Review of the presentation *"Quantum-Safe Isogeny-Based Cryptography: Extended SIDH"*

Israel Buitrón-Dámaso

December 4, 2018

Abstract

Review of Daniel Idelfonso Cervantes Vázquez presentation titled *"Quantum-Safe Isogeny-Based Cryptography: Extended SIDH"* as a part of *PhD seminar* class.

1 Review

The Diffie-Hellman (DH) problem is a mathematical problem about exchanging a *secret*. It is based on Discrete Logarithm Problem (DLP) and this, in turn, can be used with certain sets, e.g., as integer numbers or elliptic curves.

In the review of the state-of-the-art, he found a proposal of a DH protocol [FJP11] that considers as operations the use of isogenies on supersingular elliptic curves and their curves as the secret to share. This is called Diffie-Hellman based on Isogenies over Supersingular Elliptic Curves (SIDH) protocol. It has as its main advantage the use of *small* keys but as a disadvantage a slower performance compared to other post-quantum protocols.

In this work, Daniel has studied SIDH internals, and he has made interesting contributions. Those are focused on reducing SIDH disadvantage by proposing a variant which they named extended SIDH (eSIDH). It uses curves $E/\mathbb{F}_{p^2}$ where p is a prime of the form $p = 2^{e_A} l_B^{e_B} l_C^{e_C} f \pm 1$, other small primes l_B and l_C and l_C, and $e_A, e_B, e_C \in \mathbb{Z}^+$ that satisfy $l_A^{e_A} \approx (l_B^{e_B} l_C^{e_C})$. Additionally, it makes use of Montgomery and Edward models that allow performing arithmetic operations faster. This takes advantage of the best of both models.

Among, the contributions achieved, he developed a software implementation that takes advantage of the parallel execution of arithmetic operations. This had as experimental result, the reduction of the cost of isogeny generation and evaluation. Obtaining an acceleration factor of 1.67 and maintaining a quantum security level of 128 bits, compared to SIDH original version.

2 Remarks

- It would be interesting to study other ways to parallelize protocol processes in several levels.
- Although it can be deduced that a s-isogeny refers to an *isogeny of degree* s, the concept was not clearly explained in the presentation.
- I suggest to use images instead of text in a slideshow to share ideas. His presentation has many good examples, i.e., slide 1 titled *"Secret Sharing - Diffie Hellman"*, which explains DH idea with colors. On the other hand, slide 2 titled *"Discrete Log on finite fields"* is not a good example. It has several text and it is not easy to distinguish Alice and Bob conversation. I guess he could use visual resources in slides 6 and 15. It could be better to distribute the content in many slides with less information or with too detailed. Images are often useful for relating to concepts. Linking ideas or concepts by showing them with images is a good strategy [YLC].

- Following with the didactic intention of the Remark 2, I consider that tables in slides 26 and 27 could be replaced by graphics to ease highlight the differences between the results.

References

[FJP11] Luca De Feo, David Jao, and Jérôme Plût. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*. 2011. URL: https://eprint.iacr.org/2011/506 (visited on 11/22/2018).

[YLC] Jung-Chuan Yen, Chun-Yi Lee, and I-Jung Chen. "The effects of image-based concept mapping on the learning outcomes and cognitive processes of mobile learners". In: *British Journal of Educational Technology* 43.2 (), pp. 307–320. DOI: 10.1111/j.1467-8535.2011.01189.x. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1467-8535.2011.01189.x. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-8535.2011.01189.x.