

Optimized Vectorization Implementation of CRYSTALS-Dilithium

Jieyu Zheng, Haoliang Zhu, Zhenyu Song, Zheng Wang, Yunlei Zhao

Abstract—CRYSTALS-Dilithium is a lattice-based signature scheme to be standardized by NIST as the primary post-quantum signature algorithm. In this work, we make a thorough study of optimizing the implementations of Dilithium by utilizing the Advanced Vector Extension (AVX) instructions, specifically AVX2 and the latest AVX-512. We first present an improved parallel small polynomial multiplication with tailored early evaluation (PSPM-TEE) to further speed up the signing procedure. Our PSPM algorithm outperform the NTT by 47%-66% in AVX2 and AVX-512 implementation. We then present a tailored reduction method that is simpler and faster than Montgomery reduction. We minimize the CPU cycles of tailored reduction AVX-512 implementation by using AVX-512IFMA. Finally, we propose a fully and highly vectorized implementation of Dilithium using AVX-512. This is achieved by carefully vectorizing most of Dilithium functions with the AVX-512 instructions in order to improve efficiency both for time and for space simultaneously. With all the optimization efforts, our AVX-512 implementation improves the performance by 43.2%/39.3%/45.6% in key generation, 36.6%/41.6%/43.7% in signing, and 45.3%/46.5%/47.4% in verification for the parameter sets of Dilithium2/3/5 respectively. To the best of our knowledge, our AVX-512 implementation has the best performance for Dilithium on the Intel x86-64 CPU platform to date.

Index Terms—Post-Quantum Cryptography, Lattice-Based Cryptography, CRYSTALS-Dilithium, AVX2, AVX-512, Software Optimization.

I. INTRODUCTION

WITH the popularity of authentication and non-repudiation, it is more common to construct digital signatures using asymmetric cryptographic techniques. Currently, millions of web servers use digital signatures as part of Transport Level Security (TLS) [1]–[3], which allows users to verify the server’s identity. Both hardware and software vendors rely on digital signatures to guarantee entity integrity. Digital signatures are also essential for cybersecurity infrastructure. Most of the current digital signatures are implemented based on Rivest-Shamir-Adleman (RSA) [4], Elliptic Curve Cryptography (ECC), or Digital Signature Algorithm (DSA).

However, in the era of continuous development of quantum computers, traditional public key cryptography and DSA appear to be in jeopardy. Using Shor’s algorithm [5], an attacker with a powerful quantum computer can obtain the corresponding private key in polynomial time by analyzing the public key of RSA or ECC. The National Institute of Standards and Technology (NIST) proposed in [6] that by 2030 an RSA 2048-bit key may be broken by a quantum computer within a few hours. As a result, NIST has launched a competition to solicit standard algorithms for PQC, including soliciting and evaluating quantum-resistant secure digital signature algo-

rithms. On July 5th 2022, NIST announced the first algorithms to be standardized. There are three signature schemes selected: CRYSTALS-Dilithium, FALCON and SPHINCS+ [7], among them CRYSTALS-Dilithium is recommended by NIST as the primary signature algorithm to be used. NIST recently released three draft standards. FIPS 204 [8] is among these drafts and pertains to CRYSTALS-Dilithium. CRYSTALS-Dilithium is a digital signature scheme based on lattice theory, whose security is based on the Module Learning With Errors (MLWE) [9] and the Module Short Integer Solution (MSIS) [10] problems. The majority of Dilithium’s operations rely on cyclotomic polynomial ring arithmetic, and it leverages the Number Theoretic Transform (NTT) as a common technique for accelerating polynomial multiplication. The Dilithium scheme adopts the Fiat-Shamir with Aborts structure [11], resulting in a signature process that carefully scrutinizes and rejects sampling through a series of conditional checks. This rigorous process ensures that the generated signature does not divulge any private key information.

NIST chose the 64-bit Intel architecture (i.e. x86-64) as the main benchmarking platform of NIST PQC candidates. Advanced Vector Extension (AVX) is Intel x86-64 instruction set architecture [12]. The first AVX instruction was proposed by Intel in 2008. AVX-512 is the newest version of Intel Advanced Vector eXtensions [13]. It has 32 512-bit vector registers called zmm registers. The vector registers are partitioned into distinct data lanes, allowing instructions to be executed concurrently within each lane. This parallel processing technique is referred to as Single Instruction Multiple Data (SIMD). The AVX-512 instruction set excels at accelerating non-sequential processes and delivers optimal performance compared to all other Intel SIMD instruction sets. AVX-512 offers a range of permutation instructions and masked load/stores, which are particularly efficient for implementing hash functions, NTT, and rejection sampling. Additionally, AVX-512IFMA has the potential to significantly accelerate multiply and add operations.

a) Related Work: Dilithium’s optimization efforts encompass both software and hardware aspects. However, this paper places its emphasis on the software-optimized implementation of Dilithium. The basic software implementation is the C REF implementation that the CRYSTALS team submitted to NIST [14]. However, the C REF implementation is not optimized and has lower efficiency. Additionally, the CRYSTALS team provided a faster AVX2 optimized version [14] on x86-64 CPUs. Recently, software optimization studies mainly focus on CPU/GPU environments and embedded systems like ARM. Ravi et al. [15] presented a signed polynomial

representation implementation for Cortex-M4 and proposed various stack consumptions and speed trade-offs for the signing procedure. Kim et al. [16] presented a method for designing the NTT multiplications of CRYSTALS-Dilithium using advanced SIMD instructions and vector registers. “Asymmetric multiplication” for matrix-to-vector polynomial multiplication was introduced in [17]. Abdulrahman et al. [18] proposed to switch to a smaller prime modulus for small polynomial multiplication in the signing procedure of Dilithium. [19] presented optimizations of Dilithium on IBM z15 architecture, and mentioned that employing some optimization methods with advanced instruction sets like AVX-512 as future work. Zheng et al. [20] presented a parallel small polynomial multiplication (PSPM) algorithm that can fastly compute small vector polynomial multiplication in Dilithium, based on which the C and ARM Neon implementations were proposed.

For AVX-512 implementations of PQC algorithms, some arithmetics like large integer multiplication, Montgomery multiplication, and NTT AVX-512 implementation have received researchers’ attention [21]–[26]. Cheng et al. [27] proposed a highly vectorized implementation for SIKE. [28] presented an implementation using AVX-512 to batch CSIDH group actions. [29] presented an implementation using AVX-512 for SPHINCS+. Cabral et al. [30] presented an optimized AVX-512 implementation for SHA-3 family. Duowei Lei et al. [31] present parallel polynomial sampling and arithmetic implementation to speed up Dilithium scheme.

b) Contributions: This paper enhances the parallel small polynomial multiplication, as previously seen in ACSAC 2022 [20], by introducing a tailored early evaluation approach. We proceed to implement Dilithium across all security levels, utilizing SIMD instruction sets on x86-64 CPUs, consequently establishing a new speed record on this platform. Our contributions can be summarized as follows.

- 1) We introduce an enhanced parallel small polynomial multiplication with tailored early evaluation (PSPM-TEE) to expedite the signing process. PSPM-TEE is implemented using C, AVX2, and AVX-512 instructions. Notably, PSPM-TEE surpasses NTT in performance across all three implementations.
- 2) We introduce a tailored reduction method that outperforms Montgomery reduction. We apply it to the first level of NTT(t_0), NTT(t_1) for Dilithium2/3/5 and NTT(y) for Dilithium2.
- 3) We introduce an optimized implementation of the tailored reduction, requiring only two instructions and leveraging AVX-512IFMA. This yields a reduction of one instruction and two cycle counts compared to the AVX-512F implementation. When compared to Montgomery reduction, the tailored reduction with AVX-512IFMA demonstrates superior efficiency, saving up to two instructions and six cycle counts.
- 4) We propose a fully and highly vectorized implementation of Dilithium utilizing AVX-512. We meticulously vectorize a majority of Dilithium functions, focusing on performance bottlenecks such as NTT, NTT^{-1} , Montgomery reduction, hashing, and parallel reject sampling. Notably, we present an effi-

cient implementation of parallel rejection sampling using AVX-512, eliminating the need for a large precomputation table. Through these optimization efforts, our AVX-512 implementation achieves remarkable performance improvements of 43.2%/39.3%/45.6% in key generation, 36.6%/41.6%/43.7% in signing, and 45.3%/46.5%/47.4% in verification across the parameter sets of Dilithium2/3/5, respectively. To the best of our knowledge, our AVX-512 implementation achieves the best performance for Dilithium on the Intel x86-64 CPU platform thus far.

c) Code: We will later open source our code.

d) Structure of this paper: This paper is organized as follows. Section II reviews some preliminaries. Section III presents an improved PSPM with early evaluation. Section IV introduces the proposed special Tailored reduction. Section V deals with the AVX-512 implementation of Dilithium and presents various optimization strategies. In Section VI we go through the performance results and comparison.

II. PRELIMINARIES

A. Notation

We denote polynomials by lowercase Latin letter c (the coefficient of a polynomial is c_i , which represents the i -th element of c), vectors of polynomials by bold lowercase letter \mathbf{t} , and matrices by bold upper case letter \mathbf{A} . If they are transformed to NTT-domain, then we add a hat to make a tag, e.g., \hat{c} , $\hat{\mathbf{t}}$ and $\hat{\mathbf{A}}$.

Let $\mathbb{Z}_q \stackrel{\text{def}}{=} \mathbb{Z}/q\mathbb{Z}$, $\mathcal{R} \stackrel{\text{def}}{=} \mathbb{Z}[x]/(x^n + 1)$, and $\mathcal{R}_q \stackrel{\text{def}}{=} \mathbb{Z}_q[x]/(x^n + 1)$. Element $a_i \in \mathbb{Z}_q$ will be represented by one element in $\{-\frac{q-1}{2}, \dots, 0, \dots, \frac{q-1}{2}\}$. Polynomial $a \in \mathcal{R}_q$ can be represented by $a = \sum_{i=0}^{n-1} a_i \cdot x^n$, where $a_i \in \mathbb{Z}_q$.

The operator \circ denotes coefficient-wise multiplication. The operator \parallel concatenates two inputs into a byte stream. For $a_i \in \mathbb{Z}_q$, $\|a_i\|_\infty$ denotes $|a_i \bmod \pm q|$ (the absolute value of $(a_i \bmod \pm q)$). For a finite set S or a distribution D , $x \leftarrow S$ denotes random sampling of an element from the set S , and $x \leftarrow D$ denotes sampling x according to distribution D . $\lfloor z \rfloor$ means rounding down z and $\lceil z \rceil$ means rounding to the nearest integer of z .

B. CRYSTALS-Dilithium Signature Scheme

CRYSTALS-Dilithium is a post-quantum digital signature algorithm based on the hardness of MSIS and MLWE lattice problems. ML-DSA is derived from CRYSTALS-Dilithium. Algorithm 1, 2, and 3 specify the ML-DSA key generation, signature generation, and signature verification, respectively. The polynomial ring in ML-DSA is $\mathbb{Z}_q[x]/(x^n + 1)$, where $n = 256$, $q = 8380417$.

The function `NumberOfOne` means to count the number of 1’s in a vector of polynomials. For the details about the seed expansion functions `ExpandA`, `ExpandS` and `ExpandMask`, the rounding functions `Power2Round`, `HighBits`, `LowBits` and `Decompose`, and the hint functions `MakeHint` and `UseHint`, the generating c polynomial function `SampleInBall`, the reader can refer to the Dilithium standard draft [8].

Algorithm 1 ML-DSA.KeyGen()

Input: $\zeta \leftarrow \{0, 1\}^{256}$
Output: Public and secret keys $(pk = (\rho, t_1), sk = (\rho, K, tr, s_1, s_2, t_0))$

- 1: $(\rho, \rho', K) \in \{0, 1\}^{256} \times \{0, 1\}^{512} \times \{0, 1\}^{256} := H(\zeta)$ \triangleright H is instantiated as SHAKE-256
- 2: $\mathbf{A} \in \mathcal{R}_q^{k \times \ell} := \text{ExpandA}(\rho)$ \triangleright \mathbf{A} is generated and stored in NTT Representation as $\hat{\mathbf{A}}$
- 3: $(\mathbf{s}, \mathbf{e}) \in S_\eta^\ell \times S_\eta^k := \text{ExpandS}(\rho')$
- 4: $\mathbf{t} := \mathbf{As} + \mathbf{e}$ \triangleright Compute \mathbf{As} as $\text{NTT}^{-1}(\hat{\mathbf{A}} \circ \text{NTT}(\mathbf{s}))$
- 5: $(\mathbf{t}_1, \mathbf{t}_0) := \text{Power2Round}_{q, d}(\mathbf{t})$
- 6: $tr \in \{0, 1\}^{256} := H(\rho \| t_1)$
- 7: **return** $(pk = (\rho, t_1), sk = (\rho, K, tr, \mathbf{s}, \mathbf{e}, t_0))$

C. Hashing

The hash functions are two eXtendable Output Functions (XOF), namely SHAKE-256 and SHAKE-128 [32]. XOF maps an arbitrary-length bit string to a string of infinitely many bits. These XOF functions are mainly used for generating random bytes of SHAKE-128 to sample matrix \mathbf{A} and for generating random bytes of SHAKE-256 to sample \mathbf{s} , \mathbf{e} and \mathbf{y} .

Algorithm 2 ML-DSA.Sign(sk, M)

Input: Secret key $sk = (\rho, K, tr, \mathbf{s}, \mathbf{e}, t_0)$, Message $M \in \{0, 1\}^*$
Output: Signature $\sigma = (\tilde{c}, \mathbf{z}, \mathbf{h})$

- 1: $\mathbf{A} \in \mathcal{R}_q^{k \times \ell} := \text{ExpandA}(\rho)$ \triangleright \mathbf{A} is generated and stored in NTT Representation as $\hat{\mathbf{A}}$
- 2: $\mu \in \{0, 1\}^{512} := H(tr \| M)$
- 3: $\kappa := 0, (\mathbf{z}, \mathbf{h}) := \perp$
- 4: $\rho' \in \{0, 1\}^{512} := H(K \| \mu)$ (or $\rho' \leftarrow \{0, 1\}^{512}$ for randomized signing)
- 5: **while** $(\mathbf{z}, \mathbf{h}) = \perp$ **do** \triangleright Pre-compute $\hat{\mathbf{s}} := \text{NTT}(\mathbf{s}), \hat{\mathbf{e}} := \text{NTT}(\mathbf{e}),$ and $\hat{\mathbf{t}}_0 := \text{NTT}(t_0)$
- 6: $\mathbf{y} \in \tilde{S}_{\gamma_1}^\ell := \text{ExpandMask}(\rho', \kappa)$
- 7: $\mathbf{w} := \mathbf{Ay}$ $\triangleright \mathbf{w} := \text{NTT}^{-1}(\hat{\mathbf{A}} \circ \text{NTT}(\mathbf{y}))$
- 8: $\mathbf{w}_1 := \text{HighBits}_q(\mathbf{w}, 2\gamma_2)$
- 9: $\tilde{c} \in \{0, 1\}^{256} := H(\mu \| \mathbf{w}_1)$
- 10: $c \in B_\tau := \text{SampleInBall}(\tilde{c})$ \triangleright Store c in NTT representation as $\hat{c} = \text{NTT}(c)$
- 11: $\mathbf{z} := \mathbf{y} + cs$ \triangleright Compute cs as $\text{NTT}^{-1}(\hat{c} \circ \hat{\mathbf{s}})$
- 12: $\mathbf{r}_0 := \text{LowBits}_q(\mathbf{w} - ce, 2\gamma_2)$ \triangleright Compute ce as $\text{NTT}^{-1}(\hat{c} \circ \hat{\mathbf{e}})$
- 13: **if** $\|\mathbf{z}\|_\infty \geq \gamma_1 - \beta$ or $\|\mathbf{r}_0\|_\infty \geq \gamma_2 - \beta$ **then** $(\mathbf{z}, \mathbf{h}) := \perp$
- 14: **else**
- 15: $\mathbf{h} := \text{MakeHint}_q(-ct_0, \mathbf{w} - ce + ct_0, 2\gamma_2)$ \triangleright Compute ct_0 as $\text{NTT}^{-1}(\hat{c} \circ \hat{\mathbf{t}}_0)$
- 16: **if** $\|ct_0\|_\infty \geq \gamma_2$ or $\text{NumberOfOne}(\mathbf{h}) > \omega$ **then** $(\mathbf{z}, \mathbf{h}) := \perp$
- 17: $\kappa := \kappa + \ell$
- 18: **return** $\sigma = (\tilde{c}, \mathbf{z}, \mathbf{h})$

Algorithm 3 ML-DSA.Verify($pk, M, \sigma = (\tilde{c}, \mathbf{z}, \mathbf{h})$)

Input: Public key $pk = (\rho, t_1)$, Message $M \in \{0, 1\}^*$, Signature $\sigma = (\tilde{c}, \mathbf{z}, \mathbf{h})$
Output: Result $r \in \{0, 1\}$

- 1: $\mathbf{A} \in \mathcal{R}_q^{k \times \ell} := \text{ExpandA}(\rho)$ \triangleright \mathbf{A} is generated and stored in NTT Representation as $\hat{\mathbf{A}}$
- 2: $\mu \in \{0, 1\}^{512} := H(H(\rho \| t_1) \| M)$
- 3: $c := \text{SampleInBall}(\tilde{c})$
- 4: $\mathbf{w}' := \text{UseHint}_q(\mathbf{h}, \mathbf{Az} - ct_1 \cdot 2^d, 2\gamma_2)$ \triangleright Compute as $\text{NTT}^{-1}(\hat{\mathbf{A}} \circ \text{NTT}(\mathbf{z}) - \text{NTT}(c) \circ \text{NTT}(\mathbf{t}_1 \cdot 2^d))$
- 5: **return** $\tilde{c} = H(\mu \| \mathbf{w}')$ and $\|\mathbf{z}\|_\infty < \gamma_1 - \beta$ and $\text{NumberOfOne}(\mathbf{h}) \leq \omega$

D. Number Theoretical Transform

Polynomial multiplications are one of the most expensive parts in massive lattice-based cryptographic schemes. The commonly used technique to accelerate computation is the number theoretic transform (NTT). In Dilithium, the modulus q is chosen so that $q \equiv 1 \pmod{2n}$ and thus there exists a primitive $2n$ -th root of unity in \mathbb{Z}_q . Concretely, the recommended parameter setting is $q = 8380417$, $n = 256$ for the sake of security, and the expected primitive 512-th root of unity is $r = 1753$. The NTT algorithm maps $\mathbf{f} = f_0 + f_1x + \cdots + f_{255}x^{255} \in \mathbb{Z}_q[x]/(x^{256} + 1)$ to

$$\begin{aligned} & (\mathbf{f} \bmod \mathbb{Z}_q/(x^{128} - r^{128}), \mathbf{f} \bmod \mathbb{Z}_q/(x^{128} + r^{128})) \\ &= ((f_0 + r^{128}f_{128}) + \cdots + (f_{127} + r^{128}f_{255})x^{127}, \\ & \quad (f_0 - r^{128}f_{128}) + \cdots + (f_{127} - r^{128}f_{255})x^{127}) \\ & \in \mathbb{Z}_q[x]/(x^{128} - r^{128}) \times \mathbb{Z}_q[x]/(x^{128} + r^{128}) \end{aligned}$$

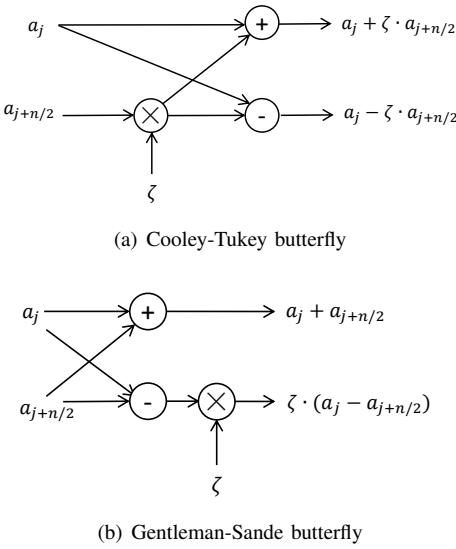
using FFT trick [33]. We call this transformation forward NTT (denoted as NTT from here on). To transform back from the NTT domain to the regular domain, the inverse NTT (denoted as NTT^{-1}) is computed. By recursively applying this, \mathbf{f} is transformed into its NTT form

$$\begin{aligned} \text{NTT}(\mathbf{f}) &= \hat{\mathbf{f}} = (\hat{f}_0, \dots, \hat{f}_{255}) \in \mathbb{Z}_q^{256} \\ \text{where } \hat{f}_i &= \mathbf{f} \bmod (x - r^{2i-1}) = f(r^{2i-1}), \quad i = 1, \dots, 255 \end{aligned}$$

Since the NTT transform is an isomorphism, we have

$$\mathbf{f} \circ \mathbf{g} = \text{NTT}^{-1}(\text{NTT}(\mathbf{f}) \circ \text{NTT}(\mathbf{g}))$$

Note that the direct output of NTT/ NTT^{-1} may not result in the natural order as presented, but in a “bit-reversed” order. However, each polynomial undergoes two times of bit reversal during NTT multiplication, one in NTT and one in NTT^{-1} , so the result finally turns out in the expected natural order. The core operation to split polynomial $\mathbb{Z}_q[x]/(x^{256} + 1)$ to polynomial $\mathbb{Z}_q[x]/(x^{128} - r^{128})$ and $\mathbb{Z}_q[x]/(x^{128} + r^{128})$ is Cooley-Tukey (CT) butterfly [34]. The NTT performs 128 CT butterflies to pairs of coefficients in every iteration of splitting. Each iteration is referred to as a level. Figure 1(a) depicts the CT butterfly. One might invert the FFT trick using Gentleman-Sande (GS) butterfly [35]. Figure 1(b) depicts the GS butterfly.

**Fig. 1:** Butterfly diagrams

Algorithm 4 A parallel index-based polynomial multiplication algorithm with translations

Input: (c, \mathbf{a}) , where $\mathbf{a} = [a^{(0)}, \dots, a^{(r-1)}]^T \in \mathcal{R}_q^r$, every $a^{(j)} = \sum_{i=0}^{n-1} a_i^{(j)} \cdot x^i \in \mathcal{R}_q$, and $c = \sum_{i=0}^{n-1} c_i \cdot x^i \in B_\tau$
Output: $\mathbf{u} = c \cdot \mathbf{a} = [u^{(0)}, \dots, u^{(r-1)}]^T \in \mathcal{R}_q^r$, where $u^{(j)} = c \cdot a^{(j)} = \sum_{i=0}^{n-1} u_i^{(j)} \cdot x^i \in \mathcal{R}_q$

- 1: **for** $i \in \{0, 1, \dots, n-1\}$ **do**
- 2: $w_i := 0$
- 3: $v_i := 0$
- 4: $v_{i-n} := 0$
- 5: **for** $j \in (0, 1, \dots, r-1)$ **do**
- 6: $v_i := v_i \cdot M + (U + a_i^{(j)})$
- 7: $v_{i-n} := v_{i-n} \cdot M + (U - a_i^{(j)})$
- 8: $\gamma := 2U \cdot \frac{M^{r-1}}{M-1}$
- 9: **for** $i \in \{0, 1, \dots, n-1\}$ **do**
- 10: **if** $c_i = 1$ **then**
- 11: **for** $j \in \{0, 1, \dots, n-1\}$ **do**
- 12: $w_j := w_j + v_{j-i}$
- 13: **if** $c_i = -1$ **then**
- 14: **for** $j \in \{0, 1, \dots, n-1\}$ **do**
- 15: $w_j := w_j + (\gamma - v_{j-i})$
- 16: **for** $i \in \{0, 1, \dots, n-1\}$ **do**
- 17: $t := w_i$
- 18: **for** $j \in (0, 1, \dots, r-1)$ **do**
- 19: $u_i^{(r-1-j)} := (t \bmod M) - \tau U(\bmod q)$
- 20: $t := |t/M|$
- 21: **return** $\mathbf{u} = [u^{(0)}, \dots, u^{(r-1)}]^T$

E. Parallel Small Polynomial Multiplication

As we shall see previously in Section II-B, one distinctive feature of the polynomial multiplication operations in Dilithium is that many of the time, one of the two multiplicands involved, namely $c \in B_\tau$, has exactly τ coefficients from 1, -1, the rest being 0. Multiplication by 1 or -1 can be reduced to an addition or subtraction with a sign-based conditional judgment. This is an optimized work presented in [20]. Algorithm 4 is the parallel small polynomial multipli-

cation (PSPM) algorithm, and one single call can compute several products of c and small polynomials, it can speed up the signing and verification of Dilithium. We call lines 1-7 of pseudocode in Algorithm 4 *preparing* process, lines 9-21 *evaluating* process.

F. AVX-512 Instruction Set

Intel Advanced Vector Extensions 512 (AVX-512) is the set of Intel's latest x86-64 vector instructions. AVX-512 adopts the SIMD vectorization parallel approach. Unlike the previous AVX2 instruction set, the size of the vector register is first expanded to 512 bits, and the number of vector registers is also increased from the previous 16 to 32 vector registers ($zmm0-zmm31$). The AVX-512 vector registers can store more values, and reduce the number of loads from memory to vector registers. In particular, there are eight mask registers in AVX-512 ($k0-k7$). The mask registers can be used to store the comparison results of two vector registers, enabling more comparison instructions in AVX-512. The mask register can be used for "maskmov" type instructions for masking load and store. Generally, we use this type of instructions to select the vector data lane within zmm registers we need to load or store. AVX-512 has many permutation instructions for adjusting the position of 16-bit, 32-bit, and 64-bit words residing in a zmm register. Such instructions are very important for implementing rejection sampling, NTT and NTT^{-1} , as we shall see. AVX-512F is a vector extension of the x86 instruction set architecture (ISA) that provides 512-bit vector operations, allowing the execution of up to 16 double-precision floating-point or 32 single-precision floating-point operations per cycle. AVX-512F also includes new instructions for integer operations, gather and scatter instructions, and support for masked operations, which allows operations to be selectively applied to vector elements. AVX-512IFMA is an extension to AVX-512F that provides instructions for integer multiplication using the Fused Multiply-Add (FMA) technique, which can perform two multiply-add operations in a single instruction. AVX-512IFMA provides two new IFMA instructions for 52-bit integer $vpmadd521uq$ and $vpmadd52huq$.

III. PSPM WITH TAILORED EARLY EVALUATION (PSPM-TEE)

The signing procedure employs conditional checks for the infinity norm \mathbf{z} , \mathbf{r}_0 , and $c\mathbf{t}_0$ to perform rejection sampling. Since these checks are performed over single coefficients, it is not necessary to compute all the polynomials of the vector. Instead, one polynomial is computed and checked immediately. If the check fails, further computation is unnecessary, saving significant computation time. The probability that $\|\mathbf{z}\|_\infty < \gamma_1 - \beta$ is $\left(\frac{2(\gamma_1 - \beta) - 1}{2\gamma_1 - 1}\right)^{256 \cdot \ell} = \left(1 - \frac{\beta}{\gamma_1 - 1/2}\right)^{\ell n} \approx e^{-256 \cdot \beta \ell / \gamma_1}$, and the probability of \mathbf{r}_0 in the good range is $\left(\frac{2(\gamma_2 - \beta) - 1}{2\gamma_2}\right)^{256 \cdot k} \approx e^{-256 \cdot \beta k / \gamma_2}$. It is worth noting that the majority of loop repetitions occur due to the infinity checks of \mathbf{z} and \mathbf{r}_0 . Therefore, we will only consider the probabilities of these two vectors. In previous implementations, the infinite norm of the vector \mathbf{z} was first evaluated, followed by the

evaluation of the infinite norm of vector \mathbf{r}_0 . In this paper, for the first time, we propose to adjust the order of evaluation of vector \mathbf{z} and vector \mathbf{r}_0 based on the different rejection probabilities of vector \mathbf{z} and vector \mathbf{r}_0 for different parameters of Dilithium. We can compute the probabilities of the two conditional checks for three parameter sets. As shown in Table I, the probability of vector \mathbf{z} falling within a good range is always greater than the probability of vector \mathbf{r}_0 . Hence, checking \mathbf{r}_0 prior to checking \mathbf{z} can result in a faster signature procedure since repetition is more likely to occur after checking \mathbf{r}_0 and the computation of \mathbf{z} can be saved. We tested the performance of the Dilithium C REF implementation between checking \mathbf{r}_0 first and checking \mathbf{z} first. We observe that checking \mathbf{r}_0 before checking \mathbf{z} results in a 2% to 3% improvement in the signing procedure, as demonstrated in Table II. The idea of first evaluating the infinite norm of the vector with higher rejection probability is applicable to signature schemes that use rejection sampling.

The parallel algorithm presented in [20] poses difficulties for *early-evaluation* as it calculates the entire polynomial vector multiplication results simultaneously. To overcome this issue, we introduce a PSPM algorithm in this section that incorporates early evaluation. Our algorithm includes the computation of $c \cdot \mathbf{s} + \mathbf{y}$ and $\text{LowBits}(\mathbf{w} - c \cdot \mathbf{e}, 2\gamma_2)$ in the evaluating process, enabling us to promptly perform reject checks for each coefficient. If the reject checks fail, the computation is terminated. This approach results in faster signature speeds. Additionally, there are various PSPM algorithms available. In Dilithium3/5, the coefficients of \mathbf{s} and vector \mathbf{e} are stored in separate precomputed tables, allowing for independent early checks of \mathbf{z} and \mathbf{r}_0 . In contrast, Dilithium2 stores the coefficients of \mathbf{s} and \mathbf{e} in the same precomputed table. Consequently, the early checks for \mathbf{z} and \mathbf{r}_0 are performed simultaneously, as depicted in Algorithm 5. It is important to note that during rejection checks, verifying the \mathbf{r}_0 always takes precedence over checking vector \mathbf{z} for all three parameter sets of Dilithium, as previously analyzed.

TABLE I: Probability of vector in a good range.

Scheme	$\Pr(\ \mathbf{z}\ \leq \gamma_1 - \beta)$	$\Pr(\ \mathbf{r}_0\ \leq \gamma_1 - \beta)$
Dilithium2	0.543591	0.429801
Dilithium3	0.619647	0.315712
Dilithium5	0.663515	0.389636

TABLE II: Comparative performance of checking \mathbf{z} first and checking \mathbf{r}_0 first (Cycles).

Scheme	Round3 C REF		Imp. (%)
	(check \mathbf{z} first)	(check \mathbf{r}_0 first)	
Dilithium2	992696	972244	2.06%
Dilithium3	1670374	1627560	2.56%
Dilithium5	2088720	2026818	2.96%

TABLE III: Comparative performance of improved PSPM and original PSPM [20] (Cycles).

Scheme	Sign (Original PSPM)	Sign (Improved PSPM)	Imp. (%)
Dilithium2	670970	636326	5.16%
Dilithium3	1171086	1101330	6.00%
Dilithium5	1491124	1415452	5.07%

Algorithm 5 A parallel index-based polynomial multiplication algorithm with early evaluating \mathbf{r}_0 and \mathbf{z} for Dilithium2

Input: $(c, \mathbf{s}, \mathbf{e}, \mathbf{y}, \mathbf{w})$, where $\mathbf{s} = [s^{(0)}, \dots, s^{(l-1)}]^T \in \mathcal{R}_q^l$, $\mathbf{y} \in \mathcal{R}_q^l$, $\mathbf{e} \in \mathcal{R}_q^k$, $\mathbf{w} \in \mathcal{R}_q^k$, every $s^{(j)} = \sum_{i=0}^{n-1} s_i^{(j)} \cdot x^i \in \mathcal{R}_q$, $y^{(j)} = \sum_{i=0}^{n-1} y_i^{(j)} \cdot y^i \in \mathcal{R}_q$, $e^{(j)} = \sum_{i=0}^{n-1} e_i^{(j)} \cdot e^i \in \mathcal{R}_q$, $w^{(j)} = \sum_{i=0}^{n-1} w_i^{(j)} \cdot w^i \in \mathcal{R}_q$, and $c = \sum_{i=0}^{n-1} c_i \cdot x^i \in B_\tau$
Output: $\mathbf{z} = c \cdot \mathbf{s} + \mathbf{y} = [z^{(0)}, \dots, z^{(l-1)}]^T \in \mathcal{R}_q^l$, where $z^{(j)} = c \cdot s^{(j)} + y^{(j)} = \sum_{i=0}^{n-1} z_i^{(j)} \cdot x^i \in \mathcal{R}_q$, $\mathbf{r} = \mathbf{w} - c \cdot \mathbf{e} = [r^{(0)}, \dots, r^{(k-1)}]^T \in \mathcal{R}_q^k$, where $r^{(j)} = w^{(j)} - c \cdot e^{(j)} = \sum_{i=0}^{n-1} r_i^{(j)} \cdot x^i \in \mathcal{R}_q$

```

1: for  $i \in \{0, 1, \dots, n-1\}$  do
2:    $m_i := 0$ 
3:    $v_i := 0$ 
4:    $v_{i-n} := 0$ 
5:   for  $j \in (0, 1, \dots, l-1)$  do
6:      $v_i := v_i \cdot M + (U + s_i^{(j)})$ 
7:      $v_{i-n} := v_{i-n} \cdot M + (U - s_i^{(j)})$ 
8:   for  $j \in (0, 1, \dots, k-1)$  do
9:      $v_i := v_i \cdot M + (U + e_i^{(j)})$ 
10:     $v_{i-n} := v_{i-n} \cdot M + (U - e_i^{(j)})$ 
11:    $\gamma := 2U \cdot \frac{M^{l+k-1}}{M-1}$ 
12:   for  $i \in \{0, 1, \dots, n-1\}$  do
13:     if  $c_i = 1$  then
14:       for  $j \in \{0, 1, \dots, n-1\}$  do
15:          $m_j := m_j + v_{j-i}$ 
16:     if  $c_i = -1$  then
17:       for  $j \in \{0, 1, \dots, n-1\}$  do
18:          $m_j := m_j + (\gamma - v_{j-i})$ 
19:   for  $i \in \{0, 1, \dots, n-1\}$  do
20:      $t := m_i$ 
21:     for  $j \in (0, 1, \dots, k-1)$  do
22:        $r_i^{(k-1-j)} := (t \bmod M) - \tau U \pmod q$ 
23:        $r_i^{(k-1-j)} := w_i^{(k-1-j)} - r_i^{(k-1-j)}$ 
24:        $r_i^{(k-1-j)} := \text{LowBits}_q(r_i^{(k-1-j)}, 2\gamma_2)$ 
25:       if  $|r_i^{(k-1-j)}| \geq \gamma_2 - \beta$  then Restart signature process.
26:        $t := \lfloor t/M \rfloor$ 
27:     for  $j \in (0, 1, \dots, l-1)$  do
28:        $z_i^{(l-1-j)} := (t \bmod M) - \tau U \pmod q$ 
29:        $z_i^{(l-1-j)} := z_i^{(l-1-j)} + y_i^{(l-1-j)}$ 
30:       if  $|z_i^{(l-1-j)}| \geq \gamma_1 - \beta$  then Restart signature process.
31:        $t := \lfloor t/M \rfloor$ 
32:   return  $\mathbf{z} = [z^{(0)}, \dots, z^{(l-1)}]^T, \mathbf{r} = [r^{(0)}, \dots, r^{(k-1)}]^T$ 

```

IV. TAILORED REDUCTION

We present an optimized modular reduction tailored for Dilithium modulus $q = 8380417$, which might be of independent interest and can be applied to optimize the implementations of Dilithium in other platforms. The modulus q can be represented as $2^{23} - 2^{13} + 1$. We can apply a fast specialized reduction algorithm for modulus prime having such a form.

We exemplify with the Dilithium prime and the process is shown in Algorithm 6.

Algorithm 6 Tailored reduction for the Dilithium prime $q = 2^{23} - 2^{13} + 1$

Require: $-2^{40} < z \leq 2^{40}$, $q = 2^{23} - 2^{13} + 1$

Ensure: $r = z \pmod{q}$, $-2^{31} < r < 2^{31}$

1: $p_1 = \lfloor \frac{z}{2^{23}} \rfloor$

2: $r = z - qp_1$

Proposition 1. If $-2^{40} < z \leq 2^{40}$, then Algorithm 6 computes an integer r congruent to z modulo $q = 2^{23} - 2^{13} + 1$ such that $-2^{31} < r \leq 2^{31}$.

Proof. If $-2^{40} < z \leq 2^{40}$, in line 1, $p_1 = \lfloor z/2^{23} \rfloor < 2^{17}$, let $r_1 = z - 2^{23}p_1 < 2^{23}$, $r = z - qp_1 = z - (2^{23} - 2^{13} + 1)p_1 = (2^{13} - 1)p_1 + r_1$, so

$$|r| \leq |(2^{13} - 1)p_1| + |r_1| \leq (2^{13} - 1)2^{17} + 2^{23} < 2^{31}.$$

□

Algorithm 7 Signed Montgomery reduction for 32-bit q [33]

Require: $0 < q < 2^{31}$ odd, $-2^{31}q \leq z = z_12^{32} + z_0 < 2^{31}q$ where $0 \leq z_0 < 2^{32}$

Ensure: $r' \equiv \beta^{-1}z \pmod{q}$, $-q < r' < q$

1: $m \leftarrow z_0q^{-1} \pmod{\pm 2^{32}}$ ▷ signed low product, q^{-1} precomputed

2: $t_1 \leftarrow \left\lfloor \frac{mq}{\beta} \right\rfloor$ ▷ signed high product

3: $r' \leftarrow z_1 - t_1$

A. Comparisons

Montgomery reduction is an efficient algorithm to reduce product in NTT by computing Hensel remainder. The disadvantage of Montgomery reduction is the Hensel remainder r' is congruent to $z \cdot 2^{-32} \pmod{q}$ instead of representative of the residue class of z modulo q . Algorithm 7 presents the pseudocode of Signed Montgomery reduction. This operation involves two bit-shiftings, two multiplications, and one subtraction. In contrast, our Tailored reduction algorithm is more efficient as it only requires one bit-shifting, one subtraction, and one multiplication. This makes it a better choice than Montgomery reduction when dealing with products smaller than 2^{40} for NTT with lazy reduction. Furthermore, the Tailored reduction can be implemented with the new AVX-512IFMA instruction in just two instructions, resulting in a lower latency during reduction (see Subsection V-C for a detailed discussion).

V. IMPLEMENTATION DETAILS

We present an optimized vectorization implementation of Dilithium for CPUs that both support the AVX2 and AVX-512 instruction sets. In this section, we will thoroughly explore the implementation details of each optimized module.

TABLE IV: Percentages of used functions in Keygen, Signature and Verification.

Functions	Keygen	Sign	Verify
montgomery_reduce	38.24%	23.02%	16.04%
KeccakF1600_StatePermute	17.68%	38.84%	42.99%
invtt_tomont	17.48%	6.28%	5.22%
ntt	6.94%	9.30%	3.35%
poly_pointwise_montgomery	4.96%	1.86%	2.22%

A. Dilithium Software Performance Profiling

A critical step in software optimization is to identify the performance bottlenecks of the algorithm. In this section, we utilize the Linux performance analysis tool perf to profile the Dilithium C REF implementation of Dilithium3 parameter set. The performance data was collected by executing the Dilithium3 codes 1000 times and calculating the average execution time. Table IV depicts the detailed percentages. KeccakF1600_StatePermute which is predominantly used in hash functions, is the most time-consuming function in key generation, signing, and verification. This is followed by Montgomery reduction and poly_uniform and poly_uniform_eta, and then NTT and NTT⁻¹. The functions of poly_uniform and poly_uniform_eta are used to sample coefficients using the rejection sampling method, while the functions of NTT, NTT⁻¹ and Montgomery reduction are used for polynomial multiplication. Consequently, we can identify the computation bottleneck functions as polynomial multiplication, hash function, and rejection sampling. In the following sections, we propose a series of optimization techniques for these functions.

B. Data Alignment

We represent each polynomial as an array of 256 32-bit signed integers. For this representation, we can use the AVX-512 SIMD instruction to vectorize different functions. Alternatively, we can represent this array as an array of 16 512-bit vectors of type `__m512i` in AVX-512 intrinsics, where the symbol “i” represents integers. In AVX-512 assembly, we store the 256 coefficients in 16 `zmm` vector registers. The 512-bit Intel AVX-512 registers have an alignment requirement of 64 bytes to ensure optimal vectorization. Optimal memory access is achieved when the data starts at an address on a 64-byte boundary, which means that the address in memory is divisible by 64. Therefore, we align all arrays to 64 bytes in our implementation.

C. Vectorization of NTT with AVX-512

We now give details about our AVX-512 parallel implementation of NTT for Dilithium polynomial ring $\mathbb{Z}_q[x]/(x^n + 1)$, where $n = 256$, $q = 8380417$, the modulus q is a 32-bit prime. The whole NTT-based polynomial multiplication is divided into three parts, NTT, NTT⁻¹, and point-wise multiplication.

a) *Register allocation:* Here we introduce our register arrangement. Note that AVX-512 has 32 512-bit vector zmm registers ($\text{zmm}0\text{-}\text{zmm}31$). If a 32-bit integer is directly stored in a zmm vector register without zero-padded, a zmm register can store 16 32-bit coefficients, and hence 16 vector registers are enough to load all 256 coefficients. In doing so, we merge the eight levels without reloading coefficients. Later in the implementation of the butterfly implementation, we will carefully explain why there is no need to reserve 64-bit space for intermediate products. We arrange $\text{zmm}1\text{-}\text{zmm}16$ to store all the polynomial coefficients consecutively. We use $\text{zmm}17$ to store the precomputed results $\zeta q^{-1} \bmod 2^{32}$, and $\text{zmm}18$ to store ζ (ζ is the twiddle factor). The $\text{zmm}19$, $\text{zmm}20$, and $\text{zmm}21$ are used to store temporary computation values.

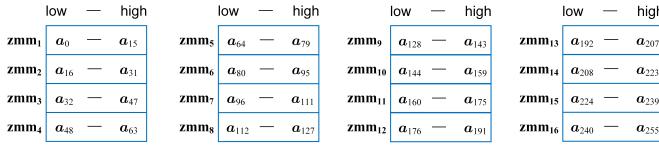


Fig. 2: The storage coefficients order in zmm registers

b) *Coefficients loading and shuffling:* We exemplify a polynomial $a_0 + a_1x + \dots + a_{255}x^{255}$ as input of NTT. Before the first level, we load the consecutive 16 coefficients in every zmm register as shown in Figure 2. In the first level, the distance of CT butterfly is 128. So the two vector registers $\text{zmm}1$ and $\text{zmm}9$ perform a pair of butterfly operations, and $\text{zmm}2$ and $\text{zmm}10$ perform a pair of butterfly operations; that is, the subscript distance of zmm register is 8. In the second level, the distance is 64. The corresponding registers subscript distance becomes 4. Analogously, the registers subscript distances in the third level and fourth level are two and one respectively. Starting from the fifth level, the distance is 8 while a consecutive 16 coefficients reside in a zmm register. Therefore, in the fifth level, we need to swap the upper 8 coefficients of one register with the lower 8 coefficients of another register. After the fifth level, coefficients are stored in a permuted order in registers. In the sixth level, the distance is 4. The upper four coefficients and the lower four coefficients in every 256-bit data lane are shuffled. Similarly, two coefficients are swapped in every 128-bit data lane in the seventh level and one coefficient is shuffled in every 64-bit data lane in the eighth level. The shuffling process is illustrated in Figure 3(a), Figure 3(b), and Figure 3(c). **Shuffle8** means to shuffle 8 coefficients, **Shuffle4** means to shuffle 4 coefficients, **Shuffle2** means to shuffle 2 coefficients, and **Shuffle1** means to shuffle one coefficient. We implement **Shuffle8** using the `vshufi32x4` instruction. The function of this instruction is to rearrange each 128-bit data lane of the two vector registers \mathbf{a} and \mathbf{b} through an 8-bit immediate value. We want to rearrange eight consecutive coefficients, which correspond to a 128-bit data lane. According to the instruction pseudocode¹, we set the immediate value to `0x44` and `0xEE`.

The shuffling of the four coefficients is more complicated because at this time the four consecutive coefficients

¹<https://www.intel.com/content/www/us/en/docs/intrinsics-guide/index.html>

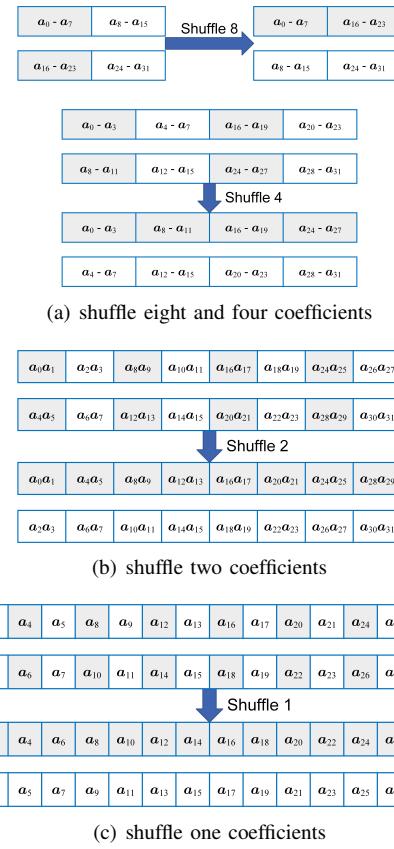


Fig. 3: Coefficients shuffling in two vector registers

correspond to a 64-bit data lane. Here we use two permute instructions, one is `vpermq` and the other is `vpblendmd`. First, we splice the lower 64-bit in register \mathbf{a} and the lower 64-bit in register \mathbf{b} using `vpblendmd`. However, this instruction can only be spliced by the value of the mask register according to the index. Specifically, if we use the `vpblendmd` directly, the order of the coefficients we will obtain is $\{a_0, a_1, a_2, a_3, b_4, b_5, b_6, b_7, a_8, a_9, a_{10}, a_{11}, b_{12}, b_{13}, b_{14}, b_{15}\}$. This is not the order we want. Therefore, we duplicate the lower 64-bit to the upper 64-bit of register \mathbf{b} in every 128-bit data lane and duplicate the upper 64-bit to the lower 64-bit of register \mathbf{a} in every 128-bit data lane. We implement this by using `vpermq` with constant argument `0x4E` and then using the `vpblendmd` instruction to splice the 64-bit data lane in the two registers through the mask register. Here, we use the `kmovw` instruction to store `0x0F0F` into mask register $k6$. For the permutation of two coefficients, we use `vpunpcklqdq` and `vpunpckhqdq`. For the shuffling of one coefficient, because there is no ready-made instruction that can be realized, we adopt the same idea as shuffling four coefficients. First, the upper 32 bits of every 64 bits data lane in register \mathbf{b} are obtained by shifting 32 bits to the left. Then use the `vpblendmd` to splice 32 bits of the two registers with mask register value `0xAAAA`. For copying the upper 32-bit to the lower 32-bit, we directly use the `vmovshdup` to copy the upper 32-bit.

c) *Butterflies:* In Section II-D, we introduce NTT and CT/GS butterflies. In the CT butterfly transform, half of the

coefficients need to be multiplied by the twiddle factors. Note that the twiddle factors are fixed constants, so we precompute their values and store them in a look-up table. As mentioned earlier, to save multiplication in Montgomery reduction, we also precompute $\zeta q^{-1} \bmod 2^{32}$ and store them in the look-up table. Here we would like to explain why it is not necessary to reserve 64-bit for multiplication results. At the start, the 16 consecutive coefficients are loaded into a zmm register. During the butterfly operation calculation, we split the coefficients that need to be multiplied by the twiddle factor into two parts according to the odd and even subscripts. The odd and even subscript coefficients are stored in two zmm registers. The odd/even coefficient splitting is achieved by copying the upper 32 bits using `vmovshdup` instruction. After splitting, a register only stores eight coefficients, and each coefficient occupies 64 bits of space. Thus, there is no need to reserve 64 bits of space when loading. Finally, it is reduced to 32-bit by Montgomery reduction. Then the odd-index and even-index coefficients are spliced into a 512-bit vector register by `vpblendmd` instruction. In this way, although the splitting operation takes some clock cycles, it ensures the maximum degree of parallelism. Generally speaking, this implementation idea is faster than the idea of loading zero-padded 64-bit integers in [31].

Algorithm 8 2-instruction Tailored reduction using AVX512IFMA

Input: A 40-bit signed integer $-2^{40} < z \leq 2^{40}$
Output: $r = z(\bmod q), -2^{31} < r < 2^{31}$

- 1: `vpsrlq` $23, z, r$
- 2: `vpmadd52luq` $-q, z, r$ $\triangleright z - \frac{z}{2^{23}} \cdot q$
- 3: **return** r

Algorithm 9 3-instruction Tailored reduction using AVX512

Input: A 40-bit signed integer $-2^{40} < z \leq 2^{40}$
Output: $r = z(\bmod q), -2^{31} < r < 2^{31}$

- 1: `vpsrlq` $23, z, r$
- 2: `vpmuldq` q, z, t $\triangleright t = \frac{z}{2^{23}} \cdot q$
- 3: `vpsubq` t, z, r $\triangleright r = z - t$
- 4: **return** r

d) Vectorized Tailored reduction: We present a vectorized Tailored reduction implementation using AVX-512IFMA instruction. We use this vectorized Tailored reduction implementation in $\text{NTT}(\mathbf{t}_0)$ and $\text{NTT}(\mathbf{t}_1)$. Previous work implements a four-instruction Montgomery reduction that is both suited for AVX2 and AVX-512 vectorized implementation. The total latency of these four instructions is 12 cycles. In this work, we present a 2-instruction Tailored reduction using AVX-512IFMA `vpmadd52luq` instruction that can reduce both latency and instruction count and shown in Algorithm 8. This vectorized Tailored reduction reduces the cycle counts down to 6 cycles by eliminating one `vpmuldq` and one `vpsubq`.

Algorithm 10 4-instruction Montgomery reduction using AVX512 [14]

Input: A signed integer $-2^{31}q < z \leq 2^{31}q$
Output: $r' = 2^{-32}z(\bmod q), -q < r' < q$

- 1: `vpmuldq` q^{-1}, z, m $\triangleright m = z \bmod 2^{32} \cdot q$
- 2: `vpmuldq` q, m, t $\triangleright t = m \bmod 2^{32} \cdot q$
- 3: `vpsubq` t, z, r'
- 4: `vpsrlq` $32, r', r'$ $\triangleright r' = z - t$
- 5: **return** r'

e) Lazy reduction: Dilithium involves NTT operations on polynomials with small coefficients. We observe that, for CT butterfly of NTT with small coefficients such as c and the noise vectors \mathbf{s} and \mathbf{e} , the first level does not need to perform Montgomery reduction, because the upper bound data width of \mathbf{s}/\mathbf{e} is 4 bits, and the multiplication of a 4-bit coefficient and a 23-bit twiddle factor will not exceed 32 bits. c is a small polynomial with only $\tau \pm 1$, so the product of a 1-bit coefficient and a 23-bit twiddle factor will not exceed 32 bits as well. Specifically, we do not need to perform modular reductions in the first level of $\text{NTT}(c)$, $\text{NTT}(\mathbf{s})$ and $\text{NTT}(\mathbf{e})$. For $\text{NTT}(\mathbf{t}_0)$ and $\text{NTT}(\mathbf{t}_1)$ in all the three security levels of Dilithium2/3/5, as well as $\text{NTT}(\mathbf{y})$ in Dilithium2, in the first level of NTT we only need to perform the above tailored reduction algorithm instead of Montgomery reduction. For instance, in Dilithium2, where $\gamma_1 = 2^{17}$, the data width of vector \mathbf{y} is 18-bit. The product of vector \mathbf{y} and the twiddle factor multiplication is a 41-bit integer in $(-2^{40}, 2^{40}]$. Hence, we use the Tailored reduction Algorithm 6 proposed above. Specifically, in this case, we do not need to completely reduce the coefficient to \mathbb{Z}_q in the first level of NTT, our only requirement is to prevent the coefficient from overflowing. Starting from the second level, the product will be reduced by Montgomery reduction.

D. Hashing

Dilithium makes use of XOF to expand seeds and sample polynomials. SHAKE-128 is used to generate matrix \mathbf{A} , and SHAKE-256 is used to generate vectors \mathbf{s}, \mathbf{e} and \mathbf{y} . As we discussed in Section V-A, hashing is an expensive operation in the entire scheme. The previous AVX2 implementation used a 4-way SHAKE-128 and SHAKE-256; that is, they use a vectorized SHAKE implementation that operates on 4 parallel sponges and hence can absorb and squeeze blocks in and out of these 4 sponges at the same time [14]. We use the AVX-512 implementation and can calculate and generate 8 hash results at the same time due to the expansion of the register bit width. We embedded this 8-way hash implementation into the expansion of matrix \mathbf{A} , vector \mathbf{y} , and vector \mathbf{s}, \mathbf{e} . Dilithium uses SHAKE-256 to generate arbitrary length random bytes which is the function H . We implement the SHAKE-256 using AVX-512. We use five zmm registers to store the 1600-bit keccak state. Each register stores five 64-bit states in its five 64-bit data lanes, while the remaining three data lanes are zero. In this way, we can achieve 5-way parallelism compared with sequential implementation using C.

E. Parallel Rejection Sampling

The rejection sampling process generates a 23-bit random number by sampling and then checks whether it is greater than or less than q using conditional judgment. If the number is greater than q , it is rejected, and if it is less than q , it is accepted. To obtain the 23-bit random number, the byte stream obtained by hashing needs to be spliced, and then the random number is accepted or rejected sequentially. This process poses a challenge to vectorizing rejection sampling. The previous method used by AVX2 was to create a two-dimensional array of size $2^8 \times 8 = 2048$, which stored all possible acceptance positions for 8 32-bit integers in a 256-bit vector register. However, this method is not suitable for AVX-512 implementation because a vector register in AVX-512 can store 16 32-bit integers, requiring a two-dimensional array of size $2^{16} \times 16 = 1048576$, which is not feasible for AVX-512 implementation. Therefore, a more space-efficient implementation method was used.

One of the main concepts of rejection sampling is to compare numbers in all positions with q and then store them in order. Fortunately, AVX-512 has a built-in function called `_mm512_mask_compressstoreu_epi32`, which stores 32-bit integers in their corresponding positions sequentially through the values of the mask register. This allows us to compressively store the values and meet our requirements. The function is described in Figure 4. We can also set the mask register using the function `_mm512_cmp_epi32_mask`. By setting the comparison operand value of the `_mm512_cmp_epi32_mask` function to `_MM_CMPINT_LT`, we compare the values of the input vector register `a` and vector register `b`. If `a` is smaller than `b`, we set the value of the mask register at the corresponding position to 1, otherwise, we set it to 0. Note that the mask register is a 16-bit binary integer. We can determine how many coefficients are received in a vector register by counting the number of 1's in the mask register using the function `_mm_popcnt_u32`.

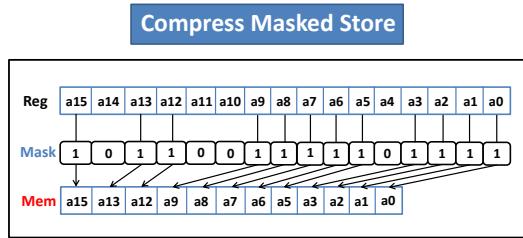


Fig. 4: The `_mm512_mask_compressstoreu_epi32` function.

We optimized the vectorized implementation of generating 23-bit random integers to reduce the number of calls to SHAKE-128. Since we only need 48 out of the 64 bytes streams loaded to obtain 16 23-bit numbers, we should avoid wasting the extra 16 bytes generated by SHAKE-128.

To achieve this, we first initialize a vector register with all zeros, and then use the functions `_mm512_permutexvar_epi8` and

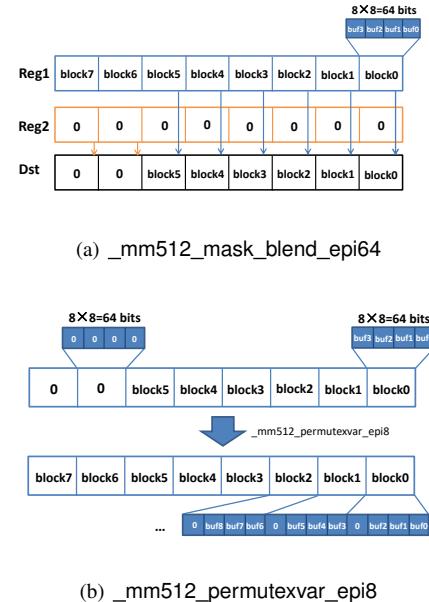


Fig. 5: Packing random byte stream

`_mm512_mask_blend_epi64` to adjust and splice this all-0 register and the register loaded with 64-byte random byte streams. We illustrate this process in Figure 5(a) and Figure 5(b). The upper $6 \times 64 = 384$ bits are the random byte streams, and the lower $2 \times 64 = 128$ bits are zeros. By adjusting the order of the spliced vector registers in the 8-bit data lane using the function `_mm512_permutexvar_epi8`, we can obtain three consecutive random bytes of every four bytes, and the last byte of the four bytes is just 0. Then, we use `_mm512_and_si512` to perform a bitwise AND with 23 ones to obtain 16 23-bit random integers.

The above describes the rejection sampling process for generating numbers in the range $[0, q]$. However, in Dilithium, there is also rejection sampling of numbers in the range $[-\eta, \eta]$. We have also optimized the previous AVX2 implementation for this purpose. In our implementation, we first separate the high 4 bits and low 4 bits of each 8-bit random byte, and then use the `_mm512_cmp_epi32_mask` function to judge and store the high 4 bits and low 4 bits separately using mask registers. To ensure the correctness of the test vector, we also adjust the order of the high 4 bits and low 4 bits accordingly.

F. Expanding Matrix A and Sampling Vectors

We present an 8-way `poly_uniform_8x` function to sample 8 polynomials in R_q simultaneously, using 8-way SHAKE-128 and parallel rejection sampling. For the expansion of matrix A , in Dilithium2 where $k = l = 4$, we can directly call the `poly_uniform_8x` function twice to generate 4 row vectors. In Dilithium3, where $k = 6, l = 5$, `poly_uniform_8x` is called four times to generate 30 polynomials of 6 row vectors. In Dilithium5, `poly_uniform_8x` is called eight times to generate 56 polynomials of 8 row vectors. Similarly, for sampling vectors, we propose an 8-way function `poly_uniform_eta_8x` and `poly_uniform_gamma1_8x`

using 8-way SHAKE-256 to sample vectors \mathbf{s}/\mathbf{e} and \mathbf{y} respectively.

G. Implementing PSPM-TEE

This work implements AVX2 and AVX-512 for PSPM-TEE. In original PSPM implementation from [20], coefficients were packed into 64-bit words. However, to ensure consistency in the data lane of the vector register and make it easier to operate on the same size operand, we chose to pack coefficients into 32-bit words. This eliminates the need to zero-extend 32-bit coefficients to 64-bit and simplifies the vectorization of PSPM implementation. For Dilithium2/3/5, we provide a specific description of the implementation of the parallel small polynomial algorithm for Dilithium3 parameters, where $k = 6, l = 5$. Our implementation is based on the parallel small polynomial parameter sets shown in Table XII.

TABLE V: Performance comparison of 32-bit version and 64-bit version PSPM.

Operation	Scheme	32-bit version (Cycles)	64-bit version (Cycles)
Preparing $\mathbf{s} \mathbf{e}$	Dilithium2	264	536
	Dilithium3	320	378
Preparing \mathbf{s}	Dilithium5	440	918
	Dilithium3	338	448
Preparing \mathbf{e}	Dilithium5	486	1052
	Dilithium3	5358	5800
Evaluating $\mathbf{cs} \mathbf{ce}$	Dilithium3	3760	5160
	Dilithium5	4794	6502
Evaluating \mathbf{cs}	Dilithium3	6280	7846
	Dilithium5	3156	4892

Firstly, we introduce the splicing of the noise vector \mathbf{s}, \mathbf{e} . Although each coefficient of \mathbf{s} and \mathbf{e} lies in the range of $[-4, 4]$, the coefficients grow by $2\tau U$ after the addition operation in Algorithm 4, where $U = 4, \tau = 49$ in Dilithium3. As a result, the upper bound of coefficients is 392. Therefore, each coefficient needs to set aside at least 9 bits for storage. One 32-bit word can pack up to 3 polynomial coefficients. Therefore, vectors \mathbf{s}, \mathbf{e} need two precomputed tables to store all coefficients.

The preparing process is implemented using intrinsic functions because it is easily vectorizable. However, the loop operation in Algorithm 4 is not suitable for parallel implementation. Therefore, our AVX-512 implementation uses parallel computing to implement the accumulation process through AVX-512 assembly. Specifically, when determining whether challenge polynomial c is 1 or -1, we pass the corresponding array address to AVX-512 assembly and perform parallel addition. Combining with the parallelism achieved by Algorithm 5, the implementation of \mathbf{cs} can achieve a maximum of $8 \times 3 = 24$ parallelism at most.

We implemented the evaluating process of extracting computation results from the 32-bit packed words using the intrinsic functions. To perform the conditional check of vector coefficients, we used the `_mm512_cmp_ep132_mask` function, which allows us to check 8 coefficients in parallel and obtain a 16-bit mask for every 32-bit data lane. If the mask is non-zero, the function immediately returns 1.

```

void polyw1_pack(uint8_t * restrict r, const poly * restrict a) {
    unsigned int i;
    __m512i f0, f1, f2, f3, f4, f5, f6, f7;
    const __m512i shift = _mm512_set1_epi16((16 << 8) + 1);
    const __m512i shufbidx1 = _mm512_set_epi32(15, 11, 7, 3, 14, 10, 6, 2, 13, 9, 5, 1, 12, 8, 4, 0);
    const __m512i shufbidx = _mm512_set_epi8(15, 14, 11, 10, 7, 6, 3, 2, 13, 12, 9, 8, 5, 4, 1, 0,
                                              15, 14, 11, 10, 7, 6, 3, 2, 13, 12, 9, 8, 5, 4, 1, 0,
                                              15, 14, 11, 10, 7, 6, 3, 2, 13, 12, 9, 8, 5, 4, 1, 0);

    for(i = 0; i < N/128; ++i) {
        [128*i+64] a->coeffs[128*i+80] a->coeffs[128*i+96] a->coeffs[128*i+112]
        f0 = _mm512_loadu_si1512(&a->coeffs[128*i+0]);
        f1 = _mm512_loadu_si1512(&a->coeffs[128*i+16]);
        f2 = _mm512_loadu_si1512(&a->coeffs[128*i+32]);
        f3 = _mm512_loadu_si1512(&a->coeffs[128*i+48]);
        f4 = _mm512_loadu_si1512(&a->coeffs[128*i+64]);
        f5 = _mm512_loadu_si1512(&a->coeffs[128*i+80]);
        f6 = _mm512_loadu_si1512(&a->coeffs[128*i+96]);
        f7 = _mm512_loadu_si1512(&a->coeffs[128*i+112]);
        f0 = _mm512_packus_epi32(f0,f1);
        f1 = _mm512_packus_epi32(f2,f3);
        f2 = _mm512_packus_epi32(f4,f5);
        f3 = _mm512_packus_epi32(f6,f7);
        f0 = _mm512_packus_epi16(f0,f1);
        f1 = _mm512_packus_epi16(f2,f3);
        f0 = _mm512_maddubs_epi16(f0,shift);
        f1 = _mm512_maddubs_epi16(f1,shift);
        f0 = _mm512_packus_epi16(f0,f1);
        f0 = _mm512_permutexvar_epi32(shufbidx1,f0);
        f0 = _mm512_shuffle_epi8(f0,shufbidx);
        _mm512_storeu_si512(&r[64*i], f0);
    }
}

```

Fig. 6: Packing w_1 function using AVX-512.

H. Vectorized Packing

a) Obstacle in vectorizing packing: In Dilithium implementation, polynomial vectors need to be encoded as byte strings (packing) and vice versa (unpacking). We have completed the vectorization of unpacking of \mathbf{z} and packing of \mathbf{w}_1 using AVX-512. To ensure that our optimized implementation works on all platforms and matches the NIST Known Answer Tests (KAT) test vectors, we faced a difficulty in vectorizing polynomial packing and unpacking. Directly vectorizing the packing/unpacking process is not feasible. For instance, a 512-bit vector register can store 16 coefficients, and bit-wise instructions are operated on two vector registers. If register r_1 stores coefficients $a_0 - a_{15}$, r_2 stores coefficients $a_{16} - a_{31}$. A pair of coefficients a_0 and a_{16} are packed, whereas we need a_0 and a_1 . Therefore, direct vectorization is not possible.

b) How to vectorize packing: The vectorization of unpacking \mathbf{z} using AVX-512 is similar to parallel rejection sampling. For packing of \mathbf{w}_1 . We take Dilithium3/5 parameter for example, the coefficient range of \mathbf{w}_1 is $[0, 15]$. Every two \mathbf{w}_1 coefficients can be packed into one byte. We need to sequentially pack 4-bit \mathbf{w}_1 coefficients in one zmm register and store back to memory in 8-bit data lane. As shown in Figure 6, we use a series of convert instructions to convert 32-bit coefficients to packed 8-bit coefficients. Since there is no instruction to directly convert 32-bit to 4-bit, we propose to shift of odd indices coefficients to the left by 4 bits and then pack with the even indices 4 bits. Finally, we adjust the order by using permutation instruction to ensure the the correctness of the KAT test.

VI. EXPERIMENT RESULTS AND DISCUSSIONS

We implemented all three security levels of Dilithium, using both C language and Intel AVX-512 assembly and AVX-512 intrinsic functions. For a more comprehensive comparison, we provide both the Round3 submission version of Dilithium [14] and the FIPS 204 version of Dilithium [8], known as ML-DSA. We also optimized the previous Round3 submitted AVX2 code using the presented optimization technique. Our optimized vectorization implementation has successfully passed the NIST Known Answer Tests, thereby confirming its compatibility across all platforms. We proceed to conduct a thorough performance evaluation, highlighting the improvements achieved through the optimizations discussed in Section V. The Round3 Dilithium codes are collected from <https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>. The FIPS204 ML-DSA codes are collected from <https://github.com/pq-crystals/dilithium/tree/standard>. The compiler is gcc-9.4.0 and the optimization flags are -Wshadow -Wpointer-arith -mavx2 -mAVX-512F -mAVX-512vbmi -mAVX-512bw -mAVX-512cd -mAVX-512vl -mpopcnt -maes -march=native -mtune=native -O3. The benchmark experiments were conducted on a desktop machine with Ubuntu 20.04 operating system and Intel(R) Core(TM) i7-11700F CPU (Rocket Lake) running at 2.5GHz. As usual, we disable the TurboBoost and Hyper-Threading to ensure the reproduction of the experiments. Each experiment is repeated 100000 times, and we present the median results.

A. Polynomial Multiplication Performance

Table VI presents performance results for polynomial multiplication within Dilithium. We report benchmark results for polynomial-vector multiplication $c \cdot s$ and $c \cdot e$ using NTT and PSPM techniques. On Intel CPUs, PSPM achieves speed improvements ranging from 47% to 66% compared to NTT, for both AVX2 and AVX-512 implementations. Furthermore, the data indicates that our AVX-512 implementations of $c \cdot s$ and $c \cdot e$ using the NTT technique are 53% faster than their AVX2 counterparts.

TABLE VI: Performance of $c \cdot s$ and $c \cdot e$ in Dilithium3 (Cycles).

	AVX2 [14]	AVX-512
$c \cdot s$ (PSPM)	6748	2556
$c \cdot s$ (NTT)	14636	6740
$c \cdot e$ (PSPM)	8358	2560
$c \cdot e$ (NTT)	16010	7480

B. PSPM-TEE Performance

Table VII illustrates the performance of the Improved PSPM algorithm. When we apply the Improved PSPM, our AVX2 implementation achieves a speedup of approximately 7.7% for Dilithium3, while Dilithium5 experiences a more modest acceleration of only 2.9%. These results demonstrate the discernible advantages of the improved PSPM algorithm in enhancing the signing procedure of Dilithium. Consequently, we incorporate the improved PSPM algorithm in the implementation of Dilithium using AVX-512 as well.

TABLE VII: Performance of Signing Procedure with Improved PSPM (Cycles).

	AVX2	AVX2 (PSPM – TEE)	Speedup
Dilithium2	251050	231766	7.7%
Dilithium3	406248	393454	3.1%
Dilithium5	516200	501304	2.9%

C. Other Vectorization Functions Performance

We conducted an experiment primarily to evaluate the performance of our AVX-512 vectorized functions within the context of Dilithium, as detailed in Table VIII. Our benchmark results encompass two versions of SHAKE-256: the parallel version and the sequential version. The parallel version of SHAKE-256 generates four or eight hashing results simultaneously, while the sequential version generates only one hashing result. Since we can store five 64-bit states in one AVX-512 register, the sequential version exhibits 5-way parallelism.

TABLE VIII: Experimental results of vectorization functions for Dilithium (Cycles).

Function	Vectorization	Cycles	Speedup
Poly_uniform	1-way	5784	1.00x
	4-way	19488	2.97x
	8-way	13450	4.30x
Poly_uniform_eta	1-way	30158	1.00x
	4-way	17858	1.69x
	8-way	9054	3.33x
Poly_uniform_gamma1	1-way	48148	1.00x
	4-way	24594	1.95x
	8-way	12094	3.98x
SHAKE-256 (sequential)	1-way	1300	1.00x
	5-way	918	1.41x
SHAKE-256 (parallel)	1-way	5934	1.00x
	4-way	2896	2.05x
	8-way	1014	5.85x
SHAKE-128 (parallel)	1-way	6126	1.00x
	4-way	3006	2.04x
	8-way	1114	5.50x
rej_uniform	1-way	450	1.00x
	8-way	230	1.96x
	16-way	80	5.63x
rej_eta	1-way	1122	1.00x
	8-way	322	3.48x
	16-way	230	4.88x
NTT	1-way	6896	1.00x
	4-way	1326	5.00x
	16-way	494	13.95x
NTT^{-1}	1-way	9438	1.00x
	4-way	1090	8.66x
	16-way	526	17.94x
poly_pointwise	1-way	1374	1.00x
	4-way	146	9.41x
	16-way	124	11.08x
polyz_unpack	1-way	962	1.00x
	32-way	-	-
	64-way	32	30x
polyw1_pack	1-way	32	1.00x
	8-way	32	1.00x
	16-way	16	2.00x

In the case of NTT, we adopted an efficient approach for loading coefficients, enabling us to load 16 coefficients simultaneously, a significant improvement over AVX2's four-coefficient loading capacity. This optimization resulted in a

substantial 16-way parallelism in our NTT AVX-512 implementation, effectively reducing memory access. Consequently, we achieved a remarkable acceleration factor of nearly 14 times in NTT. Similarly, in NTT^{-1} , we realized a commendable speedup of nearly 18 times. The improvements in NTT are primarily attributed to the inherent vectorization capabilities of AVX-512, as well as our well-structured instruction scheduling and efficient utilization of registers, which significantly reduce load and store operations through layer merging technology. In comparison to the NTT AVX-512 implementation in [31], which demonstrated speedups of 12.13x, 13.46x, and 11.50x in NTT, NTT^{-1} , and polynomial pointwise multiplication respectively, our AVX-512 implementation exhibits superior performance due to its enhanced parallelism.

D. Scheme Performance

In this work, we pursued peak performance by employing a range of optimization techniques in the implementation of Dilithium. These optimizations encompassed various aspects, including enhancements in NTT, rejection sampling, decomposition, computing hints, bit-packing, and more. Table X provides a summary of cycle counts and comparisons for all three security levels of Round3 Dilithium, encompassing key generation (KeyGen), signing (Sign), and verification (Verify).

[8] presented benchmark results for Round3 Dilithium3; however, due to their unavailability of open-source code, our comparison focused on speedups. In key generation, signing, and verification, we achieved speedups of 65.1%, 52.8%, and 56.2%, respectively, surpassing their speedups of 33.6%, 43.2%, and 40.1%. These performance improvements were primarily driven by our optimized NTT implementation and the introduction of the PSPM-TEE algorithm. Additionally, our sequential SHAKE-256 implementation using AVX-512 contributed to the overall performance enhancements. We

TABLE IX: Execution times (in Cycles) of implementation of Round3 Dilithium2, Dilithium3 and Dilithium5 on an Intel Core i7-11700F processor.

Scheme	Operation	C [14]		AVX-512		Speedup vs AVX2
		Cycles	Cycles	Cycles	Speedup vs C	
Dilithium2	KeyGen	266772	106000	47168	82.3%	55.5%
	Sign	1033894	251050	125554	87.9%	50.0%
	Verify	298384	107338	48320	83.8%	55.0%
Dilithium3	KeyGen	503306	246988	86114	82.9%	65.1%
	Sign	1699294	406248	191946	88.7%	52.8%
	Verify	478660	174218	76256	84.1%	56.2%
Dilithium5	KeyGen	725802	286534	118568	83.7%	58.6%
	Sign	2111234	516200	223776	89.4%	56.6%
	Verify	770794	275894	114412	85.2%	58.5%

enhanced Round3 AVX2 implementation by incorporating the improved PSPM and tailored reduction techniques, resulting in a speedup of 3% to 8% in the signature procedure. In our Dilithium AVX-512 implementation, certain parts have not yet been vectorized, such as hash functions other than polynomial sampling. Consequently, the overall improvement in signature speed cannot exceed twice the AVX2 software speed. Nonetheless, our speedup primarily stems from the vectorization of specific functions and the optimization techniques we introduced. Dilithium was chosen as one of the digital signature standards on July 22th, 2022. On August 24th, 2023, NIST published the standardization document FIPS 204 [8],

TABLE X: Performance comparison in Signing procedure (Cycles).

Scheme	AVX2 [14]	AVX2 (Our work)	Speedup
Dilithium2	251050	231410	7.8%
Dilithium3	406248	392436	3.4%
Dilithium5	516200	500882	3.0%

which aligns with the Dilithium scheme. There exist several distinctions between the FIPS 204 ML-DSA Standard and Round3 Dilithium, and we have also implemented the FIPS 204 scheme ML-DSA, providing benchmark results in Section XI.

TABLE XI: Execution times (in Cycles) of implementation of ML-DSA [8] on an Intel Core i7-11700F processor.

Scheme	Operation	C [8]	AVX2 [8]	Cycles	Speedup vs C	AVX-512
		Cycles	Cycles			Speedup vs AVX2
ML-DSA-44	KeyGen	299120	84270	47760	84.0%	43.2%
	Sign	1068726	194320	123160	88.4%	36.6%
	Verify	328798	90314	49396	84.9%	45.3%
ML-DSA-65	KeyGen	558152	144114	87378	84.3%	39.3%
	Sign	1804702	327856	191152	89.4%	41.6%
	Verify	533314	145990	78008	85.3%	46.5%
ML-DSA-87	KeyGen	818616	224466	122032	85.1%	45.6%
	Sign	2208464	402276	226272	89.7%	43.7%
	Verify	856658	227138	119428	86.1%	47.4%

E. Discussions about Side-Channel Security and Memory Cost

Constant-time implementation (CTI) was not the focus of this work, but we indeed take it in mind. We have carefully avoided using branching statements depending on secret information, and we have not used the modulo operator %. For the side-channel security of the PSPM-TEE technique, we have the following observations. On the one hand, as the intermediate hashing c 's rejected with the tailored early evaluation are never output, the intermediate values are actually blinded to an outside observer. On the other hand, the PSPM technique consolidates coefficients of identical dimensions from multiple small polynomials into a single word for operations. This approach can potentially introduce greater complexity and obstacles for side-channel attacks when compared to traditional NTT technique.

For space cost, our implementation pre-calculates the tables in improved PSPM, which requires an additional 8192 bytes of storage space in Dilithium3/5 and 4096 bytes in Dilithium2. However, our implementation of parallel rejection sampling saves 1048576 bytes. Overall, our implementation significantly reduces the required space compared to the previous AVX2 implementations.

F. Deployment on Other Platforms

Due to the absence of AVX-512 compatible CPUs, there may be questions surrounding deployment on alternative platforms. However, it is still worthwhile to consider the performance enhancements achievable on x86-64 CPUs utilizing the latest AVX instructions. Moreover, some of the optimization techniques we propose can be implemented in other systems. The upgraded 32-bit version of the PSPM algorithm is especially advantageous for ARM Cortex-M4 implementation,

as it solely utilizes 32-bit general registers. Additionally, the Tailored reduction technique exclusively employs subtraction and multiplication, making it readily deployable on other platforms. Furthermore, our implementation addresses issues that arise when vectorizing serial processes or functions, ensuring the accuracy of test vectors.

VII. CONCLUSION

This paper demonstrates the potential of AVX-512 in accelerating the implementation of Dilithium. Specifically, we enhance PSPM through the introduction of PSPM-TEE, significantly expediting the Dilithium signing process. We illustrate how tailored reduction can be applied to Dilithium's modulus, presenting a fast implementation using AVX-512IFMA. We extensively vectorize numerous functions within Dilithium, with a particular focus on addressing performance bottlenecks such as polynomial multiplication, hashing, and more. In summary, we provide a fully vectorized implementation of Dilithium utilizing AVX-512. Leveraging these optimization techniques, our implementation achieves substantial speed improvements over previous AVX2 implementations, thereby establishing the most efficient Dilithium implementation on the x86-64 platform to date.

REFERENCES

- [1] X. . ITU-T Recommendation, "Information technology-open systems interconnection-the directory: public-key and attribute certificate framework," *ISO/IEC 9594-8: 2001*, 2000.
- [2] T. Dierks and E. Rescorla, "The transport layer security (TLS) protocol version 1.2," Tech. Rep., 2008.
- [3] E. Rescorla, "The transport layer security (TLS) protocol version 1.3," Tech. Rep., 2018.
- [4] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [5] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.
- [6] K. McKay, L. Bassham, M. Sönmez Turan, and N. Mouha, "Report on lightweight cryptography," National Institute of Standards and Technology, Tech. Rep., 2016.
- [7] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, C. Miller, D. Moody, R. Peralta *et al.*, "Status report on the third round of the NIST post-quantum cryptography standardization process," *US Department of Commerce, NIST*, 2022.
- [8] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard," Department of Commerce, Washington, D.C., Federal Information Processing Standards Publication (FIPS) NIST FIPS 204 ipd, 2023. [Online]. Available: <https://doi.org/10.6028/NIST.FIPS.204.ipd>
- [9] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," *Des. Codes Cryptogr.*, vol. 75, no. 3, pp. 565–599, 2015. [Online]. Available: <https://doi.org/10.1007/s10623-014-9938-4>
- [10] M. Ajtai, "Generating hard instances of lattice problems," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 99–108.
- [11] V. Lyubashevsky, "Fiat-shamir with aborts: applications to lattice and factoring-based signatures," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2009, pp. 598–616.
- [12] C. Lomont, "Introduction to intel advanced vector extensions," *Intel white paper*, vol. 23, 2011.
- [13] I. Corporation, "10th generation intel core processor based on ice lake microarchitecture instruction throughput and latency." Available online at <https://software.intel.com/content/www/us/en/develop/download/10t-h-generation-intel-core-processor-instruction-throughput-and-latency-docs.html>, 2020.
- [14] R. Avanzi, J. Bos, and L. Ducas, "Submission to the NIST post-quantum cryptography standardization project," Available for download at <https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-3/submissions/Dilithium-Round3.zip>, 2022.
- [15] D. O. C. Greconici, M. J. Kannwischer, and D. Sprekels, "Compact Dilithium implementations on Cortex-M3 and Cortex-M4," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2021, no. 1, pp. 1–24, 2021. [Online]. Available: <https://doi.org/10.46586/tches.v2021.i1.1-24>
- [16] Y. Kim, J. Song, T.-Y. Youn, and S. C. Seo, "CRYSTALS-Dilithium on ARMv8," *Security and Communication Networks*, vol. 2022, 2022.
- [17] H. Becker, V. Hwang, M. J. Kannwischer, B. Yang, and S. Yang, "Neon NTT: faster Dilithium, Kyber, and Saber on Cortex-A72 and Apple M1," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2022, no. 1, pp. 221–244, 2022. [Online]. Available: <https://doi.org/10.46586/tches.v2022.i1.221-244>
- [18] A. Abdulrahman, V. Hwang, M. J. Kannwischer, and D. Sprekels, "Faster Kyber and Dilithium on the Cortex-M4," in *Applied Cryptography and Network Security - 20th International Conference, ACNS 2022, Rome, Italy, June 20–23, 2022, Proceedings*, ser. Lecture Notes in Computer Science, G. Ateniese and D. Venturi, Eds., vol. 13269. Springer, 2022, pp. 853–871. [Online]. Available: https://doi.org/10.1007/978-3-031-09234-3_42
- [19] J. Bradbury and B. Hess, "Fast quantum-safe cryptography on IBM Z," Technical report, 2021. URL: <https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/hess-fast-quantum-safe-pqc2021.pdf>, 2021.
- [20] J. Zheng, F. He, S. Shen, C. Xue, and Y. Zhao, "Parallel small polynomial multiplication for dilithium: a faster design and implementation," in *Annual Computer Security Applications Conference, ACSAC 2022, Austin, TX, USA, December 5–9, 2022*. ACM, 2022, pp. 304–317. [Online]. Available: <https://doi.org/10.1145/3564625.3564629>
- [21] J. W. Bos, P. L. Montgomery, D. Shumow, and G. M. Zaverucha, "Montgomery multiplication using vector instructions," in *International Conference on Selected Areas in Cryptography*. Springer, 2014, pp. 471–489.
- [22] S. Gueron and F. Schlieker, "Speeding up R-LWE post-quantum key exchange," in *Nordic conference on secure IT systems*. Springer, 2016, pp. 187–198.
- [23] G. Orisaka, D. F. Aranha, and J. López, "Finite field arithmetic using AVX-512 for isogeny-based cryptography," in *Anais do XVIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*. SBC, 2018, pp. 49–56.
- [24] T. Edamatsu and D. Takahashi, "Acceleration of large integer multiplication with intel AVX-512 instructions," in *20th IEEE International Conference on High Performance Computing and Communications; 16th IEEE International Conference on Smart City; 4th IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2018, Exeter, United Kingdom, June 28–30, 2018*. IEEE, 2018, pp. 211–218. [Online]. Available: <https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00059>
- [25] D. Takahashi, "An implementation of parallel number-theoretic transform using Intel AVX-512 instructions," in *International Workshop on Computer Algebra in Scientific Computing*. Springer, 2022, pp. 318–332.
- [26] J. Robert and P. Véron, "Faster multiplication over $f_2[x]$ using AVX512 instruction set and VPCLMULQDQ instruction," *CoRR*, vol. abs/2201.10473, 2022. [Online]. Available: <https://arxiv.org/abs/2201.10473>
- [27] H. Cheng, G. Fotiadis, J. Großschädl, and P. Y. A. Ryan, "Highly vectorized SIKE for AVX-512," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2022, no. 2, pp. 41–68, 2022. [Online]. Available: <https://doi.org/10.46586/tches.v2022.i2.41-68>
- [28] H. Cheng, G. Fotiadis, J. Großschädl, P. Y. A. Ryan, and P. B. Rønne, "Batching CSIDH group actions using AVX-512," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2021, no. 4, pp. 618–649, 2021. [Online]. Available: <https://doi.org/10.46586/tches.v2021.i4.618-649>
- [29] D. M. Alter, "Optimizing the NIST post quantum candidate SPHINCS+ using AVX-512," <https://github.com/DorAlter/sphincsplus/tree/avx512-implementation>, 2021.
- [30] R. Cabral and J. López, "Implementation of the SHA-3 family using AVX512 instructions," in *Anais do XVIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*. SBC, 2018, pp. 25–32.
- [31] D. Lei, D. He, C. Peng, M. Luo, Z. Liu, and X. Huang, "Faster implementation of ideal lattice-based cryptography using avx512," *ACM Transactions on Embedded Computing Systems*, 2023.

- [32] M. J. Dworkin *et al.*, “SHA-3 standard: permutation-based hash and extendable-output functions,” 2015.
- [33] G. Seiler, “Faster AVX2 optimized NTT multiplication for ring-lwe lattice cryptography.” *IACR Cryptol. ePrint Arch.*, p. 39, 2018. [Online]. Available: <http://eprint.iacr.org/2018/039>
- [34] J. W. Cooley and J. W. Tukey, “An algorithm for the machine calculation of complex fourier series,” *Mathematics of computation*, vol. 19, no. 90, pp. 297–301, 1965.
- [35] W. M. Gentleman and G. Sande, “Fast fourier transforms: for fun and profit,” in *Proceedings of the November 7-10, 1966, fall joint computer conference*, 1966, pp. 563–578.

APPENDIX

A. PSPM with Early Evaluation pseudocode for Dilithium3/5

Algorithm 11 A parallel index-based polynomial multiplication algorithm with early evaluating \mathbf{z} for Dilithium3/5

Input: $(c, \mathbf{e}, \mathbf{w})$, where $\mathbf{e} = [e^{(0)}, \dots, e^{(k-1)}]^T \in \mathcal{R}_q^k$, $\mathbf{w} \in \mathcal{R}_q^k$, every $e^{(j)} = \sum_{i=0}^{n-1} e_i^{(j)} \cdot x^i \in \mathcal{R}_q$, $w^{(j)} = \sum_{i=0}^{n-1} w_i^{(j)} \cdot x^i \in \mathcal{R}_q$, and $c = \sum_{i=0}^{n-1} c_i \cdot x^i \in B_\tau$
Output: $\mathbf{r} = c \cdot \mathbf{e} - \mathbf{w} = [r^{(0)}, \dots, r^{(k-1)}]^T \in \mathcal{R}_q^k$, where $r^{(j)} = c \cdot e^{(j)} - w^{(j)} = \sum_{i=0}^{n-1} r_i^{(j)} \cdot x^i \in \mathcal{R}_q$

```

1: for  $i \in \{0, 1, \dots, n-1\}$  do
2:    $m_i := 0$ 
3:    $v_i := 0$ 
4:    $v_{i-n} := 0$ 
5:   for  $j \in (0, 1, \dots, k-1)$  do
6:      $v_i := v_i \cdot M + (U + e_i^{(j)})$ 
7:      $v_{i-n} := v_{i-n} \cdot M + (U - e_i^{(j)})$ 
8:    $\gamma := 2U \cdot \frac{M^l - 1}{M - 1}$ 
9:   for  $i \in \{0, 1, \dots, n-1\}$  do
10:    if  $c_i = 1$  then
11:      for  $j \in \{0, 1, \dots, n-1\}$  do
12:         $m_j := m_j + v_{j-i}$ 
13:    if  $c_i = -1$  then
14:      for  $j \in \{0, 1, \dots, n-1\}$  do
15:         $m_j := m_j + (\gamma - v_{j-i})$ 
16:   for  $i \in \{0, 1, \dots, n-1\}$  do
17:      $t := m_i$ 
18:     for  $j \in (0, 1, \dots, l-1)$  do
19:        $z_i^{(l-1-j)} := (t \bmod M) - \tau U \pmod q$ 
20:        $z_i^{(l-1-j)} := z_i^{(l-1-j)} + y_i^{(l-1-j)}$ 
21:       if  $|z_i^{(l-1-j)}| >= \gamma_1 - \beta$  then Restart signature process.
22:      $t := \lfloor t/M \rfloor$ 
23:   return  $\mathbf{z} = [z^{(0)}, \dots, z^{(l-1)}]^T$ 

```

Algorithm 12 A parallel index-based polynomial multiplication algorithm with early evaluating \mathbf{r}_0 for Dilithium3/5

Input: $(c, \mathbf{e}, \mathbf{w})$, where $\mathbf{e} = [e^{(0)}, \dots, e^{(k-1)}]^T \in \mathcal{R}_q^k$, $\mathbf{w} \in \mathcal{R}_q^k$, every $e^{(j)} = \sum_{i=0}^{n-1} e_i^{(j)} \cdot x^i \in \mathcal{R}_q$, $w^{(j)} = \sum_{i=0}^{n-1} w_i^{(j)} \cdot x^i \in \mathcal{R}_q$, and $c = \sum_{i=0}^{n-1} c_i \cdot x^i \in B_\tau$
Output: $\mathbf{r} = c \cdot \mathbf{e} - \mathbf{w} = [r^{(0)}, \dots, r^{(k-1)}]^T \in \mathcal{R}_q^k$, where $r^{(j)} = c \cdot e^{(j)} - w^{(j)} = \sum_{i=0}^{n-1} r_i^{(j)} \cdot x^i \in \mathcal{R}_q$

```

1: for  $i \in \{0, 1, \dots, n-1\}$  do
2:    $m_i := 0$ 
3:    $v_i := 0$ 
4:    $v_{i-n} := 0$ 
5:   for  $j \in (0, 1, \dots, k-1)$  do
6:      $v_i := v_i \cdot M + (U + e_i^{(j)})$ 
7:      $v_{i-n} := v_{i-n} \cdot M + (U - e_i^{(j)})$ 
8:    $\gamma := 2U \cdot \frac{M^k - 1}{M - 1}$ 
9:   for  $i \in \{0, 1, \dots, n-1\}$  do
10:    if  $c_i = 1$  then
11:      for  $j \in \{0, 1, \dots, n-1\}$  do
12:         $m_j := m_j + v_{j-i}$ 
13:    if  $c_i = -1$  then
14:      for  $j \in \{0, 1, \dots, n-1\}$  do
15:         $m_j := m_j + (\gamma - v_{j-i})$ 
16:   for  $i \in \{0, 1, \dots, n-1\}$  do
17:      $t := m_i$ 
18:     for  $j \in (0, 1, \dots, k-1)$  do
19:        $r_i^{(k-1-j)} := (t \bmod M) - \tau U \pmod q$ 
20:        $r_i^{(k-1-j)} := m_i^{(k-1-j)} - r_i^{(k-1-j)}$ 
21:        $r_i^{(k-1-j)} := \text{LowBits}_q(r_i^{(k-1-j)}, 2\gamma_2)$ 
22:       if  $|r_i^{(k-1-j)}| >= \gamma_2 - \beta$  then Restart signature process.
23:      $t := \lfloor t/M \rfloor$ 
24:   return  $\mathbf{r} = [r^{(0)}, \dots, r^{(k-1)}]^T$ 

```

B. Parameter for PSPM

TABLE XII: Parallel Parameters of Dilithium.

Scheme	Operation	τ	U	$2\tau U$	M	r
Dilithium2	cs_1	39	2	156	2^8	4
	cs_2	39	2	156	2^8	4
	ct_0	39	2^{12}	319488	2^{19}	4
	ct_1	39	2^{10}	79872	2^{17}	4
Dilithium3	cs_1	49	4	392	2^9	5
	cs_2	49	4	392	2^9	6
	ct_0	49	2^{12}	401408	2^{19}	6
	ct_1	49	2^{10}	100352	2^{17}	6
Dilithium5	cs_1	60	2	240	2^8	7
	cs_2	60	2	240	2^8	8
	ct_0	60	2^{12}	491520	2^{19}	8
	ct_1	60	2^{10}	122880	2^{17}	8