Efficient Implementation of Supersingular Isogeny-based Diffie-Hellman Key Exchange on ARM

Amir Jalali, Reza Azarderakhsh, Mehran Mozaffari Kermani

I-SENSE Division of Reseach

Florida Atlantic University

`ajalali2016@fau.edu, razarderakhsh@fau.edu, mmkeme@rit.edu`

1. Abstract

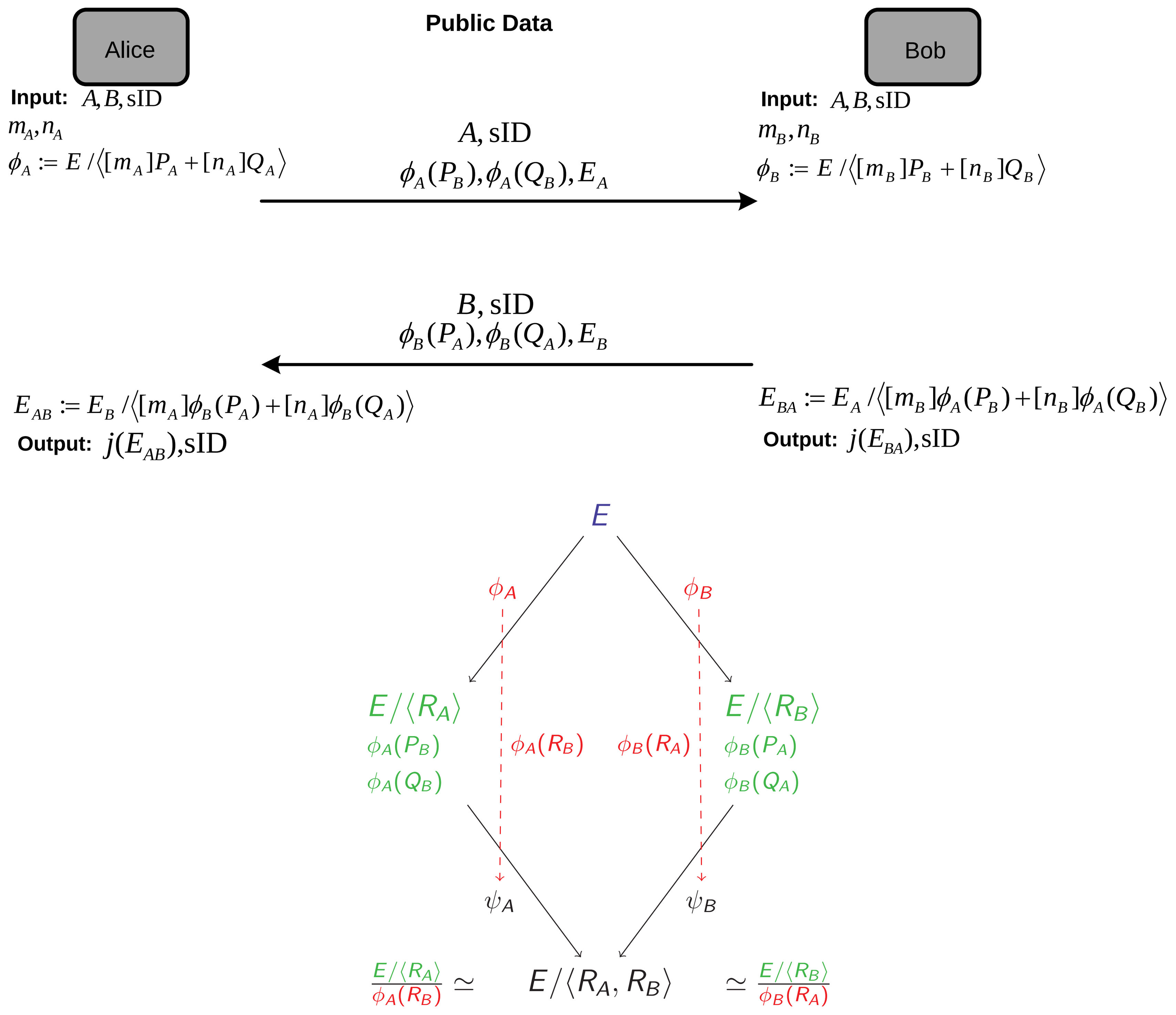
This work investigates the efficiency of implementing the isogeny-based post-quantum key exchange protocol on ARM-powered embedded platforms. The proposed implementation is constatnt-time and resistant against the best known **quantum attacks**. We analyze the recent projective isogeny formulas presented by Microsoft research.

Results are the **fastest** implementation of SIDH protocol on ARM-powered devices found in the literature.

2. Background

- **Isogenies of Elliptic Curves:** Suppose E_1 and E_2 are elliptic curves defined over a finite field $\mathbb{F}_q$. An isogeny $\phi : E_1 \to E_2$ is a non-constant rational map defined over $\mathbb{F}_q$ such that ϕ is a group homomorphism from $E_1(\mathbb{F}_q)$ to $E_2(\mathbb{F}_q)$. If E_1 and E_2 are isogenous, their j-invariant values are the same.
- **SIDH Key Exchange:**

Figure 1: *SIDH Key Exchange Protocol by Jao and De Feo [2011]*

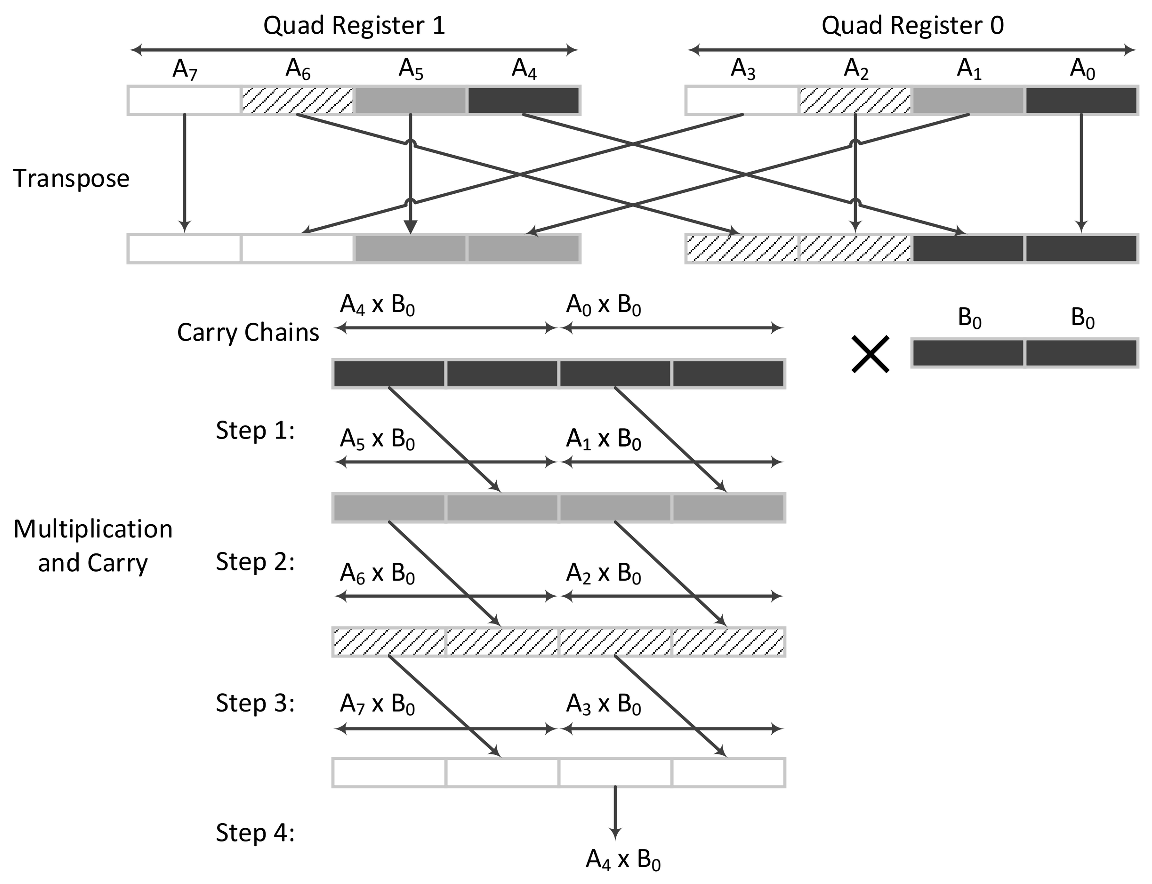


3. Finite Field Arithmetic Implementation

The required finite field arithmetic are implemented using ARMv7 NEON capabilities to boost the performance:

- **Multiplication:** Comba-based multiplication using NEON
- **Reduction:** Comba-based Montgomery reduction using NEON
- **Multiplication over $\mathbb{F}_p$:**

Figure 2: *Finite Field Multiplication Using ARMv7 NEON*



4. Target Platforms

Figure 3: *ARMv7 (Jetson TK1) and ARMv8 (Nexus 6P) Target Platforms in this work*

5. Results

Table 1: *Comparison of affine and projective isogeny implementations on ARM embedded processors.*

Work	Field size [bits]	Device	Isogeny formulas	Timings [$cc \times 10^6$] Alice R1	Bob R1	Alice R2	Bob R2	Total
Costello et al. [2016] [1]	751	ARMv7	Proj.	1,794	2,120	1,665	2,001	7,580
Azarderakhsh et al. [2014]	521		Affine	N/A	N/A	N/A	N/A	1,069
	771			N/A	N/A	N/A	N/A	3,009
	1035			N/A	N/A	N/A	N/A	6,477
This work	503	ARMv7	Affine	83	87	66	68	**302**
	751			437	474	346	375	**1,632**
	1008			603	657	516	484	**2,259**
	751	ARMv8	Proj.	151	135	107	128	**485**
	964			224	252	209	239	**924**

1. Targeted x86-64 architectures, but is portable on ARM. All arithmetic is in generic C.

6. Conclusions

1. In this work, we proved that SIDH can be implemented efficiently on emerging ARM embedded devices and represent a new alternative to classical cryptosystems.
2. We conclude that affine isogeny formulas are comparative in terms of performance with its projective counterpart on ARM devices.
3. In terms of security, projective SIDH performs all the required computations in constant-time, while affine SIDH suffers from non-constant time field inversion computations.
4. Different optimized libraries for different quantum security levels are proposed.
5. SIDH smaller key size compare to other PQC schemes makes this scheme suitable for the applications where the communication bandwidth is a concern.

References

Reza Azarderakhsh, Dieter Fishbein, and David Jao. Efficient Implementations of A Quantum-Resistant Key-Exchange Protocol on Embedded systems. Technical report, 2014. `http://cacr.uwaterloo.ca/techreports/2014/cacr2014-20.pdf`.

Craig Costello, Patrick Longa, and Michael Naehrig. Efficient algorithms for supersingular isogeny Diffie-Hellman. In *Advances in Cryptology*. Springer, 2016.

David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *International Workshop on Post-Quantum Cryptography*, pages 19–34. Springer, 2011.

Efficient Implementation of Supersingular Isogeny Diffie-Hellman Key Exchange on ARM Processors

Amir Jalali, Reza Azarderakhsh, Mehran Mozaffari-Kermani

Abstract

We investigate the efficiency of implementing the Jao and De Feo isogeny-based post-quantum key exchange protocol (from PQCrypto2011) on ARM-powered embedded platforms. In this work, we propose new primes to speed up constant-time finite field arithmetic and per- form isogenies quickly. Montgomery multiplication and reduction are employed to produce a speedup of 3 over the GNU Multiprecision Library. We analyze the recent projective isogeny formulas presented in Costello et al. (Crypto 2016) and conclude that affine isogeny formulas, in terms of performance, are comparable with projective SIDH on ARM devices. However, projective SIDH implementation can be implemented in constant-time for all the key exchange and key generation computations; therefore provides resistancy against timing and cashe attacks. We provide fast affine and projective SIDH libraries over different post-quantum security levels, taking advantage of Single Instruction Multiple Data (SIMD) capabilities of ARMv7 processors along with vectorization. Our assembly-optimized field arithmetic cuts the computation time for the protocol by 50% in comparison to our portable C implementation and performs approximately 3 times faster than the only other ARM-powered results found in the literature. The goal of this work is to show that isogeny-based cryptosystems can be implemented further and be used as an alternative to classical cryptosystems on embedded devices.