Optimal and Side-Channel resistant Post-Quantum TLS1.3 as part of wolfSSL for ARMv7-M

Mila Anastasova[1], Reza Azarderakhsh[1], and Mehran Mozaffari Kermani[2]

Computer and Electrical Engineering and Computer Science Department and I-SENSE at Florida Atlantic University, Boca Raton, FL, USA
(manastasova2017, razarderakhsh)@fau.edu

Computer Engineering and Science Department at University of South Florida, Tampa, FL, USA,
mehran2@usf.edu

Abstract & Introduction

The advancement in quantum computing presents a threat to current encryption methods, thus raise concerns regarding the security of traditional network protocols. In this work:

- We deploy optimal Cortex-M4 Curve448 and Ed448 ECC architecture primitives into wolfSSL TLS1.3.
- We present a side-channel-resistant Curve448 and Ed448 based on Differential Power Analysis (DPA) countermeasures using TVLA traces.
- We focus on deploying Curve448 and Ed448 primitives along with Post-Quantum Crystals-Kyber and Crystals-Dilithium into wolfSSL TLS 1.3 protocol and report performance using the NIST-recommended STM32F407-DK and STM32F413-DK.

ARMv7-M Architecture

The ARM Cortex-M4 processor's architecture delivers a set of powerful instructions that are devoid of structural hazards.

Table 1. ARMv7-M ISA for memory access and MAC instructions

Instruction	Functionality	Latency [CC]
(V)LDR/ (V)STR	$R_n \leftarrow memory$ $memory \leftarrow R_n$ $S_n \leftarrow memory$ $S_m \leftarrow R_n$	2
UMULL	$Rd_1, Rd_2 \leftarrow R_n \times R_m$	1
UMAAL	$Rd_1, Rd_2 \leftarrow R_n \times R_m + Rd_1 + Rd_2$	1

Field Arithmetic Design

We deploy our technique for multi-precision multiplication and squaring, with an emphasis on increasing row (inner loop) size and hence decreasing memory accesses.

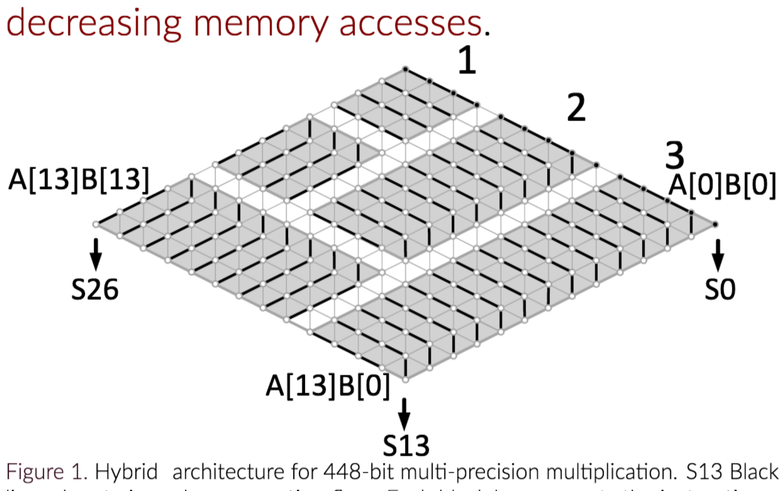

Figure 1. Hybrid architecture for 448-bit multi-precision multiplication. S13 Black lines denote inner loop execution flow. Each black box presents the instructions executed per black line. The white boxes define the instructions executed per white dot.

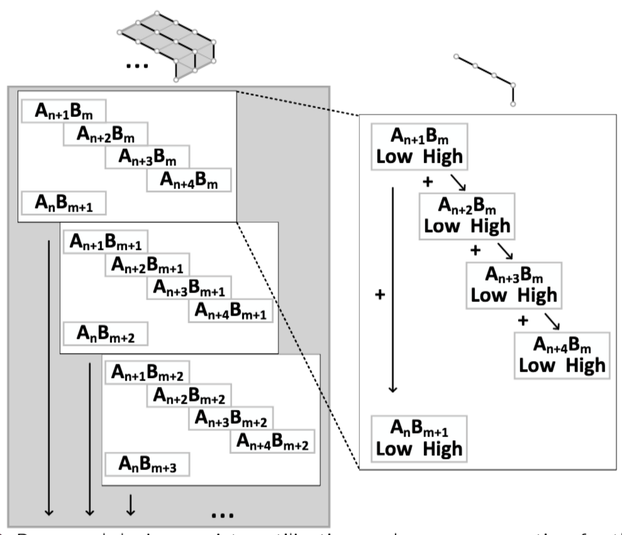

Figure 2. Proposed design, register utilization and carry propagation for the multi-precision multiplication outer (left) and inner (right) loop execution flow.

Side-Channel Analysis & Countermeasures

We examine the Montgomery Ladder-based implementation of the Curve448 and Ed448 based on our multi-precision multiplication and squaring. We use TVLA based on t-statistic to assess distinguishability and study potential DPA threats.

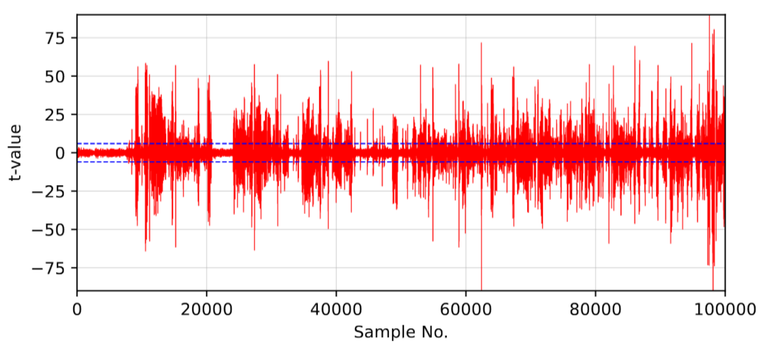

Figure 3. TVLA graphs showing data leak for the unprotected Montgomery Ed448 Curve448 Ladder execution using 10,000 traces.

Scalar Blinding *hides* the point swapping data dependency during point multiplication by randomly generating r and multiplying it by the group order, $k \leftarrow sk_A + r \quad \#Ed.$

Point randomization randomizes base point $G_{rand} \quad (\quad x, \quad)$ and $G_{rand} \quad (\quad X, \quad Y, \quad)$ in affine and projective coordinates, respectively. Upon conversion to affine space, $x \quad \frac{X}{Z} \quad \frac{X}{Z}$ resuls in $(x, y) \quad sk_A \quad G_{rand} \quad sk_A \quad G.$

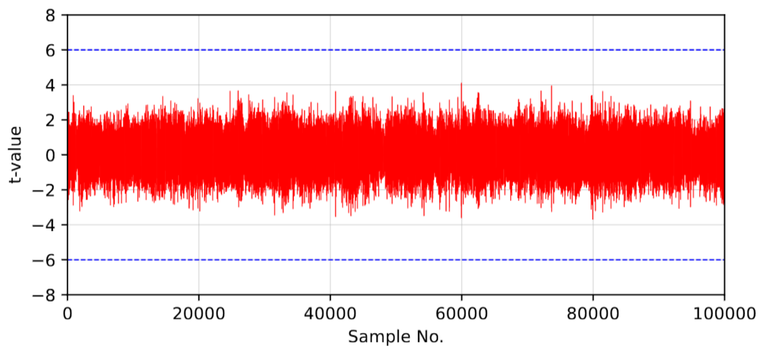

Figure 4. TVLA graphs showing data leak for the protected Montgomery Ladder design based on point randomization and scalar blinding 10,000 traces.

wolfSSL PQ TLS1.3

This study centers on the integration of PQ TLS1.3 into the wolfSSL cryptographic library. In order to transition into PQ (hybrid) operation

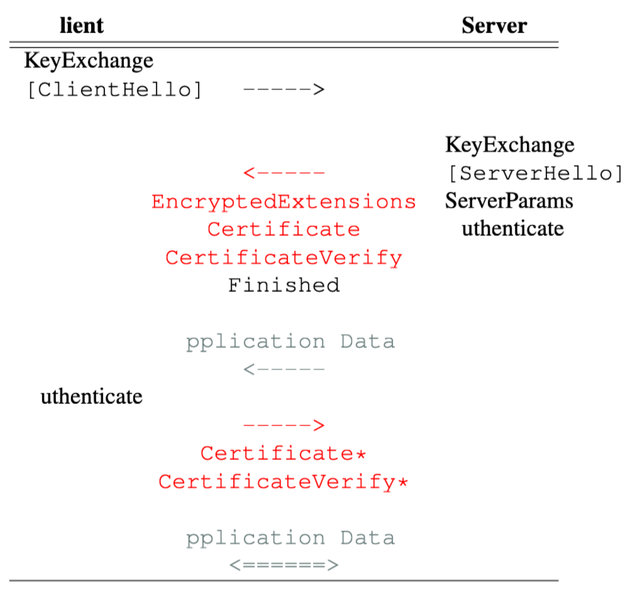

Figure 5. Simplified graph of PQ TLS1.3 (required changes marked in red).

mode, it is necessary to integrate the underlying primitives with PQ-robust algorithms. Consequently, this leads to a modification in the execution flow of the protocol.

Performance Evaluation & Conclusions

We compare our work with existing literature on Curve448- and Ed448-based algorithms in Table 2. We mark around 48.2(36.8)% of speedup for X448 @24(168)MHz. We report a speedup of 13.1%, 8.1%, and 12.4% for Ed448 EdDSA. The inclusion of SCA countermeasures results in an approximate latency

Table 2. Curve25519 and Curve448 ECDH and EdDSA SCA unprotected vs. protected implementations [KCC]

Work	Freq. [MHz]	X448	Ed448 KeyGen	Ed448 Sign	Ed448 Verify	Protected
Curve448 [4]	24	6,218	-	-	-	U
	168	6,286	-	-	-	
Ed448 [2]	24	-	4,069	6,571	8,452	U
	168	-	4,195	6,699	8,659	
Curve448 [1]	24	3,221	3,536	6,038	7,404	U
	168	3,975	4,282	6,787	8,854	
This work	24	**3,503**	**3,826**	**6,328**	**7,404**	PR
		4,151	**4,510**	**7,012**	**7,404**	SB
		4,465	**4,841**	**7,343**	**7,404**	F
	168	**4,344**	**4,669**	**7,173**	**8,854**	PR
		5,128	**5,472**	**7,975**	**8,854**	SB
		5,538	**5,913**	**8,417**	**8,854**	F

overhead of 27(28)% of latency overhead for X448 @24(168)MHz. We report a overhead of 27(27.5)% and 17.8(19.4)% for Ed448 EdDSA KeyGen and Sign @24(168)MHz.

Table 3. Curve448 ECDH and EdDSA SCA unprotected vs. protected implementations in wolfSSL benchmark test and as part of the TLS 1.3 handshake.

Work	Operation	Curve448 ECDH		Ed448DSA			Protected
		keygen	agree	keygen	sign	verify	
wolfSSL [3]	ops	3	4	6	6	2	U
	sec	1.278	1.706	1.071	1.142	1.020	
	avg ms	426.000	426.500	178.500	190.333	510.000	
	ops/sec	2.347	2.345	5.602	5.254	1.961	
	TLS 1.3 Client	3.411987 [ms]					
Curve448 [1]	ops	5	6	5	6	2	U
	sec	1.051	1.255	1.063	1.491	1.141	
	avg ms	210.200	209.167	212.600	248.500	570.500	
	ops/sec	4.757	4.781	4.704	4.024	1.753	
	TLS 1.3 Client	2.996094 [ms]					
This work	ops	4	4	4	4	2	F
	sec	1.086	1.082	1.094	1.236	1.150	
	avg ms	271.500	270.500	273.500	309.000	575.000	
	ops/sec	3.683	3.697	3.656	3.236	1.739	
	TLS 1.3 Client	3.110107 [ms]					

After integrating fully protected SCA design, Table 3, we add only 9% latency overhead for the execution of TLS1.3 Client compared to the original woflSSL design.

Conclusion

This study introduces and implements optimum and side-channel attack (SCA)-resistant Curve448 and Ed448 cryptographic algorithms within the wolfSSL TLS1.3 framework. Our research focuses on the integration of the NIST PQ finalists, specifically Crystals-Kyber and Crystals-Dilithium, into the wolfSSL embedded library.

References

[1] Mila Anastasova, Reza Azarderakhsh, Mehran Mozaffari Kermani, and Lubjana Beshaj. Time-Efficient Finite Field Microarchitecture Design for Curve448 and Ed448 on Cortex-M4. *International Conference of Information Security and Cryptology*, 2022.

[2] Mila Anastasova, Mojtaba Bisheh-Niasar, Hwajeong Seo, Reza Azarderakhsh, and Mehran Mozaffari Kermani. Efficient and Side-Channel Resistant Design of High-Security Ed448 on ARM Cortex-M4. In *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 93–96. IEEE, 2022.

[3] Zhe Liu, Patrick Longa, Geovandro CCF Pereira, Oscar Reparaz, and Hwajeong Seo. FourQ on Embedded Devices with Strong Countermeasures Against Side-Channel Attacks. In *International Conference on Cryptographic Hardware and Embedded Systems*, pages 665–686. Springer, 2017.

[4] Hwajeong Seo and Reza Azarderakhsh. Curve448 on 32-bit ARM Cortex-M4. In *International Conference on Information Security and Cryptology*, pages 125–139. Springer, 2020.