Curvas Elípticas

Marcel A. B. Carvalho, Luis C. S. Lima e Rogério B. Santos
Especialização em Gestão da Segurança da Informação
Universidade de Brasília

Setembro 09, 2009

Resumo

A Criptografia de Curvas Elípticas (ECC) surgiu como uma forma alternativa ao criptossistema RSA. Os procedimentos de geração de chaves e de assinatura são mais rápidos e requerem parâmetros menores para prover o mesmo grau de segurança quando comparado ao RSA. Este artigo aborda um histórico sobre curvas elípticas, mostrando o que são e o que representam para a criptografia nos dias de hoje.

1 Introdução

Suponha uma coleção de bolas de canhão empilhadas como uma pirâmide quadrada[1], com uma bola na camada superior, quatro na segunda camada, nove na terceira camada, e assim por diante, conforme figura (1). Se esta pilha desabar, seria possível rearranjar estas bolas como um quadrado? (WASHINGTON, 2008)

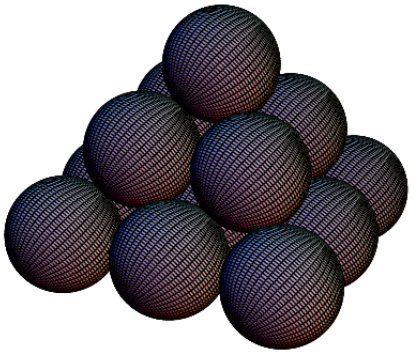

Figura 1: Pirâmide de Bolas de Canhão

Se esta pirâmide possui altura x então o número de bolas empilhadas é definido pela equação (1).

$$1^2 + 2^2 + 3^2 + ... + x^2 = \frac{x(x+1)(2x+1)}{6} \tag{1}$$

Como o que se busca é que esse número seja uma quadrado perfeito, significa que o resultado da equação (2), para os números inteiros positivos x e y representa a solução do problema supracitado.

[1] Pirâmide com uma base quadrada

$$y^2 = \frac{x(x+1)(2x+1)}{6} \tag{2}$$

Uma equação desse tipo representa uma curva elíptica. Cabe ressaltar que curvas elípticas não são elipses, como pode ser verificado no gráfico desta equação dado na figura (2), elas têm esse nome pois são definidas como um objeto matemático (uma curva) descrito por uma equação cúbica, as mesmas que são usadas para calcular o comprimento de arco de uma elipse.

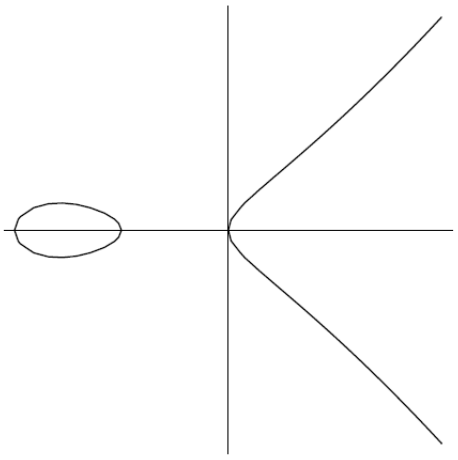

Figura 2: Gráfico de $y^2 = \frac{x(x+1)(2x+1)}{6}$

Curvas elípticas são estudas e usadas em diversas áreas há mais de um século, um exemplo foi sua utilização na prova do *Último Teorema de Fermat*, que formulava o seguinte, dada a equação $x^n + y^n = z^n$, esta não possui solução inteira diferente de zero para (x, y, z) quando o inteiro n é maior que *2*. Existem ainda aplicações em fatoração de números inteiros (LENSTRA, 1987) e testes de primalidade (GOLDWASSER; KILIAN, 1999; MORAIN; ATKIN, 1993).

Em 1985, Neal Koblitz (KOBLITZ, 1987) e Victor Miller (MILLER, 1986) independentemente propuseram o uso de curvas elípticas no projeto de sistema criptográfico de chaves públicas, tendo como base um grupo de curvas elípticas sobre um campo finito. Desde então várias pesquisas são publicadas sobre a segurança e uma eficiente implementação de criptografia usando curvas elípticas. No final da década de 90, sistemas de curvas elípticas começaram a ser aceitos comercialmente, quando esta tecnologia recebeu crédito pelas organizações responsáveis por padrões internacionais e as companhias privadas incluíram estes protocolos nos seus produtos de segurança. Podem ser citadas outras iniciativas que reforçaram o uso da criptografia com curvas elípticas, como por exemplo, a decisão do governo americano de empregar ECC em comunicações *classificadas* e *sensíveis, mas não classificadas* e o seu uso pela Microsoft no esquema de proteção de direitos digitais.

Este trabalho apresenta o uso das curvas elípticas em criptografia. Sua segurança está baseada no problema do logaritmo discreto. Este problema aparentemente é significativamente mais difícil de resolver, comparado com o problema do logaritmo discreto usado por outros sistemas de criptografia. O melhor algoritmo conhecido para resolução deste problema tem complexidade exponencial, o que confere um alto grau de segurança ao sistema.

2 Protocolos Criptográficos

Os principais algoritmos baseados em curvas elípticas são ECDSA e EC-KCDSA para assinatura digital, STS e ECMQV para estabelecimento de chaves e ECIES para cifração. Segue relação dos protocolos com os padrões que os contemplam:

- ECDSA : Elliptic Curve Digital Signature Algorithm. Descrito nos seguintes documentos ANSI X9.62, FIPS 186-2, IEEE 1363-2000 e ISO/IEC 15946-2.
- EC-KCDSA : Elliptic Curve - Korean Certificate-based Digital Signature Algorithm. Descrito no seguinte documento ISO/IEC 15946-2.
- STS : Station-To-Station. Descrito no seguinte documento ANSI X9.63.
- ECMQV : Elliptic Curve Menezes-Qu-Vanstone. Descrito nos seguintes documentos ANSI X9.63, IEEE 1363-2000, e ISO/IEC 15946-3.
- ECIES : Elliptic Curve Digital Integrated Encryption Scheme. Descrito nos seguintes documentos ANSI X9.63 e ISO/IEC 15946-3.

3 Definição de Curva Elíptica

Seja K um campo. Por exemplo, K pode ser o campo finito F_q, ou o campo de primos Z_p, onde p é um número primo grande, o campo R de números reais, o campo Q de números racionais ou o campo C de números complexos. Uma curva elíptica sobre o campo K é definida pela equação de Weierstrass:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3}$$

onde a_1, a_3, a_2, a_4, $a_6 \in K$

A equação de Weierstrass pode ser transformada e simplificada para diferentes formas por uma troca linear de variáveis. Para um campo de característica diferente de 2 e de 3, ou seja, para um campo Z_p, para $p > 2$, a curva elíptica E sobre este campo Z_p é definida por uma equação da forma:

$$y^2 = x^3 + ax + b \tag{4}$$

onde a, $b \in Z_p$ e $4a^3 + 27b^2 (mod\ p) \neq 0$, de modo que o polinômio não tenha raízes múltiplas, e ainda um elemento ϕ chamado **ponto no infinito**.

O conjunto $E(Z_p)$ consiste em todos os pontos que satisfazem a equação $(x, y)|x, y \in Z_p$, juntamente com o ponto ϕ.

3.1 Aritmética sobre curvas elípticas

Existe uma regra para somar dois pontos pertencentes a uma curva elíptica, de tal forma que esta soma seja um terceiro ponto sobre a mesma curva. O conjunto de pontos $E(Z_p)$, juntamente com a operação de soma, formam um grupo abeliano[2], onde o ponto no infinito ϕ é o elemento neutro.

Sejam, $P = (x_1, y_1)$ e $Q = (x_2, y_2)$ dois pontos distintos tomados em uma curva elíptica E. A soma de P e Q, denotada por $R = (x_3, y_3)$ é definida através do traçado de uma linha que atravesse P e Q. Esta linha intercepta a curva elíptica E em um terceiro ponto, onde R é a reflexão deste ponto sobre o

[2]Os grupos abelianos receberam esse nome em homenagem à Niels Henrik Abel. Em matemática, um grupo abeliano, chamado também de grupo comutativo, é um grupo $(G, *)$ tais que $a * b = b * a$ para todo a,$b \in G$. Ou seja, a ordem em que a operação binária é executada não importa

eixo x. Este ponto R é portanto o resultado da operação de soma $P + Q$. Se $P = (x_1, y_1)$, então o dobro de P, denotado por $R = (x_3, y_3)$ define-se pelo traçado de uma reta tangente à curva elíptica no ponto P. Esta reta intercepta a curva em um segundo ponto, cuja reflexão sobre o eixo x é o ponto R.

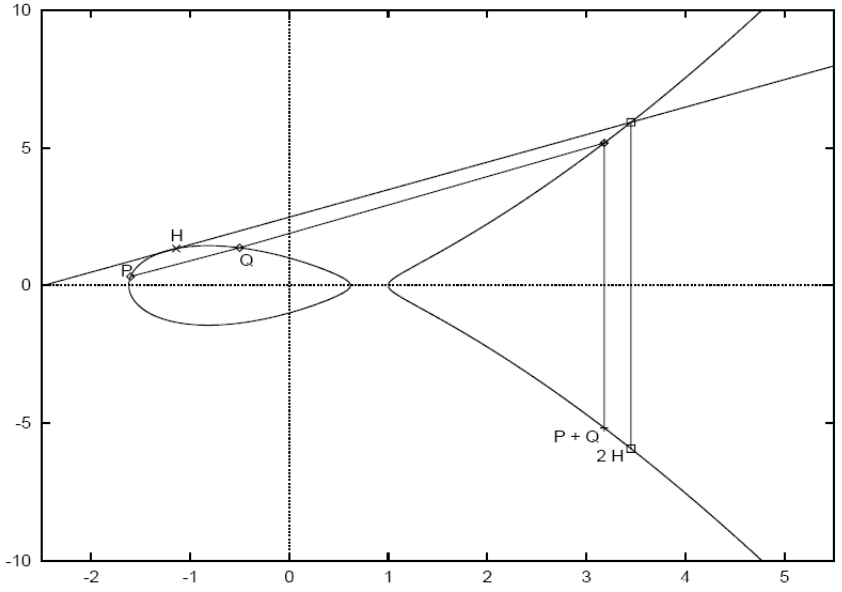

Figura 3: Adição de dois ponto diferentes P e Q e adição do ponto H com ele mesmo, resultando em $2H$ (RAUSCHER; BOHNSACK, 1999)

4 O Problema do Logaritmo Discreto

Sendo uma curva elíptica E transformada em um grupo abeliano por uma operação de adição (e não por uma operação de multiplicação), a **exponenciação** de um ponto em E refere-se a uma adição repetida. Assim sendo, a enésima potência de $\alpha \in E$ é o enésimo múltiplo de α, ou seja, $\beta = \alpha^n = n\alpha$. O logaritmo de β na base α é o número n, o inverso da exponenciação.

Para um grupo qualquer G, suponha-se que $\alpha, \beta \in G$. Num problema de logaritmo discreto, tenta-se resolver para um inteiro x tal que $\alpha^x = \beta$. Analogamente, no problema do logaritmo discreto em curvas elípticas, tenta-se resolver para um inteiro x tal que $x\alpha = \beta$, para $\alpha, \beta \in E$. Para que este problema numa curva sobre $E(F_q)$ seja computacionalmente intratável, é importante selecionar uma curva com E e q apropriados.

O problema do logaritmo discreto pode ser expresso de outra maneira: dados P e Q, pontos pertencentes ao grupo, encontrar um número k tal que $kP = Q$; k é denominado o logaritmo discreto de Q na base P.

5 Comparando força

Segundo NIST (2007) seguem a tabela (1) mostrando uma comparação do nível de segurança provido pelos algoritmos aprovados por este instituto e a tabela (2) com a relação entre o nível de segurança e sua validade.

Tabela 1: Comparativo de nível de segurança

Bits de Segurança	Algoritmo simétrico	Criptografia em campo finito (DSA, D-H)	Criptografia baseada em fatoração de inteiros (RSA)	Criptografia baseada em Curvas Elípticas (ECDSA)
80	2TDEA[3]	L = 1024 N = 160	k = 1024	f = 160-223
112	3TDEA	L = 2048 N = 224	k = 2048	f = 224-255
128	AES-128	L = 3072 N = 256	k = 3072	f = 256-383
192	AES-192	L = 7680 N = 384	k = 7680	f = 384-511
256	AES-256	L = 15360 N = 512	k = 15360	f = 512+

Tabela 2: Relação do nível de segurança com sua validade

Validade do Nível de Segurança	Algoritmo simétrico (cifração e MAC)	Criptografia em campo finito (DSA, D-H)	Criptografia baseada em fatoração de inteiros (RSA)	Criptografia baseada em Curvas Elípticas (ECDSA)
Até 2010 (min. 80 bits de segurança)	2TDEA 3TDEA AES-128 AES-192 AES-256	Min. L = 1024 N = 160	Min. k = 1024	Min. f = 160
Até 2030 (min. 112 bits de segurança)	3TDEA AES-128 AES-192 AES-256	Min. L = 2048 N = 224	Min. k = 2048	Min. f = 224
Além de 2030 (min. 128 bits de segurança)	AES-128 AES-192 AES-256	Min. L = 3072 N = 256	Min. k = 3072	Min. f = 256

Segue uma explicação sobre a tabela (1) e tabela (2):

- Coluna 1: os bits de segurança não são o mesmo que o tamanho da chave para os algoritmos, devido aos ataques a estes algoritmos que fornecem uma vantagem computacional;
- Coluna 2: fornece o algoritmo de criptografia simétrica que fornece o referido nível de segurança;
- Coluna 3: tamanho mínimo dos parâmetros dos algoritmos desta categoria, sendo L o tamanho da chave pública e N o tamanho da chave privada;
- Coluna 4: o valor k representa o tamanho do *modulus* n, comumente designado o tamanho da chave;
- Coluna 5: indica a faixa para f, que representa o tamanho de n, ou a ordem do ponto base G, comumente designado o tamanho da chave;

[3]Algoritmo TDEA (também conhecido como Triple DES) com duas chaves diferentes

6 Bibliotecas Criptográficas

Com o crescente uso da ECC no mercado, verifica-se o surgimento de um conjunto de ferramentas que suportem o uso desta criptografia em aplicações distintas. Em Uto (2005) são elencadas 6 (seis) bibliotecas em C e C++ que dão suporte à criptografia usando curvas elípticas e traz uma análise de desempenho entre elas. Na página da empresa Certicom (2009) existem soluções implementadas em hardware e software que suportam ECC.

7 Desafio ECC

Em 1997 Certicom (2009) propôs uma série de desafios relativos ao problema do logaritmo discreto sobre curvas elípticas (ECDLP). O desafio pedia a solução em três tipos de curvas:

- Curvas geradas aleatoriamente sobre campos primos: ECCp-79, ECCp-89, ECCp-97, ECCp-109, ECCp-131, ECCp-163, ECCp-191, ECCp-239, e ECCp-359
- Curvas geradas aleatoriamente sobre campos finitos com característica 2: ECC2-79, ECC2-89, ECC2-97, ECC2-109, ECC2-131, ECC2-163, ECC2-191, ECC2-238, e ECC2-353.
- Curvas de Koblitz sobre F_2: ECC2K-95, ECC2K-108, ECC2K-130, ECC2K-163, ECC2K-238, e ECC2K-358.

O desafio foi resolvido usando uma variante do algoritmo ρ de Pollard em outubro de 2002. A computação deste algoritmo usou 10.000 estações de trabalho distribuídas pela Internet trabalhando durante 540 dias. Os desafios mais complexos resolvidos nesta ocasião foram o ECCp-109 e o ECC2-109. Estima-se que a chave de comprimento mínimo recomendado para ECC, de 163 bits, exigirá recursos 10^8 vezes maiores do que aqueles usados para resolver o problema da chave de 109 bits.(CERTICOM, 2009)

Em Bos et al. (2009) foi relatada a quebra do ECCp-112, usando um cluster de 200 consoles PlayStation 3 (PS3), veja figura 4, durante três meses e meio. A curva quebrada não se refere ao desafio original descrito acima e sim a uma das curvas descritas nas recomendações de parâmetros ditas pela Certicom (2000).

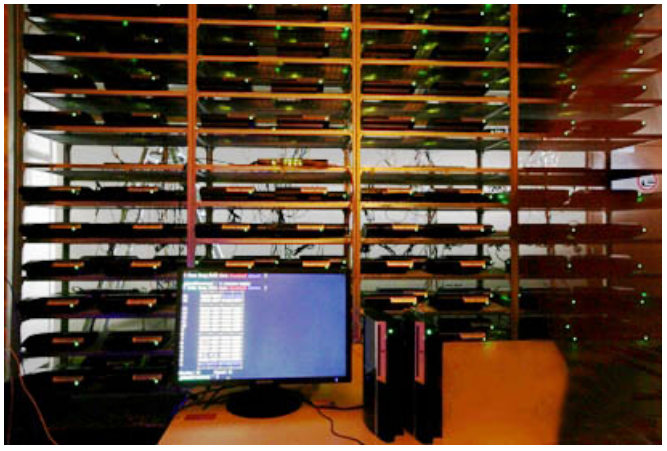

Figura 4: Cluster de 200 PS3 usados na quebra do ECCp-112

8 Conclusão

Este artigo descreve brevemente a aplicação das curvas elípticas para um sistema de criptografia de chaves assimétricas. As curvas elípticas provêm uma dificuldade maior para o problema do logaritmo discreto, se comparadas às técnicas comumente usadas de fatoração de números grandes ou o sistema Diffie-Hellman. Isso significa que, para chaves de tamanhos menores, um sistema baseado em curvas elípticas mostra ter um nível de segurança comparável ao sistema RSA com chaves substancialmente maiores. Apesar da matemática envolvida no conceito de curvas elípticas ser de razoável complexidade, o artigo pretendeu introduzir os conhecimentos mínimos para assimilação do mecanismo de funcionamento do sistema e disponibilizar, no levantamento bibliográfico, referências úteis para maior aprofundamento.

Referências

BOS, J. W. et al. *112-bit prime ECDLP solved*. [S.l.], 2009. Disponível em: <http://lacal.epfl.ch-/page81774.html>. Acesso em: 09 setembro 2009.

CERTICOM. *SEC 2 - Recommended Elliptic Curve Domain Parameters*. [S.l.], 2000. Disponível em: <http://www.secg.org/collateral/sec2%5Ffinal.pdf>. Acesso em: 09 setembro 2009.

CERTICOM. *Elliptic Curve Cryptography (ECC)*. [S.l.], 2009. Disponível em: <http://www.certicom-.com/>. Acesso em: 09 setembro 2009.

GOLDWASSER, S.; KILIAN, J. Primality testing using elliptic curves. *J. ACM*, v. 46, n. 4, 1999.

KOBLITZ, N. Elliptic curve cryptosystems. *Mathematics of Computation*, v. 43, n. 177, p. 203–209, 1987.

LENSTRA, H. Factoring integers with elliptic curves. *Ann. of Math.(2)*, v. 126, p. 649–673, 1987.

MILLER, V. Use of elliptic curves in cryptography. *Advances in Criptology - CRYPTO 85*, v. 468, p. 417–426, 1986.

MORAIN, F.; ATKIN, A. O. L. Elliptic curves and primality proving. *Math. Comp.*, v. 61, n. 203, 1993.

NIST. *Recommendation for Key Management Part 1: General (Revised)*. [S.l.], 2007. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2%5FMar08-2007.pdf>. Acesso em: 09 setembro 2009.

RAUSCHER, R.; BOHNSACK, F. Results of an elliptic-curve-approach for use in cryptosystems. *25th EUROMICRO CONFERENCE*, v. 2, p. 415–422, 1999.

UTO, N. A survey of cryptographic libraries supporting elliptic curve cryptography. *3er Congreso Iberoamericano de Seguridad Informática*, Valparaíso - Chile, p. 159–176, 2005.

WASHINGTON, L. C. *Elliptic Curves - Number Theory and Cryptography*. 2^o. ed. [S.l.]: CRC Press, 2008. 1-2 p.