8.3. Cơ chế chữ ký ElGamal (ElGamal Signature Scheme)

Trong phần này, chúng tôi trình bày về Cơ chế Chữ ký ElGamal, cơ chế này đã được mô tả trong một bài báo vào năm 1985. Một bản tinh chỉnh của cơ chế này được sử dụng trong Thuật toán Chữ ký số (Digital Signature Algorithm - DSA) bởi Viện Tiêu chuẩn và Công nghệ Quốc gia (National Institute of Standards and Technology – NIST). DSA cũng kết hợp một số ý tưởng được sử dụng trong một cơ chế gọi là cơ chế chữ ký Schnorr. Tất cả các cơ chế này được thiết kế chuyên dụng để sử dụng cho các chữ ký, không giống với hệ mật RSA - nó có thể được sử dụng đồng thời như là một hệ mật mã hóa khóa công khai và một cơ chế chữ ký.

Hệ mật 8.2: Cơ chế chữ ký ElGamal

Giả sử p là một số nguyên tố sao cho bài toán logarit rời rạc trong Z_p là bất trị, giả sử $\alpha \in Z_p^*$ là một phần tử nguyên thủy. Giả sử $P = Z_p^*$, $A = Z_p^* \times Z_{p-1}$, và định nghĩa:

$$\mathcal{K} = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod{p}\}.$$

Các giá trị p, α và β là các khóa công khai (public key), và a là khóa riêng tư (private key).

Với K = (p, α, a, β) và với một số ngẫu nhiên (bí mật) $k \in Z_{p-1}^*$, định nghĩa:

$$\mathbf{sig}_K(x, k) = (\gamma, \delta),$$

trong đó:

$$\gamma = \alpha^k \bmod p$$

và:

$$\delta = (x - a\gamma)k^{-1} \bmod (p - 1).$$

Với x, ɣ $\in Z_p^*$ và $\delta \in Z_{p-1}$, định nghĩa:

$$\mathbf{ver}_K(x,(\gamma,\delta)) = true \Leftrightarrow \beta^\gamma \gamma^\delta \equiv \alpha^x \pmod{p}.$$

Cơ chế chữ ký Elgamal là ngẫu nhiên (Hệ mật khóa công khai Elgamal cũng là ngẫu nhiên). Điều này có nghĩa là có nhiều chữ ký hợp lệ cho mỗi thông điệp, và thuật toán xác thực phải có khả năng chấp nhận bất cứ chữ ký hợp lệ nào trong số đó là chính xác. Mô tả cho cơ chế chữ ký Elgamal được đưa ra trong hệ mật 8.2.

Chúng ta hãy bắt đầu với một số quan sát dự trù. Một chữ ký Elgamal bao gồm 2 thành phần, được ký hiệu là ɣ và δ. Thành phần đầu tiên, ɣ, có được bằng cách lấy lũy thừa α theo một cơ số modulo ngẫu nhiên p; nó không phụ thuộc vào thông điệp (được đặt tên là x) đang được ký. Thành phần thứ hai, δ, phụ thuộc vào thông điệp x và khóa riêng tư a. Việc xác thực chữ ký được thực hiện bằng cách kiểm tra xem một đồng dư cụ thể chứa modulo p; đồng dư này tất nhiên không chứa khóa riêng tư.

Chúng ta chỉ ra rằng, khi chữ ký được xây dựng đúng cách, quá trình xác thực sẽ diễn ra thành công. Điều này được suy diễn một cách dễ dàng từ đồng dư sau đây:

$$\begin{aligned} \beta^\gamma \gamma^\delta &\equiv \alpha^{a\gamma}\alpha^{k\delta} \pmod{p} \\ &\equiv \alpha^x \pmod{p}, \end{aligned}$$

với

$$a\gamma + k\delta \equiv x \pmod{p-1}.$$

Thật ra, bắt đầu với phương trình xác thực sẽ dễ nắm bắt hơn, và sau đó suy ra hàm ký tương ứng. Giả sử chúng ta có đồng dư:

$$\alpha^x \equiv \beta^\gamma \gamma^\delta \pmod{p}. \tag{8.1}$$

Sau đó chúng ta có các phép thế

$$\gamma \equiv \alpha^k \pmod{p}$$

và

$$\beta \equiv \alpha^a \pmod{p},$$

nhưng chúng ta không thay thế ɣ trong lũy thừa của (8.1). Ta có:

$$\alpha^x \equiv \alpha^{a\gamma + k\delta} \pmod{p}.$$

Bây giờ, α là một phần tử nguyên thủy modulo p; do đó đồng dư này là đúng khi và chỉ khi các lũy thừa là đồng dư p - 1, cụ thể là, khi và chỉ khi:

$$x \equiv a\gamma + k\delta \pmod{p-1}.$$

Cho x, a, γ, và k, đồng dư này có thể được giải để tìm ra δ, tạo ra công thức được sử dụng trong hàm ký của Hệ mật 8.2.

Alice tính toán một chữ ký sử dụng cả khóa riêng tư, a, và một số ngẫu nhiên, k, (được sử dụng để ký một thông điệp, x). Việc xác thực có thể được thực hiện mà chỉ sử dụng thông tin công khai.

Hãy cùng làm một ví dụ nhỏ để minh họa việc tính toán:

Ví dụ 8.1 Giả sử chúng ta có p = 467, $\alpha = 2$, $a = 127$; ta có

$$\begin{aligned} \beta &= \alpha^a \bmod p \\ &= 2^{127} \bmod 467 \\ &= 132. \end{aligned}$$

Giả sử Alice muốn ký thông điệp $x = 100$ và cô ấy chọn số ngẫu nhiên là $k = 213$ (chú ý rằng gcd(213, 466) = 1 và $213^{-1} \bmod 466 = 431$). Ta có

$$\gamma = 2^{213} \bmod 467 = 29$$

và

$$\delta = (100 - 127 \times 29)\ 431 \bmod 466 = 51$$

Người khác có thể xác thực chữ ký (29,51) bằng cách kiểm tra rằng

$$132^{29} 29^{51} \equiv 189 \pmod{467}$$

và

$$2^{100} \equiv 189 \pmod{467}$$

Do đó, chữ ký là hợp lệ.

8.3.1 Tính bảo mật của Cơ chế chữ ký ElGamal

Cùng xem tính bảo mật của Cơ chế chữ ký ElGamal. Giả sử Oscar muốn giả mạo một chữ ký cho thông điệp x, trong khi không biết a. Nếu Oscar chọn một giá trị γ và sau đó cố gắng tìm δ tương ứng, anh ta phải tính logarit rời rạc $\log_{\gamma}\alpha^{x}\beta^{-\gamma}$. Mặt khác, nếu trước tiên anh ta chọn δ và sau đó cố gắng tìm γ, nghĩa là anh ta đang cố "giải" phương trình

$$\beta^{\gamma}\gamma^{\delta} \equiv \alpha^{x} \pmod{p}$$

để tìm ra γ "chưa biết". Đây là một bài toán chưa có lời giải khả thi; tuy nhiên, nó dường như không có liên quan đến bất cứ một bài toán nổi tiếng nào ví dụ như bài toán **Logarit Rời rạc.** Vẫn còn lại khả năng tồn tại một cách nào đó để có thể tính đồng thời cả γ và δ sao cho (γ,δ) là một chữ ký. Hiện chưa có ai tìm ra cách để làm điều này, nhưng ngược lại, chưa có ai chứng minh được là nó là bất khả thi.

Nếu Oscar chọn γ và δ và sau đó cố gắng giải để tìm ra x, anh ta lại một lần nữa phải đối mặt với một bài toán Logarit Rời rạc, cụ thể là phép tính $\log_{\alpha}\beta^{\gamma}\gamma^{\delta}$. Do đó, Oscar không thể ký một thông điệp x cho trước sử dụng hướng đi này.

Tuy nhiên, có một phương pháp Oscar có thể sử dụng để ký một tin nhắn ngẫu nhiên bằng cách chọn γ, δ, và x đồng thời. Do đó một giả mạo tồn tại (existential forgery) có thể thực hiện dưới một cuộc tấn công chỉ sử dụng khóa (giả sử rằng một hàm băm không được sử dụng). Chúng tôi sẽ mô tả cách làm việc này bây giờ.

Giả sử i và j là các số nguyên sao cho $0 \le i \le p - 2$, $0 \le j \le p - 2$, và giả sử chúng ta biểu diễn γ theo dạng $\gamma = \alpha^{i}\beta^{j} \bmod p$. Điều kiện xác thực có dạng

$$\alpha^x \equiv \beta^\gamma (\alpha^i \beta^j)^\delta \pmod{p}.$$

Tương đương với

$$\alpha^{x-i\delta} \equiv \beta^{\gamma+j\delta} \pmod{p}.$$

Biểu thức đồng dư thứ hai này sẽ được thỏa mãn nếu

$$x - i\delta \equiv 0 \pmod{p-1}$$

và

$$\gamma + j\delta \equiv 0 \pmod{p-1}.$$

Cho i và j, chúng ta có thể dễ dàng giải hai đồng dư modulo p - 1 để tìm ra δ và x, biết rằng gcd(j, p - 1) = 1. Ta có:

$$\begin{aligned} \gamma &= \alpha^i \beta^j \bmod p, \\ \delta &= -\gamma j^{-1} \bmod (p-1), \quad \text{and} \\ x &= -\gamma i j^{-1} \bmod (p-1). \end{aligned}$$

Thông qua cách chúng ta đã xây dựng (γ,δ), đây rõ ràng là một chữ ký hợp lệ cho thông điệp x.

Chúng ta hãy minh họa nó bằng một ví dụ.

Ví dụ 8.2 Như trong ví dụ trước, giả sử p = 467, α = 2, và β = 132. Giả sử Oscar chọn i = 99 và j = 179; ta có j^{-1} mod (p - 1) = 151. Anh ta sẽ tính như sau:

$$\begin{aligned} \gamma &= 2^{99}132^{179} \bmod 467 &&= 117 \\ \delta &= -117 \times 151 \bmod 466 &&= 41 \\ x &= 99 \times 41 \bmod 466 &&= 331. \end{aligned}$$

Ta được (117,41) là một chữ ký hợp lệ cho thông điệp 331, có thể được xác thực bằng cách kiểm tra:

$$132^{117}117^{41} \equiv 303 \pmod{467}$$

và

$$2^{331} \equiv 303 \pmod{467}.$$

Trong dạng giả mạo thứ hai, Oscar bắt đầu với một thông điệp được ký trước đó bởi Alice. Đây là một cuộc tấn công giả mạo tồn tại (existential forgery) với thông điệp được biết trước. Giả sử (γ,δ) là một chữ ký hợp lệ cho thông điệp x. Oscar có khả năng ký nhiều thông điệp khác. Giả sử h, i, và j là các số nguyên, $0 \leq h,i,j \leq p - 2$, và $\gcd(h\gamma - j\delta, p - 1) = 1$. Ta cần tính:

$$\begin{aligned} \lambda &= \gamma^h \alpha^i \beta^j \bmod p \\ \mu &= \delta\lambda(h\gamma - j\delta)^{-1} \bmod (p-1), \quad \text{and} \\ x' &= \lambda(hx + i\delta)(h\gamma - j\delta)^{-1} \bmod (p-1). \end{aligned}$$

Sau đó, sẽ khá mất thời gian nhưng nó là dễ tiếp cận để kiểm tra điều kiện xác thực

$$\beta^\lambda \lambda^\mu \equiv \alpha^{x'} \pmod{p}$$

là đúng. Do đó, (λ, μ) là chữ ký hợp lệ cho x'.

Cả hai phương pháp này là giả mạo tồn tại (existential forgery), nhưng chúng khó có khả năng có thể được sửa đổi để tạo ra giả mạo lựa chọn (selective forgery). Do đó, chúng dường như không đem lại mối đe dọa nào cho tính báo mật của Cơ chế chữ ký ElGamal, với điều kiện một hàm băm bảo mật được sử dụng như đã mô tả ở **phần 8.2.1**.

Chúng tôi cũng đề cập đến một số cách Cơ chế chữ ký ElGamal có thể bị phá nếu được sử dụng không cẩn thận (đó là các trường hợp rộng hơn của lỗi giao thức (protocol failures), được giới thiệu trong các bài tập của **chương 6**). Đầu tiên, giá trị ngẫu nhiên k được sử dụng trong việc tính toán chữ ký không nên bị để lộ. Vì, nếu k được biết và $\gcd(\gamma, p - 1) = 1$, thì nó sẽ là rất đơn giản để tính toán

$$a = (x - k\delta)\gamma^{-1} \bmod (p-1).$$

Một khi a được biết thì hệ thống đã hoàn toàn bị phá hỏng và Oscar có thể tự do giả mạo chữ ký.

Một cách sử dụng hệ thống sai khác là sử dụng cùng một giá trị k để ký hai thông điệp khác nhau. Việc này sẽ dẫn đến một giá trị γ trùng lặp, và nó cũng cho phép Oscar có thể dễ dàng tính a và do đó phá hỏng hệ thống. Việc này có thể được làm như sau. Giả sử (γ, δ_1) là một chữ ký của x_1 và (γ, δ_2) là một chữ ký của x_2. Ta có

$$\beta^{\gamma}\gamma^{\delta_1} \equiv \alpha^{x_1} \pmod{p}$$

và

$$\beta^{\gamma}\gamma^{\delta_2} \equiv \alpha^{x_2} \pmod{p}.$$

Nên

$$\alpha^{x_1-x_2} \equiv \gamma^{\delta_1-\delta_2} \pmod{p}.$$

Viết $\gamma = \alpha^k$, ta có phương trình sau với k chưa biết:

$$\alpha^{x_1-x_2} \equiv \alpha^{k(\delta_1-\delta_2)} \pmod{p},$$

tương đương với

$$x_1 - x_2 \equiv k(\delta_1 - \delta_2) \pmod{p-1}. \tag{8.2}$$

Đặt $d = \gcd(\delta_1 - \delta_2, p - 1)$. Nếu $d = 1$, chúng ta có thể ngay lập tức giải (8.2), ta được

$$k = (x_1 - x_2)(\delta_1 - \delta_2)^{-1} \pmod{p-1}.$$

Tuy nhiên, ngay cả khi $d > 1$, chúng ta vẫn có khả năng xác định giá trị của k, với điều kiện là d không quá lớn. Vì $d \mid (p - 1)$ và $d \mid (\delta_1 - \delta_2)$, ta có $d \mid (x_1 - x_2)$. Định nghĩa

$$\begin{aligned} x' &= \frac{x_1 - x_2}{d} \\ \delta' &= \frac{\delta_1 - \delta_2}{d} \\ p' &= \frac{p-1}{d}. \end{aligned}$$

Đồng dư (8.2) trở thành:

$$x' \equiv k\delta' \pmod{p'}.$$

Vì gcd(δ', p') = 1, chúng ta có thể tính

$$\epsilon = (\delta')^{-1} \bmod p'.$$

Giá trị của k là

$$k = x'\epsilon \bmod p'.$$

k có *d* giá trị khả thi:

$$k = x'\epsilon + ip' \bmod (p-1)$$

với một vài giá trị *i*, $0 \le i \le d$ - 1. Trong số *d* giá trị khả thi đó, giá trị (duy nhất) đúng có thể được xác định bằng cách thử điều kiện

$$\gamma \equiv \alpha^k \pmod{p}.$$