Criptografía de curva elíptica

De Wikipedia, la enciclopedia libre

La **Criptografía de Curva Elíptica** (del inglés: Elliptic curve cryptography, ECC) es una variante de la criptografía asimétrica o de clave pública basada en las matemáticas de las curvas elípticas. Sus autores argumentan que la CCE puede ser más rápida y usar claves más cortas que los métodos antiguos — como RSA — al tiempo que proporcionan un nivel de seguridad equivalente. La utilización de curvas elípticas en criptografía fue propuesta de forma independiente por Neal Koblitz y Victor Miller en 1985.

Índice

- 1 Introducción
- 2 Introducción Matemática
  - 2.1 Ejemplo
- 3 Uso en criptografía
- 4 Referencias
- 5 Enlaces externos

Introducción

Los sistemas de criptografía asimétrica o de clave pública utiliza dos claves distintas: una de ellas puede ser pública, la otra es privada. La posesión de la clave pública no proporciona suficiente información para determinar cuál es la clave privada. Este tipo de sistemas se basa en la dificultad de encontrar la solución a ciertos problemas matemáticos. Uno de estos problemas es el llamado logaritmo discreto. Encontrar el valor de *b* dada la ecuación $a^b = c$, cuando *a* y *c* son valores conocidos, puede ser un problema de complejidad exponencial para ciertos grupos finitos de gran tamaño; mientras el problema inverso, la exponenciación discreta puede ser evaluado eficientemente usando por ejemplo exponenciación binaria

Una curva elíptica es una curva plana definida por una ecuación de la forma

$$y^2 = x^3 + ax + b.$$

Con el conjunto de puntos *G* que forman la curva (i.e., todas las soluciones de la ecuación más un punto *O*, llamado punto en el infinito) más una operación aditiva +, se forma un grupo abeliano. Si las coordenadas *x* e *y* se escogen desde un cuerpo finito, entonces estamos en presencia de un grupo abeliano finito. El problema del logaritmo discreto sobre este conjunto de puntos (PLDCE) se cree que es más difícil de resolver que el correspondiente a los cuerpos finitos (PLD). De esta manera, las longitudes de claves en criptografía de curva elíptica pueden ser más cortas con un nivel de seguridad comparable.

Introducción Matemática

Sea $p > 3$ primo. La curva elíptica $E: y^2 = x^3 + ax + b$ sobre $\mathbb{Z}_p$ es el conjunto de soluciones $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ en la congruencia

$$y^2 = x^3 + ax + b \pmod{p},$$

donde $a, b \in \mathbb{Z}_p$ son constantes tal que $4a^3 + 27b^2 \neq 0 \pmod{p}$

Se define una operación aditiva como sigue: Considerando que

$$P = (x_1, y_1)$$

y

$$Q = (x_2, y_2)$$

son puntos en E y $\mathcal{O}$ es un punto en el infinito. Si $x_2 = x_1$ e $y_2 = -y_1$, entonces $P + Q = \mathcal{O}$; de lo contrario $P + Q = (x_3, y_3)$, donde

$$x_3 = \lambda^2 - x_1 - x_2,$$
$$y_3 = \lambda(x_1 - x_3) - y_1,$$

y

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{si } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{si } P = Q \end{cases}.$$

Finalmente, definimos

$$P + \mathcal{O} = \mathcal{O} + P = P \ \forall P \in E.$$

Con esto se puede mostrar que *E* es un grupo abeliano con elemento identidad $\mathcal{O}$. Cabe notar que la inversa de (*x*, *y*) (que se escribe como -(*x*, *y*) ya que la operación es aditiva) es (*x*, -*y*), para todo $(x, y) \in E$

De acuerdo al teorema de Hasse, el número de puntos #*E* que contiene *E* es cercano a *p*. Más precisamente se satisface la siguiente desigualdad

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

Como se sabe que cualquier grupo de orden primo es cíclico, lo que se requiere es encontrar un subgrupo de *E* de orden *q* (*q* primo) para tener un isomorfismo con $\mathbb{Z}_q$ donde el problema del logaritmo discreto sea intratable. En este caso, siendo α un generador del grupo cíclico (el cual puede ser cualquier elemento del grupo distinto de $\mathcal{O}$, la identidad), se pueden calcular las «potencias» de α (las que se escriben como múltiplos de α, debido a que la operación del grupo es aditiva).

Ejemplo

Sea *E* la curva elíptica $y^2 = x^3 + x + 6$ sobre $\mathbb{Z}_{11}$. Se calculan los puntos sobre *E* verificando los posibles valores de $x \in \mathbb{Z}_{11}$, y luego verificando si $z = x^3 + x + 6 \pmod{11}$ es un residuo cuadrático. Los valores se tabulan en la siguiente Tabla:

$$x^3 + x + 6 \pmod{11}$$

x	*y*
0	NO EXISTE
1	NO EXISTE
2	4, 7
3	5, 6
4	NO EXISTE
5	2, 9
6	NO EXISTE
7	2, 9
8	3, 8
9	NO EXISTE
10	2, 9

Como *E* tiene 12 puntos + O, sigue que es cíclico e isomorfo a $\mathbb{Z}_{13}$. Considerando el generador $\alpha = (2,7)$, entonces :$2\alpha = (2,7) + (2,7)$

$$\begin{aligned}\lambda &= (3 \times 2^2 + 1)(2 \times 7)^{-1} \pmod{11} \\ &= 2 \times 3^{-1} \pmod{11} \\ &= 2 \times 4 \pmod{11} \\ &= 8\end{aligned}$$

Entonces tenemos

$$x_3 = 8^2 - 2 - 2 \pmod{11} = 5$$

y

$$y_3 = 8(2-5) - 7 \pmod{11} = -31 \pmod{11} = -9 \pmod{11} = 2$$

Por lo tanto $2\alpha = (5,2)$

Uso en criptografía

En criptografía, se elige un punto base G específico y publicado para utilizar con la curva $E(q)$. Se escoge un número entero aleatorio k como clave privada, y entonces el valor $P = k*G$ se da a conocer como clave pública (nótese que la supuesta dificultad del PLDCE implica que k es difícil de deducir a partir de P). Si María y Pedro tienen las claves privadas k_A y k_B, y las claves públicas P_A y P_B, entonces María podría calcular $k_A \times P_B = (k_A \times k_B) \times G$; y Pedro puede obtener el mismo valor dado que $k_B \times P_A = (k_B \times k_A) \times G$.

Esto permite establecer un valor «secreto» que tanto María como Pedro pueden calcular fácilmente, pero que es muy complicado de derivar para una tercera persona. Además, Pedro no consigue averiguar nada nuevo sobre k_A durante ésta transacción, de forma que la clave de María sigue siendo privada.

Los métodos utilizados en la práctica para cifrar mensajes basándose en este valor secreto consisten en adaptaciones de antiguos criptosistemas de logaritmos discretos originalmente diseñados para ser usados en otros grupos. Entre ellos se podrían incluir Diffie-Hellman, ElGamal y DSA.

La realización de las operaciones necesarias para ejecutar este sistema es más lenta que para un sistema de factorización o de logaritmo discreto módulo entero del mismo tamaño. De todas maneras, los autores de sistemas de CCE creen que el PLDCE es significativamente más complicado que los problemas de factorización o del PLD, y así se puede obtener la misma seguridad mediante longitudes de clave mucho más cortas utilizando CCE, hasta el punto de que puede resultar más rápido que, por ejemplo, RSA. Los resultados publicados hasta la fecha tienden a confirmar esto, aunque algunos expertos se mantienen escépticos.

La CCE ha sido ampliamente reconocida como el algoritmo más fuerte para una determinada longitud de clave, por lo que podría resultar útil sobre enlaces que tengan requisitos muy limitados de ancho de banda.

NIST y ANSI X9 han establecido unos requisitos mínimos de tamaño de clave de 1024 bits para RSA y DSA y de 160 bits para ECC, correspondientes a un bloque simétrico de clave de 80 bits. NIST ha publicado una lista de curvas elípticas recomendadas de 5 tamaños distintos de claves (80, 112, 128, 192, 256). En general, la CCE sobre un grupo binario requiere una clave asimétrica del doble de tamaño que el correspondiente a una clave simétrica.

Certicom es la principal empresa comercial de CCE, esta organización posee 130 patentes, y ha otorgado licencias sobre tecnología a la National Security Agency (NSA) por 25 millones de dólares. Certicom también ha patrocinado varios desafíos al algoritmo CCE. El más complejo resuelto hasta ahora, es una clave de 109 bits, que fue roto por un equipo de investigadores a principios de 2003. El equipo que rompió la clave utilizó un ataque masivo en paralelo basado en el 'birthday attack', mediante más de 10000 PC de tipo Pentium funcionando continuamente durante 540 días. Se estima que la longitud de clave mínima recomendada para CCE (163 bits) requeriría 10^8 veces los recursos utilizados para resolver el problema con 109 bits.

Referencias

- Neal Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation* 48, 1987, pp203–209.
- V. Miller, "Use of elliptic curves in cryptography", CRYPTO 85, 1985.
- Blake, Seroussi, Smart, "Elliptic Curves in Cryptography", Cambridge University Press, 1999
- Hankerson, Menezes, Vanstone: "Guide to Elliptic Curve Cryptography", Springer-Verlag, 2004

Enlaces externos

- Recommended Elliptic Curves for Government Use, NIST document (PDF file) (http://csrc.nist.gov/CryptoToolkit/dss/ecdsa/NISTReCur.pdf)
- Certicom press release regarding 109 bit ECC challenge (http://www.certicom.com/index.php?action=company,press_archive&view=121)
- Certicom Online ECC Tutorial (http://www.certicom.com/index.php?action=ecc_tutorial,home)
- Digital Signature Standard; includes info on ECDSA (http://csrc.nist.gov/cryptval/dss.htm)
- libecc: Open source ECC library (http://libecc.sourceforge.net/)
- Introducción a las curvas elípticas, hiperelípticas y libcurve (http://math.co.ro/colfinal/coloquio-ce-ch.pdf)
- Demo of elliptic curve point counting and domain parameter generation (http://www.cryptomathic.com/labs/ellipticcurvedemo.html)
- eccGnuPG: Parche experimental para el GnuPG (http://www.calcurco.cat/eccGnuPG/index.es.html)

Obtenido de «http://es.wikipedia.org/w/index.php?title=Criptografía_de_curva_elíptica&oldid=67778911»
Categoría: Criptografía de curva elíptica
