Post-Quantum Cryptography

PI: Reza Azarderakhsh, Florida Atlantic University

http://faculty.eng.fau.edu/azarderakhsh/research/

Design, Implementation, and Analysis of Quantum-Resistant Algorithms on Smart Handheld Embedded Devices

- The goal of this project is to assess feasibility of designing and implementing isogeny-based cryptography on emerging embedded systems.

- Outcomes from this research will enable design of quantum-resistant security protocols and identify their security and performance on smart handheld devices using ARM-powered processors.

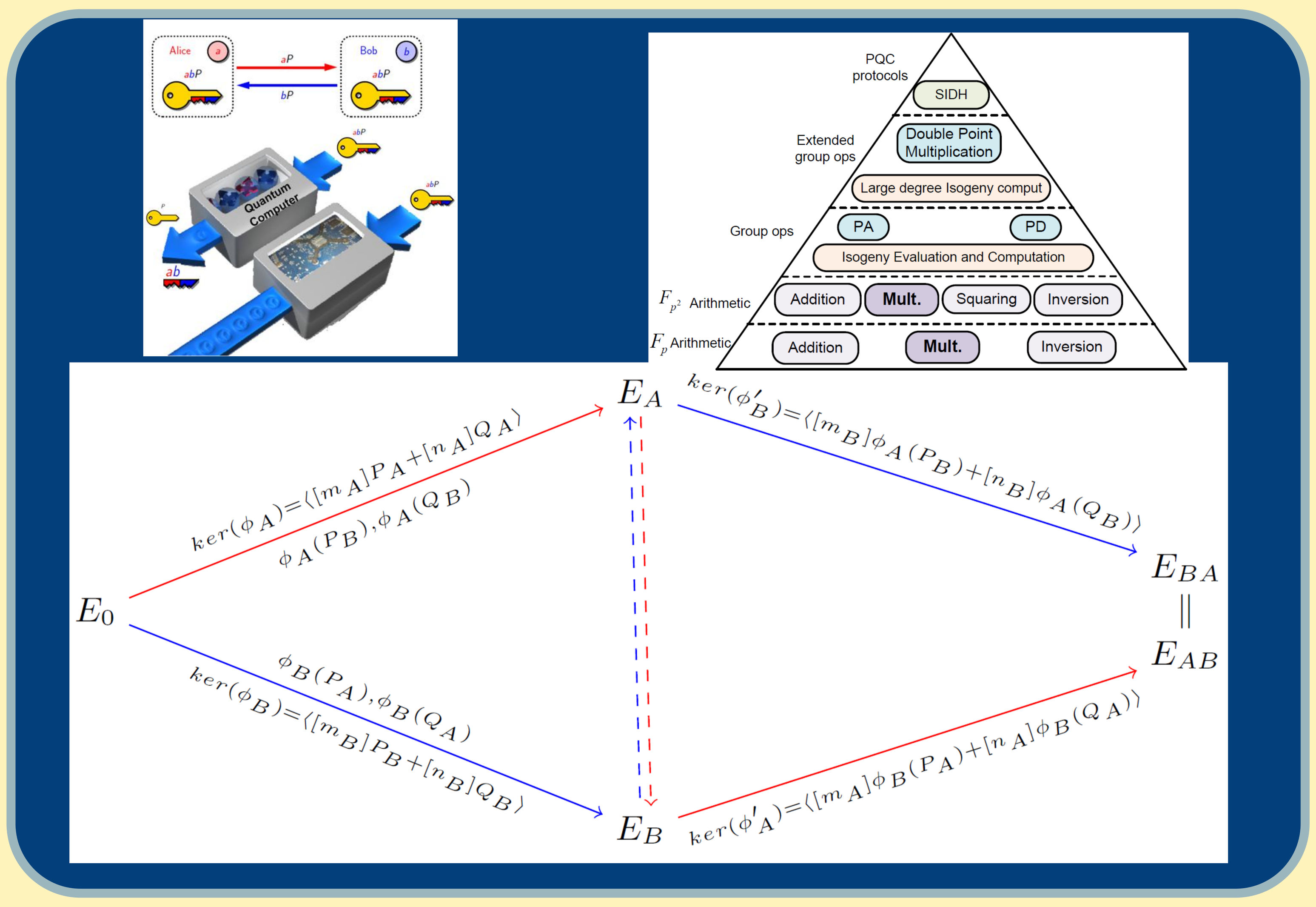


Table 1: Comparison of key sizes (in bits) for different PQC algorithms for 128-bit security level [14]

Algorithm	NTRU [43]	Ring-LWE [62]	SPHINCS [16]	Hash [36]	McEliece [10]	SIDH [45]	SIDH Compr.[1] [6]	RSA	ECC
Public Key	4,939	7,498	1,024	7,296	1,991,880	6,144	**3,072**	3,072	256
Private Key	1,398	14,000	1,024	152	1,537,536	768	768	3,072	256
Signature	–	5,600	41,984	19,608	2,960	9,216	9,216	24,576	768

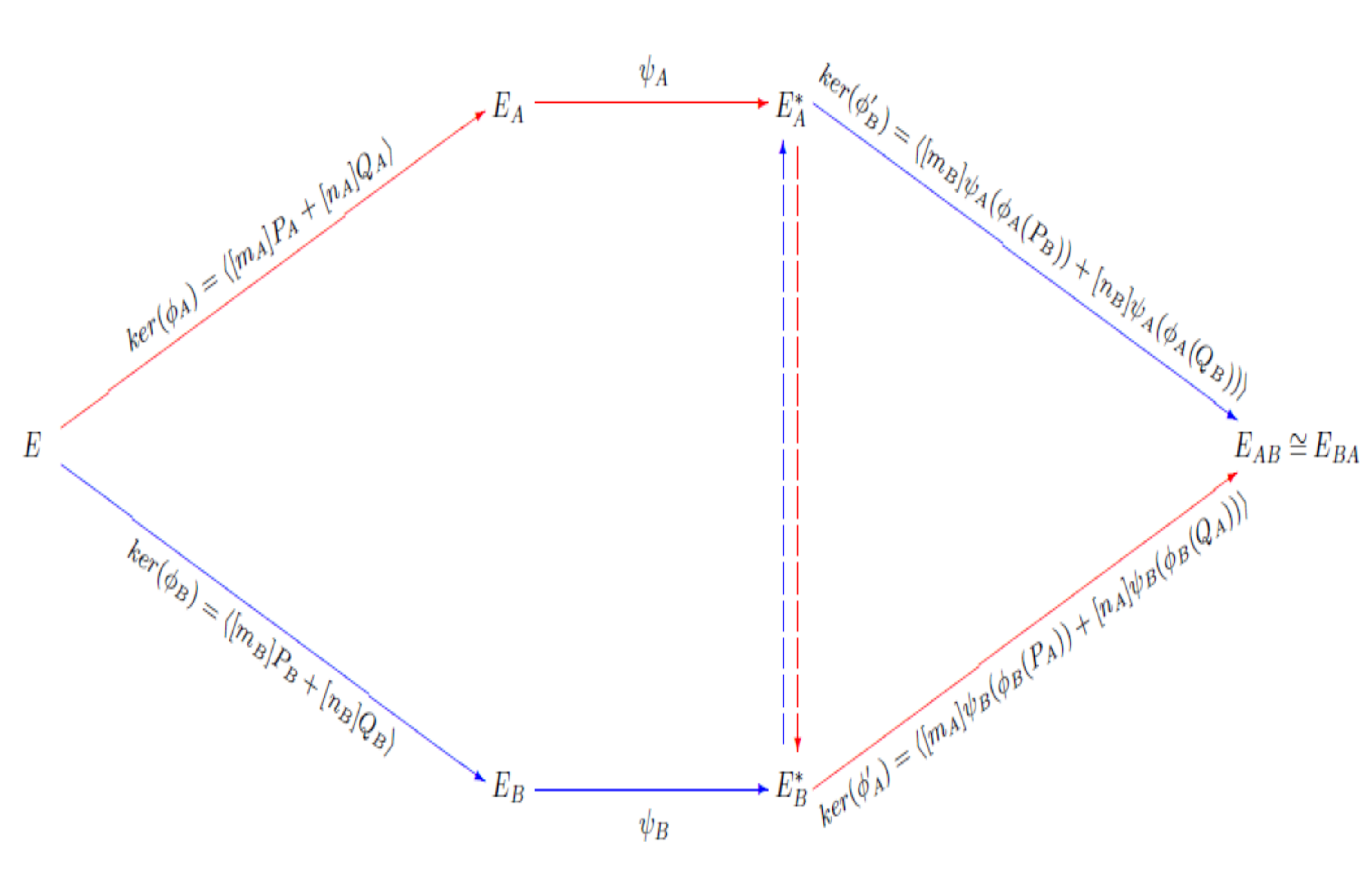
[1] The PI's prior work with key compression. Note that the calculation in Wikipedia [72] is incorrect.

Approach

To study the use of new families of isogeneis in designing and implementing quantum-resistant cryptosystems.
- Analyze the security of isogeney-based cryptosystems from the computational standpoint.
- Improve the performance isogeny algorithms for quantum setting

- Extreme need for high-speed computations of post-quantum crypto.
- Explore lower-level and finite field arithmetic computations
- Investigate time efficiency of implemntations.

- Fastest implementations of SIDH on ARM processors.
- Key compression cut the key size by half



Beagle Board Black (ARM v7) Cortex-A8 at 1.0 GHz using C											
Field	$\mathbb{F}_p$ [cc]					$\mathbb{F}_{p^2}$ [cc]				Key Exch. [cc × 10^3]	
Size	A	S	M	mod	I	A	S	M	I	Alice	Bob
p_{512}	115	1866	2295	3429	40100	1241	12229	14896	72400	483,968	514,786
p_{768}	142	3652	4779	6325	71500	1404	23167	28459	135400	1,406,381	1,525,215
p_{1024}	168	5925	8202	10150	111900	1558	38046	46891	211400	3,135,526	3,367,448

Beagle Board Black (ARM v7) Cortex-A8 at 1.0 GHz using ASM and NEON											
Field	$\mathbb{F}_p$ [cc]					$\mathbb{F}_{p^2}$ [cc]				Key Exch. [cc × 10^3]	
Size	A	S	M	mod	I	A	S	M	I	Alice	Bob
p_{512}	70	718	953	962	40100	279	4445	6736	52756	216,503	229,206
p_{1024}	120	2714	3723	3956	111900	375	15714	23682	150795	1,597,504	1,708,383

Authenticated Key-exchange based on Isogenies on elliptic curves

Digital Signature based on isogenies on elliptic curves

Interested in meeting the PIs? Attach post-it note below!