Reseña de presentación *"Quantum-Safe Isogeny-Based Cryptography: Extended SIDH"*

Israel Buitrón-Dámaso

3 de diciembre de 2018

Resumen

Reseña de la presentación de Daniel Idelfonso Cervantes Vázquez titulada *"Quantum-Safe Isogeny-Based Cryptography: Extended SIDH"* en el marco de exposiciones estudiantiles del *Seminario de Doctorado*.

1. Reseña general

El protocolo Diffie-Hellman (DH) es un protocolo para el intercambio de un *secreto* que tiene su base en el Problema del Logaritmo Discreto (PLD) y éste a su vez puede ser usado con ciertos conjuntos, p. ej. como números enteros o curvas elípticas.

En la revisión del estado del arte de este trabajo se encontró una propuesta [FJP11] de un protocolo DH que considera como operaciones el uso de *isogenias en curvas elípticas supersingulares* y como secreto a compartir las curvas elípticas, conocido como protocolo Diffie-Hellman basado en Isogenias entre Curvas Elípticas Supersingulares (SIDH). Este protocolo tiene como ventaja principal el uso de claves *pequeñas* pero como desventaja tiene un rendimiento más lento respecto a otros protocolos poscuánticos.

En este trabajo se ha estudiado el funcionamiento de SIDH y han logrado contribuciones interesantes. Éstas están enfocadas principalmente en mitigar dicha desventaja de SIDH mediante la propuesta de una variante que han nombrado SIDH extendido (eSIDH). Éste usa curvas $E/\mathbb{F}_{p^2}$ donde p es un número primo de la forma $p = 2^{e_A} l_B^{e_B} l_C^{e_C} f \pm 1$, con primos pequeños l_B y l_C y $e_A, e_B, e_C \in \mathbb{Z}^+$ que satisfacen $l_A^{e_A} \approx (l_B^{e_B} l_C)^{e_C}$. Adicionalmente, se hace uso de los modelos de Montgomery y de Edward que permiten realizar operaciones aritméticas con mayor eficiencia, con lo que se puede aprovechar lo mejor de ambos modelos.

Entre las contribuciones alcanzadas hasta el momento, además de la propuesta de eSIDH, está su implementación en software que saca aprovecho de la programación en paralelo de operaciones aritméticas. Esto tiene como resultado experimental la reducción del costo en la construcción y la evaluación de isogenias, que comparado con la versión original de SIDH ha demostrado un factor de aceleración de 1,67 manteniendo un nivel cuántico de seguridad de 128 bits.

2. Observaciones

1. Sería interesante estudiar otras formas de paralelizar procesos del protocolo a varios niveles.

2. Aunque se pueda deducir que una s-isogenia refiera a una *isogenia de grado s*, en la presentación no se explica con claridad el concepto.

3. Considero que se debe considerar con seriedad el uso de imágenes en una presentación para transmitir ideas, en vez de usar texto. Tu presentación tiene ejemplos muy buenos, como el caso de la lámina 1 *"Secret Sharing - Diffie Hellman"*, pero también tiene casos donde no aplicaste esto mismo como el caso de la lámina 2 *"Discrete Log on finite fields"*, en donde hay mucho

texto y además no se distingue con facilidad el contenido, particularmente la comunicación entre Alice y Bob. Otras láminas donde creo que se pudo haber utilizado este recurso visual son 6 y 15, donde creo que conviene distruibuir el contenido en láminas con menos información y en su lugar más láminas con datos muy puntuales. Lás imágenes suelen ser útiles para relacionar con conceptos y a su vez, el proceso de relación de conceptos puede reducirse a la relación de imágenes [YLC].

4. Siguiendo con la intención didáctica de la observación 3, considero que las tablas de las láminas 26 y 27 podrían haberse sustituido por gráficas que permitieran destacar visualmente las diferencias entre los resultados.

Referencias

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

[YLC] Jung-Chuan Yen, Chun-Yi Lee e I-Jung Chen. «The effects of image-based concept mapping on the learning outcomes and cognitive processes of mobile learners». En: *British Journal of Educational Technology* 43.2 (), págs. 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.