Técnicas de compressão de chaves para criptossistemas baseados em isogenias

Gustavo H. M. Zanon[1], **Marcos A. Simplicio Jr.**[1]

[1]Departamento de Engenharia de Computação e Sistemas Digitais
Universidade de São Paulo (USP), São Paulo, Brasil

gustavo.zanon@alumni.usp.br, mjunior@larc.usp.br

Abstract. *Supersingular isogeny-based cryptography is one of the most recent families among proposals resistant to attacks with quantum computers. Its low bandwidth occupation is noteworthy compared to other key agreement protocols, enhanced by the possibility of key compression at the cost of a significant overhead in processing time. In this work, efficient techniques are suggested to minimize the main processing bottlenecks involved in key compression and decompression. Together, these techniques produce observed gains of up to three times over the best results of previously proposed techniques.*

Resumo. *Criptografia baseada em isogenias supersingulares constitui uma das famílias mais recentes dentre as propostas resistentes a ataques com computadores quânticos. Destaca-se sua baixa ocupação de banda em comparação a outros protocolos de acordo de chave, potencializada pela possibilidade de compressão de chaves ao custo de uma sobrecarga significativa no tempo de processamento. Neste trabalho, sugerem-se técnicas eficientes para minimizar os principais gargalos de processamento envolvidos na compressão e descompressão de chaves. Em conjunto, essas técnicas produzem ganhos observados de até três vezes em relação aos melhores resultados de técnicas anteriormente propostas.*

1. Introdução

Pode-se argumentar que o acordo de chaves é o protocolo criptográfico quantitativamente mais importante, pois hoje em dia quase todos serviços online são feitos através do protocolo `TLS`, como comércio eletrônico, acesso a e-mail pessoal ou comercial, ou ainda por protocolos similares, como a criptografia ponta-a-ponta empregada por aplicativos como WhatsApp e Signal. Dado que esses protocolos são construídos por meio de acordo de chaves, justifica-se sua importância em termos de volume.

Por muito tempo a segurança foi negligenciada em detrimento de desempenho, porém com o passar do tempo foi reavaliada como fator sumamente relevante a ponto de se tornar o padrão de acesso, seja porque as máquinas (cliente e servidor) estão mais baratas, seja porque a cultura dos provedores de serviços *online* deslocou-se para uma preocupação maior com segurança em vez de desempenho. Evidência disso encontra-se

Agradecimentos. O presente trabalho foi realizado com apoio parcial do CNPq (bolsa de produtividade 304643/2020-3) e pela Ripple através da *University Blockchain Research Initiative*.

no acesso a sites de serviços como *e-commerce*, a fim de proteger o consumidor de ataques a transações, e também a sites institucionais, como por exemplo os serviços oferecidos pela Google, que agora estão sendo feitos por via de regra via `https` [Lidzborski 2014]. Ainda, a Google adotou o padrão de exibir resultados de buscas com a versão `https` de páginas que oferecerem esse tipo de segurança [Bahajji 2015].

Em paralelo, nota-se nos últimos anos uma preocupação crescente com ataques montados com o auxílio de computadores quânticos, que contornam eficientemente todas as proteções oferecidas pela criptografia assimétrica convencional [Shor 1994]. Um exemplo disto está nas experiências conduzidas pela Google em seu navegador Chrome para Desktops, onde parte das comunicações seguras eram feitas através do acordo de chaves pós-quântico NewHope [Braithwaite 2016]). Essa preocupação é inteiramente justificada face aos avanços recentes na construção de computadores quânticos eficientes: empresas como IBM, Intel, Microsoft e Google têm investido recursos em busca de um computador quântico de propósito geral. Também computadores quânticos com propósitos mais limitados como é o caso do D-Wave, que, apesar de limitado, é capaz de resolver eficientemente o problema da fatoração inteira em que se apoia o criptossistema RSA tradicional [Peng et al. 2019]. Tendo isso em vista, um protocolo moderno de acordo de chaves deve também resistir a ataques quânticos.

2. Motivação

Entre o final de 2015 e início de 2016, o Instituto Nacional de Padrões e Tecnologias dos Estados Unidos (NIST) iniciou um esforço conjunto entre pesquisadores através de uma competição com a finalidade de definir algoritmos a serem utilizados como padrões de segurança no cenário pós-quântico. Surpreendentemente, candidatos a protocolos de acordo de chaves resistentes a ataques quânticos apoiam-se em um número reduzido de problemas computacionais: como reticulados [Alkim et al. 2016], códigos corretores de erros [Aragon et al. 2017] e isogenias entre curvas elípticas; Há também outros problemas, porém de âmbito muito mais restrito, como assinaturas baseadas em *hash*, sistemas multivariados quadráticos e protocolos de identificação baseados em núcleos e percéptrons permutados.

Dentre as famílias de problemas computacionais citadas, a mais recente é a baseada em isogenias, que possuí como principal vantagem o tamanho reduzido de chaves em relação aos demais candidatos, com possibilidade de se tornarem ainda menores através de técnicas de compressão de chaves. Entretanto, as técnicas utilizadas para a (des)compressão de chaves resultam em perdas significativas de desempenho [Azarderakhsh et al. 2016, Costello et al. 2017]. Outro contraponto em relação aos criptossistemas baseados em isogenias surge exatamente pelo fato de serem propostas recentes e não possuírem a mesma maturidade tecnológica dos concorrentes. Para que essa maturidade seja adquirida, muita pesquisa deverá ser feita sob essa área, assim como as alternativas baseadas em códigos, reticulados e semelhantes começaram ineficientes e ganharam melhorias ao longo de anos ou décadas.

3. Objetivos

O trabalho aqui delineado propõe melhorias tecnológicas para tornar madura a família de algoritmos baseados em isogenia de acordo com as métricas de ocupação de banda, desempenho e resistência a ataques de ambos computadores clássicos e quânticos.

O escopo limita-se em investigar técnicas para melhorar o criptossistema SIKE, uma vez que foi submetido à padronização do NIST e portanto acredita-se que tenha segurança pós-quântica. Esse criptossistema reduz a ocupação de banda através da compressão de chaves ao custo de desempenho, uma vez que esse processo é computacionalmente intensivo.

Esta pesquisa de mestrado busca investigar novos algoritmos eficientes para compressão de chaves de modo que se possa reduzir ocupação de banda sem impacto significativo de desempenho. Assim, pode-se definir uma constante entre tempo e banda de tal forma que, ao se obter uma economia de metade da banda, não mais do que o dobro de processamento seja gasto como consequência. Como resultado, estima-se que o tempo gasto com compressão não seja superior ao tempo gasto na utilização das chaves.

Por se tratar de uma literatura recente, há pouco material disponível em português sobre o assunto e espera-se que a dissertação forneça um material auto-contido na medida do possível que supra essa necessidade.

4. Justificativa e métodos

A notável escassez de problemas computacionais capazes de sustentar as propriedades de segurança de criptossistemas efetivos cria a necessidade de não apenas investigar a resistência desses esquemas (diante de computadores clássicos e quânticos), mas também de otimizar os poucos sistemas conhecidos segundo as principais métricas de custo.

Tratando-se de protocolos de acordos de chaves criptográficas para sessões *online*, as métricas naturais são:

- Ocupação de banda.
- Velocidade de processamento;

Métricas específicas de aplicações particulares como redes de sensores sem fio podem incluir eficiência energética também, mas tipicamente essas métricas adicionais são correlacionadas com as métricas principais (por exemplo, o consumo de energia é comumente proporcional, nas plataformas típicas de redes de sensores sem fio, aos tempos de processamento e/ou à ocupação de banda).

Contudo, a característica mais distintiva e marcante de criptossistemas isógenos em comparação com outras propostas pós-quânticas (por assim dizer, o seu *sales pitch*) é a banda potencialmente reduzida que ocupa, menor que qualquer outra família de criptossistemas pós-quânticos na literatura e apenas pouco maior que a banda ocupada por criptossistemas convencionais (suscetíveis a ataques quânticos). Por essa razão, esses esquemas são a opção mais óbvia para cenários onde a ocupação de banda é um gargalo crítico, e isso torna a métrica da ocupação de banda a mais crucial para esses esquemas (sem deixar de lado a velocidade de processamento, que ainda é importante embora não seja o mais central).

Isso tudo justifica a investigação de métodos para reduzir a ocupação de banda em sistemas isógenos supersingulares, mantendo a eficiência de processamento tão alta quanto possível para uma largura específica de banda, que é exatamente o objetivo deste trabalho.

5. Sumário das contribuições de pesquisa

Cada um dos resultados obtidos pela pesquisa realizada constitui pequenas melhorias complementares. Esses resultados são sumarizados a seguir:

- *Geração eficiente de bases de torção.*
  - Assumindo os parâmetros usuais $\ell_{\mathsf{A}} = 2, \ell_{\mathsf{B}} = 3$, melhora-se a geração de base para $E[2^m]$ e $E[3^n]$. O algoritmo denominado geração de *bases emaranhadas* proposto para gerar bases de 2^m-torção é aproximadamente $15.9\times$ vezes mais rápido que a geração usual apresentada no trabalho anterior e tem aplicações não apenas em troca de chaves, mas também em funções hash baseadas em isogenias [Doliskani et al. 2017]. Para 3^n-torção, observa-se que o algoritmo ingênuo é mais eficiente (tanto na teoria quanto na prática) do que a versão explícita 3-descenso de [Schaefer and Stoll 2004] usado por Costello *et al.*.
  - Introduz-se a técnica *Elligator compartilhado* para acelerar ainda mais a construção da base de torção durante a descompressão, que permite uma geração de base ternária $1.5 - 2.8\times$ mais rápida quando comparada com a técnica de geração simples anterior. Quando a nova geração de base emaranhada é acoplada ao Elligator compartilhado, as melhorias são ainda mais significativas, chegando a ser $29.9\times$ mais rápido.
- *Cálculo eficiente de logaritmos discretos.*
  - Inspirado pelo método de *estratégia ótima* de De Feo *et al* para calcular isogenias de grau suave [DeFeo et al. 2014], propõe-se um algoritmo para calcular logaritmos discretos no μ_{ℓ^n} dado um método eficiente para calcular logaritmos discretos em μ_ℓ onde ℓ é um primo pequeno, ou mais geralmente, um algoritmo para computar logaritmos discretos no grupo $\mu_{(\ell^w)^{n/w}}$ quando $w \mid n$, dado um método eficiente para calcular logaritmos discretos em μ_{ℓ^w}.
  - Descreve-se como calcular Pohlig-Hellman no grupo μ_{ℓ^n} a partir de uma adaptação da estratégia ótima de percurso, dado um método eficiente para computar logaritmos discretos no grupo μ_{ℓ^w} quando $w \nmid n$.
- *Cálculo eficiente de emparelhamentos sobre curvas supersingulares.*
  - Introduz-se a técnica de *decomposição reversa de base*, que combinado com as melhorias anteriores, permite otimizações adicionais de compressão e descompressão. Por exemplo, cada parte só precisa computar 4 emparelhamentos em vez de 5. Além disso, duas multiplicações custosas pelo cofator 3^n são poupadas durante a compactação de uma parte e uma multiplicação pelo cofator 3^n é poupada durante a descompactação da outra parte.
  - As formas especiais de pares de pontos gerados como bases emaranhadas e a existência de um subcorpo descartado por [Costello et al. 2017] para otimizar o emparelhamento Tate foram exploradas. Com isso, atinge-se uma melhoria de $1.4\times$ para a fase de emparelhamento sobre os algoritmos usados por [Costello et al. 2017] para combinações binárias e ternárias.

Em conjunto, o resultado das melhorias complementares obtidas geram um impacto substancial, como pode-se observar na seguinte tabela com resultados práticos para as operações de alto nível de (des)compressão de chaves:

	2^m-torção ($w = 2$)			3^n-torção ($w = 6$)		
operação	SIDH v2.0	este trabalho	razão	SIDH v2.0*	este trabalho	razão
um logaritmo discreto	5.88	2.57	**2.3**	4.71	1.17	**4.0**
fase de emparelhamento	33.23	25.37	**1.3**	37.72	29.04	**1.3**
compressão	75.49	37.07	**2.0**	79.33	54.14	**1.5**
descompressão	28.76	8.97	**3.2**	25.95	12.91	**2.0**

Note que a descompressão incorpora a otimização do Elligator compartilhado.
* "SIDH v2.0" refere-se aos resultados relatados em [Costello et al. 2017].

Tabela 1. Resultados do obtidos por etapa do protocolo.

6. Produção científica

Este trabalho produziu dois artigos, o primeiro aceito na conferência internacional PQ-Crypto [Zanon et al. 2018] e o segundo, aceito na revista científica *IEEE Transactions on Computers*, [Zanon et al. 2019]. Os resultados serviram de base para os trabalhos de Geovandro Pereira, Javad Doliskani e David Jao [Pereira et al. 2020], bem como de Michael Naehrig e Renes Joost [Naehrig and Renes 2019], e possibilitaram que o uso de compressão de chaves se tornasse uma opção do esquema SIKE, atualmente um dos finalistas na competição de padronização do NIST.

Para maiores detalhes, a dissertação completa encontra-se em: `https://www.teses.usp.br/teses/disponiveis/3/3141/tde-23092021-104520/pt-br.php`.

Referências

Alkim, E., Ducas, L., Pöppelmann, T., and Schwabe, P. (2016). Post-quantum key exchange: A new hope. In *Proceedings of the 25th USENIX Conference on Security Symposium*, SEC'16, page 327–343, USA. USENIX Association.

Aragon, N., Barreto, P. S. L. M., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C., Gaborit, P., Gueron, S., Guneysu, T., Aguilar Melchor, C., Misoczki, R., Persichetti, E., Sendrier, N., Tillich, J.-P., and Zémor, G. (2017). BIKE: Bit Flipping Key Encapsulation. Submission to the NIST post quantum standardization process.

Azarderakhsh, R., Jao, D., Kalach, K., Koziel, B., and Leonardi, C. (2016). Key compression for isogeny-based cryptosystems. In *Proceedings of the 3rd ACM International Workshop on ASIA Public-Key Cryptography*, pages 1–10, Abu Dhabi, EAU. ACM.

Bahajji, Z. A. (2015). Indexing https pages by default. `https://webmasters.googleblog.com/2015/12/indexing-https-pages-by-default.html`. Acessado em 4 de agosto de 2019.

Braithwaite, M. (2016). Experimenting with post-quantum cryptography. `https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html`. Acessado em 5 de agosto de 2019.

Costello, C., Jao, D., Longa, P., Naehrig, M., Renes, J., and Urbanik, D. (2017). Efficient compression of SIDH public keys. In *Advances in Cryptology – Eurocrypt 2017*, number 10210 in Lecture Notes in Computer Science, pages 679–706, Paris, France. Springer.

DeFeo, L., Jao, D., and Plût, J. (2014). Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247.

Doliskani, J., Pereira, G. C. C. F., and Barreto, P. S. L. M. (2017). Faster cryptographic hash function from supersingular isogeny graphs. Cryptology ePrint Archive, Report 2017/1202. `https://eprint.iacr.org/2017/1202`.

Lidzborski, N. (2014). Staying at the forefront of email security and reliability: Https-only and 99.978 percent availability. `https://googleblog.blogspot.com/2014/03/staying-at-forefront-of-email-security.html`. Acessado em 4 de agosto de 2019.

Naehrig, M. and Renes, J. (2019). Dual isogenies and their application to public-key compression for isogeny-based cryptography. In Galbraith, S. D. and Moriai, S., editors, *Advances in Cryptology – ASIACRYPT 2019*, pages 243–272, Cham. Springer International Publishing.

Peng, W., Wang, B., Hu, F., Wang, Y., Fang, X., Chen, X., and Wang, C. (2019). Factoring larger integers with fewer qubits via quantum annealing with optimized parameters. *Science China Physics, Mechanics and Astronomy*, 62.

Pereira, G., Doliskani, J., and Jao, D. (2020). x-only point addition formula and faster compressed sike. *Journal of Cryptographic Engineering*, pages 1–13.

Schaefer, E. and Stoll, M. (2004). How to do a p-descent on an elliptic curve. *Transactions of the American Mathematical Society*, 356(3):1209–1231.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, SFCS '94, pages 124–134, Washington, DC, USA. IEEE Computer Society.

Zanon, G. H. M., Simplicio Jr, M. A., Pereira, G. C. C. F., Doliskani, J., and Barreto, P. S. L. M. (2018). Faster isogeny-based compressed key agreement. In *International Workshop on Post-Quantum Cryptography – PQCrypto 2018*, volume 10786 of *Lecture Notes in Computer Science*, pages 248–268, Fort Lauderdale (FL), US. Springer.

Zanon, G. H. M., Simplicio Jr, M. A., Pereira, G. C. C. F., Doliskani, J., and Barreto, P. S. L. M. (2019). Faster key compression for isogeny-based cryptosystems. *IEEE Transactions on Computers*, 68(5):688–701.