Hardware Acceleration with Backdoor and Side-Channel Analysis for Lattice-based Cryptography

Suraj Mandal, Advisor: Dr. Debapriya Basu Roy
Indian Institute of Technology Kanpur, India

Suraj's Hompage

Motivation:

- Execution of lattice-based algorithms involves large-degree polynomial multiplication, hash operations etc. that makes the software implementation slower.
- Need for efficient, lightweight, and low-latency polynomial multiplication unit using NTT.
- As the transition to post-quantum cryptography accelerates, the growing reliance on hybrid cryptosystems also raises the risk of backdoor insertion.
- To ensure post-quantum cryptographic algorithms remain secure in real-world deployments, it is essential to analyze and mitigate side-channel vulnerabilities that could leak sensitive information despite strong theoretical security.

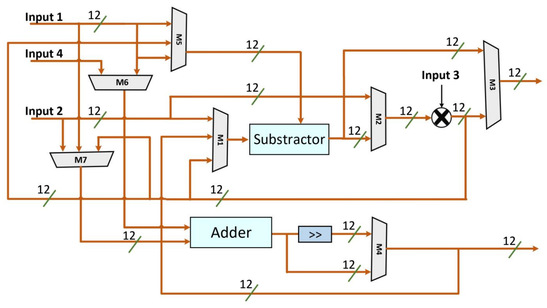
Challenges:

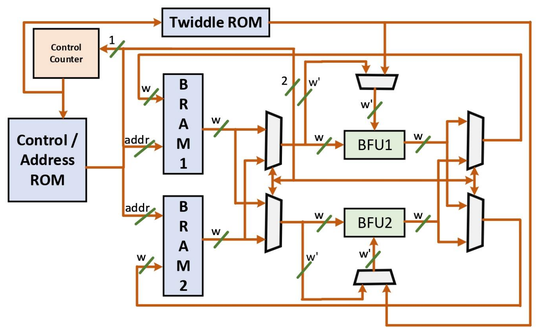
- Designing lightweight hardware accelerator for PQC algorithms.
- Designing low-latency hardware accelerator for lattice based PQC algorithms.

- Analyzing possible backdoors on lattice-based PQC.
- Side-channel analysis on NTT/INVNTT/PWM of CRYSTALS-Kyber and CRYSTALS-Dilithium.

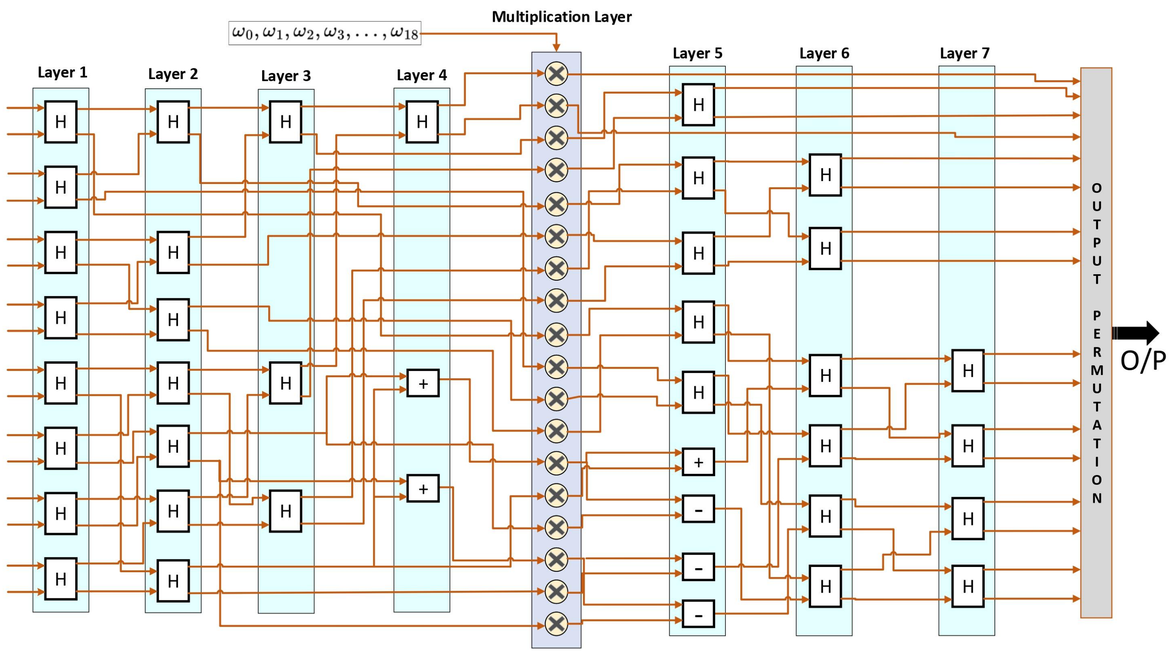
Related Publications:

- S. Mandal and D. B. Roy, "Kid: A hardware design framework targeting unified ntt multiplication for crystals-kyber and crystals-dilithium on fpga," VLSID,2024.
- S. Mandal and D. Basu Roy, "Design of a lightweight fast Fourier transformation for Falcon using hardware-software co-design," GLSVLSI 2024.
- S. Mandal and D. B. Roy, "Winograd for NTT: A case study on higher-radix and low-latency implementation of NTT for post quantum cryptography on FPGA," IEEE Transactions on Circuits and Systems I: Regular Papers,2024.
- S. Mandal and D. B. Roy, "A lightweight unified keccak module for efficient hashing in ml-kem and ml-dsa," ACM QSec 2025 (Co-Located with ACM CCS).
- S. Mandal, P. Ravi, M Dhilipkumar, D.B. Roy, A. Chattopadhyay, "Hardware Implementation of Stealthy and Lightweight Backdoor for CRYSTALS-Kyber". (Major revision in ACM TECS).
- S. Mandal, N. Chaurasia and D.B. Roy "Design Exploration of Lightweight Radix-4 NTT Multiplication Unit for ML-KEM and ML-DSA on FPGA" (In Submission)
- Sayan Das, Suraj Mandal, Thales Paiva, Prasanna Ravi, Debapriya Basu Roy, and Anupam Chattopadhyay. "Analyzing Backdoors on Post-Quantum Cryptography". (In submission).
- Harish Prasad Alam, Suraj Mandal, Debapriya Basu Roy. "How to Multiply: A Comparative Analysis between Karatsuba, Toom-Cook and NTT Multiplier for Polynomial Multiplication in NTRU", AsianHOST 2023.





Shared multipliers/adder/subtractor. Unified BFU that performs NTT/NTT−1/PWM for ML-KEM/ML-DSA. Lightweight Control unit and pipelined memory access for radix-2. The state-of-the-art work consumed 3487 LUTs, 4 DSPs, achieving an ADP-LUT of 6612. In contrast, our NTTCore took 2893 LUTs, 4.5 BRAMs with 4 DSPs with a frequency of 342 MHz, achieving an ADP-LUT of 3662.

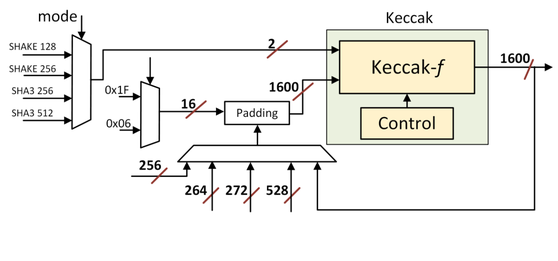


BFU	DSP	LUT	FF	Frequency (Mhz)	Latency			ADP-LUT	ADP-DSP
					NTT	NTT	PWM	NTT/NTT	NTT/NTT
Cooley-Tukey	64	17296	10218	163	58	58	44	6154	23
Winograd	50	12141	7941	254				2772	12

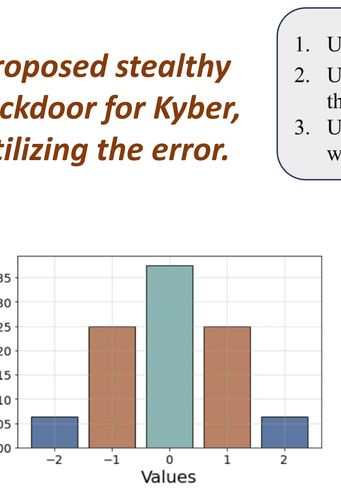
Table 1. Comparision between Cooley-Tukey/Gentleman-Sande and Winograd's radix-16 NTT PMU

NTT Type	Design	Board	LUT	slice	FFs	BRAM	DSP	Latency (NTT)	Latency (INTT)	Latency (PWM)	Freq.(MHz)	AT
Radix-2	[2]	Artix-7	9018	2255	6292	2	16	256	256	-	250	3948
Radix-4	[9]	Zynq 7000	2386	597	932		8			64	217	1648
Radix-2	[3]	Artix-7	11000	2750	5182	12	64	156	198	552	140	10196
			63000	15750	18000	48	256	103	121	345	126	33802
	[4]	Kintex U+	26520	3315	15171	24	48	113	-	-	194	4727
Radix-16 (Winograd)	TW	Zynq 7000	12141	3664	7941	14.5	50	58	58	44	254	1978
		ZCU+ 102	11963	1813	7187						297	1330
		Artix-7	12720	3667	7834						183	2747

Table 2. Comparison Results for CRYSTALS-Dilithium..



	FPGA	LUT	FFs	DSP	SLICE	Latency of Round Function	Generation of A_{ij}	Frequency	ATP
[21]	Kintex 7	7376*	3059	4	1844	48	366	391	2100.52
[1]	Zynq Ultrascale+	12326	3560	0	3082	-	216	270	2465.6
Our work	Kintex 7	4174*	5627	0	1272	24	278	222	1592.86
		7860	12773	0	2507	24	278	220	3167.94
Our work	Ultrscale +	4145*	5604	0	1067	24	278	310	956.86
		7854	12743	0	2015	24	278	310	1807



Proposed stealthy backdoor for Kyber, utilizing the error.

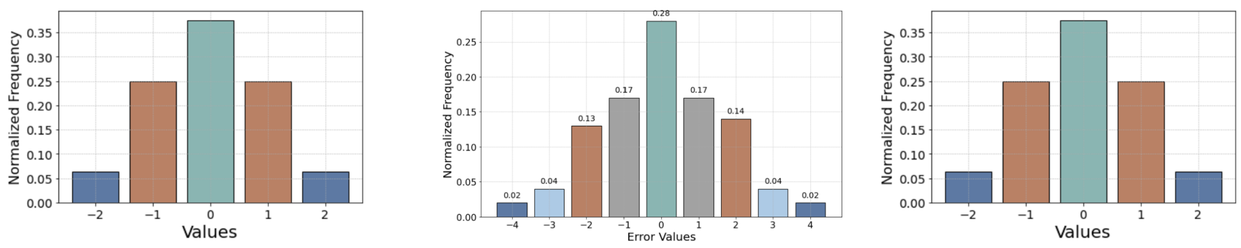
1. User generates a random scalar B.
2. User calculates $ct_{bd}=B.P$, where P is the base point of ECC.
3. User generates $m_{bd}=B.P_A=B.P.A$, where P_A is the public key of ECC.

$Enc_{bd}(pk_{bd})$ in User's Side

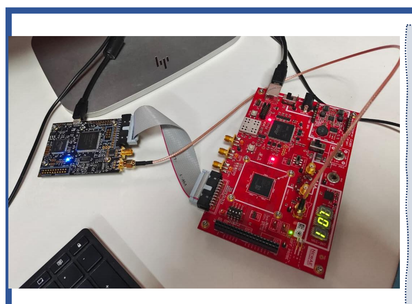
User's Public Key

1. Attacker finds out ct_{bd} from keygen public key.
2. User calculates $m_{bd}=ct_{bd}.A=B.P.A$, as attacker already have A.

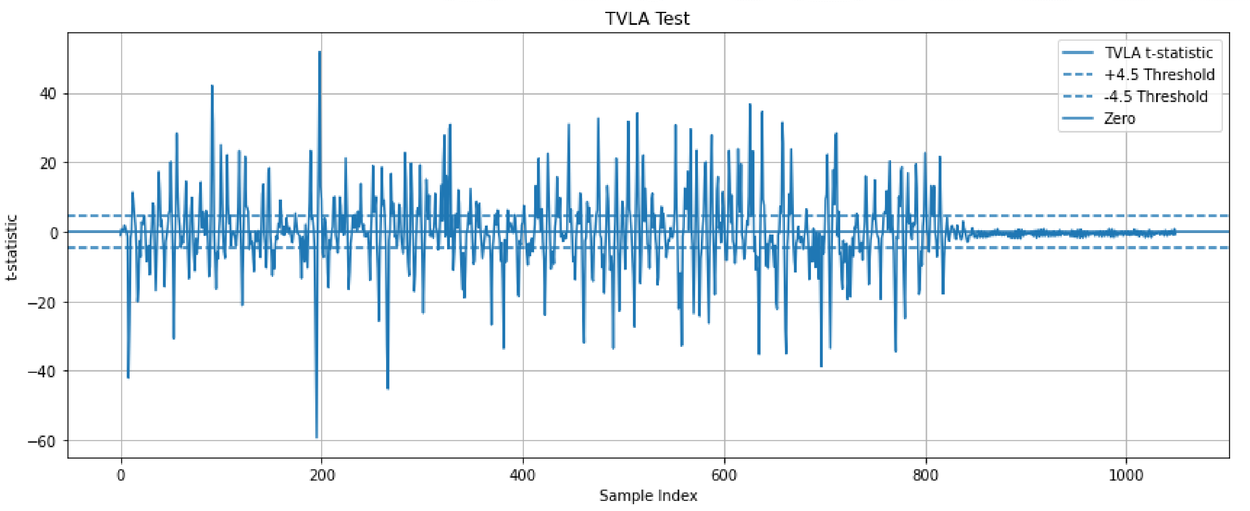
$Dec_{bd}(sk_{bd}, ct_{bd})$ in Attacker's Side



(a) Original Kyber (b) Algorithm of [17] (c) Proposed Algorithm

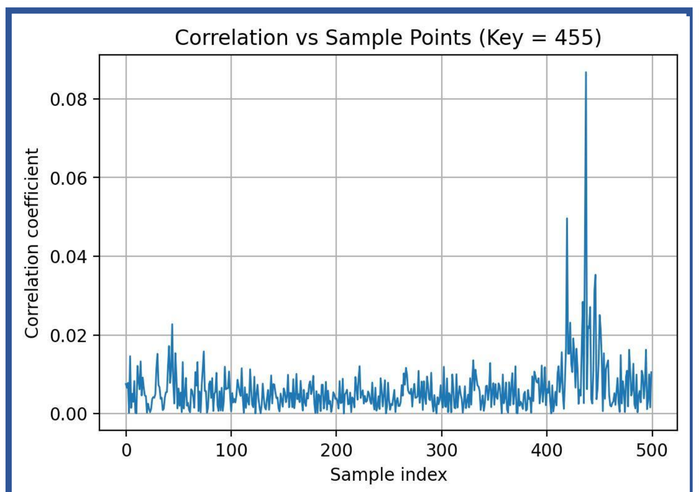


- Kyber uses the secret key in the decapsulation phase by executing ($v - s^Tu$), where v and u are the ciphertext vector and s is the secret vector.
- We have performed a chosen ciphertext attack on the hardware implementation of the Kyber.
- For the collection of power traces, we have used ChipWhisperer CW305 with ChipWhisperer Lite.



TVLA of PWM Kyber

Our chosen ciphertext attack is able to recover one polynomial of the secret key for Kyber in (10k * (256/d)) number of traces, where d is the pipeline depth of the design.



Correlation Power Attack

Ongoing Works:

- BRAM-free/ Multiplieress Radix-4 NTT Multiplication Unit (In submission).
- More efficient side-channel attacks and countermeasures on ML-KEM/ ML-DSA.
- Hardware acceleration of Isogeny-based cryptography.
- Low-latency hardware accelerator for ML-KEM/ML-DSA.