Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 10, n. 1, 2023.

Trabalho apresentado no XLII CNMAC, Universidade Federal de Mato Grosso do Sul - Bonito - MS, 2023

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Sobre a aplicação de Curvas Elípticas na criptografia em Redes Sociais

Aline de L. Z. Lunkes[1], Fábio Borges[2]
LNCC, Petrópolis, RJ

Resumo. O uso da internet vem crescendo ao longo dos anos, consequentemente, o uso de meios de comunicação online entre pessoas. Por isso, para garantir a privacidade e a segurança dos usuários ao navegar na web mostramos neste trabalho a aplicação de Curvas Elípticas em envio de mensagens instantâneas via internet, a saber, *Facebook Messenger* e *WhatsApp*, com o auxílio da criptografia. Motivando assim, o estudo de curva elíptica em matemática com aplicação em criptografia. A segurança dos algoritmos de criptografia com a curva elíptica sobre corpos finitos é baseada no Problema do Logaritmo Discreto (PLD), em inglês, Discrete Logarithm Problem (DLP), tornando mais sigilosa a comunicação entre os pares envolvidos. Além disso, os esquemas de criptografia baseados no grupo de pontos de uma curva elíptica, garantem a mesma segurança que os construídos sobre o grupo multiplicativo de um corpo finito (por exemplo, RSA), mas com chaves menores.

Palavras-chave. Criptografia, Curva Elíptica, Problema do Logaritmo Discreto, Privacidade, Segurança, Redes Sociais

1 Introdução

A demanda de novas tecnologias e da internet tem se destacado ao longo dos anos, tanto na indústria quanto no dia-a-dia. Crescendo assim, o uso de aplicativos para facilitar a conexão entre pessoas nas redes sociais, tanto em celulares quanto em computadores. Devemos levar em conta, a segurança e privacidade dos dados compartilhados. Deste modo, apresentamos neste trabalho a aplicação de Criptografia com curva elíptica nos aplicativos mais utilizados na última década.

Em 1976, W. Diffie e M. Hellman propuseram uma solução para a comunicação em um canal inseguro, estabelecendo o uso de chaves criptográficas, ver [5]. O esquema de criptografia depende do compartilhamento de um par de chaves, pública e privada, entre os envolvidos na troca de uma mensagem. Assim, cada usuário possui duas chaves, a saber, uma pública e outra privada. Nos esquemas de criptografia para cifrar uma mensagem utilizamos a chave pública do usuário remetente, e consequentemente para decifrar utilizamos a sua chave privada. Somente a chave privada pode decifrar a mensagem corretamente.

O conceito de curva elíptica em criptografia assimétrica foi proposto independentemente em 1985, por Victor S. Miller [12] e Neal Koblitz [9]. Tal conceito se dá pelo uso do Problema do Logaritmo Discreto sobre curva elíptica. Uma vantagem deste algoritmo é que permite o uso de chaves menores que o algoritmo clássico de criptografia assimétrica, a saber RSA, ver [11]. A matemática envolvida é complexa e requer uma autoridade certificadora para garantir a identidade e a confiabilidade das chaves públicas, garantindo assim, uma maior segurança no algoritmo de curva elíptica. Portanto, torna-se difícil a quebra do algoritmo.

[1]alunkes@lncc.br
[2]borges@lncc.br

As curvas elípticas estão presentes em importantes problemas matemáticos, como na prova do último Teorema de Fermat, ver [16], desempenharam um papel importante na fatoração de inteiros, testes de primalidade (ver [10]) e, na criptografia de chave pública. Além disso, a criptografia com curva elíptica não é resistente à computação quântica, ou seja, ainda não está estabelecida. Existe um estudo mais aprofundado sobre isogenia entre curva elíptica utilizando o algoritmo de SIKE, que no passado sofreu um ataque, e está sendo revisado por pesquisadores para se adequar a este novo ataque, ver [4] e [15]. Por isso, devemos escolher com cuidado a curva elíptica no uso de nossos algoritmos. Este trabalho está dividindo entre a formulação matemática da curva elíptica e a aplicação em criptografia de chave pública assimétrica.

2 Curvas Elípticas

Nesta seção tratamos do conceito de curva elíptica, que será utilizado ao longo deste trabalho. Seja $\mathcal{F}$ um corpo finito de característica maior que 3, e suponha que c e d sejam elementos em $\mathcal{F}$ para os quais $x^3 + cx + d$ não tem raízes múltiplas, ou, equivalentemente, que o discriminante satisfaça $4c^3 + 27d^2 \neq 0$, ver [1]. Considere a seguinte equação afim de *Weierstrass*,

$$y^2 = x^3 + cx + d. \tag{1}$$

Definição 2.1. *Uma curva elíptica, denotada por* $\mathbf{E}$ *é o conjunto de pares ordenados* $(x, y) \in \mathcal{F} \times \mathcal{F}$ *de soluções para a equação* (1) *junto com um elemento especial, a saber, o ponto no infinito, denotado por* $\mathcal{O}$ *e chamado de identidade da curva elíptica.*

Devido à simetria das curva elíptica em relação ao eixo x, o inverso sempre existe, e o inverso da identidade é a própria identidade. Uma curva elíptica forma um grupo abeliano com a operação de soma e vale as seguintes propriedades de grupo:

1. A soma está bem definida;
2. Vale a associatividade e a comutatividade;
3. Vale o elemento neutro da soma e a existência da identidade.

Vamos considerar $\mathbf{E}$ sobre os reais, e sejam P e Q dois pontos em $\mathbf{E}$. Definimos $\mathbf{E}$ em quatro casos:

- **CASO 1:** Suponha que o ponto $P = (x, y)$ é a identidade aditiva, então o resultado é igual ao outro ponto, ou seja, $P + \mathcal{O} = \mathcal{O} + P = P$ para todo $P \in \mathbf{E}$.
- **CASO 2:** Suponha que o ponto $P = (x, y)$ é o inverso do ponto $Q = (x, y)$, resultando na identidade, ou seja, $P = -Q \Longrightarrow -P = (x, -y)$. Assim, $P + Q = -Q + Q = 0$, implicando no elemento neutro da soma, ou ainda no ponto do infinito (identidade).
- **CASO 3:** Suponha que os pontos $P \neq \pm Q$, então traçamos uma reta que passe pelo ponto P e Q, e não é tangente ao gráfico em P ou Q. Então a reta que conecta P e Q deve interceptam o gráfico em um único ponto, que é o terceiro ponto, denotado por R. Assim, $P + Q = -R$.

  Observação 2.1. *O caso particular do* ***CASO 3*** *é o* ***CASO 2****, pois a reta intercepta o* $\mathcal{O}$*.*

- **CASO 4:** Suponha que $P = \pm Q$, e é diferente de $\mathcal{O}$, então traçamos uma reta que passe por P e Q, de modo que Q seja tangente ao gráfico no ponto P. Assim, $P + P = 2P = R$.

  a) Suponha que o ponto $P = (x, y)$ não seja um ponto de inflexão. Então a reta tangente em P deve interceptar o gráfico em um único ponto R. Assim, $P + P = -R$.

DOI: 10.5540/03.2023.010.01.0099

b) Suponha que o ponto $P = (x, y)$ seja um ponto de inflexão. Assim, $P + P = -P$.

Com o Teorema 2.1, e o Teorema 2.2 para uma $\mathbf{E}$ sobre $\mathbb{Z}_p$, expressamos algebricamente a operação de adição.

Teorema 2.1. *Seja p um primo com $p > 3$, e suponha que $\mathbf{E}$ seja uma curva elíptica sobre $\mathbb{Z}_p$. Então, $\mathbf{E}$ é isomorfo ao produto direto $\mathbb{Z}_m \times \mathbb{Z}_n$ dos grupos $\mathbb{Z}_m$ e $\mathbb{Z}_n$ com a operação de adição para alguns inteiros m e n com $n|m$ e $n|(p-1)$, ver [8].*

O teorema abaixo está relacionado com a ordem de uma curva elíptica. A ordem ($\#\mathbf{E}$) de uma curva elíptica é dada pelo número total de pontos e o ponto no infinito ($\mathcal{O}$), ver [8].

Teorema 2.2. *(Teorema de Hasse) Seja $\mathbf{E}$ uma curva elíptica definida sobre $\mathbb{Z}_p$ para o primo p. Então*

$$p + 1 - 2\sqrt{p} \leq |\#\mathbf{E}| \leq p + 1 + 2\sqrt{p}.$$

Exemplo 2.1. *Considere a curva $\mathbf{E} : y^2 = x^3 + 5x + 1$ e o corpo $\mathbb{Z}_{11}$. Desta forma, a curva elíptica $\mathbf{E}(\mathbb{Z}_{11})$ é formada pelos seguintes pontos:*

$$\mathcal{O}, (0,1), (0,10), (6,4), (6,7), (7,4), (7,7), (8,5), (8,6), (9,4), (9,7).$$

Como mostramos os casos de uma $\mathbf{E}$ sobre os $\mathbb{R}$, vamos mostrar sobre $\mathbb{Z}_p$. Assim,

- **CASO 1:** Suponha que $P = -Q$, então $P + Q = \mathcal{O}$.
- **CASO 2:** Suponha que $P = Q$, então $P + Q = (x_3, y_3)$, onde

$$x_3 = \left(\left(\frac{3x_1^2 + c}{2y_1}\right)^2 - x_1 - x_2\right) \mod p, \quad \text{e}$$
$$y_3 = \left(\left(\frac{3x_1^2 + c}{2y_1}\right)(x_1 - x_3) - y_1\right) \mod p$$

- **CASO 3:** Suponha que $P \neq \pm Q$, então $P + Q = (x_3, y_3)$, onde

$$x_3 = \left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2\right) \mod p, \quad \text{e}$$
$$y_3 = \left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1\right) \mod p$$

Suponha p um primo com $p > 3$, c e d elementos em $\mathbb{Z}_p$ para os quais $4c^3 + 27d^2 \neq 0 \mod p$. A construção das soluções para a equação (1) módulo p, se dá por:

1. Determine os valores de $x \in \mathbb{Z}_p$ para os quais $z = (x^3 + cx + d) \mod p$ é um quadrado perfeito em $\mathbb{Z}_p$. Os valores de z determinados são 0, considerando o homomorfismo $s(y) = y_2$ em $\mathbb{Z}_p^*$.
2. Determine os valores de $y \in \mathbb{Z}_p$ para os quais $y_2 = z \mod p$. Os valores de z determinados são os resíduos quadráticos em $\mathbb{Z}_p^*$.

Na próxima seção tratamos da criptografia de curva elíptica, e mostramos como ocorre a troca de mensagens instantânea e a troca de chaves compartilhada via aplicativos de conversas.

3 Criptografia com Curvas Elípticas

Um esquema de criptografia é constituído por três algoritmos, a saber, 1) Geração das chaves pública (p_k) e secreta (s_k); 2) Cifrar ($E(m)$), onde encriptamos a mensagem m; e 3) Decifrar ($D(E(m))$). O algoritmo de Whitfield Diffie e Martin E. Hellman é utilizado para o compartilhamento de chaves secretas em um canal inseguro, e é considerado a primeira versão de criptografia de chave pública. Cada usuário possui uma chave pública e secreta. Para criptografar utiliza-se a chave pública do usuário remetente, e para decifrar a chave privada. O processo de decifrar a mensagem somente ocorre com a chave privada.

Segue um exemplo, Alice deseja enviar por um canal inseguro um documento secreto de sua empresa para Dave, para isso, necessitam uma troca de chave secreta compartilhada. Assim, seja $G =< g >$, onde g é um gerador do grupo cíclico de ordem q (primo). Portanto, Alice escolhe aleatoriamente um inteiro secreto $a \in \mathbb{Z}/q\mathbb{Z},\ a \geq 2$ gerando a sua chave secreta, e envia para Dave $A = g^a \mod q$. Dave escolhe aleatoriamente um inteiro secreto $d \in \mathbb{Z}/q\mathbb{Z}$, gerando a sua chave secreta, e envia para Alice $D = g^d$. Logo, a troca de chave secreta compartilhada ocorre do seguinte modo

$$D^a = g^{ad} = A^d. \tag{2}$$

A segurança deste protocolo está baseada na dificuldade computacional de calcular a dados g e q, visto que as variáveis são relativamente grandes, tornando o problema inviável de se calcular, sendo também conhecido como PLD.

3.1 O algoritmo El Gamal com Inteiros

El Gamal propôs um algoritmo também baseado na dificuldade de resolver o PLD, ver [6]. Vamos supor que Bob queira enviar uma mensagem $m \in \mathbb{Z}_q^*$ para Alice. Inicialmente, Alice escolhe $a \in \mathbb{Z}_q$, e logo após calcula $y = g^a \mod q$. Assim, a $p_k = y$ e a $s_k = a$. Bob escolhe aleatoriamente $a \in \mathbb{Z}_q$ e calcula

$$E(m_1) = g^b \mod q \text{ e } E(m_2) = m \cdot y^b \mod q,$$

enviando para Alice o par de mensagem cifrada $(E(m_1), E(m_2))$.

Para decifrar m, Alice calcula

$$\begin{aligned} E(m_2) \cdot E(m_1^a)^{-1} &= m \cdot y^b \cdot (g^{ab})^{-1} \mod q &(3)\\ &= m \cdot (g^{ab}) \cdot (g^{ab})^{-1} \mod q &(4)\\ &= m \mod q. &(5)\end{aligned}$$

Recuperando, a mensagem original m. Desde então muitos algoritmos de criptografia assimétrica usam o PLD como base de sua segurança.

3.2 O algoritmo El Gamal com Curva Elíptica

Como o algoritmo El Gamal trabalha com um grupo, podemos usá-lo sobre curva elíptica. Vamos supor que Alice deseja enviar uma mensagem para Bob, seja m esta mensagem mapeada num ponto de uma curva elíptica. Assim, Bob escolhe aleatoriamente e mantém secreto um inteiro $b \in \mathbb{N}^*$ e envia à Alice $A = b \cdot P$, sendo P um ponto da curva elíptica conhecido publicamente. Alice escolhe um inteiro secreto $A \in \mathbb{N}^*$ e calcula $E(m_1) = a \cdot P$ e $E(m_2) = m + a \cdot A$. Logo, para decifrar a mensagem m, Bob calcula

$$E(m_2) - b \cdot E(m_1) = m + a \cdot b \cdot P - b \cdot a \cdot P = m.$$

DOI: 10.5540/03.2023.010.01.0099

3.3 *Curve 25519*

A escolha da curva elíptica para se utilizar no sistema criptográfico de chave pública para a troca de chaves e mensagens não é trivial, e deve ser escolhida de maneira a otimizar o processo de computação, ver [3]. Assim, para os aplicativos de conversas *WhatsApp*[3] e o *Facebook Messenger*[4] que utilizam o *Signal Protocol* a curva elíptica usada é *Curve 25519* com 256 *bits* de comprimento, introduzida por Daniel Bernstein ver [2], [7] e [14]. Sendo utilizada para o cálculo de chaves compartilhadas por um canal inseguro, gerando chaves de tamanho menores, mas com o mesmo nível de segurança. Assim, sejam os pontos conhecidos da curva elíptica P e Q, devemos determinar o número n

$$P = nQ. \tag{6}$$

Além disso, como mostrado na Seção 2 qualquer curva elíptica pode ser escrita na forma de equação afim de *Weierstrass*. Por exemplo, a curva elíptica na forma de *Montgomery* dada na Definição 3.1 com os parâmetros (x, y) pode ser transformada na forma de Weierstrass para os parâmetros (t, v) dada por $v^2 = t^3 + ct + d$. Uma vantagem do uso da curva na forma de Montgomery, é o cálculo acelerado das operações de adição.

Definição 3.1. *Seja* $\mathbf{E}$ *tal que* $\mathcal{F}_q = \mathbb{Z}_q$ *é corpo de* $G\mathcal{F}(q)$*,* q *primo onde* $q = 2^{255} - 19$*, existindo exatamente* $\dfrac{q-1}{2}$ *quadrados em* $\mathcal{F}_q$*. Assim, definimos a curva de Curve 25519 como*

$$\mathbf{E} : y^2 = x^3 + 486662x^2 + x. \tag{7}$$

Cada usuário possui uma chave de identificação ao instalar o aplicativo de mensagens instantâneas, para o cálculo de suas mensagens compartilhadas. A troca de chaves compartilhada ocorre do seguinte modo, o cálculo é realizado pelo *Signal Protocol* com a chave secreta (s_k) e a chave pública (p_k), retornando uma chave pública para os usuários do tipo (*Curve 25519*, p_k). A curva elíptica *Curve 25519* têm as seguintes vantagens, rapidez nos cálculos para a autenticação e a validação de chave, baixo custo de implementação, e a proteção contra ataques de tempo.

A *Curve 25519* é utilizada para este compartilhamento de chaves na troca de mensagens por um canal inseguro, esta troca é feita internamente pelo *Signal Protocol*. Para a encriptação total das conversas é utilizado um outro algoritmo de criptografia, a saber, AES[5] de 256 bits.

3.4 *Paillier* sobre curvas elípticas

Além do algoritmo de El Gamal com curvas elíptivas e a *Curve 25519* no uso nas redes sociais, temos o algoritmo de criptografia de chave pública homomórfico aditivo tradicional de *Paillier*, que foi adaptado pelo próprio *Paillier* sobre curvas elípticas. Este algoritmo de criptografia é baseado em um esquema de encriptação probabilística sobre curvas elípticas, [13], que também é baseado no PDL. Porém, o nível de segurança deste algoritmo é menos eficiente do que utilizar os algoritmos de El Gamal com curvas elípticas, e com a *Curve 25519*.

Este algoritmo ocorre do seguinte modo: para a Geração das Chaves - suponha que $E_{p^2}(a_p, b_p)$ é alguma elevação de uma curva de traço $(p+2)$, do mesmo modo, $E_{q^2}(a_q, b_q)$ é alguma elevação de uma curva de traço $(q+2)$, definidas sobre $\mathbb{F}_p$ e $\mathbb{F}_q$, respectivamente. Considerando $E_{n^2}(a, b)$ como o remanejamento do teorema do resto chinês de $E_{p^2}(a_p, b_p)$ e $E_{q^2}(a_q, b_q)$ (portanto, é definido sobre o anel $\mathbb{Z}_{n^2}$), onde $n = pq$, temos que $E_{n^2}(a, b)$ é da ordem $n\mu$ onde $\mu = \mu(n) = mmc(p + 2, q + 2)$.

[3] `https://cryptome.org/2016/04/whatsapp-crypto.pdf`

[4] `https://about.fb.com/wp-content/uploads/2016/07/messenger-secret-conversations-technical-whitepaper.pdf`

[5] `https://cryptome.org/2016/04/whatsapp-crypto.pdf`

E por fim, o ponto base $G \in E_{n^2}$ é escolhido de ordem divisível por n, possivelmente de ordem máxima $n\mu$. Portanto, $p_k = (n, b, \sigma, G)$, e $s_k = (p, q)$ ou $\mu = \text{mmc}(p+1, q+1)$.

Seja a mensagem $m \in \mathbb{Z}_n$ a ser cifrada, escolha um número aleatório $r < n$. Assim,

$$E(m) = (m + nr) \cdot G.$$

Para recuperar m, vamos definir sobre $E[n] = \mu \cdot E_{n^2}(a, b)$, um logaritmo elíptico n-ádico $\psi_n(x, y) = -\dfrac{x}{y} \mod n^2$. Desde que $P = m \cdot G$ para $P, G \in E[n]$ e $G \neq \mathcal{O}_{n^2}$, recuperamos m pelo cálculo, $m = \dfrac{\psi_n(P)}{\psi_n(G)} \mod n$. Assim,

$$D(E(m)) = [\psi_n(\mu \cdot E(m)) \cdot (\psi_n(\mu \cdot G))^{-1}] \mod n = m. \tag{8}$$

Portanto, qualquer ponto de E_{n^2} é a imagem de alguma mensagem. Isso é válido pelo fato de que todas as curvas que trabalhamos neste algoritmo são cíclicas.

4 Considerações Finais

A criptografia é uma importante técnica que utiliza a matemática em seus algoritmos. Nesse trabalho apresentamos que ambas são aliadas na segurança e a privacidade de conversas em aplicativos de mensagens instantâneas do tipo *WhatsApp* e *Facebook Messenger*. Descrevemos os conceitos de curva elíptica em matemática, e logo em seguida aplicamos um algoritmo de criptografia do tipo Diffie-Hellman, e El Gamal, para a aplicação de curva elíptica em criptografia. Lembrando que a segurança do algoritmo de curva elíptica em criptografia, se dá pelo PLD, e consequentemente obtemos algoritmos com tamanhos menores de chave pública assimétrica. Deste modo, motivamos o estudo de criptografia com curva elíptica, além de instigar o pensamento sobre a proteção de nossos dados na web.

Agradecimentos

Agradeço a agência de fomento CNPQ pelo auxílio financeiro.

Referências

[1] S. Andria, R. Gondim e R. Salomão. **Introdução à Criptografia com Curvas Elípticas**. 32 Colóquio Brasileiro de Matemática, editora do IMPA, 2019. 139 pp. ISBN: 978-85-244-0428-3. URL: https://impa.br/wp-content/uploads/2022/03/32CBM09_eBook.pdf.

[2] D. J. Bernstein. "Curve25519: New Diffie-Hellman Speed Records". Em: **Public Key Cryptography - PKC 2006**. Ed. por Moti Yung et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 207–228. ISBN: 978-3-540-33852-9.

[3] V. Bhuse. "Review of End-to-End Encryption for Social Media". Em: **International Conference on Cyber Warfare and Security**. Vol. 18. 1. 2023, pp. 35–37.

[4] W. Castryck e T. Decru. **An efficient key recovery attack on SIDH**. Cryptology ePrint Archive, Paper 2022/975. https://eprint.iacr.org/2022/975. 2022. URL: https://eprint.iacr.org/2022/975.

[5] W. Diffie e M. Hellman. "New directions in cryptography". Em: **IEEE Transactions on Information Theory** 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638.

[6] T. El Gamal. "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms". Em: **Proceedings of CRYPTO 84 on Advances in Cryptology**. Santa Barbara, California, USA: Springer-Verlag, 1985, pp. 10–18. ISBN: 0387156585.

[7] A. Gangemi. "WhatsApp: cryptographic aspects". Dissertação de mestrado. POLITECNICO DI TORINO, 2019. URL: https://webthesis.biblio.polito.it/11988/.

[8] R. Klima, N. Sigmon e E. Stitzinger. "Applications of Abstract Algebra with MAPLE". Em: 1nd. CRC Press, 1999.

[9] N. Koblitz. "Elliptic Curve Cryptosystems". Em: **Mathematics of Computation** 48.177 (jan. de 1987), pp. 203–209. ISSN: 0025-5718.

[10] S. Lang. "Elliptic Functions". Em: **Elliptic Functions**. New York, NY: Springer New York, 1987, pp. 5–28. ISBN: 978-1-4612-4752-4. DOI: 10.1007/978-1-4612-4752-4_1. URL: https://doi.org/10.1007/978-1-4612-4752-4_1.

[11] A. Lunkes e F. Borges. "Sobre a aplicação de homomorfismo na criptografia". Em: **Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, n. 1**. Vol. 9. XLI CNMAC, 2022. DOI: 10.5540/03.2022.009.01.0306010306-1. URL: https://proceedings.sbmac.emnuvens.com.br/sbmac/article/view/3878/3928.

[12] V. S. Miller. "Use of Elliptic Curves in Cryptography". Em: **Advances in Cryptology — CRYPTO '85 Proceedings**. Ed. por H. C. Williams. Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, pp. 417–426. ISBN: 978-3-540-39799-1.

[13] P. Paillier. "Trapdooring Discrete Logarithms on Elliptic Curves over Rings". Em: **Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology**. Springer-Verlag, 2000, pp. 573–584. ISBN: 3540414045.

[14] N. Rastogi e J. A. Hendler. "WhatsApp security and role of metadata in preserving privacy". Em: **CoRR** abs/1701.06817 (2017). arXiv: 1701.06817. URL: http://arxiv.org/abs/1701.06817.

[15] C. Téllez, D. Pereira e F. Borges. "Supersingular Isogeny and Ring Learning With Errors-Based Diffie-Hellman Cryptosystems: A Performance and Security Comparison". Em: **Proceedings do WRAC+2018: IV Workshop sobre regulação, avaliação da conformidade, testes e padrões de segurança** (2018).

[16] A. Wiles. "Modular Forms, Elliptic Curves, and Fermat's Last Theorem". Em: **Proceedings of the International Congress of Mathematicians**. Ed. por S. D. Chatterji. Basel: Birkhäuser Basel, 1995, pp. 243–245. ISBN: 978-3-0348-9078-6.

