Criptografia com curvas elípticas – uma pequena introdução

Titus Laska
Institut für Mathematik, Freie Universität Berlin
Arnimallee 7, 14195 Berlin, Alemanha
e-mail: titus.laska@fu-berlin.de

Resumo: Na era digital, a criptografia joga um papel cada vez mais importante tanto na organização social e económica da sociedade como no nosso dia-a-dia. Ao mesmo tempo, trata-se de um assunto de grande interesse, que liga várias áreas da matemática. Apresentamos uma pequena introdução a um dos métodos mais importantes nesta área – a criptografia com curvas elípticas. O artigo é escrito de forma a que não pressuponha conhecimentos prévios nem da teoria das curvas elípticas nem de criptografia.

Abstract In the digital age, cryptography plays an increasingly important role, both in the social and economical organization of society and in our everyday life. At the same time, it is a subject of big mathematical interest that connects various scientific areas. We give a small introduction to one of the most important techniques in the field – Elliptic Curve Cryptography (ECC). The article is written in a way that does not require prior knowledge neither of the theory of elliptic curves nor of cryptography.

palavras-chave: Curvas elípticas, Criptografia

keywords: Elliptic Curves, Cryptography

1 Introdução

A criptografia com curvas elípticas atrai muita atenção quer pelas suas interessantes aplicações e implicações, quer pela pura beleza da teoria matemática envolvida. O artigo divide-se em duas partes: a primeira é uma introdução às curvas elípticas e a segunda descreve os métodos criptográficos fundamentais que se baseiam nelas.

O ponto de partida deste trabalho foram as aulas de Criptografia e Protocolos de Segurança com o Professor Carlos Caleiro no Instituto Superior Técnico em Lisboa, que frequentei como estudante de Erasmus em 2014, e uma apresentação que fiz sobre o tema.

2 Curvas elípticas

O objetivo desta secção é dar uma pequena introdução às curvas elípticas que seja facilmente compreensível para quem não tenha conhecimentos nesta área. Para estudos mais profundos da teoria aqui apresentada e como referência bibliográfica geral, refere-se [6].

Definição. Uma curva elíptica sobre $\mathbb{R}$ é um conjunto da forma

$$E(\mathbb{R}) = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

com números $A, B \in \mathbb{R}$ tais que $4A^3+27B^2 \neq 0$. A equação $y^2 = x^3+Ax+B$ é chamada *equação de Weierstrass*. Aqui, ∞ é um ponto distinguido. Por razões esclarecidas mais abaixo, convém imaginar ∞ como posicionado no *fim* do eixo y. Excluindo este ponto, podemos visualizar os conjuntos $E(\mathbb{R})$ como curvas em $\mathbb{R}^2$. A Figura 1 mostra dois exemplos.[1]

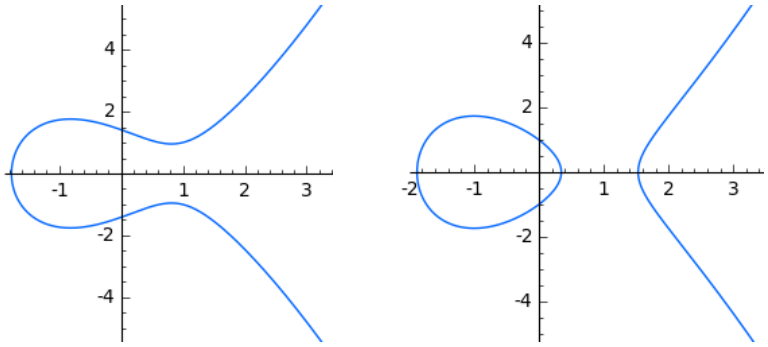

Figura 1: As curvas $y^2 = x^3 - 2x + 2$ e $y^2 = x^3 - 3x + 1$ sobre $\mathbb{R}$.

Temos as seguintes propriedades, cuja demonstração não é difícil:

(i) As curvas são simétricas em relação ao eixo x: Se $(x, y) \in E(\mathbb{R})$, então $(x, -y) \in E(\mathbb{R})$, pela equação que define $E(\mathbb{R})$.

(ii) A condição $4A^3 + 27B^2 \neq 0$ assegura que a curva é não-singular no sentido que as duas derivadas parciais de $F(x, y) := y^2 - x^3 - Ax - B$ são diferentes de zero para todo o $(x, y) \in E(\mathbb{R})$. Exemplos de curvas singulares são dados na Figura 2.

[1] Curvas visualizadas com *Sage*, `www.sagemath.org`.

(iii) Uma curva elíptica $E(\mathbb{R})$ intersecta o eixo x ou uma só vez ou três vezes. O primeiro caso ocorre para $4A^3+27B^2 > 0$, enquanto o segundo ocorre para $4A^3 + 27B^2 < 0$. Na Figura 1, temos um exemplo de cada caso.

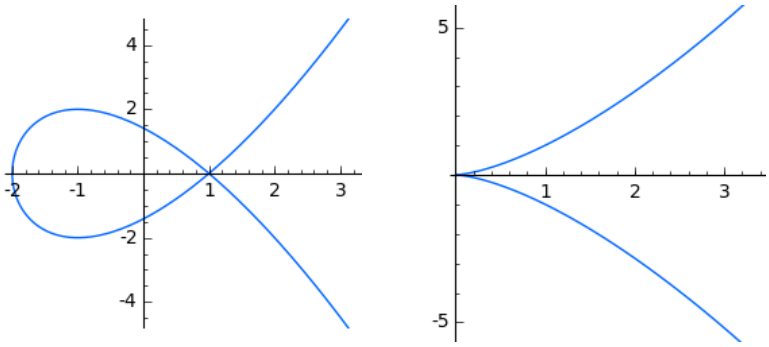

Figura 2: As curvas singulares dadas por $y^2 = x^3 - 3x + 2$ e $y^2 = x^3$.

2.1 Adição de pontos

A propriedade fundamental das curvas elípticas é que permitem a definição de uma operação de adição com propriedades interessantes. Damos uma descrição geométrica dessa operação antes de passar à sua formulação algébrica.

Descrição geométrica Sejam P e Q dois pontos numa curva elíptica $E(\mathbb{R})$. Então a soma $P+Q$ é um ponto em $E(\mathbb{R})$ obtido da seguinte maneira:

Se $P \neq Q$, consideramos a recta que passa por P e Q em $\mathbb{R}^2$. Se esta recta não é vertical, definimos R' como sendo o terceiro ponto de intersecção da recta com a curva $E(\mathbb{R})$ (Se a recta não tem mais intersecções com a curva, então a recta é a linha tangente à nossa curva num dos pontos P e Q, e definimos R' como este ponto de intersecção tangencial). Refletimos R' no eixo x e designamos a sua reflexão como a soma $R := P + Q$ de P e Q (ver Figura 3 para uma ilustração).

No caso em que a recta é vertical, lembremo-nos do comentário feito mais acima que queríamos pensar em ∞ como um ponto no fim do eixo y. Seguindo este caminho, ∞ pode ser visto como o terceiro ponto de intersecção da recta que passa por P e Q com $E(\mathbb{R})$. Por consequência, definimos $P + Q = \infty$

Agora, se $P = Q$, então a recta a considerar é a linha tangente à curva em $P = Q$. Definimos R' como sendo o outro ponto de intersecção dessa recta com a curva e prosseguimos como antes para definir $R = P + Q$.

De acordo com o nosso ponto de vista em relação ao ponto ∞ explica-se também a definição $P + \infty = \infty + P = P$ para todo o ponto P em $E(\mathbb{R})$, que completa a nossa descrição geométrica da adição em curvas elípticas.

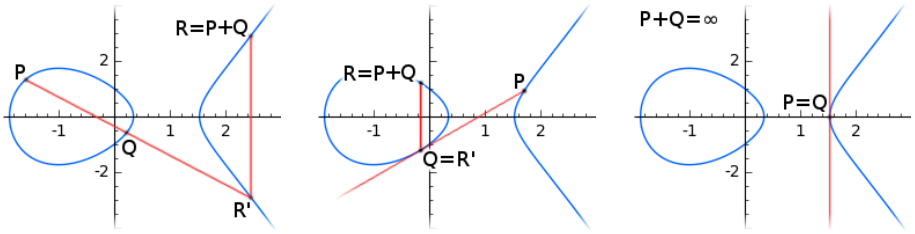

Figura 3: Adição em curvas elípticas: Alguns casos.

Deixamos o cálculo das equações que definem a adição, ou seja, as coordenadas do ponto $R = P + Q$, como exercício. O resultado é este:

Descrição algébrica Definimos uma operação $+ : E(\mathbb{R}) \times E(\mathbb{R}) \to E(\mathbb{R})$ do seguinte modo: Sejam $P, Q \neq \infty$ com $P = (x_1, y_1)$, $Q = (x_2, y_2)$ pontos em $E(\mathbb{R})$.

– Se $P \neq Q$ mas $x_1 = x_2$, então $P + Q = \infty$

– Se $P = Q$ e $y_1 = 0$, então $P + Q = \infty$

– Nos outros casos, $P + Q = R = (x_3, y_3)$, onde

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$
$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\ \frac{3x_1^2 + A}{2y_1} & P = Q \end{cases}.$$

Finalmente, definimos $P + \infty = \infty + P = P$ para todo o $P \in E(\mathbb{R})$.

2.2 Propriedade de grupo

A propriedade fundamental das curvas elípticas é a seguinte:

Teorema. *Seja $E(\mathbb{R})$ uma curva elíptica sobre $\mathbb{R}$ e $+ : E(\mathbb{R}) \times E(\mathbb{R}) \to E(\mathbb{R})$ a operação definida acima. Então $(E(\mathbb{R}), +)$ é um grupo abeliano.*

Demonstração. O elemento neutro da operação é ∞, por construção. Se $P = (x_1, y_1) \neq \infty$ então $Q = (x_1, -y_1)$ é o seu inverso: $P + Q = \infty$. A comutatividade segue-se directamente da definição geométrica dada, ou alternativamente das fórmulas apresentadas.

Porém, a associatividade desta operação é um resultado altamente não trivial. De facto, é a propriedade que destaca a construção considerada das muitas outras construções possíveis. A demonstração requer o tratamento de vários casos especiais e encontra-se fora do âmbito deste artigo. Ver, por exemplo, [6, secção 2.4]. Contentamo-nos com a motivação que nos dá a Figura 4. □

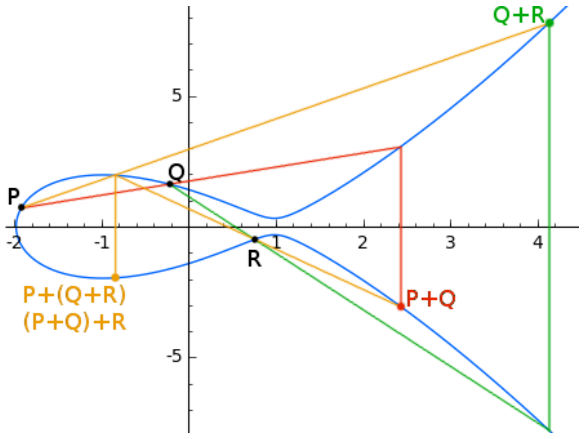

Figura 4: Associatividade da adição: $P + (Q + R) = (P + Q) + R$.

2.3 Curvas sobre corpos finitos

Até agora considerámos curvas elípticas sobre os números reais $\mathbb{R}$. Esses têm a vantagem de possuírem uma representação geométrica muito intuitiva. No entanto, nada nos impede de considerar curvas elípticas sobre outros corpos. De facto, para as aplicações em criptografia, vamos precisar de curvas sobre corpos *finitos*. No que se segue, K denota um corpo finito com característica $char(K) \neq 2, 3$.[2] Uma curva elíptica sobre K é um conjunto da forma

$$E(K) = \{(x, y) \in K \times K \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

[2] Se $char(K) \in \{2, 3\}$, não é possível definir curvas elípticas pela equação de Weierstrass. Teríamos de usar uma definição mais geral para cobrir este caso, ver [6, p. 10].

com $A, B \in K$ tais que $4A^3 + 27B^2 \neq 0$.

Notamos que, apesar do nome, já não podemos visualizar os conjuntos $E(K)$ como curvas no sentido comum. A Figura 5 mostra duas curvas elípticas sobre corpos finitos. Podemos verificar uma simetria análoga à simetria pelo eixo x encontrada anteriormente.

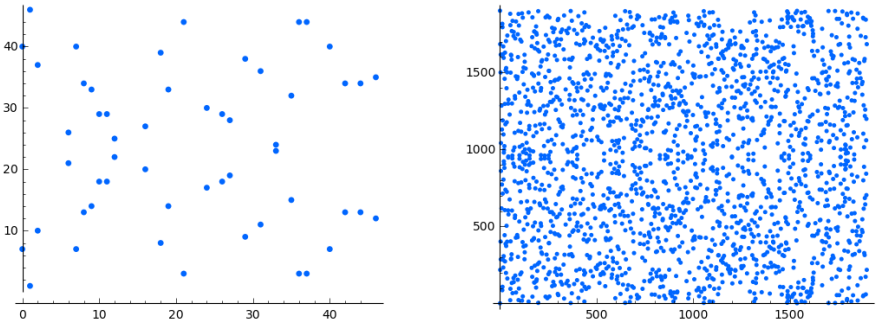

Figura 5: As curvas $y^2 = x^3 - 2x + 2$ e $y^2 = x^3 - 3x + 1$ sobre os corpos finitos $\mathbb{F}_{47}$ e $\mathbb{F}_{1901}$, respectivamente.

De facto, toda a elaboração feita no caso das curvas elípticas sobre $\mathbb{R}$ transfere-se para este caso, incluindo a propriedade de grupo:

Corolário. *Seja $E(K)$ uma curva elíptica sobre K e $+ : E(K) \times E(K) \to E(K)$ definida pelas mesmas equações que antes (ver secção 2.1), agora lidas como equações em K.*[3] *Então $(E(K), +)$ é um grupo abeliano.*

Por construção, os grupos resultantes são grupos finitos. Para melhor compreender os objetos que acabámos de definir, convém considerar um

Exemplo. Seja $K = \mathbb{F}_5$ e $E(\mathbb{F}_5)$ a curva $y^2 = x^3 + 2x + 4 \mod 5$, i.e.

$$E(\mathbb{F}_5) = \{(x, y) \in \mathbb{F}_5 \times \mathbb{F}_5 \mid y^2 = x^3 + 2x + 4\} \cup \{\infty\}.$$

Para examinar os pontos de $E(\mathbb{F}_5)$, basta atentar no seguinte quadro:

x	$x^3 + 2x + 4$	y	pontos
0	4	± 2	$(0, 2), (0, 3)$
1	2	–	
2	1	± 1	$(2, 1), (2, 4)$
3	2	–	
4	1	± 1	$(4, 1), (4, 4)$
			∞

[3] As frações têm de ser traduzidas para inversos em K, i.e. $\lambda = (y_2 - y_1)(x_2 - x_1)^{-1}$ para $P \neq Q$ e $\lambda = (3x_1^2 + A)(2y_1)^{-1}$ para $P = Q$.

A curva é visualizada na Figura 6. Vemos que possui exactamente 7 elementos, do qual deduzimos que é homomórfica ao grupo cíclico $\mathbb{Z}_7$.

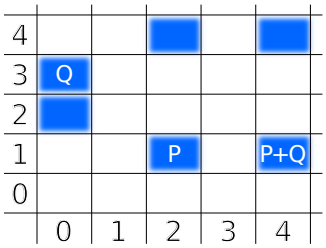

Figura 6: A curva $y^2 = x^3 + 2x + 4$ sobre $\mathbb{F}_5$.

Seja $P = (2, 1)$ e $Q = (0, 3)$. Para obter $P + Q = (x_3, y_3)$, calculamos

$$\lambda = (y_2 - y_1)(x_2 - x_1)^{-1} = (3 - 1)(0 - 2)^{-1} = 2 \cdot 3^{-1} = 2 \cdot 2 = 4 \mod 5.$$

Logo,

$$\begin{aligned} x_3 &= \lambda^2 - x_2 - x_1 = 4^2 - 0 - 2 = 14 = 4 \mod 5 \\ y_3 &= \lambda(x_1 - x_3) - y_1 = 4(2 - 4) - 1 = -9 = 1 \mod 5, \end{aligned}$$

do que se segue que $(2, 1) + (0, 3) = (4, 1)$.

Uma questão interessante é determinar os grupos (finitos abelianos) que aparecem como curvas elípticas sobre corpos finitos. Limitamo-nos aqui a citar dois resultados importantes. O primeiro diz-nos que a ordem do grupo $E(\mathbb{F}_q)$ é aproximadamente igual a q:

Teorema (Hasse)**.** *Seja $E(\mathbb{F}_q)$ uma curva elíptica sobre $\mathbb{F}_q$. Então*

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}.$$

O segundo resultado mostra que os grupos $E(\mathbb{F}_q)$ têm estrutura relativamente simples:

Teorema. *Seja $E(\mathbb{F}_q)$ uma curva elíptica sobre $\mathbb{F}_q$. Então*

$$E(\mathbb{F}_q) \cong \mathbb{Z}_n \quad \textit{ou} \quad E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

com $n \geq 1$, ou $n_1, n_2 \geq 1$ tais que $n_1 | n_2$.[4]

[4]Note-se que, na prática, é difícil encontrar um isomorfismo explícito.

3 Criptografia com curvas elípticas

Agora, conhecendo as propriedades fundamentais das curvas elípticas, passamos à criptografia. Embora já conhecidas há muito mais de um século, foi só em 1985 que as curvas elípticas foram sugeridas para uso criptográfico, independentemente por Koblitz e Miller [1, p. 2].

Como referência bibliográfica para esta secção recomenda-se [2, capítulo 9]. Um tratamento mais matemático é dado em [6, capítulo 6].

3.1 Criptografia simétrica e assimétrica

Criptografia simétrica Até à década de 1970, toda a criptografia usada era *simétrica*: duas pessoas, na literatura frequentemente chamadas de *Alice* e *Bob*, trocam uma informação secreta (a *chave*), que a seguir é usada tanto para cifrar como para decifrar mensagens.

Um exemplo é o seguinte método atribuído a Júlio César: Para cifrar mensagens, ele substituiu cada letra com a terceira letra que a segue no alfabeto: $A \longmapsto D, B \longmapsto E, \ldots, Z \longmapsto C$.[5] Embora os métodos se tenham desenvolvido significativamente ao longo do tempo, o esquema básico de usar uma só chave tanto para cifrar como para decifrar ficou sem alternativa até à segunda metade do século passado.[5]

O problema fundamental deste método é que *Alice* e *Bob* têm de ter acordado a chave anteriormente. Ou seja, precisa-se de *outro* canal seguro para a troca da chave (e.g. um encontro em pessoa).

Criptografia assimétrica Uma solução para este dilema é a criptografia *assimétrica*, que surgiu com a invenção do algoritmo RSA baseado na fatorização de números inteiros em primos em 1976 (ver [2, pp. 173 ff.]): Agora, a *Alice* e o *Bob* possuem, cada um, um par de chaves – uma chave pública, que todas as pessoas podem saber, e uma chave privada, que é secreta. Se *Alice* quer mandar uma mensagem para *Bob*, ela cifra-a usando a chave pública dele. A seguir, *Bob* usa a sua própria chave privada para decifrar a mensagem. A ideia é que, uma vez cifrada usando uma chave pública, a mensagem só pode ser decifrada com a chave privada associada a essa chave pública.

Tecnicamente, isto é realizado por uma construção que emprega uma *função de sentido único*, que é fácil de calcular mas praticamente impossível (ou seja, computacionalmente difícil) de inverter. No caso do RSA, isto é

[5] Para detalhes sobre a história fascinante da criptografia, ver [3].

a multiplicação de dois números primos, por oposição à fatorização o seu produto.

3.2 O problema do logaritmo discreto

O problema do logaritmo discreto descreve a *função de sentido único* que sustenta toda a criptografia com curvas elípticas. Observe-se que, dado um ponto $P \in E(\mathbb{F}_q)$, podemos eficientemente calcular o ponto

$$n \cdot P := \underbrace{P + \ldots + P}_{n \text{ vezes}} \in E(\mathbb{F}_q), \quad n \in \mathbb{N},$$

por exemplo usando o algoritmo "Square and Multiply" (que, na verdade, em grupos aditivos, torna-se "Double and Add"). Este algoritmo permite o cálculo de $n \cdot P$ em $\mathcal{O}(\log_2 n)$ passos, ver [4, pp. 176 ff., 265 ff.] para detalhes.

Contudo, o problema inverso é dificil: não se conhece nenhum algoritmo polinomial que calcule n a partir de dois pontos $P, Q \in E(\mathbb{F}_q)$, tais que $Q = n \cdot P$. Este problema de obter n, para P e Q dados, é chamado o *problema do logaritmo discreto*.[6] A Figura 7 ilustra-o com um pequeno exemplo.

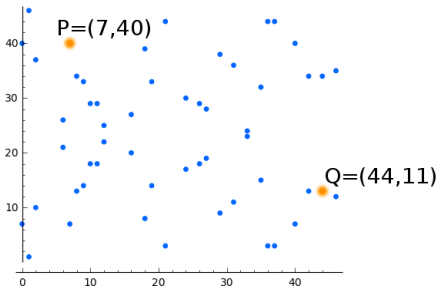

Figura 7: $y^2 = x^3 - 2x + 2$ sobre $\mathbb{F}_{47}$. Aqui, $Q = 43 \cdot P$.

3.3 Acordo de chaves Elliptic Curve Diffie-Hellman

Em vez de usá-las diretamente para cifrar mensagens (que também é possível), as curvas elípticas são frequentemente usadas para estabelecer uma chave simétrica como segredo comum. Toda a comunicação seguinte é cifrada com essa chave simétrica. Assim aproveita-se o facto de que computacionalmente é mais eficiente usar cifras simétricas do que assimétricas.

[6] O nome fica mais claro se pensamos num grupo escrito de forma multiplicativa.

Para o acordo sobre uma chave simétrica, é preciso algum protocolo de segurança que estabeleça os detalhes do processo. Um dos protocolos mais conhecidos no âmbito das curvas elípticas é o acordo de chaves "Elliptic Curve Diffie-Hellman" (ECDH) que funciona da seguinte forma:

(i) Escolher
- $q = p^k$, onde p é um número primo grande
- uma curva elíptica $E : y^2 = x^3 + Ax + B$ sobre $\mathbb{F}_q$
- um ponto P em E

tais que $n = ord(P) = \min\{m \in \mathbb{N} \mid mP = \infty\}$ é suficientemente grande (tipicamente $n > 2^{160}$). Toda esta informação é pública.

(ii)
- *Alice* escolhe uniformemente um número segredo $a \in \{2, 3, \ldots, n-1\}$, calcula $k_A = aP$ e envia k_A a *Bob*.
- *Bob* escolhe uniformemente um número segredo $b \in \{2, 3, \ldots, n-1\}$, calcula $k_B = bP$ e envia k_B a *Alice*.

(iii)
- *Alice* calcula $T = ak_B\,(= abP)$.
- *Bob* calcula $T = bk_A\,(= baP)$.

(iv) Os dois têm conhecimento dum segredo comum, do ponto $T = abP = baP = (x_T, y_T)$ em E.

Agora, o segredo comum T de *Alice* e *Bob* pode ser usado para gerar uma chave simétrica secreta. Deste modo, os dois conseguem estabelecer um canal de comunicação segura mesmo se não se conheciam antes e sem trocar informação secreta.

Nota. *Notamos brevemente que é possível estender este sistema a um sistema de cifra: Para a Alice enviar uma mensagem representada como um ponto $M \in E$, ela escolhe mais um número inteiro arbitrário m e envia o par $(mP, M + m(bP))$ ao* Bob. *Para decifrar a mensagem, o* Bob *multiplica o primeiro destes pontos com o seu segredo b e subtrai o resultado da segunda componente.*

3.4 Comparação com outros sistemas

Logaritmo discreto em $\mathbb{Z}_q^*$ Generalizando as considerações acima, pode-se considerar o problema do logaritmo discreto em qualquer grupo finito G. Isto permite realizar o acordo de chaves Diffie-Hellman e o sistema de cifra

que acabámos de descrever em outros grupos G. De facto, no caso $G = \mathbb{Z}_q^*$ dos grupos cíclicos, onde $q = p^k$ para um primo p grande, obtemos sistemas criptográficos robustos (ver [2, capítulo 8]).

No entanto, a estrutura dos grupos $E(\mathbb{F}_q)$ é muito menos conhecida do que a dos grupos cíclicos (já comentámos que os isomorfismos $E(\mathbb{F}_q) \cong \mathbb{Z}_n$ ou $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ são em geral difíceis de encontrar). Nomeadamente, o ataque mais forte conhecido a sistemas de logaritmo discreto, o chamado *index calculus* (ver [4, p. 244 ff.]), explora explicitamente a estrutura de $\mathbb{Z}_q^*$ e portanto não se aplica ao caso das curvas elípticas.

Isto faz com que seja possível obter semelhante nível de segurança usando números primos menores: Para as curvas elípticas, a fim de obter $n = 160$, precisamos de primos p de aproximadamente 160 bits (ver também o teorema de Hasse no fim da secção 2), enquanto semelhante nível de segurança com sistemas em $\mathbb{Z}_q^*$ exige primos do tamanho de 1024 bits.

RSA Um dos sistemas criptográficos mais conhecidos e mais usados é o sistema RSA, que marcou o início da criptografia assimétrica. Comparado com sistemas que usam curvas elípticas, é outra vez o tamanho de chaves que faz a diferença: uma chave RSA com 1024 bits garante um nível de segurança comparável com uma chave com 160 bits num sistema que usa curvas elípticas, chaves RSA de 3072 bits equivalem a curvas do tamanho de meramente 256 bits ([2, p. 156]).

3.5 Ataques e segurança

Ataques ao logaritmo discreto Embora se acredite que, no caso geral, é impossível solucionar o problema do logaritmo discreto de forma eficiente, existem situações que permitem o cálculo de logaritmos discretos com esforço razoável, explorando a estrutura algébrica de certas curvas $E(\mathbb{F}_q)$. O quadro seguinte menciona os ataques mais importantes deste tipo juntamente com propriedades que impeçam a efectividade destes ataques.[1, p. 179].

Ataque	**Propriedade a exigir**
Pohlig-Hellman	n divide $\#E(\mathbb{F}_q)$ para $n > 2^{160}$ primo
Ataque de isomorfismo ($E(\mathbb{F}_p) \cong (\mathbb{F}_p, +)$)	$\#E(\mathbb{F}_p) \neq p$
Menezes, Okamoto, Vanstone (Mergulho em $(\mathbb{F}_{q^k}^*, \cdot)$)	$ord(P)$ não divide $(q^k - 1)$ para $1 \leq k \leq 20$

Usar curvas que satisfaçam todas as propriedades do quadro assegura que os sistemas criptográficos não são vulneráveis a ataques conhecidos. Note-se que o ataque mais robusto ao logaritmo discreto, o *index calculus*, não se aplica às curvas elípticas. Na prática, é comum usar curvas estandardizadas especialmente construídas para reduzir a probabilidade da existência de ataques.

Para quebrar o acordo de chaves descrito acima, é preciso solucionar o *problema de Diffie-Hellman*: Dados P, aP e bP em $E(\mathbb{F}_q)$, calcular o segredo abP. Se um atacante pudesse solucionar o problema do logaritmo discreto, poderia, por exemplo, obter a a partir de aP e depois calcular abP. No entanto, não se sabe se o contrário também é verdade, ou seja, se é possível resolver o problema de Diffie-Hellman sem saber calcular logaritmos discretos, nomeadamente sem obter a (ou b).

Ataques ativos à comunicação Também é possível atacar o protocolo de segurança ativamente. Um atacante *passivo* que observa toda a comunicação entre *Alice* e *Bob* não consegue adivinhar o segredo T. Contudo, um atacante *ativo*, que modifica a comunicação entre os dois, consegue tomar o controlo de toda a comunicação (*man-in-the-middle attack*). Isto mostra a necessidade de precauções adicionais como métodos de autenticação.

Referências

[1] N. Koblitz, A. Menezes, e S. Vanstone, "The State of Elliptic Curve Cryptography", *Designs, Codes and Cryptography*, 19 (2000), pp. 173-193.

[2] C. Paar e J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, 2010.

[3] S. Singh, *The Code Book*, Fourth Estate, 1999.

[4] D. R. Stinson, *Cryptography. Theory and Practice*, third edition, Chapman & Hall, 2006.

[5] C. Suetonius Tranquillus, *The lives of the twelve Caesars*, I. 56., Loeb Classical Library, 1913. Disponível em `http://penelope.uchicago.edu/Thayer/E/Roman/Texts/Suetonius/12Caesars/home.html` [Tradução da obra original *De vitis Caesarum*, 121 d.C.]

[6] L. C. Washington, *Elliptic Curves. Number Theory and Cryptography*, second edition, Chapman & Hall, 2008.