex numbers. Instead of working with powers of the $n$-th complex root of unity $\exp(-2\pi j/n)$, NTT uses the $n$-th primitive root of unity $\omega_n$ in the ring $\mathbb{Z}_q$, that is, $\omega_n$ is an element in $\mathbb{Z}_q$ such that $\omega_n^n = 1 \mod q$ and $\omega_n^i \not= 1 \mod q$ for $i \not= n$. In order to have elements of order $n$, the modulus $q$ is chosen to be a prime such that $q \equiv 1 \mod n$. A polynomial $a(x) \in \mathcal{R}_q$ with coefficients $a(x) = (a_0, a_1, \cdots, a_{n-1})$ has the NTT representation $\hat{a}(x) = (\hat{a}_0, \hat{a}_1, \cdots, \hat{a}_{n-1})$, where

$$\hat{a}_i = \sum_{j=0}^{n-1} a_j \omega_n^{ij} \mod q \forall i \in [0, n-1].$$

The inverse NTT (INTT) operation converts $\hat{a}(x) = (\hat{a}_0, \hat{a}_1, \cdots, \hat{a}_{n-1})$ back to $a(x)$ as

$$a_i = \frac{1}{n} \sum_{j=0}^{n-1} \hat{a}_j \omega_n^{-ij} \mod q \forall i \in [0, n-1].$$

Note that the INTT operation is similar to NTT, except that $\omega_n$ is replaced by $\omega_n^{-1} \mod q$ and the final results is divided by $n$. An iterative in-place version of the NTT algorithm is provided in Algorithm 1 [30, 31]. The PolyBitRev function performs a permutation on the input polynomial $a$ such that $\hat{a}[i] = \text{PolyBitRev}(a)[i] = a[\text{BitRev}(i)]$, where BitRev is formally defined as $\text{BitRev}(i) = \sum_{j=0}^{\lg n-1} ((i \gg$
### Algorithm 1 Iterative In-Place NTT [30]

**Require:** Polynomial $a(x) \in \mathcal{R}_q$ and $n$-th primitive root of unity $\omega_n \in \mathbb{Z}_q$

**Ensure:** Polynomial $\hat{a}(x) \in \mathcal{R}_q$ such that $\hat{a}(x) = \text{NTT}(a(x))$

```plaintext
1: $\hat{a} \leftarrow \text{PolyBitRev}(a)$
2: for ($s = 1; s \leq \log n; s = s + 1$) do
3:   $m \leftarrow 2^s$
4:   $\omega_m \leftarrow \omega_n^m$
5:   for ($k = 0; k < n; k = k + m$) do
6:     $\omega \leftarrow 1$
7:     for ($j = 0; j < m/2; j = j + 1$) do
8:       $t \leftarrow \omega \cdot \hat{a}[k + j + m/2] \mod q$
9:       $u \leftarrow \hat{a}[k + j]$
10:      $\hat{a}[k + j] \leftarrow u + t \mod q$
11:     $\hat{a}[k + j + m/2] \leftarrow u - t \mod q$
12:   end for
13: end for
14: end for
15: return $\hat{a}$
```

(j & 1) \(\ll\) (\log n - 1 - i) (for positive integer $i$ and power-of-two $n$), that is, bit-wise reversal of the binary representation of the index $i$. Since there are $\log n$ stages in the NTT outer loop, with $O(n)$ operations in each stage, its time complexity is $O(n \log n)$. The factors $\omega$ are called the twiddle factors, similar to FFT.

The NTT provides a fast multiplication algorithm in $\mathcal{R}_q$ with time complexity $O(n \log n)$ instead of $O(n^2)$ for schoolbook multiplication. Given two polynomials $a, b \in \mathcal{R}_q$, their product $c = a \cdot b \in \mathcal{R}_q$ can be computed as

$$c = \text{NTT} \left( \text{NTT}(a) \odot \text{NTT}(b) \right)$$

where $\odot$ denotes coefficient-wise multiplication of the polynomials. Since the product of $a$ and $b$, before reduction modulo $f(x) = x^n + 1$, has $2n$ coefficients, using the above equation directly to compute $a \cdot b$ will require padding both $a$ and $b$ with $n$ zeros. To eliminate this overhead, the negative-wrapped convolution [32] is used, with the additional requirement $q \equiv 1 \mod 2n$ so that both the $n$-th and $2n$-th primitive roots of unity modulo $q$ exist, respectively denoted as $\omega_n$ and $\psi = \sqrt[n]{\omega_n} \mod q$. By multiplying $a$ and $b$ coefficient-wise by powers of $\psi$ before the NTT computation, and by multiplying $\text{INTT}(\text{NTT}(a) \odot \text{NTT}(b))$ coefficient-wise by powers of $\psi^{-1} \mod q$, no zero padding is required and the $n$-point NTT can be used directly.

Similar to FFT, the NTT inner loop involves butterfly computations. There are two types of butterfly operations – Cooley-Tukey (CT) and Gentleman-Sande (GS) [33]. The CT butterfly-based NTT requires inputs in normal order and generates outputs in bit-reversed order, similar to the decimation-in-time FFT. The GS butterfly-based NTT requires inputs to be in bit-reversed order while the outputs are generated in normal order, similar to the decimation-in-frequency FFT. Using the same butterfly for both NTT and INTT requires a bit-reversal permutation. However, the bit-reversal can be avoided by using CT for NTT and GS for INTT [33].

### 2.3 Sampling

In lattice-based protocols, the public vectors $a$ are generated from the uniform distribution over $\mathbb{Z}_q$ through rejection sampling. The secret vectors $s$ and error terms $e$ are sampled from the distribution $\chi$ typically with zero mean and appropriate standard deviation $\sigma$. Accurate sampling of $s$ and $e$ is critical to the security of these protocols, and the sampling must be constant-time to prevent side-channel leakage of the secret information. Although the original LWE proof used discrete Gaussian distributions for sampling the error terms, several lattice-based schemes use binomial, uniform and ternary distributions for efficiency. A detailed survey of different sampling techniques is available in [21].
3 Modular Arithmetic and NTT

The core arithmetic and logic unit (ALU) of Sapphire consists of a 24-bit data-path, with modular operations in \( \mathbb{F}_q \) for configurable \( q \). In this section, we describe the details of our energy-efficient modular arithmetic implementation, the ALU design and our area-efficient NTT memory architecture.

3.1 Modular Arithmetic Implementation

The modular arithmetic core consists of a 24-bit adder, a 24-bit subtractor and a 24-bit multiplier along with associated modular reduction logic. Our modular adder and subtractor designs are shown in Fig. 1, and the corresponding pseudo-codes are shown in Algorithms 2 and 3. Both designs use a pair of adder and subtractor, with the sum, carry bit, difference and borrow bit denoted as \( s, c, d \) and \( b \) respectively. Modular reduction is performed using conditional subtraction and addition, which are computed in the same cycle to avoid timing side-channels. The synthesized areas of the adder and the subtractor are around 550 GE (gate equivalent) each in area.

For modular multiplication, we use a 24-bit multiplier followed by Barrett reduction [34] modulo a prime \( q \) of size up to 24 bits. Barrett reduction does not exploit any special property of the modulus \( q \), thus making it ideal for supporting configurable moduli. Let \( z \) be the 48-bit product to be reduced to \( Z \mod q \), then Barrett reduction computes \( z \mod q \) by estimating the quotient \( \lfloor z/q \rfloor \) without performing any division, as shown in Algorithm 4. Barrett reduction involves two multiplications, one subtraction, one bit-shift and one conditional subtraction. The value of \( 1/q \) is approximated as \( m/2^k \), with the error of approximation being \( e = 1/q - m/2^k \), therefore the reduction is valid as long as \( ze < 1 \). Since \( z < q^2 \), \( k \) is set to be the smallest number such that \( e = 1/q - (\lfloor 2^k/q \rfloor / 2^k) < 1/q^2 \). Typically, \( k \) is very close to \( 2^{\lceil \lg q \rceil} \), that is, the bit-size of \( q^2 \).

In order to understand the trade-offs between flexibility and efficiency in modular multiplication, we have implemented two different architectures of Barrett reduction logic: (1) with fully configurable modulus (\( q \) can be an arbitrary prime) and (2) with pseudo-configurable modulus (\( q \) belongs to a specific set of primes), as shown in Fig. 2.

Apart from the prime \( q \) (which can be up to 24 bits), the fully configurable version requires two

Algorithm 2 Modular Addition

\begin{align*}
\text{Require:} & \quad x, y \in \mathbb{Z}_q \\
\text{Ensure:} & \quad z = x + y \mod q \\
1: & \quad (c, s) \leftarrow x + y \\
2: & \quad (b, d) \leftarrow s - q \\
3: & \quad \text{if } c = 1 \text{ or } b = 0 \text{ then} \\
4: & \quad z \leftarrow d \\
5: & \quad \text{else} \\
6: & \quad z \leftarrow s \\
7: & \quad \text{end if} \\
8: & \quad \text{return } z
\end{align*}

Algorithm 3 Modular Subtraction

\begin{align*}
\text{Require:} & \quad x, y \in \mathbb{Z}_q \\
\text{Ensure:} & \quad z = x - y \mod q \\
1: & \quad (b, d) \leftarrow x - y \\
2: & \quad (c, s) \leftarrow d + q \\
3: & \quad \text{if } b = 1 \text{ then} \\
4: & \quad z \leftarrow s \\
5: & \quad \text{else} \\
6: & \quad z \leftarrow d \\
7: & \quad \text{end if} \\
8: & \quad \text{return } z
\end{align*}
Algorithm 4 Modular Multiplication with Barrett Reduction [34]

Require: \( x, y \in \mathbb{Z}_q, m \) and \( k \) such that \( m = \lfloor 2^k / q \rfloor \)
Ensure: \( z = x \cdot y \mod q \)
1: \( z \leftarrow x \cdot y \)
2: \( t \leftarrow (z \cdot m) \gg k \)
3: \( z \leftarrow z - (t \cdot q) \)
4: if \( z \geq q \) then
5: \( z \leftarrow z - q \)
6: end if
7: return \( z \)

Algorithm 5 Reduction mod 7681

Require: \( q = 7681, x \in [0, q^2) \)
Ensure: \( z = x \mod q \)
1: \( t \leftarrow (x \ll 8) + (x \ll 4) + x \)
2: \( t \leftarrow t \gg 21 \)
3: \( t \leftarrow (t \ll 13) - (t < 9) + t \)
4: \( z \leftarrow x - t \)
5: if \( z \geq q \) then
6: \( z \leftarrow z - q \)
7: end if
8: return \( z \)

Algorithm 6 Reduction mod 8380417

Require: \( q = 8380417, x \in [0, q^2) \)
Ensure: \( z = x \mod q \)
1: \( t \leftarrow (x \ll 23) + (x \ll 13) + (x \ll 3) - x \)
2: \( t \leftarrow t \gg 46 \)
3: \( t \leftarrow (t \ll 23) - (t \ll 13) + t \)
4: \( z \leftarrow x - t \)
5: if \( z \geq q \) then
6: \( z \leftarrow z - q \)
7: end if
8: return \( z \)
block while the inputs to the other blocks are data-gated to save power. Since the reduction blocks have the parameters $m$, $k$ and $q$ coded in digital logic and do not require explicit multipliers, they involve lesser computation than the fully configurable reduction circuit from Fig. 2a, albeit at the cost of some additional area and decrease in flexibility. The reduction becomes particularly efficient when at least one of $m$ and $q$ or both can be written in the form $2^{l_1} \pm 2^{l_2} \pm \cdots \pm 1$, where $l_1, l_2, \ldots$ are not more than four positive integers. For example, we consider the CRYSTALS primes: for $q = 7681 = 2^{13} - 2^9 + 1$ we have $k = 21$ and $m = 273 = 2^8 + 2^3 + 1$, and for $q = 8380417 = 2^{23} - 2^{13} + 1$ we have $k = 46$ and $m = 8396807 = 2^{23} + 2^{13} + 2^3 - 1$. Therefore, the multiplications by $q$ and $m$ can be converted to significantly cheaper bit-shifts and additions / subtractions, as shown in Algorithms 5 and 6. Implementation details and reduction parameters for each customized modular reduction block are provided in Appendix A. This design also performs modular multiplication in a single cycle. It was synthesized at 100 MHz (with near-zero slack) and occupies around 19k GE area, including the area of the 24-bit multiplier.

In Fig. 3, we compare the simulated energy consumption of the fully configurable and pseudo-configurable modular multiplier architectures for all the primes mentioned earlier. As expected, the multiplication itself consumes the same energy in both cases, but the modular reduction energy is up to $6 \times$ lower for the pseudo-configurable design. The overall decrease in modular multiplication energy, considering both multiplication and reduction together, is up to $3 \times$, clearly highlighting the benefit of the dedicated modular reduction data-paths when working with prime moduli. For reduction modulo $2^m$ ($m < 24$), e.g., in the case of Frodo, the output of the 24-bit multiplier is simply bit-wise AND-ed with $2^m - 1$ implying that the modular reduction energy is negligible.

### 3.2 Butterfly Unit and ALU

Next, we elaborate how the modular arithmetic units described earlier are integrated together to build the butterfly module. As discussed in Section 2, NTT computations involve butterfly operations similar to the Fast Fourier Transform, with the only difference being that all arithmetic is performed modulo $q$ instead of complex numbers. There are two butterfly configurations – Cooley-Tukey (or DIT) and Gentleman-Sande (or DIF). In terms of arithmetic, the DIT butterfly computes $(a + \omega b \text{ mod } q, a - \omega b \text{ mod } q)$ and the DIF butterfly computes $(a + b \text{ mod } q, (a - b)\omega \text{ mod } q)$, where $a$ and $b$ are the inputs to the butterfly and $\omega$ is the twiddle factor. The DIT butterfly requires inputs to be in bit-reversed order and the DIF butterfly generates outputs in bit-reversed order, thus making DIF and DIT suitable for NTT and INTT respectively. While software implementations have the flexibility to program both configurations, hardware designs typically implement either DIT or DIF, thus requiring bit-reversals. To solve this problem, we have implemented a unified butterfly architecture [39] which can be configured as both DIT and DIF, as shown in Fig. 4. It consists of two sets of modular adders and subtractors along with some multiplexing circuitry to select whether the multiplication with $\omega$ is performed before or after the addition and subtraction. Since the critical path of the design is inside the modular multiplier, there is no impact on system performance. The associated area overhead is also negligible.

The modular arithmetic blocks inside the butterfly are re-used for coefficient-wise polynomial arithmetic operations as well as for multiplying polynomials with the appropriate powers of $\psi$ and $\psi^{-1}$.
Figure 4: Unified butterfly in Cooley-Tukey and Gentleman-Sande configurations.

during negative-wrapped convolution. Apart from butterfly and arithmetic modulo $q$, the Sapphire ALU also supports the following bit-wise operations – AND, OR, XOR, left shift and right shift.

3.3 NTT Memory Architecture

Hardware architectures for polynomial multiplication using NTT consist of memory banks for storing the polynomials along with the ALU which performs butterfly computations. Since each butterfly needs to read two inputs and write two outputs all in the same cycle, these memory banks are typically implemented using dual-port RAMs [9, 41, 31, 19] or four-port RAMs [17]. Although true dual-port memory is easily available in state-of-the-art commercial FPGAs in the form of block RAMs (BRAMs), use of dual-port SRAMs in ASIC can pose large area overheads in resource-constrained devices. Compared to a simple single-port SRAM, a dual-port SRAM has double the number of row and column decoders, write drivers and read sense amplifiers. Also, the bit-cells in a low-power dual-port SRAM consist of ten transistors (10T) compared to the usual six transistor (6T) bit-cells in a single-port SRAM [42]. Therefore, the area of a dual-port SRAM can be as much as double the area of a single-port SRAM with the same number of bits and column muxing. To reduce this area overhead, we implement an area-efficient NTT memory architecture [39] which uses the constant-geometry FFT data-flow [43] and consists of single-port SRAMs only.

**Algorithm 7 Constant Geometry Out-of-Place NTT [40]**

**Require:** Polynomial $a(x) \in \mathbb{R}_q$ and $n$-th primitive root of unity $\omega_n \in \mathbb{Z}_q$

**Ensure:** Polynomial $\hat{a}(x) \in \mathbb{R}_q$ such that $\hat{a}(x) = \text{NTT}(a(x))$

1: $a \leftarrow \text{PolyBitRev}(a)$
2: for ($s = 1; s \leq \lg n; s = s + 1$) do
3: for ($j = 0; j < n/2; j = j + 1$) do
4: $k \leftarrow \lfloor j/2^{s} \rfloor \cdot 2^{\lg(n-s)}$
5: $\hat{a}[j] \leftarrow a[2j] + a[2j+1] \cdot \omega_n^k \mod q$
6: $\hat{a}[j + n/2] \leftarrow a[2j] - a[2j + 1] \cdot \omega_n^k \mod q$
7: end for
8: if $s = \lg n$ then
9: $a \leftarrow \hat{a}$
10: end if
11: end for
12: return $\hat{a}$
The constant geometry NTT is described in Algorithm 7 \cite{40, 41}. Clearly, the coefficients of the polynomial are accessed in the same order for each stage, thus simplifying the read/write control circuitry. For constant geometry DIT NTT, the butterfly inputs are \( a[2j] \) and \( a[2j+1] \) and the outputs are \( \hat{a}[j] \) and \( \hat{a}[j+n/2] \), while the inputs are \( a[j] \) and \( a[j+n/2] \) and the outputs are \( \hat{a}[2j] \) and \( \hat{a}[2j+1] \) for DIF NTT. However, the constant geometry NTT is inherently out-of-place, therefore requiring storage for both polynomials \( a \) and \( \hat{a} \). For our hardware implementation, we create two memory banks – left and right – to store these two polynomials while allowing the butterfly inputs and outputs to ping-pong between them during each stage of the transform. Although out-of-place NTT requires storage for both the input and output polynomials, this does not affect the total memory requirements of the crypto-processor because the total number of polynomials required to be stored during the protocol execution is greater than two, e.g., four polynomials are involved in any computation of the form \( b = a \cdot s + e \).

Next, we describe how these memory banks are constructed using single-port SRAMs so that each butterfly can be computed in a single cycle without causing read/write hazards. As shown in Fig. 5a, each polynomial is split among four single port SRAMs Mem 0-3 on the basis of the least and most significant bits (LSB and MSB) of the coefficient index (or address \( addr \)). This allows simultaneously accessing coefficient index pairs of the form \( (2j, 2j+1) \) and \( (j, j+n/2) \). Our NTT memory architecture
Figure 7: Memory access patterns for 8-point DIT and DIF NTT using our single-port SRAM-based memory architecture (R and W denote read and write respectively).

is shown in Fig. 5b, which consists of two such memory banks labelled as LWE Poly Cache. In every cycle, the butterfly inputs are read from two different single-port SRAMs (out of four SRAMs in the input memory bank) and the outputs are also written to two different single-port SRAMs (out of four SRAMs in the output memory bank), thus avoiding hazards. The data flow in the first two cycles of NTT is shown in Fig. 6, where the input polynomial \( a \) is stored in the left bank and the output polynomial \( \hat{a} \) is stored in the right bank. As the input and output polynomials exchange their memory banks from one stage to the next, our NTT control circuitry ensures that the same data-flow is maintained. To illustrate this, the memory access patterns for all three stages of an 8-point NTT are shown in Fig. 7 for both decimation-in-time and decimation-in-frequency.

The two memory banks consist of four \( 1024 \times 24 \)-bit single-port SRAMs each (24 KB total). Together they store 8192 entries, which can be split into four 2048-dimension polynomials or eight 1024-dimension polynomials or sixteen 512-dimension polynomials or thirty-two 256-dimension polynomials or sixty-four 128-dimension polynomials or one-hundred-twenty-eight 64-dimension polynomials. By constructing this memory using single-port SRAMs (and some additional read-data multiplexing circuitry), we have achieved area savings equivalent to 124k GE compared to a dual-port SRAM-based implementation. This is particularly important since SRAMs account for a large portion of the total hardware area in ASIC implementations of lattice-based cryptography [17, 44].

In order to allow configurable parameters, our NTT hardware also requires additional storage (labelled as NTT Constants RAM in Fig. 5) for the pre-computed twiddle factors: \( \omega_j^{2i} \mod q \) for \( i \in [1, \lg n] \) and \( j \in [0, 2^{-1}) \) and \( \psi^i, n^{-1}\psi^{-1} \mod q \) for \( i \in [0, n) \). Since \( n \leq 2048 \) and \( q < 2^{24} \), this would require another 24 KB of memory. To reduce this overhead, we exploit the following properties of \( \omega \) and \( \psi \): \( \omega_{n/2} = \omega_n^2 \), \( \omega_{n/2}^{-1} = \omega_n^{-n} \) and \( \omega = \psi^2 \) [31]. Then, it’s sufficient to store only \( \omega_j^i \) for \( j \in [0, n/2) \) and \( \psi^i \),
Table 1: Comparison of our NTT performance with state-of-the-art

<table>
<thead>
<tr>
<th>Design</th>
<th>Platform</th>
<th>Tech (nm)</th>
<th>VDD (V)</th>
<th>Freq (MHz)</th>
<th>Parameters</th>
<th>NTT Cycles</th>
<th>NTT Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>This work</td>
<td>ASIC</td>
<td>40</td>
<td>1.1</td>
<td>72</td>
<td>$(n = 256, q = 7681)$</td>
<td>1,289</td>
<td>165.98 nJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 512, q = 12289)$</td>
<td>2,826</td>
<td>410.52 nJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 1024, q = 12289)$</td>
<td>6,155</td>
<td>894.28 nJ</td>
</tr>
<tr>
<td>Software [45]</td>
<td>ARM Cortex-M4</td>
<td>-</td>
<td>3.0</td>
<td>100</td>
<td>$(n = 256, q = 7681)$</td>
<td>22,031</td>
<td>13.55 µJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 512, q = 12289)$</td>
<td>34,262</td>
<td>21.07 µJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 1024, q = 12289)$</td>
<td>75,006</td>
<td>46.13 µJ</td>
</tr>
<tr>
<td>Song et al. [17]</td>
<td>ASIC</td>
<td>40</td>
<td>0.9</td>
<td>300</td>
<td>$(n = 256, q = 7681)$</td>
<td>160</td>
<td>31 nJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 512, q = 12289)$</td>
<td>492</td>
<td>96 nJ</td>
</tr>
<tr>
<td>Nejatollahi et al. [14]</td>
<td>ASIC</td>
<td>45</td>
<td>1.0</td>
<td>100</td>
<td>$(n = 512, q = 12289)$</td>
<td>2,854</td>
<td>1016.02 nJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>11,053</td>
<td>596.86 nJ</td>
</tr>
<tr>
<td>Fritzmann et al. [44]</td>
<td>ASIC</td>
<td>65</td>
<td>1.2</td>
<td>25</td>
<td>$(n = 256, q = 7681)$</td>
<td>2,056</td>
<td>254.52 nJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 512, q = 12289)$</td>
<td>4,616</td>
<td>549.98 nJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 1024, q = 12289)$</td>
<td>10,248</td>
<td>1205.03 nJ</td>
</tr>
<tr>
<td>Roy et al. [9]</td>
<td>FPGA</td>
<td>-</td>
<td>-</td>
<td>313</td>
<td>$(n = 256, q = 7681)$</td>
<td>1,691</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 512, q = 12289)$</td>
<td>3,443</td>
<td>-</td>
</tr>
<tr>
<td>Du et al. [31]</td>
<td>FPGA</td>
<td>-</td>
<td>-</td>
<td>233</td>
<td>$(n = 256, q = 7681)$</td>
<td>4,066</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 512, q = 12289)$</td>
<td>8,806</td>
<td>-</td>
</tr>
</tbody>
</table>

\[ n^{-1} \psi^{-i} \mod q \text{ for } i \in [0, n), \text{ thus reducing the twiddle factor memory size by 37.5% down to 15 KB.} \]

Finally, we compare the energy-efficiency and performance of our NTT with state-of-the-art software and ASIC hardware implementations in Table 1. For the software implementation, we have used assembly-optimized code for ARM Cortex-M4 from the PQM4 crypto library [45], and measurements were performed using the NUCLEO-F411RE development board [46]. Total cycle count of our NTT is \((\frac{n}{2} + 1)\log n + (n + 1)\), including the multiplication of polynomial coefficients with powers of \(\psi\). All measurements for our NTT implementation were performed on our test chip operating at clock frequency 72 MHz and nominal supply voltage 1.1 V. Our hardware-accelerated NTT is up to 11× more energy-efficient than the software implementation, after accounting for voltage scaling. It is 2.5× more energy-efficient compared to the fast NTT design from [14] with similar cycle count, and 1.5× more energy-efficient compared to the slow NTT design from [14] with 4× cycle count. Our NTT is almost twice as fast as [44], since our memory architecture allows computing one butterfly per cycle even with single-port SRAMs, while having similar energy consumption. The energy-efficiency of our NTT implementation is largely due to the careful design of low-power modular arithmetic, as discussed earlier, which decreases overall modular reduction complexity and simplifies the logic circuitry. However, our NTT is still about 4× less energy-efficient compared to [17], primarily due to the fact that [17] uses 16 parallel butterfly units along with dedicated four-port scratch-pad buffers to achieve higher parallelism and lower energy consumption at the cost of significantly larger chip area (2.05 mm²) compared to our design (0.28 mm²). As will be discussed in Section 6, sampling accounts for majority of the computational cost in Ring-LWE and Module-LWE schemes, therefore justifying our choice of area-efficient NTT architecture at the cost of some energy overhead.
4 Discrete Distribution Sampler

Hardness of the LWE problem is directly related to statistical properties of the error samples. Therefore, an accurate and efficient sampler is a critical component of any lattice cryptography implementation. Sampling accounts for a major portion of the computational overhead in software implementations of ideal and module lattice-based protocols [47]. A cryptographically secure pseudo-random number generator (CS-PRNG) is used to generate uniformly random numbers, which are then post-processed to convert them into samples from different discrete probability distributions. In this section, we describe our design of energy-efficient CS-PRNG along with fast sampling techniques for configurable distribution parameters.

4.1 Energy-Efficient CS-PRNG

Some of the standard choices for CS-PRNG are SHA-3 in the SHAKE mode [48], AES in counter mode [49] and ChaCha20 [50]. In order to identify the most efficient among these, we have compared them in terms of area, pseudo-random bit generation performance and energy consumption, as shown in Table 2. Only place-and-route area and measured energy are considered for all analysis, and synthesis area is reported for reference. For fair comparison, all the three primitives – SHA-3, AES and ChaCha20 – were implemented as full data path architectures. From Fig. 8, we observe that although all three primitives have comparable area-energy product, SHA-3 is $2 \times$ more energy-efficient than ChaCha20 and $3 \times$ more energy-efficient than AES; and this is largely due to the fact that SHA-3 generates the highest number of pseudo-random bits per round.

The basic building block of SHA-3 is the Keccak permutation function [51]. Therefore, our PRNG consists of a 24-cycle Keccak-f[1600] core [39] which can be configured in different SHA-3 modes and consumes 2.33 nJ per round at nominal voltage of 1.1 V (and 0.89 nJ per round at 0.68 V). Its 1600-bit state is processed in parallel, thus avoiding expensive register shifts and multiplexing required in serial architectures. Fig. 9 shows the overall architecture our discrete distribution sampler with the energy-

<table>
<thead>
<tr>
<th>PRNG</th>
<th>Area (kGE) a</th>
<th>Cycles/Round</th>
<th>No. of PRNG Bits</th>
<th>Energy (pJ/bit) b</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHAKE-128</td>
<td>34.5 (23.5)</td>
<td>24</td>
<td>1344</td>
<td>1.67</td>
</tr>
<tr>
<td>SHAKE-256</td>
<td>1088</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ChaCha20</td>
<td>21.1 (17.5)</td>
<td>20</td>
<td>512</td>
<td>2.07</td>
</tr>
<tr>
<td>AES-128-CTR</td>
<td>15.0 (11.1)</td>
<td>11</td>
<td>128</td>
<td>5.10</td>
</tr>
<tr>
<td>AES-256-CTR</td>
<td>15.0 (11.1)</td>
<td>15</td>
<td>128</td>
<td>7.56</td>
</tr>
</tbody>
</table>

Table 2: Comparison of CS-PRNG designs

- Area of placed-and-routed design (post-synthesis area in brackets)
- Energy measured from test chip operating at 1.1 V

Figure 8: Analysis of SHAKE-128, SHAKE-256, AES-128-CTR, AES-256-CTR and ChaCha20 in terms of energy per bit, bits per cycle and area-energy product.
efficient SHA-3 core. Pseudo-random bits generated by SHAKE-128 or SHAKE-256 are stored in the 1600-bit Keccak state register, and shifted out 32 bits at a time as required by the sampler. The sampler then feeds these bits, AND-ed with the appropriate bit mask to truncate them to desired size, to the post-processing logic to perform one of the following five types of operations – rejection sampling in $[0, q)$, binomial sampling with standard deviation $\sigma$, discrete Gaussian sampling with standard deviation $\sigma$ and desired precision up to 32 bits, uniform sampling in $[-\eta, \eta]$ for $\eta < q$ and trinary sampling in $\{-1, 0, +1\}$ with specified weights for the $+1$ and $-1$ samples.

4.2 Rejection Sampling

The public polynomial $a$ in Ring-LWE and the public vector $a$ in Module-LWE have their coefficients uniformly drawn from $\mathbb{Z}_q$ through rejection sampling, where uniformly random numbers of desired bit size are obtained from the PRNG as candidate samples and only numbers smaller than $q$ are accepted. The probability that a random number is not accepted is known as the rejection probability.

Table 3: Rejection probabilities for different primes with and without fast sampling

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7681</td>
<td>13</td>
<td>0.06</td>
<td>1</td>
<td>0.06</td>
<td>-</td>
</tr>
<tr>
<td>12289</td>
<td>14</td>
<td>0.25</td>
<td>5</td>
<td>0.06</td>
<td>0.19</td>
</tr>
<tr>
<td>40961</td>
<td>16</td>
<td>0.37</td>
<td>3</td>
<td>0.06</td>
<td>0.31</td>
</tr>
<tr>
<td>65537</td>
<td>17</td>
<td>0.50</td>
<td>7</td>
<td>0.12</td>
<td>0.38</td>
</tr>
<tr>
<td>120833</td>
<td>17</td>
<td>0.08</td>
<td>1</td>
<td>0.08</td>
<td>-</td>
</tr>
<tr>
<td>133121</td>
<td>18</td>
<td>0.49</td>
<td>7</td>
<td>0.11</td>
<td>0.38</td>
</tr>
<tr>
<td>184321</td>
<td>18</td>
<td>0.30</td>
<td>11</td>
<td>0.03</td>
<td>0.27</td>
</tr>
<tr>
<td>8380417</td>
<td>23</td>
<td>$\approx 0$</td>
<td>1</td>
<td>$\approx 0$</td>
<td>-</td>
</tr>
<tr>
<td>8058881</td>
<td>23</td>
<td>0.04</td>
<td>1</td>
<td>0.04</td>
<td>-</td>
</tr>
<tr>
<td>4205569</td>
<td>23</td>
<td>0.50</td>
<td>7</td>
<td>0.12</td>
<td>0.38</td>
</tr>
<tr>
<td>4206593</td>
<td>23</td>
<td>0.50</td>
<td>7</td>
<td>0.12</td>
<td>0.38</td>
</tr>
<tr>
<td>8404993</td>
<td>24</td>
<td>0.50</td>
<td>7</td>
<td>0.12</td>
<td>0.38</td>
</tr>
</tbody>
</table>

For prime $q$, the rejection probability is calculated as $\left(1 - \frac{q}{2^\lceil \lg q \rceil}\right)$. In Table 3, we list the rejection probabilities for primes mentioned earlier in Section 3. Clearly, different primes have very different rejection probabilities, often as high as 50%, which can be a bottleneck in lattice-based protocols. To solve this problem, we refer to [52] where pseudo-random numbers smaller than $5q$ are accepted for $q = 12289$, thus reducing the rejection probability from 25% to 6%. We extend this technique for any prime $q$ by scaling the rejection bound from $q$ to $kq$, for appropriate small integer $k$, so that the rejection probability is now $\left(1 - \frac{kq}{2^\lceil \lg (kq) \rceil}\right)$. We list these scaling factors for the primes in Table 3 along with the corresponding decrease in rejection probability.

Although this method reduces rejection rates, the output samples now lie in $[0, kq)$ instead of $[0, q)$.
In [52], for $q = 12289$ and $k = 5$, the accepted samples are reduced to $\mathbb{Z}_q$ by subtracting $q$ from them up to four times. Since $k$ is not fixed for our rejection sampler, we employ Barrett reduction [34] for this purpose. Unlike modular multiplication, where the inputs lie in $[0, q^2)$, the inputs here are much smaller; so the Barrett reduction parameters are also quite small, therefore requiring little additional logic. In Table 4, we compare our rejection sampler performance (SHAKE-128 used as PRNG) with software implementation on ARM Cortex-M4 using assembly-optimized Keccak [45].

### 4.3 Binomial Sampling

For binomial sampling, we take two $k$-bit chunks from the PRNG and computes the difference of their Hamming weights, as proposed in [24]. The resulting samples follow a binomial distribution with standard deviation $\sigma = \sqrt{k/2}$. We allow configuring $k$ to any value up to 32, thus providing the flexibility to support different standard deviations. We compare our binomial sampling performance (SHAKE-256 used as PRNG) with state-of-the-art software and hardware implementations in Table 5. Our sampler is more than two orders of magnitude more energy-efficient compared to the software implementation on ARM Cortex-M4 which uses assembly-optimized Keccak [45]. It is also 14× more efficient than [17] which uses Knuth-Yao sampling [53] for binomial distributions with ChaCha20 as PRNG.

### 4.4 Discrete Gaussian Sampling

Our discrete Gaussian sampler implements the inversion method of sampling [54] from a discrete symmetric zero-mean distribution $\chi$ on $\mathbb{Z}$ with small support which approximates a rounded continuous Gaussian distribution, e.g., in Frodo [23] and R.EMBLEM [35]. For a distribution with support $S_\chi = \{-s, \cdots, -1, 0, 1, \cdots, s\}$, where $s$ is a small positive integer, the probabilities $\Pr(z)$ for $z \in S_\chi$, such that $\Pr(z) = \Pr(-z)$ can be derived from the cumulative distribution table (CDT) $T_\chi = (T_\chi[0], T_\chi[1], \cdots, T_\chi[s])$, where $2^{-r} \cdot T_\chi[0] = \Pr(0)/2 - 1$ and $2^{-r} \cdot T_\chi[z] = \Pr(0)/2 - 1 + \sum_{i=1}^{z} \Pr(i)$ for $z \in [1, s]$ for a given precision $r$. Given random inputs $r_0 \in \{0, 1\}, r_1 \in [0, 2^r)$ and the distribution table

<table>
<thead>
<tr>
<th>Design</th>
<th>Platform</th>
<th>Tech (nm)</th>
<th>VDD (V)</th>
<th>Freq (MHz)</th>
<th>Parameters</th>
<th>Samp. Cycles</th>
<th>Samp. Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>This work</td>
<td>ASIC</td>
<td>40</td>
<td>1.1</td>
<td>72</td>
<td>$(n = 256, q = 7681)$</td>
<td>461</td>
<td>50.90 nJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 512, q = 12289)$</td>
<td>921</td>
<td>105.74 nJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 1024, q = 12289)$</td>
<td>1,843</td>
<td>211.46 nJ</td>
</tr>
<tr>
<td>Software [45]</td>
<td>ARM Cortex-M4</td>
<td>-</td>
<td>3.0</td>
<td>100</td>
<td>$(n = 256, q = 7681)$</td>
<td>60.433</td>
<td>37.17 µJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 512, q = 12289)$</td>
<td>139,153</td>
<td>85.58 µJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 1024, q = 12289)$</td>
<td>284,662</td>
<td>175.07 µJ</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Design</th>
<th>Platform</th>
<th>Tech (nm)</th>
<th>VDD (V)</th>
<th>Freq (MHz)</th>
<th>Parameters</th>
<th>Samp. Cycles</th>
<th>Samp. Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>This work</td>
<td>ASIC</td>
<td>40</td>
<td>1.1</td>
<td>72</td>
<td>$(n = 256, k = 4)$</td>
<td>505</td>
<td>58.20 nJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 512, k = 8)$</td>
<td>1,009</td>
<td>116.26 nJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 1024, k = 8)$</td>
<td>2,018</td>
<td>232.50 nJ</td>
</tr>
<tr>
<td>Software [45]</td>
<td>ARM Cortex-M4</td>
<td>-</td>
<td>3.0</td>
<td>100</td>
<td>$(n = 256, k = 4)$</td>
<td>52,603</td>
<td>32.35 µJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 512, k = 8)$</td>
<td>155,872</td>
<td>95.86 µJ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(n = 1024, k = 8)$</td>
<td>319,636</td>
<td>196.58 µJ</td>
</tr>
<tr>
<td>Song et al. [17]</td>
<td>ASIC</td>
<td>40</td>
<td>0.9</td>
<td>300</td>
<td>$(n = 512, k = 16)$</td>
<td>3,704</td>
<td>1.25 µJ</td>
</tr>
<tr>
<td>Oder et al. [13]</td>
<td>FPGA</td>
<td>-</td>
<td>-</td>
<td>125</td>
<td>$(n = 1024, k = 16)$</td>
<td>33,792</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 4: Comparison of rejection sampling with software

Table 5: Comparison of binomial sampling with state-of-the-art
T₇, a sample e ∈ Z from χ can be obtained using Algorithm 8 [23].

The sampling must be constant-time in order to eliminate timing side-channels, therefore the algorithm does a complete loop through the entire table T₇. The comparison r₁ > T₇[z] must also be implemented in a constant-time manner. Our implementation adheres to these requirements and uses a 64 × 32 RAM to store the CDT, allowing the parameters s ≤ 64 and r ≤ 32 to be configured according to the choice of the distribution. In Table 6, we have compared our Gaussian sampler performance (SHAKE-256 used as PRNG) with software implementation on ARM Cortex-M4 using assembly-optimized Keccak [45], and we observe up to 40× improvement in energy-efficiency after accounting for voltage scaling. Hardware architectures for Knuth-Yao sampling have been proposed by [9] and [17], but they are for discrete Gaussian distributions with larger standard deviation and higher precision, which we do not support.

4.5 Other Distributions

Several lattice-based protocols, such as CRYSTALS-Dilithium [27] and qTESLA [25], require polynomials to be sampled with coefficients uniformly distributed in the range [−η, η] for a specified bound η < q. For this, we again use rejection sampling. Unlike rejection sampling from Zₙ, we do not require any special techniques since η is typically small or an integer close to a power of two.

Finally, we have also implemented a trinary sampler for polynomials with coefficients from {−1, 0, +1}. We classify these polynomials into three categories: (1) with m non-zero coefficients, (2) with m₀ + 1’s and m₁ −1’s, and (3) with coefficients distributed as Pr(x = 1) = Pr(x = −1) = ρ/2 and Pr(x = 0) = 1 − ρ for ρ ∈ {1/2, 1/4, 1/8, · · · , 1/128}. Their implementations are described in Algorithms 9, 10 and 11. For the first two cases, we start with a zero-polynomial s of size n. Then, uniformly random coefficient indices ∈ [0, n) are generated, and the corresponding coefficients are replaced with −1 or +1 if they are zero [25, 36]. For the third case, sampling of the coefficients is based on the observation [55] that for a uniformly random number x ∈ [0, 2ᵏ) we have Pr(x = 0) = 1/2ᵏ, Pr(x = 1) = 1/2ᵏ and Pr(x ∈ [2, 2ᵏ)) = 1 − 1/2ᵏ. Therefore, for the appropriate value of k ∈ [1,7], we can generate samples from the desired trinary distribution with p = 1/2ᵏ. For all three algorithms, the symbol ∈ₜ denotes pseudo-random number generation using the PRNG.

<table>
<thead>
<tr>
<th>Design</th>
<th>Platform</th>
<th>Tech (nm)</th>
<th>VDD (V)</th>
<th>Freq (MHz)</th>
<th>Parameters</th>
<th>Samp.</th>
<th>Samp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>This work</td>
<td>ASIC</td>
<td>40</td>
<td>1.1</td>
<td>72</td>
<td>(n = 512, σ = 25.0, s = 54)</td>
<td>29,169</td>
<td>1232.71 nJ</td>
</tr>
<tr>
<td>Software [45]</td>
<td>ARM Cortex-M4</td>
<td>-</td>
<td>3.0</td>
<td>100</td>
<td>(n = 512, σ = 25.0, s = 54)</td>
<td>397,921</td>
<td>244.72 µJ</td>
</tr>
</tbody>
</table>

Table 6: Comparison of discrete Gaussian sampling with software
Algorithm 9 Trinary Sampling with \( m \) non-zero coefficients (+1’s and −1’s)

Require: \( m < n \) and a PRNG

Ensure: \( s = (s_0, s_1, \cdots, s_{n-1}) \)

1: \( s \leftarrow (0, 0, \cdots, 0) ; i \leftarrow 0 \)
2: while \( i < m \) do
3: \( pos \in R [0, n) \)
4: \( sign \in R \{0, 1\} \)
5: if \( s_{pos} = 0 \) then
6: if \( sign = 0 \) then
7: \( s_{pos} \leftarrow 1 \)
8: else
9: \( s_{pos} \leftarrow -1 \)
10: end if
11: \( i \leftarrow i + 1 \)
12: end if
13: end while
14: return \( s \)

Algorithm 10 Trinary Sampling with \( m_0 +1 \)’s and \( m_1 -1 \)’s

Require: \( m_0 + m_1 < n \) and a PRNG

Ensure: \( s = (s_0, s_1, \cdots, s_{n-1}) \)

1: \( s \leftarrow (0, 0, \cdots, 0) ; i \leftarrow 0 \)
2: while \( i < m_0 \) do
3: \( pos \in R [0, n) \)
4: if \( s_{pos} = 0 \) then
5: \( s_{pos} \leftarrow +1 \)
6: \( i \leftarrow i + 1 \)
7: end if
8: end while
9: while \( i < m_0 + m_1 \) do
10: \( pos \in R [0, n) \)
11: if \( s_{pos} = 0 \) then
12: \( s_{pos} \leftarrow -1 \)
13: \( i \leftarrow i + 1 \)
14: end if
15: end while
16: return \( s \)

Algorithm 11 Trinary Sampling with coefficients from \( \{-1, 0, +1\} \) distributed according to \( \Pr(x = 1) = \Pr(x = -1) = \rho/2 \) and \( \Pr(x = 0) = 1 - \rho \)

Require: \( k \in [1, 7] \), \( \rho = 1/2^k \) and a PRNG

Ensure: \( s = (s_0, s_1, \cdots, s_{n-1}) \)

1: for \( (i = 0; i < n; i = i + 1) \) do
2: \( x \in R [0, 2^k] \)
3: if \( x = 0 \) then
4: \( s_i \leftarrow 1 \)
5: else if \( x = 1 \) then
6: \( s_i \leftarrow -1 \)
7: else
8: \( s_i \leftarrow 0 \)
9: end if
10: end for
11: return \( s \)
5 Chip Architecture

The top-level architecture of Sapphire is shown in Fig. 10. The efficient building blocks described in Sections 3 and 4 are integrated with a 1 KB instruction memory and an instruction decoder to form the core of our crypto-processor. It can be programmed using 32-bit custom instructions to perform different polynomial arithmetic, transform and sampling operations, as well as simple branching. For example, the following instructions generate polynomials $a, s, e \in \mathbb{R}_q$, and calculate $a \cdot s + e$, which is a typical computation in the Ring-LWE-based scheme NewHope-1024:

```plaintext
config (n = 1024, q = 12289)
# sample_a
rej_sample (prng = SHAKE-128, seed = r0, c0 = 0, c1 = 0, poly = 0)
# sample_s
bin_sample (prng = SHAKE-256, seed = r1, c0 = 0, c1 = 0, k = 8, poly = 1)
# sample_e
bin_sample (prng = SHAKE-256, seed = r1, c0 = 0, c1 = 1, k = 8, poly = 2)
# ntt_s
mult_psi (poly = 1)
transform (mode = DIF_NTT, poly_dst = 4, poly_src = 1)
# a_mul_s
poly_op (op = MUL, poly_dst = 0, poly_src = 4)
# intt_a_mul_s
transform (mode = DIT_INTT, poly_dst = 5, poly_src = 0)
mult_psi_inv (poly = 5)
# a_mul_s_plus_e
poly_op (op = ADD, poly_dst = 1, poly_src = 5)
```

The `config` instruction is first used to configure the protocol parameters $n$ and $q$ which, in this example, are the parameters from NewHope-1024. For $n = 1024$, the polynomial cache is divided into 8 polynomials, which are accessed using the `poly` argument in all instructions. For sampling, the seed can be chosen from a pair of 256-bit registers $r0$ and $r1$, while two 16-bit registers $c0$ and $c1$ are used as

![Figure 10: Sapphire lattice crypto-processor top-level architecture.](image-url)
counters for sampling multiple polynomials from the same seed. For coefficient-wise operations \texttt{poly\_op},
the \texttt{poly\_src} argument indicates the first source polynomial while the \texttt{poly\_dst} argument is used to
 denote the second source (and destination) polynomial. Similarly, the following set of instructions are
 used to generate matrix of polynomials \( A \in \mathbb{R}_q^{2 \times 2} \) and vectors of polynomials \( s, e \in \mathbb{R}_q^2 \), and calculate \( A \cdot s + e \), which is a typical computation in the Module-LWE-based scheme CRYSTALS-Kyber-v1-512:

\begin{verbatim}
config (n = 256, q = 7681)
# sample_s
bin_sample (prng = SHAKE-256, seed = r1, c0 = 0, c1 = 0, k = 3, poly = 4)
bin_sample (prng = SHAKE-256, seed = r1, c0 = 0, c1 = 1, k = 3, poly = 5)
# sample_e
bin_sample (prng = SHAKE-256, seed = r1, c0 = 0, c1 = 2, k = 3, poly = 24)
bin_sample (prng = SHAKE-256, seed = r1, c0 = 0, c1 = 3, k = 3, poly = 25)
# ntt_s
mult_psi (poly = 4)
transform (mode = DIF_NTT, poly_dst = 16, poly_src = 4)
mult_psi (poly = 5)
transform (mode = DIF_NTT, poly_dst = 17, poly_src = 5)
# sample_A0
rej_sample (prng = SHAKE-128, seed = r0, c0 = 0, c1 = 0, poly = 0)
rej_sample (prng = SHAKE-128, seed = r0, c0 = 1, c1 = 0, poly = 1)
# A0_mul_s
poly_op (op = MUL, poly_dst = 0, poly_src = 16)
poly_op (op = MUL, poly_dst = 1, poly_src = 17)
init (poly = 20)
poly_op (op = ADD, poly_dst = 20, poly_src = 0)
poly_op (op = ADD, poly_dst = 20, poly_src = 1)
# sample_A1
rej_sample (prng = SHAKE-128, seed = r0, c0 = 0, c1 = 1, poly = 0)
rej_sample (prng = SHAKE-128, seed = r0, c0 = 1, c1 = 1, poly = 1)
# A1_mul_s
poly_op (op = MUL, poly_dst = 0, poly_src = 16)
poly_op (op = MUL, poly_dst = 1, poly_src = 17)
init (poly = 21)
poly_op (op = ADD, poly_dst = 21, poly_src = 0)
poly_op (op = ADD, poly_dst = 21, poly_src = 1)
# intt_A_mul_s
transform (mode = DIT_INTT, poly_dst = 8, poly_src = 20)
mult_psi_inv (poly = 8)
transform (mode = DIT_INTT, poly_dst = 9, poly_src = 21)
mult_psi_inv (poly = 9)
# A_mul_s_plus_e
poly_op (op = ADD, poly_dst = 24, poly_src = 8)
poly_op (op = ADD, poly_dst = 25, poly_src = 9)
\end{verbatim}

In this example, parameters from CRYSTALS-Kyber-v1-512 have been used. For \( n = 256 \), the
polynomial cache is divided into 32 polynomials, which are again accessed using the \texttt{poly} argument. The
\texttt{init} instruction is used to initialize a specified polynomial with all zero coefficients. The matrix \( A \) is
generated one row at a time, following a \textit{just-in-time} approach \cite{just-in-time} instead of generating and storing all
the rows together, to save memory, which becomes especially useful when dealing with larger matrices
such as in CRYSTALS-Kyber-1024 and CRYSTALS-Dilithium-IV. We have written a Perl script to
parse such plain-text programs and convert them into 32-bit binary instructions which can be decoded
by the Sapphire crypto-processor. A complete list of instructions is provided in Appendix B.

We use dedicated clock gates for fine-grained power savings during program execution, and an
interrupt pin is used to indicate completion of the program. Its memory and data registers can be
accessed through a simple memory-mapped interface. Using the same interface, it is also coupled with a
low-power RISC-V micro-processor [57], as shown in Fig. 12, with 32 KB instruction memory and 64 KB data memory, which implements the RV32IM instruction set [58] and has Dhrystone performance similar to ARM Cortex-M0. When executing cryptographic workloads in the Sapphire core, the RISC-V core can be clock-gated using the wait-for-interrupt (wfi) instruction. The processor is woken up by a dedicated interrupt from the Sapphire core, which is raised when the cryptographic operation is complete. Using the memory-mapped interface ensures that the cryptographic core can be accessed through simple load and store instructions, without requiring any custom instructions or changes to the compilation toolchain. While the cryptographic core is used to accelerate all lattice cryptography computations, the RISC-V processor is used for scheduling the cryptographic workloads as well as for compression and decompression of public keys and ciphertexts. The Keccak-f[1600] core inside Sapphire can be accessed standalone through RISC-V software, and is used to accelerate SHA-3 hashing and extendable output functions according to the requirements of the protocol.

Our test chip was fabricated in the TSMC 40nm LP CMOS process, and the chip micrograph is shown in Fig. 11 with the key design components highlighted. The final placed-and-routed design of our...
Sapphire core consists of 106k logic gates (76 kGE for synthesized design) and 40.25 KB SRAM, with a total area of 0.28 mm\(^2\) (logic and memory combined). Our test chip supports supply voltage scaling from 0.68 V to 1.1 V. Although one of our key design objectives was to demonstrate a configurable lattice cryptography processor, our architecture can be easily scaled for more specific parameter sets. For example, in order to accelerate only NewHope-512 \((n = 512, q = 12289)\), size of the polynomial cache can be reduced to 6.5 KB \(= 8 \times 512 \times 13\) bits and the pre-computed NTT constants can be hard-coded in logic or stored in a 2.03 KB ROM \(= 2.5 \times 512 \times 13\) bits) instead of the 15 KB SRAM. Also, the modular arithmetic logic in the ALU can be simplified significantly to work with a single prime only.

We use the on-chip software-configurable clock gates (shown in Fig. 10) to accurately measure power consumption of different sub-modules inside the Sapphire core, e.g., sampling, NTT, arithmetic, etc. For example, the following instructions are executed to measure the average power consumption of NTT over 1000 executions:

```c
clock_config (keccak = GATE, ntt = UNGATE, sampler = GATE)
c0 = 0
loop: mult_psi (poly = 0)
    transform (mode = DIF_NTT, poly_dst = 4, poly_src = 0)
    c0 = c0 + 1
    flag = compare (c0, 1000)
    if (flag == -1) goto loop
```

The `clock_config` instruction is used to control the clock gates, e.g., the PRNG and sampler clocks are gated when measuring NTT power (the RISC-V core is clock-gated using `wfi` as explained earlier). A simple loop is implemented using labels, comparison and conditional jump instructions, similar to assembly programs in general-purpose micro-controllers (please refer to Appendix B for details of our custom instructions). One of the chip GPIO pins is kept high during the execution of this program to indicate the measurement window, and the power consumption is measured using a source meter. This still includes leakage power from the rest of the chip, but it is only a small fraction of the total power compared to the dynamic power of the operation being measured. Similarly, power consumption of the RISC-V core is measured by clock-gating the Sapphire cryptographic core through software. Finally, leakage power of the chip is measured by externally gating the clock signal being supplied to the chip, so that all logic inside the chip is inactive.

The RISC-V processor consumes 45 \(\mu\)W/MHz at 1.1 V (18 \(\mu\)W/MHz at 0.68 V) when running the Dhrystone 2.1 benchmark. Power consumption of the cryptographic core is a strong function of the protocols being executed along with the associated parameters. Average power consumption of the lattice crypto-processor was measured to be around 8 nW at 1.1 V and 72 MHz (520 \(\mu\)W at 0.68 V and 12 MHz). Total leakage power of the chip was measured to be 391 \(\mu\)W at 1.1 V (70 \(\mu\)W at 0.68 V). Since our chip operates on a single power domain, it is not possible to measure leakage power of different components of the chip. We report the individual module-wise leakage and dynamic power consumption, as obtained from post-place-and-route simulations of our design operating at 1.1 V and 72 MHz, in the table below:

<table>
<thead>
<tr>
<th>Module</th>
<th>(P_{\text{leak}}) ((\mu)W)</th>
<th>(P_{\text{dyn}}) ((\mu)W)</th>
<th>(P_{\text{tot}}) ((\mu)W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Butterfly + ALU</td>
<td>18.28</td>
<td>9210.04</td>
<td>9228.32</td>
</tr>
<tr>
<td>LWE Polynomial Cache</td>
<td>120.28</td>
<td>1660.18</td>
<td>1780.46</td>
</tr>
<tr>
<td>NTT Constants RAM</td>
<td>76.50</td>
<td>661.61</td>
<td>738.11</td>
</tr>
<tr>
<td>Keccak Core + Sampler</td>
<td>41.15</td>
<td>1053.58</td>
<td>1094.73</td>
</tr>
<tr>
<td>RISC-V Processor + Memory</td>
<td>320.15</td>
<td>2745.68</td>
<td>3065.83</td>
</tr>
</tbody>
</table>

Before moving on to the protocol implementations and measurements, we summarize some key architectural design techniques we have used to achieve energy-efficiency:

- We have employed increased parallelism in the modular arithmetic and CS-PRNG modules in the form of single-cycle butterfly computation and 1600-bit 24-cycle Keccak data-path respectively. This reduces cycle count as well as data movement and control circuitry, thus decreasing overall energy consumption.
• Based on overall computational complexity, we know that additions are much cheaper than multiplications. Therefore, we have exploited special properties of prime $q$ and parameter $m$, wherever possible, during Barrett reduction to convert expensive multiplications into cheaper bit-shifts and additions / subtractions.

• Reading data from registers involves much smaller energy consumption compared to reading from SRAMs. We have used registers for storing PRNG seeds, temporary values and the Keccak state, and SRAMs are used to store only the polynomials. This significantly reduces overall energy consumption, especially for the Keccak core.

• Software-controlled clock gates (explicitly inserted in RTL, apart from tool-inserted clock gates) for the sampler, PRNG and NTT allow fine-grained dynamic power savings by gating inactive modules as required during program execution.

• The crypto-processor internal memory is efficiently utilized to store polynomials during protocol execution, thus avoiding access to the main processor’s data memory as much as possible and reducing energy consumption.

6 Protocol Implementations and Measurement Results

To measure the efficiency of our design, we have implemented the following NIST Round 2 lattice-based cryptography protocols on our test chip:

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Lattice Prob.</th>
<th>NIST Sec.</th>
<th>Parameter Set</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CCA-KEM Algorithms</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NewHope</td>
<td>Ring-LWE</td>
<td>1</td>
<td>NewHope-512</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>NewHope-1024</td>
</tr>
<tr>
<td>CRYSTALS-Kyber</td>
<td>Module-LWE</td>
<td>1</td>
<td>Kyber-512</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Kyber-768</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>Kyber-1024</td>
</tr>
<tr>
<td>Frodo</td>
<td>LWE</td>
<td>1</td>
<td>Frodo-640</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Frodo-976</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>Frodo-1344</td>
</tr>
<tr>
<td><strong>Signature Algorithms</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>qTESLA</td>
<td>Ring-LWE</td>
<td>1</td>
<td>qTESLA-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>qTESLA-III-size</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>qTESLA-III-speed</td>
</tr>
<tr>
<td>CRYSTALS-Dilithium</td>
<td>Module-LWE</td>
<td>1</td>
<td>Dilithium-II</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>Dilithium-III</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Dilithium-IV</td>
</tr>
</tbody>
</table>

where NIST security levels 1-6 indicate brute-force security matching or exceeding that of AES-128, SHA3-256, AES-192, SHA3-384, AES-256 and SHA3-512 respectively. Fig. 13 shows our test board and measurement setup. The test chip is housed in a QFN64 socket soldered to the board, an Opal Kelly XEM7001 FPGA development board is used to interface with the chip, and a Keithley 2602A source meter supplies power to the chip. Both the FPGA and the source meter are controlled from a host computer through USB and GPIB interfaces respectively. The FPGA is used to transfer programs from the host computer to the instruction memory of our test chip. Also, a small ring-oscillator-based true random number generator [59] implemented on the FPGA is connected to our test chip through GPIO pins for providing fresh random inputs to the randombytes function which is part of the NIST API. All lattice cryptography programs are written using custom instructions and compiled with our script, while all RISC-V software is written in C and compiled using the riscv-gcc toolchain.
6.1 Protocol Implementations and Evaluation Results

Next, we describe some key aspects of our protocol implementations along with timing and energy profiling results. All polynomial arithmetic, transforms and sampling operations are accelerated using custom programs running in the Sapphire core, and all SHA-3 computations utilize the Keccak core inside Sapphire. The RISC-V processor is used only to read / write data and programs from / to the cryptographic core (both when executing polynomial computations and when utilizing the fast Keccak core for SHA-3 operations), generate initial randomness using the `randombytes` function, encode / decode messages and compress / decompress public keys and ciphertexts. For polynomials which need to be read from the polynomial cache and encoded (or decoded and written to the polynomial cache), we directly post-process the outputs (or pre-process the inputs) of the crypto-processor’s internal memory, instead of first storing the data in intermediate temporary arrays and then processing them. This saves around 10-20% cycles in overall protocol run-time. Also, the internal clock gates are strategically enabled and disabled during program execution using the `clock_config` instruction (please refer to Appendix B for details of our custom instructions) to reduce overall energy consumption.

For the NewHope and CRYSTALS-Kyber key exchange schemes, each of the CPA-secure public key encryption functions – `CPA-PKE.KeyGen`, `CPA-PKE.Encrypt` and `CPA-PKE.Decrypt` – has been written entirely (excluding the encoding and decoding operations) using Sapphire custom instructions with each of the corresponding programs fitting completely in its 1 KB instruction memory. The CCA-secure key encapsulation functions – `CCA-KEM.KeyGen`, `CCA-KEM.Encaps` and `CCA-KEM.Decaps` – involve calls to SHA-3 and the CPA-PKE functions (according to the Fujisaki-Okamoto transform [60]), which are implemented in software. Since the signature schemes qTESLA and CRYSTALS-Dilithium both involve probabilistic rejection of intermediate values, the associated polynomial computations are split into multiple custom programs instead of one each for the `KeyGen`, `Sign` and `Verify` functions. These blocks of code are scheduled using RISC-V software, which also handles encoding and decoding operations. The only exception is the `KeyGen` step in qTESLA, where high-precision discrete Gaussian sampling using large CDT tables is implemented in software, with the SHA-3 functions accelerated in hardware.

Since Module-LWE algorithms involve working with vectors or matrices of polynomials, it is particularly important to ensure that these polynomials fit inside the crypto-processor memory as much as possible (because reads and writes to the internal memory through software are not cheap). When multiplying the public matrix $A$ with the secret vector $s$, the matrix $A$ is generated through rejection sampling, one row at a time, following the just-in-time approach from [56]. This reduces memory footprint so that the entire computation can fit in the polynomial cache.

In Table 7, we compare cycle count and energy consumption of our implementations of the Ring-LWE and Module-LWE CPA-PKE schemes with assembly-optimized software on ARM Cortex-M4 microprocessor (from PQM4 [45]), with average cycle counts for 100 executions. The energy consumption of our test chip has been measured at 1.1 V and 72 MHz, while the energy consumption of the Cortex-M4 processor is estimated from cycle counts using average power (61.5 mW or 615 pJ/cycle at 3.0 V and 100 MHz) measured on NUCLEO-F411RE operating at 100 MHz. The cycle count and energy
Table 7: Measured energy and performance of public key encryption schemes

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Cortex-M4 [45]</th>
<th>This work †</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cycles</td>
<td>Energy (µJ)</td>
</tr>
<tr>
<td>NewHope-512-CPA-PKE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Encrypt</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Decrypt</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>NewHope-1024-CPA-PKE</td>
<td>1,179,353</td>
<td>725.30</td>
</tr>
<tr>
<td>KeyGen</td>
<td>1,663,023</td>
<td>1022.76</td>
</tr>
<tr>
<td>Encrypt</td>
<td>194,439</td>
<td>119.58</td>
</tr>
<tr>
<td>Decrypt</td>
<td>609,923</td>
<td>375.10</td>
</tr>
<tr>
<td>Encrypt</td>
<td>721,925</td>
<td>443.98</td>
</tr>
<tr>
<td>Decrypt</td>
<td>95,894</td>
<td>58.97</td>
</tr>
<tr>
<td>CRYS TALS-Kyber-v1-768-CPA-PKE</td>
<td>1,001,328</td>
<td>615.82</td>
</tr>
<tr>
<td>KeyGen</td>
<td>1,116,540</td>
<td>686.67</td>
</tr>
<tr>
<td>Encrypt</td>
<td>129,560</td>
<td>79.68</td>
</tr>
<tr>
<td>Decrypt</td>
<td>1,610,114</td>
<td>990.22</td>
</tr>
<tr>
<td>Encrypt</td>
<td>1,747,687</td>
<td>1074.83</td>
</tr>
<tr>
<td>Decrypt</td>
<td>162,204</td>
<td>99.76</td>
</tr>
</tbody>
</table>

† Includes program execution and read/write from/to crypto-processor

Figure 14: Configurations of the Sapphire polynomial cache for Ring-LWE and Module-LWE schemes.

consumption for our implementation include program execution as well as the additional overhead of writing inputs to and reading outputs from the Sapphire cryptographic core. For both NewHope and CRYS TALS-Kyber, we observe up to an order of magnitude improvement in energy-efficiency compared to state-of-the-art software, after accounting for voltage scaling. Fig. 14 shows how configurability of the Sapphire polynomial cache is utilized to support different ring dimensions.

Although our lattice crypto-processor architecture primarily targets Ring-LWE and Module-LWE schemes, we also implement the LWE-based Frodo KEM protocol to demonstrate its flexibility. Since LWE-based algorithms require large matrix multiplications, the arithmetic operations dominate total computation cost unlike Ring-LWE and Module-LWE where sampling is the most expensive operation. Since the matrix dimensions are not powers of two, we tile the rows or columns so that we can use the crypto-processor’s power-of-two-sized array operations effectively, as shown in Fig. 15. For Frodo-640, we split each 640-element array into two arrays of size 512 and 128. For Frodo-976, we simply use arrays
of size 1024 with the last 48 elements zeroed out or ignored, as applicable. For Frodo-1344, we use arrays of size 1536, formed by splitting them into two arrays of size 1024 and 512, with the last 192 elements (of the 512-dimension array) zeroed out or ignored, as applicable. Clearly, the polynomial cache is split and accessed in non-uniform sizes for both Frodo-640 and Frodo-1344. However, this tiling scheme makes our version of Frodo incompatible with the reference software implementation.

Frodo involves three large matrix multiplications: $AS$, $S'A$ and $S'B$, where $A$, $S$, $S'$ and $B$ have dimensions $n \times n$, $n \times \bar{n}$, $\bar{m} \times n$ and $n \times \bar{n}$ respectively with $n \in \{640, 976, 1344\}$ and $\bar{m} = \bar{n} = 8$. We ensure that $S'$ is stored in row-major form and $B$ is stored in column-major form, which simplifies calculating $S'B$ using the schoolbook matrix multiplication technique. The $\text{poly}_\text{op}$ instruction is used to coefficient-wise multiply a row of the multiplier matrix with a column of the multiplicand matrix, and the $\text{sum}_\text{elems}$ instruction computes the sum of its elements to generate one element of the output matrix (please refer to Appendix B for details of our custom instructions). For calculating the matrix $AS$, we generate $A$ in row-major form (using rejection sampling, with zero chance of rejection since $q$ is a power of two) and $S$ in column major form (using CDT-based discrete Gaussian sampling) so that the same techniques still work. For $n \in \{640, 976\}$, the matrix $S$ is generated two columns at a time to reduce the number of outer loop iterations, as illustrated in the pseudo-code below:

```c
#if (n == 1344)
    for (j = 0; j < nbar; j = j + 1) {
#else
    for (j = 0; j < nbar/2; j = j + 2) {
#endif
    cdt_sample (prng = SHAKE-256, seed = r1, ..., poly = 0)
    #if (n != 1344)
    cdt_sample (prng = SHAKE-256, seed = r1, ..., poly = 1)
    #endif
    for (i = 0; i < n; i = i + 1) {
        rej_sample (prng = SHAKE-128, seed = r0, ..., poly = 4)
        #if (n != 1344)
        poly_copy (poly_dst = 5, poly_src = 4)
        #endif
        poly_op (op = MUL, poly_dst = 4, poly_src = 0)
        AS[i][j] = sum_elems (poly = 4)
        #if (n != 1344)
```
Since both matrices $S'$ and $A$ are generated on-the-fly in row-major fashion, this makes calculating $S'A$ a bit complicated. We multiply each element of the $i$-th row of $A$ with the $i$-th element of the $j$-th row of $S'$ to generate a partial sum. These $i$ partial sums are incrementally added together to compute the $j$-th row of the output matrix $S'A$. For $n \in \{640, 976\}$, we generate $S$ two columns at a time to reduce the number of outer loop iterations. The corresponding pseudo-code is shown below:

```
# if (n == 1344)
for (j = 0; j < nbar; j = j + 1) {
#else
for (j = 0; j < nbar/2; j = j + 2) {
#endif

  cdt_sample (prng = SHAKE-256, seed = r1, ..., poly = 0)
  init (poly = 6)
  # if (n != 1344)
  cdt_sample (prng = SHAKE-256, seed = r1, ..., poly = 1)
  init (poly = 7)
  # endif

  for (i = 0; i < n; i = i + 1) {
    rej_sample (prng = SHAKE-128, seed = r0, ..., poly = 4)
    reg = (poly = 0)[i]
    poly_op (op = CONST_MUL, poly_dst = 2, poly_src = 4)
    poly_op (op = ADD, poly_dst = 6, poly_src = 2)
    #if (n != 1344)
    reg = (poly = 1)[i]
    poly_op (op = CONST_MUL, poly_dst = 3, poly_src = 4)
    poly_op (op = ADD, poly_dst = 7, poly_src = 3)
    # endif
  }
}
```

where the $reg = (poly)[i]$ instruction is used to save the $i$-th element of the array in the 24-bit internal register $reg$, the $init$ ($poly$) instruction creates an array of zeros and the $CONST\_MUL$ operation multiplies each element of an array with the value stored in $reg$ (please refer to Appendix B for details of our instructions). The $AS + E$ and $S'A + E'$ computations (shown in Fig. 16) require 10.9M and 9.9M cycles respectively for Frodo-640, 25.3M and 23.2M cycles respectively for Frodo-976, and 67.1M and 62.7M cycles respectively for Frodo-1344, and constitute majority of the total cycle count. This is quite different from the Ring-LWE and Module-LWE schemes, where polynomial sampling accounts for 60-70% of the total computation cost. Please note that memory usage of Frodo-1344-CCA-KEM-Decaps exceeds the 64 KB processor data memory on our test chip; hence it was evaluated only in simulation, with power consumption extrapolated from measured power for Frodo-640 and Frodo-976.

In Tables 8 and 9, we have compared cycle count and energy consumption of assembly-optimized Cortex-M4 software [45] with our hardware-accelerated implementation on our test chip operating at 1.1 V and 72 MHz, with average cycle counts for 100 executions. Clearly, our design achieves up to an order of magnitude improvement in energy-efficiency and performance compared to state-of-the-art software. We note that Module-LWE schemes, although a bit slower compared to Ring-LWE, offer parameters with better scalability in terms of security and efficiency compared to Ring-LWE schemes. Among the key encapsulation schemes, NewHope and CRYSTALS-Kyber are two orders of magnitude more efficient than Frodo, owing to the inherent structure in ideal and module lattices where the key operation is polynomial multiplication as opposed to matrix multiplication in standard lattices. Among the digital signature schemes evaluated, qTESLA allows faster signature generation and verification compared to
CRYSTALS-Dilithium. However, our implementation of the key generation step in qTESLA is quite expensive since it uses CDT-based discrete Gaussian sampling with large tables and high precision. This is not a big concern since signature key-pairs are generated infrequently; also, more specialized hardware can be added to support such distribution parameters, albeit at the cost of logic area. Details of program code size and data memory usage for all these hardware-accelerated protocol implementations are available in Appendix C.

In Fig. 17, we plot the measured energy consumption of the Ring-LWE and Module-LWE-based CCA-KEM-Encaps and Sign algorithms at different post-quantum security levels, as implemented on our test chip operating at 1.1 V and 72 MHz. Due to the configurability of our lattice crypto-processor, we are able to implement all these different modes and achieve energy scalability through efficiency versus security trade-offs.

**Figure 16:** Computation of the matrices $B = AS + E$ and $B' = S'A + E'$ in Frodo KEM, where the matrices $S, E$ are generated two columns at a time and $S', E'$ are generated two rows at a time.

**Figure 17:** Energy consumption of Ring-LWE and Module-LWE-based (a) CCA-KEM-Encaps and (b) Sign algorithms at different post-quantum security levels.
Table 8: Measured energy and performance of key encapsulation schemes

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Cortex-M4 [45]</th>
<th>This work</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cycles (µJ)</td>
<td>Cycles</td>
</tr>
<tr>
<td>NewHope-512-CCA-KEM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>-</td>
<td>52,063</td>
</tr>
<tr>
<td>Encaps</td>
<td>-</td>
<td>136,077</td>
</tr>
<tr>
<td>Decaps</td>
<td>-</td>
<td>142,295</td>
</tr>
<tr>
<td>NewHope-1024-CCA-KEM</td>
<td>1,243,729</td>
<td>764.89</td>
</tr>
<tr>
<td>KeyGen</td>
<td>1,963,184</td>
<td>1207.34</td>
</tr>
<tr>
<td>Encaps</td>
<td>1,978,982</td>
<td>1217.07</td>
</tr>
<tr>
<td>CRYSTALS-Kyber-v1-512-CCA-KEM</td>
<td>726,921</td>
<td>447.06</td>
</tr>
<tr>
<td>KeyGen</td>
<td>987,864</td>
<td>607.54</td>
</tr>
<tr>
<td>Encaps</td>
<td>1,018,946</td>
<td>626.65</td>
</tr>
<tr>
<td>CRYSTALS-Kyber-v1-768-CCA-KEM</td>
<td>1,200,291</td>
<td>738.18</td>
</tr>
<tr>
<td>KeyGen</td>
<td>1,446,284</td>
<td>889.46</td>
</tr>
<tr>
<td>Encaps</td>
<td>1,477,365</td>
<td>908.58</td>
</tr>
<tr>
<td>Decaps</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>CRYSTALS-Kyber-v1-1024-CCA-KEM</td>
<td>1,771,729</td>
<td>1089.61</td>
</tr>
<tr>
<td>KeyGen</td>
<td>2,142,912</td>
<td>1317.89</td>
</tr>
<tr>
<td>Encaps</td>
<td>2,188,917</td>
<td>1346.18</td>
</tr>
<tr>
<td>Decaps</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Frodo-640-CCA-KEM</td>
<td>81,293,476</td>
<td>49995.49</td>
</tr>
<tr>
<td>KeyGen</td>
<td>86,178,252</td>
<td>52999.62</td>
</tr>
<tr>
<td>Encaps</td>
<td>87,170,982</td>
<td>53610.15</td>
</tr>
<tr>
<td>Decaps</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Frodo-976-CCA-KEM</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>KeyGen</td>
<td>26,005,326</td>
<td>6.70</td>
</tr>
<tr>
<td>Encaps</td>
<td>29,749,417</td>
<td>7.05</td>
</tr>
<tr>
<td>Decaps</td>
<td>30,421,175</td>
<td>6.94</td>
</tr>
<tr>
<td>Frodo-1344-CCA-KEM</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>KeyGen</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Encaps</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Decaps</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
### Table 9: Measured energy and performance of digital signature schemes

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Cortex-M4 [45]</th>
<th>This work</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cycles (µJ)</td>
<td>Cycles</td>
</tr>
<tr>
<td>qTESLA-I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>17,545,901</td>
<td>4,846,949</td>
</tr>
<tr>
<td>Sign</td>
<td>6,317,445</td>
<td>168,273</td>
</tr>
<tr>
<td>Verify</td>
<td>1,059,370</td>
<td>38,922</td>
</tr>
<tr>
<td>qTESLA-III-size</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>58,227,852</td>
<td>11,479,190</td>
</tr>
<tr>
<td>Sign</td>
<td>19,869,370</td>
<td>348,429</td>
</tr>
<tr>
<td>Verify</td>
<td>2,297,530</td>
<td>69,154</td>
</tr>
<tr>
<td>qTESLA-III-speed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>30,720,411</td>
<td>11,898,241</td>
</tr>
<tr>
<td>Sign</td>
<td>11,987,079</td>
<td>317,083</td>
</tr>
<tr>
<td>Verify</td>
<td>2,225,296</td>
<td>67,712</td>
</tr>
<tr>
<td>CRYSTALS-Dilithium-I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>-</td>
<td>95,202</td>
</tr>
<tr>
<td>Sign</td>
<td>-</td>
<td>376,392</td>
</tr>
<tr>
<td>Verify</td>
<td>-</td>
<td>142,576</td>
</tr>
<tr>
<td>CRYSTALS-Dilithium-II</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>-</td>
<td>130,022</td>
</tr>
<tr>
<td>Sign</td>
<td>-</td>
<td>514,246</td>
</tr>
<tr>
<td>Verify</td>
<td>-</td>
<td>184,933</td>
</tr>
<tr>
<td>CRYSTALS-Dilithium-III</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>2,322,955</td>
<td>167,433</td>
</tr>
<tr>
<td>Sign</td>
<td>9,978,000</td>
<td>634,763</td>
</tr>
<tr>
<td>Verify</td>
<td>2,322,765</td>
<td>229,481</td>
</tr>
<tr>
<td>CRYSTALS-Dilithium-IV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>-</td>
<td>223,272</td>
</tr>
<tr>
<td>Sign</td>
<td>-</td>
<td>815,636</td>
</tr>
<tr>
<td>Verify</td>
<td>-</td>
<td>276,221</td>
</tr>
</tbody>
</table>
Table 10: Comparison of our design with state-of-the-art hardware

<table>
<thead>
<tr>
<th>Design</th>
<th>Platform</th>
<th>Tech (nm)</th>
<th>VDD (V)</th>
<th>Freq (MHz)</th>
<th>Protocol</th>
<th>Area (kGE)</th>
<th>Cycles</th>
<th>Energy (µJ)</th>
</tr>
</thead>
<tbody>
<tr>
<td>This work</td>
<td>ASIC</td>
<td>40</td>
<td>1.1</td>
<td>72</td>
<td>NewHope-512-CCA-KEM-Encaps</td>
<td>106</td>
<td>136,077</td>
<td>10.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NewHope-1024-CPA-PKE-Encrypt</td>
<td></td>
<td>106,611</td>
<td>12.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Kyber-512-CCA-KEM-Encaps</td>
<td></td>
<td>131,698</td>
<td>9.37</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Kyber-768-CPA-PKE-Encrypt</td>
<td></td>
<td>94,440</td>
<td>10.31</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Kyber-768-CCA-KEM-Encaps</td>
<td></td>
<td>177,540</td>
<td>12.80</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Frodo-640-CCA-KEM-Encaps</td>
<td></td>
<td>11,609,668</td>
<td>1129.95</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dilithium-II-Sign</td>
<td></td>
<td>514,246</td>
<td>54.82</td>
</tr>
<tr>
<td>Basu et al.</td>
<td>ASIC</td>
<td>65</td>
<td>1.2</td>
<td>169</td>
<td>NewHope-512-CCA-KEM-Encaps</td>
<td>1273</td>
<td>307,847</td>
<td>69.42</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>200</td>
<td>Kyber-512-CCA-KEM-Encaps</td>
<td>1341</td>
<td>31,669</td>
<td>6.21</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>158</td>
<td>Dilithium-II-Sign</td>
<td>1603</td>
<td>155,166</td>
<td>50.42</td>
</tr>
<tr>
<td>Albrecht et al. [18]†</td>
<td>SLE 78</td>
<td>-</td>
<td>-</td>
<td>50</td>
<td>Kyber-768-CPA-PKE-Encrypt</td>
<td>-</td>
<td>4,747,291</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Kyber-768-CCA-KEM-Encaps</td>
<td>-</td>
<td>5,117,996</td>
<td></td>
</tr>
<tr>
<td>Oder et al.</td>
<td>FPGA</td>
<td>-</td>
<td>-</td>
<td>117</td>
<td>NewHope-1024-Simple-Encrypt</td>
<td>-</td>
<td>179,292</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dilithium-II-Sign</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dilithium-II-Sign</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Fritzmann et al. [61]†</td>
<td>FPGA</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>NewHope-1024-CPA-PKE-Encrypt</td>
<td>-</td>
<td>589,285</td>
<td>-</td>
</tr>
<tr>
<td>Hutter et al. [62]†</td>
<td>ASIC</td>
<td>130</td>
<td>1.2</td>
<td>1</td>
<td>Curve25519-ECDHE</td>
<td>50</td>
<td>1,622,354</td>
<td>113.56</td>
</tr>
<tr>
<td>Banerjee et al. [57]</td>
<td>ASIC</td>
<td>65</td>
<td>1.2</td>
<td>20</td>
<td>NIST-P256-ECDHE</td>
<td>149</td>
<td>680,000</td>
<td>24.07</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NIST-P256-ECDSA-Sign</td>
<td></td>
<td>180,000</td>
<td>6.48</td>
</tr>
</tbody>
</table>

† Only post-synthesis area and energy consumption reported

In Table 10, we compare our design with existing hardware-accelerated implementations of NIST Round 2 lattice-based protocols. Our crypto-processor is significantly smaller than the multiple designs generated using high-level synthesis in [20], and is also more flexible and energy-efficient. Our Kyber implementation is faster than [18] which uses RSA, AES and SHA hardware accelerators on the SLE 78 security controller platform to accelerate lattice cryptography. Efficiency of our design is greater than or comparable to state-of-the-art FPGA implementations of Ring-LWE [13, 61]. Notably, [61] also uses a RISC-V processor with NTT and SHA accelerators to implement the NewHope protocol. However, our implementation of Frodo, which re-purposes the Ring/Module-LWE hardware for LWE computations, is not as efficient as the dedicated LWE accelerator in [16]. Finally, we also compare our design with state-of-the-art pre-quantum elliptic curve cryptography hardware [57, 62], and we observe our implementation of CCA-secure lattice-based key encapsulation using NewHope-512 to be around 5× more efficient compared to elliptic curve Diffie-Hellman key exchange using the NIST P-256 curve at comparable pre-quantum security level.

6.2 Side-Channel Analysis

Side-channel security is an important aspect of all public-key cryptography implementations and lattice-based cryptography is not an exception. In order to prevent information leakage through timing side channels, the most important requirement is to ensure that the timing and memory access patterns of underlying computations are independent of the secret data being computed upon. In our implementation, this is achieved either by making the computations constant-time, e.g., binomial sampling, discrete Gaussian sampling, NTT and polynomial arithmetic, or by using rejection sampling, e.g., sampling numbers from [0, q) or [−η, η] or probabilistic rejection during signature schemes. Since our cryptographic core and RISC-V processor both have a single-level memory hierarchy, the possibility of cache timing attacks is also eliminated.
Figure 18: Measured power waveforms for different polynomial sampling, transform and arithmetic operations along with histograms of energy consumption for 10,000 measurements for each operation, obtained from our test chip operating at 1.1 V and 12 MHz.
Our power side-channel measurement setup is shown in Fig. 19. Our test board has an 18 Ω resistor connected in series between the power supply and the VDD pin of our test chip. The voltage across this resistor, proportional to the chip’s current draw, is magnified using a non-inverting differential amplifier (consists of an AD8001 op-amp chip, with 6 dB flat gain up to 100 MHz, in the non-inverting configuration with resistors of appropriate sizes) and then observed through a 2.5 GS/s Tektronix MDO3024 mixed domain oscilloscope.

The execution times of binomial sampling, discrete Gaussian sampling, NTT, polynomial coefficient-wise multiplication and addition (with \( n = 1024 \) and \( q = 12289 \)) were measured for 10,000 random executions to verify that these computations are indeed constant-time. The corresponding power waveforms and energy consumption histograms, measured from our test chip operating at 1.1 V and 12 MHz, are shown in Fig. 18.

Typical simple power analysis (SPA) attacks on lattice cryptography implementations exploit information leakage through conditional branching or data-dependent execution times during the modular arithmetic computations in NTT or polynomial coefficient-wise multiplication [63, 64, 65]. As explained in Fig. 18, our implementation of polynomial arithmetic is constant-time. To quantitatively evaluate SPA resistance of our design, we perform a difference-of-means test [66, 65, 67] on three polynomial operations – NTT, coefficient-wise multiplication and coefficient-wise addition – which are traditionally used as attack points. In this test, we try to differentiate two sets of measurements – those with a particular coefficient (‘0’-th coefficient in our case) in the input polynomial set to 0 (denoted as set ‘0’ or \( S_0 \)) versus the same coefficient set to \( q - 1 \) (denoted as set ‘1’ or \( S_1 \)) – by comparing their means separately for each point in the mean power trace. The difference-of-means is calculated for increasing number of measurements and plotted as a function of the number of traces \( N \). The corresponding 99.99% confidence interval for having a zero difference of means between these two sets is calculated as \( t_c \cdot \sqrt{(\sigma_0^2 + \sigma_1^2)/N} \), where \( \sigma_0 \) and \( \sigma_1 \) are the standard deviations of the two sets \( S_0 \) and \( S_1 \) respectively and \( t_c \) is the critical \( t \)-statistic for \( N - 1 \) degrees of freedom and cumulative probability \( = 1 - (1 - 0.9999)/2 = 0.99995 \). As long as the absolute difference-of-means is smaller than the confidence interval, it is a strong indicator that the sets \( S_0 \) and \( S_1 \) are indistinguishable.

Figure 19: Power side-channel measurement setup.
Figure 20: Difference-of-means test for polynomial NTT with representative power traces from set $S_0$ (top left) and $S_1$ (top right), difference waveform (bottom left) and difference of means versus number of traces with 99.99% confidence interval (bottom right).

Figure 21: Difference-of-means test for polynomial coefficient-wise multiplication with representative power traces from set $S_0$ (top left) and $S_1$ (top right), difference waveform (bottom left) and difference of means versus number of traces with 99.99% confidence interval (bottom right).

Figure 22: Difference-of-means test for polynomial coefficient-wise addition with representative power traces from set $S_0$ (top left) and $S_1$ (top right), difference waveform (bottom left) and difference of means versus number of traces with 99.99% confidence interval (bottom right).
In Fig. 20, 21 and 22, we provide preliminary difference-of-means test results, over 1000 traces, for three polynomial operations (with $n = 1024$ and $q = 12289$) as measured from our test chip operating at 1.1 V and 10 MHz. Sampling rate of the oscilloscope was set to 500 MS/s for NTT and 2.5 GS/s for coefficient-wise multiplication and addition. The red lines denote measured difference-of-means, and the dashed lines mark the 99.99% confidence interval for ideal zero difference-of-means. These results validate that our design is secure against SPA side-channel attacks.

The protocol implementations discussed earlier do not have any explicit countermeasures against differential power analysis (DPA) attacks. Although DPA attacks can be mitigated by using ephemeral keys, it is still important to analyze how these protocols can be made DPA-secure. Masking-based countermeasures have been proposed in [68, 69, 47] for Ring-LWE encryption. Since our crypto-processor is programmable, such masked protocols can be implemented using the right mix of software and hardware acceleration. For example, we consider NewHope-CPA-PKE and discuss how the masked decryption algorithm, inspired by [68, 69, 47], can be implemented using our hardware. A simplified version of the CPA-PKE scheme, excluding any key / ciphertext compression / decompression and encoding / decoding and implementation-specific details, is provided below:

```plaintext
function NewHope-CPA-PKE.KeyGen(seed):
    Sample $\hat{a}, \hat{s}, e \in \mathbb{R}_q$
    $\hat{b} \leftarrow \hat{a} \odot \hat{s} + \hat{e}$
    return $(pk = (\hat{a}, \hat{b}), sk = \hat{s})$

function NewHope-CPA-PKE.Encrypt(pk, coin, $\mu \in \{0, \cdots, 255\}^{32}$):
    Sample $s', e', e'' \in \mathbb{R}_q$
    $\hat{u} \leftarrow \hat{a} \odot s' + \hat{e}'$
    $v \leftarrow \text{Encode}(\mu) \in \mathbb{R}_q$
    $v' \leftarrow b \cdot s' + e'' + v$
    return $c = (\hat{u}, v')$

function NewHope-CPA-PKE.Decrypt(sk, c):
    $v'' \leftarrow v' - u \cdot s$
    $\mu \leftarrow \text{Decode}(v'') \in \{0, \cdots, 255\}^{32}$
    return $\mu$
```

where $\mu$ is the 32-byte message to be encrypted, $\hat{x}$ is the NTT representation of polynomial $x \in \mathbb{R}_q$, $\odot$ denotes coefficient-wise multiplication (in the transform domain) and $\cdot$ denotes polynomial multiplication in $\mathbb{R}_q$. The Encode function converts message $\mu$ into a polynomial in $\mathbb{R}_q$. To allow robustness against errors, each bit of the 256-bit message is encoded into $\lfloor n/256 \rfloor$ coefficients. For example, for $n = 1024$, the $i$-th, $(256 + i)$-th, $(512 + i)$-th and $(768 + i)$-th coefficients are set to 0 or $\lfloor q/2 \rfloor$ depending on whether the $i$-th bit in $\mu$ is 0 or 1 respectively, for $i \in \{0, \cdots, 255\}$. The Decode function maps $\lfloor n/256 \rfloor$

![Figure 23: Power trace for the NewHope-1024-CPA-PKE.Decrypt algorithm, measured from our test chip operating at 1.1 V and 12 MHz.](image-url)
coefficients of a polynomial back to the original message bit. For example, for \( n = 1024 \), it takes the \( i \)-th, \((256 + i)\)-th, \((512 + i)\)-th and \((768 + i)\)-th coefficients (each in the range \( \{0, \cdots, q - 1\} \), subtracts \([q/2]\) from each of them, accumulates their absolute values, and finally sets the \( i \)-th message bit to 0 if the sum is larger than \( q \) or to 1 otherwise, for \( i \in \{0, \cdots, 255\} \). Further details about these functions are available in the NewHope specification document [24]. The Decrypt algorithm requires one polynomial coefficient-wise multiplication \( u \odot s \), one inverse NTT (including multiplication with \( w^{-1} \psi^{-1} \)) to compute \( u \cdot s \), and one polynomial coefficient-wise subtraction \( v' - u \cdot s \). Fig. 23 shows the corresponding measured power waveform for \( n = 1024 \).

Similar to the encryption scheme studied in [69], we note that NewHope-CPA-PKE is also additively homomorphic, that is, if \( c_1 = (\hat{u}_1, v'_1) \) and \( c_2 = (\hat{u}_2, v'_2) \) are the ciphertexts corresponding to messages \( \mu_1 \) and \( \mu_2 \), respectively, under the same key-pair, then \((\hat{u}_1 + \hat{u}_2, v'_1 + v'_2)\) will be the ciphertext corresponding to \( \mu_1 \oplus \mu_2 \). Following the works of [68, 69, 47], this property can be exploited to randomize the decryption algorithm (as a first-order DPA countermeasure) as explained below:

1. Generate a secret random message \( \mu_r \)
2. Encrypt \( \mu_r \) to its corresponding ciphertext \( c_r = (\hat{u}_r, v'_r) \)
3. Compute \( c_m = (\hat{u} + \hat{u}_r, v' + v'_r) \), where \( c = (\hat{u}, v') \) is the original ciphertext
4. Decrypt masked ciphertext \( c_m \) to obtain \( \mu_m = \mu \oplus \mu_r \), where \( \mu \) is the original message
5. Recover original message \( \mu = \mu_m \oplus \mu_r \)

Therefore, the masked decryption now requires generation of a random message along with invocations of both the Encrypt and Decrypt functions. As explained earlier, these functions can be implemented entirely using Sapphire custom programs, so the masking involves minimal software overheads. Referring to the cycle counts and energy consumption of NewHope-1024-CPA-PKE in Table 7, we note that the masked decryption is about 3x less efficient compared to the unmasked version, both in terms of energy and performance. Since \( \mu_r \) is independent from the original message \( \mu \), the ciphertext \( c_r \) can be pre-computed offline in order to reduce online computation time and energy consumption. As explained in [69], this technique does not require any modifications to the Decode function. However, addition of ciphertexts increases the noise in them, thus increasing the decryption failure rate. Each of the two polynomials in the ciphertext contains one noise term whose coefficients are derived from the zero-mean binomial distribution with support \([-k, k]\) and standard deviation \( \sigma = \sqrt{k/2} \) (\( k = 8 \) for NewHope).

When two such ciphertexts are added, the resulting noise distribution (still binomial) now has support \([-2k, 2k]\) with standard deviation \( \sigma = \sqrt{2k/2} = \sqrt{k} \), that is, the noise variance is doubled. For \( k = 16 \), which is also used in NewHope-Simple, the decryption failure probability will go up from \( 2^{-216} \) [24] to \( 2^{-60} \) [70]. As discussed in [69], standard deviation of the error distribution can be decreased to allow correct decryptions at the cost of a minor deterioration in security. So, one possibility is to set \( k = 4 \) in the unmasked scheme (so that \( k = 8 \) for masked decryption and failure probability remains \( 2^{-216} \)). The corresponding decrease in security level is from 289 bits to 268 bits, as obtained from the LWE hardness estimator [71] using the following Sage module:

```python
load("https://bitbucket.org/malb/lwe-estimator/raw/HEAD/estimator.py")
n = 1024; q = 12289; stddev = sqrt(4/2); alpha = sqrt(2*pi)*stddev/q
_ = estimate_lwe(n, alpha, q, reduction_cost_model=BKZ.sieve)
```

Typically, a non-specific fixed vs. random \( t \)-test [72] is performed to statistically quantify information leakage from a cryptographic algorithm implementation in software or hardware. For the non-specific \( t \)-test, the power traces are divided into two sets \( Q_0 \) (with fixed input) and \( Q_1 \) (with random input) of sizes \( N_0 \) and \( N_1 \) respectively, where \( N_0 + N_1 = N \) is the total number of measurements. Let \( \mu_0, \mu_1 \) and \( \sigma_0^2, \sigma_1^2 \) be the means and standard variances of the sets \( Q_0, Q_1 \) respectively. Then, the \( t \)-test statistic is given by:

\[
t = \frac{\mu_0 - \mu_1}{\sqrt{\frac{\sigma_0^2}{N_0} + \frac{\sigma_1^2}{N_1}}}
\]

For the leakage test, \( t \)-values are determined for each \( N \), for increasing number \( N \) of power traces, and plotted as a function of \( N \), with \(|t| > 4.5 \) indicating information leakage. Further details about this leakage assessment methodology are available in [72]. The masking scheme in [69] was evaluated using
correlation power analysis with 5,000 traces. In Fig. 24, we show preliminary \( t \)-test results for unmasked and masked NewHope-1024-CPA-PKE.Decrypt, over 10,000 measurements each, as obtained from our test chip. While the absolute \( t \)-value crosses 4.5 around 9,000 traces in the unmasked case, it remains well below 4.5 for the masked implementation. However, as mentioned in [69], this masking technique does not provide theoretical first order security since the secret key is not masked. Therefore, detailed analysis with many more traces is required, which will be performed in the future.

7 Conclusion and Future Work

In this work, we have presented a configurable lattice cryptography processor supporting different parameters for NIST Round 2 lattice-based key encapsulation and digital signature protocols such as NewHope, qTESLA, CRYSTALS-Kyber, CRYSTALS-Dilithium and Frodo. Efficient modular arithmetic, sampling and NTT memory architectures together provide an order of magnitude improvement in performance and energy-efficiency compared to state-of-the-art software and hardware implementations. Our ASIC implementation was fabricated in a 40nm low-power CMOS process and all measurement results are obtained from our test chip operating at 1.1 V and 72 MHz. Our protocol implementations are secure against timing and simple power analysis attacks, and we also discuss how masking countermeasures against differential power analysis can be implemented using the programmability of our crypto-processor.

Since our design supports configurable lattice parameters, it will be interesting to explore other lattice-based protocols such as Saber [73] and Round5 [74], which are based on the LWR (learning with rounding) problem [75]. More concrete analysis of DPA-secure masked implementations, for CPA-PKE, CCA-KEM and signature schemes, along with leakage tests and impact on performance and energy-efficiency, will also be performed in the future. Finally, non-lattice-based post-quantum protocols can also be implemented on our platform, using a mix of hardware acceleration and software, since they can still benefit from our efficient implementation of modular arithmetic and SHA-3 computations.

Acknowledgements

The authors would like to thank Texas Instruments for funding this work, the TSMC University Shuttle Program for chip fabrication support, and Bluespec, Xilinx, Cadence, Synopsys and Mentor Graphics for providing CAD tools.
References


Appendix A  Modular Reduction Parameters

As mentioned in Section 3, our modular multiplier with pseudo-configurable prime modulus uses efficient Barrett reduction, with the parameters \( m \), \( k \) and \( q \) coded in digital logic, for a set of chosen primes. These parameters and the corresponding reduction implementations are detailed here. Please note that \( m \) and \( q \) are written in the form \( 2^{l_1} ± 2^{l_2} ± \cdots ± 1 \) only when the number of such integers \( l_1, l_2, \cdots \) is less than 5.

**Algorithm Reduction mod 7681**

Require: \( q = 2^{13} - 2^9 + 1, m = 273 = 2^8 + 2^4 + 1, k = 21, x \in [0, q^2) \)
Ensure: \( z = x \mod q \)

1. \( t \leftarrow (x \ll 8) + (x \ll 4) + x \)
2. \( t \leftarrow t \gg 21 \)
3. \( t \leftarrow (t \ll 13) - (t \ll 9) + t \)
4. \( z \leftarrow x - t \)
5. if \( z \geq q \) then
6. \( z \leftarrow z - q \)
7. end if
8. return \( z \)

**Algorithm Reduction mod 12289**

Require: \( q = 2^{13} + 2^{12} + 1, m = 10921, k = 27, x \in [0, q^2) \)
Ensure: \( z = x \mod q \)

1. \( t \leftarrow 10921 \cdot x \)
2. \( t \leftarrow t \gg 27 \)
3. \( t \leftarrow (t \ll 13) + (t \ll 12) + t \)
4. \( z \leftarrow x - t \)
5. if \( z \geq q \) then
6. \( z \leftarrow z - q \)
7. end if
8. return \( z \)

**Algorithm Reduction mod 40961**

Require: \( q = 2^{15} + 2^{13} + 1, m = 52427, k = 31, x \in [0, q^2) \)
Ensure: \( z = x \mod q \)

1. \( t \leftarrow 52427 \cdot x \)
2. \( t \leftarrow t \gg 31 \)
3. \( t \leftarrow (t \ll 15) + (t \ll 13) + t \)
4. \( z \leftarrow x - t \)
5. if \( z \geq q \) then
6. \( z \leftarrow z - q \)
7. end if
8. return \( z \)
Algorithm Reduction mod 120833

Require: \( q = 2^{17} + 2^{14} + 2^{13} - 2^{11} + 1, m = 71089, k = 33, x \in [0, q^2) \)

Ensure: \( z = x \mod q \)
1: \( t \leftarrow 71089 \cdot x \)
2: \( t \leftarrow t \gg 33 \)
3: \( t \leftarrow (t \ll 17) - (t \ll 14) + (t \ll 13) - (t \ll 11) + t \)
4: \( z \leftarrow x - t \)
5: if \( z \geq q \) then
6: \( z \leftarrow z - q \)
7: end if
8: return \( z \)

Algorithm Reduction mod 133121

Require: \( q = 2^{17} + 2^{11} + 1, m = 64527 = 2^{16} - 2^{10} + 2^4 - 1, k = 33, x \in [0, q^2) \)

Ensure: \( z = x \mod q \)
1: \( t \leftarrow (x \ll 16) - (x \ll 10) + (x \ll 4) - x \)
2: \( t \leftarrow t \gg 33 \)
3: \( t \leftarrow (t \ll 17) + (t \ll 11) + t \)
4: \( z \leftarrow x - t \)
5: if \( z \geq q \) then
6: \( z \leftarrow z - q \)
7: end if
8: return \( z \)

Algorithm Reduction mod 184321

Require: \( q = 2^{17} + 2^{15} + 2^{14} + 2^{12} + 1, m = 46603, k = 33, x \in [0, q^2) \)

Ensure: \( z = x \mod q \)
1: \( t \leftarrow 46603 \cdot x \)
2: \( t \leftarrow t \gg 46 \)
3: \( t \leftarrow (t \ll 23) - (t \ll 13) + t \)
4: \( z \leftarrow x - t \)
5: if \( z \geq q \) then
6: \( z \leftarrow z - q \)
7: end if
8: return \( z \)

Algorithm Reduction mod 8380417

Require: \( q = 2^{23} - 2^{13} + 1, m = 8396807 = 2^{23} + 2^{13} + 2^3 - 1, k = 46, x \in [0, q^2) \)

Ensure: \( z = x \mod q \)
1: \( t \leftarrow (x \ll 23) + (x \ll 13) + (x \ll 3) - x \)
2: \( t \leftarrow t \gg 46 \)
3: \( t \leftarrow (t \ll 23) - (t \ll 13) + t \)
4: \( z \leftarrow x - t \)
5: if \( z \geq q \) then
6: \( z \leftarrow z - q \)
7: end if
8: return \( z \)
Algorithm  Reduction mod \( q = 8058881 \)
\[
\text{Require: } q = 8058881, m = 8731825, k = 46, x \in [0, q^2) \\
\text{Ensure: } z = x \mod q \\
1: t \leftarrow 8731825 \cdot x \\
2: t \leftarrow t \gg 46 \\
3: t \leftarrow 8058881 \cdot t \\
4: z \leftarrow x - t \\
5: \text{if } z \geq q \text{ then} \\
6: z \leftarrow z - q \\
7: \text{end if} \\
8: \text{return } z 
\]

Algorithm  Reduction mod \( q = 4205569 \)
\[
\text{Require: } q = 2^{22} + 2^{13} + 2^{11} + 2^{10} + 1, m = 4183069, k = 44, x \in [0, q^2) \\
\text{Ensure: } z = x \mod q \\
1: t \leftarrow 4183069 \cdot x \\
2: t \leftarrow t \gg 44 \\
3: t \leftarrow (t \ll 22) + (t \ll 13) + (t \ll 11) + (t \ll 10) + t \\
4: z \leftarrow x - t \\
5: \text{if } z \geq q \text{ then} \\
6: z \leftarrow z - q \\
7: \text{end if} \\
8: \text{return } z 
\]

Algorithm  Reduction mod \( q = 4206593 \)
\[
\text{Require: } q = 2^{22} + 2^{13} + 2^{12} + 1, m = 2091025 = 2^{21} - 2^{13} + 2^{11} + 2^4 + 1, k = 43, x \in [0, q^2) \\
\text{Ensure: } z = x \mod q \\
1: t \leftarrow (x \ll 21) -(x \ll 13) + (x \ll 11) + (x \ll 4) + x \\
2: t \leftarrow t \gg 43 \\
3: t \leftarrow (t \ll 22) + (t \ll 13) + (t \ll 12) + t \\
4: z \leftarrow x - t \\
5: \text{if } z \geq q \text{ then} \\
6: z \leftarrow z - q \\
7: \text{end if} \\
8: \text{return } z 
\]

Algorithm  Reduction mod \( q = 8404993 \)
\[
\text{Require: } q = 2^{23} + 2^{14} + 1, m = 4186127 = 2^{22} - 2^{13} + 2^4 - 1, k = 45, x \in [0, q^2) \\
\text{Ensure: } z = x \mod q \\
1: t \leftarrow (x \ll 22) -(x \ll 13) + (x \ll 4) - x \\
2: t \leftarrow t \gg 45 \\
3: t \leftarrow (t \ll 23) + (t \ll 14) + t \\
4: z \leftarrow x - t \\
5: \text{if } z \geq q \text{ then} \\
6: z \leftarrow z - q \\
7: \text{end if} \\
8: \text{return } z 
\]
For the prime $q = 65537 = 2^{16} + 1$, we employ an easier reduction technique owing to the special structure of $q$. Any integer $x \in [0, q^2)$ can be written as $x = x_2 2^{32} + x_1 2^{16} + x_0$ where $x_0$ and $x_1$ are 16-bit numbers and $x_2 \in \{0, 1\}$. Since $2^{16} \equiv -1 \mod q$, we have $x \equiv x_0 - x_1 + x_2 \mod q$, which must be followed by a conditional addition to bring back the result to $[0, q)$.

**Algorithm** Reduction mod 65537

**Require:** $q = 2^{16} + 1, x = x_2 2^{32} + x_1 2^{16} + x_0 \in [0, q^2)$

**Ensure:** $z = x \mod q$

1: $z \leftarrow x_0 - x_1 + x_2$
2: if $z < 0$ then
3: $z \leftarrow z + q$
4: end if
5: return $z$

### Appendix B Custom Instruction Set Summary

In this section, we briefly describe all the custom instructions supported by our crypto-processor. Apart from the polynomials stored in its memory and the 256-bit seed registers $r_0$ and $r_1$, these are the core internal registers that can also be manipulated:

- 24-bit temporary registers $\text{reg}$ and $\text{tmp}$
- 16-bit counter registers $c_0$ and $c_1$
- 2-bit flag register to store comparison results (-1, 0 or +1)

Following is the list of instructions along with short descriptions:

<table>
<thead>
<tr>
<th>Configuration: set parameters and clock gates</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>config (n, q)</code></td>
</tr>
<tr>
<td><code>clock_config (keccak, ntt, sampler)</code></td>
</tr>
</tbody>
</table>

**Register Operations: register assignments and arithmetic**

$c_0 = \#VAL / c_0 + \#VAL / c_0 - \#VAL$
$c_1 = \#VAL / c_1 + \#VAL / c_1 - \#VAL$
$\text{reg} = \#VAL / \text{tmp}$
$\text{tmp} = \#VAL / \text{tmp} \ (\text{OP}) \ \text{reg}$

where $\#VAL$ can be any unsigned integer of appropriate size, and $(\text{OP})$ is one of the following operations: \{ADD, SUB, MUL, AND, OR, XOR, RSHIFT, LSHIFT\}

**Register-Polynomial Operations: register and polynomial interactions**

$\text{reg} = \text{max}_\text{elems} (\text{poly})$
$\text{reg} = \text{sum}_\text{elems} (\text{poly})$
$\text{reg} = (\text{poly})[\#VAL] / (\text{poly})[c_0] / (\text{poly})[c_1]$
$(\text{poly})[\#VAL] / (\text{poly})[c_0] / (\text{poly})[c_1] = \text{reg}$

**Transforms: number theoretic transform and related computations**

`transform (mode, poly_dst, poly_src)`
`mult_psi (poly) / mult_psi_inv (poly)`

where `$mode$` is one of the following: \{DIF_NTT, DIF_INTT, DIT_NTT, DIT_INTT\}
Sampling: polynomial sampling from various distributions

\begin{align*}
\text{bin\_sample} & \quad (\text{prng, seed, c0, c1, k, poly}) \\
\text{cdt\_sample} & \quad (\text{prng, seed, c0, c1, r, s, poly}) \\
\text{rej\_sample} & \quad (\text{prng, seed, c0, c1, poly}) \\
\text{uni\_sample} & \quad (\text{prng, seed, c0, c1, eta, bitlen, poly}) \\
\text{tri\_sample\_1} & \quad (\text{prng, seed, c0, c1, m, poly}) \\
\text{tri\_sample\_2} & \quad (\text{prng, seed, c0, c1, m0, m1, poly}) \\
\text{tri\_sample\_3} & \quad (\text{prng, seed, c0, c1, rho, poly})
\end{align*}

where \( \text{prng} \) can be SHAKE-128 or SHAKE-256, \( \text{seed} \) can be \( r0 \) or \( r1 \), and \( k, r, s, \eta, \) bitlen, \( m, m0, m1, \) rho are the distribution parameters

Polynomial Computations: polynomial initialization and other operations

\begin{align*}
\text{init} & \quad (\text{poly}) \\
\text{poly\_copy} & \quad (\text{poly\_dst, poly\_src}) \\
\text{poly\_op} & \quad (\text{op, poly\_dst, poly\_src}) \\
\text{shift\_poly} & \quad (\text{ring, poly\_dst, poly\_src})
\end{align*}

where \( \text{op} \) can be one of the following: \{ADD, SUB, MUL, BITREV, CONST\_ADD, CONST\_SUB, CONST\_MUL, CONST\_AND, CONST\_OR, CONST\_XOR, CONST\_RSHIFT, CONST\_LSHIFT\}, and \( \text{ring} \) can be either \( x^N+1 \) or \( x^N-1 \)

Comparison and Branching: simple branching operations

\begin{align*}
\text{flag} & = \text{eq\_check} \quad (\text{poly, poly}) \\
\text{flag} & = \text{inf\_norm\_check} \quad (\text{poly, bound}) \\
\text{flag} & = \text{compare} \quad (\text{reg / tmp / c0 / c1, #VAL}) \\
\text{if} \quad (\text{flag} == / != -1 / 0 / +1) \quad \text{goto <label>}
\end{align*}

where the \text{flag} register stores -1, 0 and +1 for the register comparison result being “lesser than”, “equal to” and “greater than” respectively, and it stores 1 or 0 depending on whether the equality check and infinity norm check has passed or failed respectively

SHA-3 Computations: hashing operations

\begin{align*}
\text{sha3\_init} \\
\text{sha3\_256\_absorb} & \quad (\text{poly}) \\
\text{sha3\_512\_absorb} & \quad (\text{poly}) \\
\text{sha3\_256\_absorb} & \quad (\text{r0 / r1}) \\
\text{sha3\_512\_absorb} & \quad (\text{r0 / r1}) \\
\text{r0 / r1} & = \text{sha3\_256\_digest} \\
\text{r0 || r1} & = \text{sha3\_512\_digest}
\end{align*}

where the seed registers are used to store the hash outputs – either \( r0 \) or \( r1 \) for SHA-3-256, and both \( r0 \) and \( r1 \) together for SHA-3-512
Table 11: Code size and data memory usage of hardware-accelerated protocol implementations

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Code Size (KB)</th>
<th>KeyGen (B)</th>
<th>Encaps (B)</th>
<th>Decaps (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NewHope-512</td>
<td>10.14</td>
<td>3,616</td>
<td>3,760</td>
<td>4,896</td>
</tr>
<tr>
<td>NewHope-1024</td>
<td>10.36</td>
<td>3,640</td>
<td>3,784</td>
<td>6,024</td>
</tr>
<tr>
<td>Kyber-v1-512</td>
<td>9.18</td>
<td>3,640</td>
<td>3,768</td>
<td>4,648</td>
</tr>
<tr>
<td>Kyber-v1-762</td>
<td>9.35</td>
<td>4,008</td>
<td>4,136</td>
<td>5,368</td>
</tr>
<tr>
<td>Kyber-v1-1024</td>
<td>9.38</td>
<td>4,456</td>
<td>4,584</td>
<td>6,168</td>
</tr>
<tr>
<td>Frodo-640</td>
<td>13.78</td>
<td>4,984</td>
<td>15,144</td>
<td>35,736</td>
</tr>
<tr>
<td>Frodo-976</td>
<td>13.44</td>
<td>3,976</td>
<td>20,200</td>
<td>51,544</td>
</tr>
<tr>
<td>Frodo-1344</td>
<td>13.79</td>
<td>4,216</td>
<td>26,312</td>
<td>69,432</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Code Size (KB)</th>
<th>KeyGen (B)</th>
<th>Sign (B)</th>
<th>Verify (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>qTesla-I</td>
<td>15.53</td>
<td>19,112</td>
<td>8,456</td>
<td>6,088</td>
</tr>
<tr>
<td>qTesla-III-size</td>
<td>15.71</td>
<td>26,736</td>
<td>10,416</td>
<td>6,000</td>
</tr>
<tr>
<td>qTesla-III-speed</td>
<td>14.55</td>
<td>28,016</td>
<td>10,944</td>
<td>6,528</td>
</tr>
<tr>
<td>Dilithium-I</td>
<td>14.25</td>
<td>11,224</td>
<td>18,792</td>
<td>9,240</td>
</tr>
<tr>
<td>Dilithium-II</td>
<td>14.53</td>
<td>13,952</td>
<td>23,520</td>
<td>10,944</td>
</tr>
<tr>
<td>Dilithium-III</td>
<td>14.94</td>
<td>16,648</td>
<td>28,328</td>
<td>12,696</td>
</tr>
<tr>
<td>Dilithium-IV</td>
<td>15.44</td>
<td>19,568</td>
<td>33,248</td>
<td>14,528</td>
</tr>
</tbody>
</table>

Appendix C Memory Usage

Details of program code size (in KB) and processor data memory usage (in bytes) for our hardware-accelerated CCA-secure KEM and digital signature protocol implementations on the test chip (memory usage of the RISC-V processor only, excluding dedicated instruction and data memory of cryptographic accelerator) are listed in Table 11. Code sizes for all the protocols vary between 9 KB and 16 KB, while there is a large variation in memory usage among different protocols and also among sub-algorithms in the same protocol. Notably, KeyGen for qTesla requires significantly more memory than Sign and Verify due to the expensive Gaussian sampling process. Also, the Encaps and Decaps memory usage of Frodo is much higher than Ring-LWE and Module-LWE key encapsulation protocols due to additional storage required for large matrices.

Appendix D Benefit of Hardware-Accelerated Keccak

The Keccak-based SHA-3 and SHAKE functions are integral to all the lattice-based protocols evaluated in this work, and the most expensive sampling operations require SHAKE-128 or SHAKE-256 as the CS-PRNG. Since SHA-3 is a standard cryptographic primitive, embedded devices are likely to have hardware acceleration support for Keccak. Therefore, we analyze the performance gains achieved through hardware acceleration of the Keccak round function as opposed to executing it in software. We compare full software implementations of the protocols running on the RISC-V processor with partially accelerated implementations where the Keccak round function is executed in hardware and rest of the computations in software. The results are summarized in Tables 12 and 13. We observe up to $2 \times$ and $1.5 \times$ reduction in cycle count for key encapsulation and signature algorithms respectively, as shown in Fig. 25 and 26. There is also a reduction of about 5 KB in code size and 200 bytes in data memory usage. Since the software implementations of Frodo require data memory greater than 64 KB, their cycle counts were measured in simulation only.
Table 12: Improvements in performance of CCA-KEM protocols with efficient Keccak core

<table>
<thead>
<tr>
<th></th>
<th>NewHope-512-CCA-KEM</th>
<th></th>
<th>NewHope-1024-CCA-KEM</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Code (KB)</td>
<td>Mem (B)</td>
<td>Time (cyc)</td>
<td>Mem (B)</td>
</tr>
<tr>
<td></td>
<td>only S/W</td>
<td>S/W + Keccak H/W</td>
<td>only S/W</td>
<td>S/W + Keccak H/W</td>
</tr>
<tr>
<td>KeyGen</td>
<td>17.19</td>
<td>12.06</td>
<td>17.48</td>
<td>12.39</td>
</tr>
<tr>
<td>Encaps</td>
<td>13.112</td>
<td>1.189,849</td>
<td>12.920</td>
<td>745,460</td>
</tr>
<tr>
<td>Decaps</td>
<td>16.264</td>
<td>1.867,066</td>
<td>16.072</td>
<td>1,160,021</td>
</tr>
<tr>
<td></td>
<td>17.464</td>
<td>1.979,394</td>
<td>17.272</td>
<td>1,383,138</td>
</tr>
<tr>
<td>Kyber-512-CCA-KEM</td>
<td>only S/W</td>
<td>S/W + Keccak H/W</td>
<td>only S/W</td>
<td>S/W + Keccak H/W</td>
</tr>
<tr>
<td></td>
<td>Code (KB)</td>
<td>Mem (B)</td>
<td>Time (cyc)</td>
<td>Mem (B)</td>
</tr>
<tr>
<td>KeyGen</td>
<td>10.688</td>
<td>1.030,194</td>
<td>10.488</td>
<td>544,274</td>
</tr>
<tr>
<td>Encaps</td>
<td>13.360</td>
<td>1.449,433</td>
<td>13.160</td>
<td>811,636</td>
</tr>
<tr>
<td>Decaps</td>
<td>14.112</td>
<td>1.556,554</td>
<td>13.912</td>
<td>1,015,754</td>
</tr>
<tr>
<td>Kyber-1024-CCA-KEM</td>
<td>only S/W</td>
<td>S/W + Keccak H/W</td>
<td>only S/W</td>
<td>S/W + Keccak H/W</td>
</tr>
<tr>
<td></td>
<td>Code (KB)</td>
<td>Mem (B)</td>
<td>Time (cyc)</td>
<td>Mem (B)</td>
</tr>
<tr>
<td></td>
<td>20.02</td>
<td>19.672</td>
<td>11,937,076</td>
<td>19.64</td>
</tr>
<tr>
<td>KeyGen</td>
<td>19.864</td>
<td>2.469,365</td>
<td>19.672</td>
<td>11,937,076</td>
</tr>
<tr>
<td>Encaps</td>
<td>23.496</td>
<td>3.083,707</td>
<td>23.304</td>
<td>1,586,160</td>
</tr>
<tr>
<td>Decaps</td>
<td>25.080</td>
<td>3.260,783</td>
<td>24.888</td>
<td>1,929,623</td>
</tr>
<tr>
<td>Frodo-640-CCA-KEM</td>
<td>only S/W</td>
<td>S/W + Keccak H/W</td>
<td>only S/W</td>
<td>S/W + Keccak H/W</td>
</tr>
<tr>
<td></td>
<td>Code (KB)</td>
<td>Mem (B)</td>
<td>Time (cyc)</td>
<td>Mem (B)</td>
</tr>
<tr>
<td>KeyGen</td>
<td>39.640</td>
<td>122,673,678</td>
<td>39.448</td>
<td>41,052,566</td>
</tr>
<tr>
<td>Encaps</td>
<td>61.320</td>
<td>147,340,683</td>
<td>61.128</td>
<td>64,070,315</td>
</tr>
<tr>
<td>Decaps</td>
<td>71.736</td>
<td>147,965,532</td>
<td>71.544</td>
<td>64,694,905</td>
</tr>
<tr>
<td>Frodo-1344-CCA-KEM</td>
<td>only S/W</td>
<td>S/W + Keccak H/W</td>
<td>only S/W</td>
<td>S/W + Keccak H/W</td>
</tr>
<tr>
<td></td>
<td>Code (KB)</td>
<td>Mem (B)</td>
<td>Time (cyc)</td>
<td>Mem (B)</td>
</tr>
<tr>
<td>KeyGen</td>
<td>79.000</td>
<td>484,919,600</td>
<td>78.808</td>
<td>163,622,557</td>
</tr>
<tr>
<td>Encaps</td>
<td>125.512</td>
<td>586,573,889</td>
<td>125.320</td>
<td>260,825,858</td>
</tr>
<tr>
<td>Decaps</td>
<td>147.112</td>
<td>587,640,788</td>
<td>146.920</td>
<td>261,892,757</td>
</tr>
</tbody>
</table>

Figure 25: Comparison of cycle counts of (a) NewHope, (b) CRYSTALS-Kyber-v1 and (c) Frodo CCA-KEM-Encaps with and without hardware-accelerated Keccak.
Table 13: Improvements in performance of Sign protocols with efficient Keccak core

<table>
<thead>
<tr>
<th></th>
<th>qTesla-I</th>
<th>qTesla-III-size</th>
<th>qTesla-III-speed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>only S/W</td>
<td>S/W + Keccak H/W</td>
<td></td>
</tr>
<tr>
<td>Code (KB)</td>
<td>24.21</td>
<td>19.12</td>
<td></td>
</tr>
<tr>
<td>Mem (B)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time (cyc)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>26,440</td>
<td>26,240</td>
<td>26,440</td>
</tr>
<tr>
<td>Sign</td>
<td>27,512</td>
<td>27,312</td>
<td>27,512</td>
</tr>
<tr>
<td>Verify</td>
<td>23,304</td>
<td>23,104</td>
<td>23,304</td>
</tr>
<tr>
<td>Mem (B)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time (cyc)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>43,472</td>
<td>43,272</td>
<td>43,472</td>
</tr>
<tr>
<td>Sign</td>
<td>49,696</td>
<td>49,496</td>
<td>49,696</td>
</tr>
<tr>
<td>Verify</td>
<td>41,328</td>
<td>41,128</td>
<td>41,328</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>CRYSALS-Dilithium-I</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>only S/W</td>
<td>S/W + Keccak H/W</td>
</tr>
<tr>
<td>Code (KB)</td>
<td>23.41</td>
<td>18.26</td>
</tr>
<tr>
<td>Mem (B)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time (cyc)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>29,344</td>
<td>29,144</td>
</tr>
<tr>
<td>Sign</td>
<td>50,800</td>
<td>50,302</td>
</tr>
<tr>
<td>Verify</td>
<td>33,326</td>
<td>32,108</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>CRYSALS-Dilithium-II</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>only S/W</td>
<td>S/W + Keccak H/W</td>
</tr>
<tr>
<td>Code (KB)</td>
<td>23.52</td>
<td>18.43</td>
</tr>
<tr>
<td>Mem (B)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time (cyc)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>41,664</td>
<td>40,644</td>
</tr>
<tr>
<td>Sign</td>
<td>70,336</td>
<td>69,356</td>
</tr>
<tr>
<td>Verify</td>
<td>45,696</td>
<td>44,356</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>CRYSALS-Dilithium-III</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>only S/W</td>
<td>S/W + Keccak H/W</td>
</tr>
<tr>
<td>Code (KB)</td>
<td>23.69</td>
<td>18.55</td>
</tr>
<tr>
<td>Mem (B)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time (cyc)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>55,920</td>
<td>55,720</td>
</tr>
<tr>
<td>Sign</td>
<td>91,760</td>
<td>91,308</td>
</tr>
<tr>
<td>Verify</td>
<td>59,952</td>
<td>59,572</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>CRYSALS-Dilithium-IV</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>only S/W</td>
<td>S/W + Keccak H/W</td>
</tr>
<tr>
<td>Code (KB)</td>
<td>24.02</td>
<td>18.93</td>
</tr>
<tr>
<td>Mem (B)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time (cyc)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>72,384</td>
<td>72,184</td>
</tr>
<tr>
<td>Sign</td>
<td>115,456</td>
<td>115,192</td>
</tr>
<tr>
<td>Verify</td>
<td>76,480</td>
<td>76,216</td>
</tr>
</tbody>
</table>

Figure 26: Comparison of cycle counts of (a) qTesla and (b) CRYSALS-Dilithium Sign with and without hardware-accelerated Keccak.
Appendix E  NewHope and Kyber-v1 CPA-PKE

As described in Section 6, the CPA-secure public key encryption functions – CPA-PKE.KeyGen, CPA-PKE.Encrypt and CPA-PKE.Decrypt – can be written entirely (excluding the encoding and decoding operations) using Sapphire custom instruction programs. In Fig. 27 and 28, we provide detailed cycle counts of our CPA-PKE implementations, with each function split into five sections:

- **decode**: decoding / decompression of inputs
- **write**: writing inputs to the accelerator
- **imem**: cryptographic computation involving polynomial sampling and arithmetic
- **read**: reading outputs from the accelerator
- **encode**: encoding / compression of outputs

Here, we analyze three different implementations of the CPA-PKE schemes:

- **only S/W**: software-only version on RISC-V (reference code without assembly optimizations)
- **pre-opt H/W**: hardware-accelerated `imem` section with encoding and decoding in software
- **opt H/W**: hardware-accelerated `imem` section with optimized encoding and decoding in software

Compared to `pre-opt H/W`, in `opt H/W` we directly process the inputs and outputs of the accelerator's internal memory, instead of first storing the data in intermediate temporary arrays and then processing them. This provides 10-20% reduction in cycle count, as shown in Fig. 27 and 28. Also, we can see that the cycle count for the `imem` section, which is the core cryptographic computation (apart from encoding / decoding), is reduced by $50 - 100\times$ when using the Sapphire accelerator compared

### Figure 27: Details of cycle count and memory usage in NewHope CPA-PKE schemes.

<table>
<thead>
<tr>
<th>NewHope-512-CPA-PKE</th>
<th></th>
<th>NewHope-1024-CPA-PKE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>KeyGen</td>
<td>Encrypt</td>
</tr>
<tr>
<td></td>
<td>only S/W</td>
<td>pre-opt H/W</td>
</tr>
<tr>
<td><strong>decode</strong></td>
<td>503</td>
<td>149</td>
</tr>
<tr>
<td><strong>write</strong></td>
<td>-</td>
<td>74</td>
</tr>
<tr>
<td><strong>imem</strong></td>
<td>1,010,518</td>
<td>10,347</td>
</tr>
<tr>
<td><strong>read</strong></td>
<td>-</td>
<td>7,256</td>
</tr>
<tr>
<td><strong>encode</strong></td>
<td>47,408</td>
<td>7,543</td>
</tr>
</tbody>
</table>

### Figure 27: Details of cycle count and memory usage in NewHope CPA-PKE schemes.
Figure 28: Details of cycle count and memory usage in Kyber-v1 CPA-PKE schemes.

to software-only implementation, thus highlighting the efficiency of our design. However, the overall performance improvement is not as large, due to the additional overheads of processing the data, which is done entirely in software. Instead of the current memory-mapped interface, using a direct memory access (DMA) path between the processor core and the accelerator can help reduce these overheads further, which will be explored in future work.

In Fig. 27 and 28, we also show portions of the Sapphire polynomial cache that are used during execution of each CPA-PKE function. For Kyber-v1, NewHope-512 and NewHope-1024, the cache is split into 32, 16 and 8 polynomials respectively, and the specific polynomials in use are shown in red. Clearly, our choice of 8192-element polynomial cache is just enough for NewHope-1024 and Kyber-v1-1024.
Table 14: Cycle count and power consumption for sampling operations

<table>
<thead>
<tr>
<th>Operation</th>
<th>CS-PRNG</th>
<th>Cycle Count</th>
<th>Avg. Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rejection Sampling</td>
<td>SHAKE-128</td>
<td>$\approx \left(\left\lceil \frac{29}{32} \cdot n \right\rceil + n \right)/(1 - P_{rej})$</td>
<td>7.43 mW</td>
</tr>
<tr>
<td>Binomial Sampling</td>
<td>SHAKE-256</td>
<td>$\left\lceil \frac{33}{34} \cdot n \right\rceil + n$ for $k \in (0, 16]$</td>
<td>8.30 mW</td>
</tr>
<tr>
<td>Gaussian Sampling</td>
<td>SHAKE-256</td>
<td>$\left\lceil \frac{33}{34} \cdot n \right\rceil + n$ for $k \in (16, 32]$</td>
<td>3.04 mW</td>
</tr>
<tr>
<td>Uniform Sampling</td>
<td>SHAKE-256</td>
<td>$\approx \left(\left\lceil \frac{33}{34} \cdot n \right\rceil + \frac{3}{2} \cdot n \right)/(2 \eta + 1)$</td>
<td>8.33 mW</td>
</tr>
<tr>
<td>Trinary Sampling (1)</td>
<td>SHAKE-256</td>
<td>$\geq \left\lceil \frac{33}{34} \cdot m_0 \right\rceil + 2 m_0 + n$</td>
<td>4.01 mW</td>
</tr>
<tr>
<td>Trinary Sampling (2)</td>
<td>SHAKE-256</td>
<td>$\geq \left\lceil \frac{33}{34} \cdot m_0 \right\rceil + \left\lceil \frac{33}{34} \cdot m_1 \right\rceil + 2 m_0 + 2 m_1 + n$</td>
<td>3.99 mW</td>
</tr>
<tr>
<td>Trinary Sampling (3)</td>
<td>SHAKE-256</td>
<td>$\left\lceil \frac{33}{34} \cdot n \right\rceil + n$</td>
<td>7.47 mW</td>
</tr>
</tbody>
</table>

Table 15: Cycle count and power consumption for polynomial arithmetic operations

<table>
<thead>
<tr>
<th>Operation</th>
<th>Cycle Count</th>
<th>Avg. Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number Theoretic Transform</td>
<td>$(\frac{n}{2} + 1) \cdot \lg n + n + 1$</td>
<td>11.40 mW</td>
</tr>
<tr>
<td>Coefficient-wise Multiplication</td>
<td>$n + 1$</td>
<td>9.50 mW</td>
</tr>
<tr>
<td>Coefficient-wise Addition</td>
<td>$n + 1$</td>
<td>6.38 mW</td>
</tr>
</tbody>
</table>

Appendix F  Sampling and Polynomial Arithmetic

We provide cycle count formulas and average power consumption of our lattice-crypto processor (measured from test chip operating at 1.1 V and 72 MHz) for sampling and polynomial arithmetic in Tables 14 and 15. Here, $n$ is the polynomial size, $P_{rej}$ denotes rejection probability and $k, s, \eta, m, m_0, m_1$ are distribution parameters (please refer to Section 4 for details). In Fig. 29, we also analyze the variation in power consumption of polynomial arithmetic modulo different primes. While polynomial coefficient-wise addition has roughly the same power consumption ($\approx 6$ mW) irrespective of the value of $q$, polynomial NTT and coefficient-wise multiplication have varying power consumption depending on the bit-size of $q$ and efficiency of modular reduction, as discussed in Section 3.

All polynomial arithmetic is performed in the ring $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$. The NTT cycle count includes pre-multiplication by powers of $\psi$. For sampling operations, pseudo-random bits are read from the 1600-bit Keccak state 32 bits (half-lane) at a time, except binomial sampling with $k > 16$ where bits are read 64 bits (full-lane) at a time. Although this leads to wastage of random bits, it greatly simplifies the control circuitry required to fetch bits from the Keccak state register, thus leading to overall energy-efficiency of the lattice-crypto accelerator. Depending on whether SHAKE-128 or SHAKE-256 is used, the number of state bits that can be used per round is 1344 and 1088 respectively. Average cycle counts for rejection sampling of coefficients in $\mathbb{Z}_q$ and uniform sampling of coefficients in $[-\eta, \eta]$ (which involves rejection sampling in $[0, 2\eta]$ followed by subtracting $\eta$ from the result) are calculated in terms of their rejection probabilities. Only lower bounds are provided for cycle counts of trinary sampling (1) and (2) with specified number(s) of non-zero coefficients.

Figure 29: Power consumption of polynomial arithmetic operations for different prime moduli.
Appendix G  Trivium as PRNG

Apart from the standard PRNGs based on AES, SHA-3 and ChaCha20, our test chip also implements a very efficient PRNG based on the Trivium stream cipher [76]. The internal state of Trivium consists of 288 flip-flops, and a straight-forward hardware implementation, requiring only 3 AND gates and 11 XOR gates, generates one bit per cycle, as shown in Fig. 30. However, each state bit of Trivium is designed to remain unchanged for at least 64 iterations after it has been modified. Therefore, the hardware can be parallelized to generate 64 bits per cycle at the cost of additional logic area. Our Trivium-based PRNG employs this 64-bit parallel design and occupies 8.4 kGE area (post place-and-route). It has energy consumption of 26 pJ at 1.1 V (10 pJ at 0.68 V), thus making it 4× more energy-efficient (and also 4× smaller) compared to the SHAKE-128-based PRNG described in Section 4. Therefore, Trivium can potentially be used as the PRNG for polynomial sampling, with huge gains in energy-efficiency, in applications where the use of non-NIST primitives is allowed.

Appendix H  Voltage Scaling

Fig. 31 shows the effect of supply voltage scaling (0.7-1.1 V) on leakage current, average active current and maximum operating frequency of our test chip.

Figure 31: Effects of supply voltage scaling as measured from our test chip - (a) leakage current (b) average active current and maximum frequency.
Appendix I FPGA Validation Results

To verify the functionality of our lattice cryptography accelerator, it was also synthesized and implemented using Xilinx Vivado 2018.1 on the Artix XC7A200T-1 FPGA, and evaluated on the Digilent Nexys Video board. The maximum clock frequency was 25 MHz, and the final area utilization results are presented below, and our design was small enough to fit in the XC7A35T device as well (slices are shared between different modules, so the sum of slices occupied by each module is larger than the total number of slices occupied by the accelerator). Please note that this FPGA implementation was only for validating the functionality of our ASIC design. The RTL used for our ASIC design was directly ported to the Vivado tool without any FPGA-specific modifications or optimizations.

<table>
<thead>
<tr>
<th>Module</th>
<th>Slices</th>
<th>LUTs</th>
<th>FFs</th>
<th>BRAMs</th>
<th>DSPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Butterfly Unit + ALU</td>
<td>957</td>
<td>2,983</td>
<td>0</td>
<td>0</td>
<td>11</td>
</tr>
<tr>
<td>LWE Polynomial Cache</td>
<td>2,335</td>
<td>3,917</td>
<td>8</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>NTT Constants RAM</td>
<td>367</td>
<td>790</td>
<td>8</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Keccak-f[1600] Core</td>
<td>1,716</td>
<td>5,784</td>
<td>1,605</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Discrete Distribution Sampler</td>
<td>334</td>
<td>784</td>
<td>47</td>
<td>0.5</td>
<td>0</td>
</tr>
<tr>
<td>Instruction Decoder + IMEM</td>
<td>190</td>
<td>435</td>
<td>1</td>
<td>0.5</td>
<td>0</td>
</tr>
<tr>
<td><strong>Sapphire (Total)</strong></td>
<td>4,173</td>
<td>14,975</td>
<td>2,539</td>
<td>14</td>
<td>11</td>
</tr>
<tr>
<td><strong>Utilization on XC7A200T</strong></td>
<td>12.48%</td>
<td>11.19%</td>
<td>0.95%</td>
<td>3.84%</td>
<td>1.49%</td>
</tr>
<tr>
<td><strong>Utilization on XC7A35T</strong></td>
<td>80.25%</td>
<td>45.00%</td>
<td>6.10%</td>
<td>28.00%</td>
<td>12.22%</td>
</tr>
</tbody>
</table>

Appendix J Power Consumption Simulator

A Python-based open-source cycle-accurate simulator for the Sapphire lattice-crypto processor is provided in [https://github.com/banerjeeutsav/sapphire_sim](https://github.com/banerjeeutsav/sapphire_sim) which can be used to profile the performance of Ring-LWE and Module-LWE algorithms. This allows quick evaluation of lattice-based protocols with varying parameter choices but without any hardware design effort, which is especially important for a fast evolving field such as lattice-based cryptography. The simulator not only reports accurate cycle counts and execution times but also macro-operation-level power and average energy consumption modelled using measurements from the Sapphire test chip at various operating conditions. Detailed description of the custom instructions, simulation options and example code are provided in [https://github.com/banerjeeutsav/sapphire_sim/blob/master/documentation.pdf](https://github.com/banerjeeutsav/sapphire_sim/blob/master/documentation.pdf).

Appendix K Implementation of Kyber-v2 CCA-KEM

The specifications of CRYSTALS-Kyber CCA-KEM [26] were modified during NIST Round 2. Implementation of the initial version, which we call Kyber-v1, was described previously in this paper. Here, we provide the implementation results of the modified version, which we call Kyber-v2. The changes from Kyber-v1 to Kyber-v2 are summarized below:

- No public key compression
- Prime $q$ changed from 7681 to 3329
- Binomial distribution noise parameter changed from $\eta \in \{3, 4, 5\}$ to $\eta = 2$
- Definition of NTT, rejection sampling of public matrix and ciphertext compression parameters $d_u$ and $d_v$ updated for the new prime
- Public key represented in the NTT domain
- Final shared key derived using SHAKE-256 instead of SHA3-256

From an implementation perspective, the most important change is in prime $q$ and consequently the definition of NTT. For Kyber-v2, we have $q \equiv 1 \mod n$ but $q \not\equiv 1 \mod 2n$, that is, $\mathbb{Z}_q^*$ contains primitive
256-th roots of unity but not primitive 512-th roots. So, the NTT now decomposes a ring element \(a \in \mathbb{Z}_q[x]/(x^{256} + 1)\) as \((a \mod x^2 - \zeta, \ldots, a \mod x^2 - \zeta^{255})\) instead of \((a \mod x - \zeta, \ldots, a \mod x - \zeta^{511})\), where \(\{\zeta, \zeta^2, \ldots, \zeta^{253}, \zeta^{256}\}\) is the set of all the 256-th primitive roots of unity. In other words, each ring element is decomposed into 128 polynomials of degree 2 modulo \(q\) instead of 256 polynomials of degree 1 modulo \(q\). Therefore, polynomial multiplication in the ring now requires extension field arithmetic. Our Sapphire crypto-core does not natively support this modified NTT representation. To solve this, we employ the "Preprocess-then-NTT" technique from [77], specifically 1-Round-Preprocess-then-NTT or 1PtNTT. Next, we briefly describe this technique and how it is used for polynomial multiplication.

Following [77], the 1PtNTT technique first divides polynomial \(f(x) \in \mathbb{Z}_q[x]/(x^{256} + 1)\) with 256 coefficients into two smaller polynomials \(f_{\text{even}}(y) \in \mathbb{Z}_q[y]/(y^{128} + 1)\) and \(f_{\text{odd}}(y) \in \mathbb{Z}_q[y]/(y^{128} + 1)\) with 128 coefficients each, where \(f_{\text{even}}\) and \(f_{\text{odd}}\) respectively contain the even and odd coefficients of \(f\) and \(y = x^2\). That is, \(f(x) = f_{\text{even}}(x^2) + f_{\text{odd}}(x^2)\). The 1PtNTT and 1PtNTT-1 operations are defined as:

\[
\hat{f} = 1\text{PtNTT}(f) = (\text{NTT}(f_{\text{even}}), \text{NTT}(f_{\text{odd}})) = (\hat{f}_{\text{even}}, \hat{f}_{\text{odd}})
\]

\[
f = 1\text{PtNTT}^{-1}(\hat{f}) = (\text{NTT}^{-1}(\hat{f}_{\text{even}}), \text{NTT}^{-1}(\hat{f}_{\text{odd}})) = (f_{\text{even}}, f_{\text{odd}})
\]

where NTT refers to the traditional 128-point number theoretic transform (which is supported by our hardware architecture). Let \(p(x) = f(x) \cdot g(x) \in \mathbb{Z}_q[x]/(x^{256} + 1)\) be the product of the two polynomials, then \(p(x) = p_{\text{even}}(x^2) + x \cdot p_{\text{odd}}(x^2)\) where

\[
p_{\text{even}}(y) = f_{\text{even}}(y) \cdot g_{\text{even}}(y) + f_{\text{odd}}(y) \cdot (y \cdot g_{\text{odd}}(y)) \in \mathbb{Z}_q[y]/(y^{128} + 1)
\]

\[
p_{\text{odd}}(y) = f_{\text{odd}}(y) \cdot g_{\text{even}}(y) + f_{\text{even}}(y) \cdot g_{\text{odd}}(y) \in \mathbb{Z}_q[y]/(y^{128} + 1)
\]

Then, the equation \(p = 1\text{PtNTT}^{-1}(1\text{PtNTT}(f) \bowtie 1\text{PtNTT}(g))\) is used for polynomial multiplication in the 1PtNTT domain, where

\[
1\text{PtNTT}(f) \bowtie 1\text{PtNTT}(g) = (\text{NTT}(f_{\text{even}}) \odot \text{NTT}(g_{\text{even}}) + \text{NTT}(f_{\text{odd}}) \odot \text{NTT}(\overline{g}_{\text{odd}})),
\]

\[
\text{NTT}(f_{\text{odd}}) \odot \text{NTT}(g_{\text{even}}) + \text{NTT}(f_{\text{even}}) \odot \text{NTT}(\overline{g}_{\text{odd}}))
\]

and \(\overline{g}_{\text{odd}} \equiv y \cdot g_{\text{odd}}(y) \in \mathbb{Z}_q[y]/(y^{128} + 1)\) and \(\odot\) denotes coefficient-wise multiplication of polynomials.

For further details, please refer to [77]. The following table summarizes the basic operation counts (\(\text{NTT}_{128} / \text{NTT}_{256}\) denote traditional 128/256-point NTT, \(\to_{128}\) denotes 128-point polynomial circular left shift computation, \(+_{128} / +_{256}\) denote 128/256-point polynomial addition, \(\odot_{128} / \odot_{256}\) denote 128/256-point coefficient-wise multiplication) for polynomial forward / inverse transform and polynomial multiplication in Kyber-v1 and Kyber-v2 using NTT and 1PtNTT respectively:

<table>
<thead>
<tr>
<th></th>
<th>NTT(_{128})</th>
<th>NTT(_{256})</th>
<th>(\to_{128})</th>
<th>(+_{128})</th>
<th>(+_{256})</th>
<th>(\odot_{128})</th>
<th>(\odot_{256})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kyber-v1</td>
<td>NTT / NTT(^{-1})</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>NTT-based PolyMul</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Kyber-v2</td>
<td>1PtNTT / 1PtNTT(^{-1})</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>1PtNTT-based PolyMul</td>
<td>1</td>
<td>-</td>
<td>1</td>
<td>2</td>
<td>-</td>
<td>4</td>
</tr>
</tbody>
</table>

Clearly, 1PtNTT-based polynomial multiplication is more computationally expensive than the NTT-based approach; the difference was theoretically estimated by [77] to be 10-20%.

Next, we describe how we implement 1PtNTT-based polynomial arithmetic for Kyber-v2 on our Sapphire lattice crypto-processor. The polynomial cache is split into 64 polynomials of \(n = 128\) elements each, and a scaling factor of 19 is used for fast rejection sampling (rejection probability reduced from 0.19 to 0.03). As an example, for polynomials \(f, g \in \mathbb{Z}_{3329}[x]/(x^{256} + 1)\), the following set of instructions compute \(p = f \cdot g\) where \(\hat{f} = (\hat{f}_{\text{even}}, \hat{f}_{\text{odd}})\) is already available in the transform domain (\(\hat{f}_{\text{even}}, \hat{f}_{\text{odd}}, g_{\text{even}}, g_{\text{odd}}, p_{\text{even}}, p_{\text{odd}}\) stored in locations 0, 32, 1, 33, 32, 36 respectively in the polynomial cache) and the shift_poly instruction (see Appendix B) is used to compute \(g_{\text{odd}}\):

```plaintext
config (n = 128, q = 3329)
# 1ptntt_g = (ntt_g_even, ntt_g_odd) and ntt_shift_g_odd
shift_poly (ring = x^N+1, poly_dst = 31, poly_src = 33)
```
Apart from the additional computations tabulated earlier, our implementation also involves poly_copy operations which require a small but finite number of cycles. Overall, our 1PtNTT-based implementation requires 4,176 – 2,835 = 1,341 additional cycles compared to our NTT-based implementation. However, NTT\((g_{even})\), NTT\((g_{odd})\) and NTT\((\rightarrow g_{odd})\) computed above are not over-written so that they can be used for multiple such polynomial multiplications as required in Module-LWE. Therefore, the computation of NTT\((g_{even})\), NTT\((g_{odd})\) and NTT\((\rightarrow g_{odd})\) gets amortized over all polynomial multiplications, and the number of additional cycles per polynomial multiplication is effectively 2,006 – 1,546 = 460 after excluding the computation of NTT\((g) / 1\text{PtNTT}(g)\). There are \(k^2, k^2 + k\) and \(k\) such polynomial multiplications in Kyber-CPA-PKE KeyGen, Encrypt and Decrypt respectively, thus leading to additional cycle counts in our CCA-KEM implementation.

The cycle counts, power and energy consumption (at 1.1 V and 72 MHz) of our hardware-accelerated Kyber-v2 CCA-KEM implementation are tabulated below. Compared to Kyber-v1 (see Table 8), the power consumption is slightly higher because we had to use the fully configurable modular multiplier instead of the pseudo-configurable one. Note that the cycle count of KeyGen is significantly lower due to the absence of public key compression, while the cycle counts of Encaps and Decaps are slightly higher due to the additional 1PtNTT-related computations described earlier.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Cycle Count</th>
<th>Power (mW)</th>
<th>Energy (µJ)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CRYSTALS-Kyber-v2-512-CCA-KEM</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>54,861</td>
<td>6.02</td>
<td>4.59</td>
</tr>
<tr>
<td>Encaps</td>
<td>134,965</td>
<td>5.43</td>
<td>10.18</td>
</tr>
<tr>
<td>Decaps</td>
<td>146,068</td>
<td>5.95</td>
<td>12.07</td>
</tr>
<tr>
<td><strong>CRYSTALS-Kyber-v2-768-CCA-KEM</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>84,110</td>
<td>6.1</td>
<td>7.13</td>
</tr>
<tr>
<td>Encaps</td>
<td>184,080</td>
<td>5.52</td>
<td>14.11</td>
</tr>
<tr>
<td>Decaps</td>
<td>198,011</td>
<td>6.05</td>
<td>16.64</td>
</tr>
<tr>
<td><strong>CRYSTALS-Kyber-v2-1024-CCA-KEM</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeyGen</td>
<td>116,841</td>
<td>6.21</td>
<td>10.08</td>
</tr>
<tr>
<td>Encaps</td>
<td>236,886</td>
<td>5.65</td>
<td>18.59</td>
</tr>
<tr>
<td>Decaps</td>
<td>256,828</td>
<td>6.12</td>
<td>21.83</td>
</tr>
</tbody>
</table>
Although not implemented in the pseudo-configurable modular multiplier in our chip, modular reduction with \( q = 3329 \) can be constructed in a future implementation as shown below:

**Algorithm** Reduciton mod 3329

**Require:** \( q = 2^{11} + 2^{10} + 2^8 + 1, m = 5039, k = 24, x \in [0, q^k) \)

**Ensure:** \( z = x \mod q \)

1. \( t \leftarrow 5039 \cdot x \)
2. \( t \leftarrow t \gg 24 \)
3. \( t \leftarrow (t \ll 11) + (t \ll 10) + (t \ll 8) + t \)
4. \( z \leftarrow x - t \)
5. if \( z \geq q \) then
6. \( z \leftarrow z - q \)
7. end if
8. return \( z \)