BG ChVIII Bài 1. Sơ đồ xưng danh Guillou-Quisquater.

Sơ đồ Guillou-Quisquater cũng được xây dựng theo cùng một cách thức như các sơ đồ Schnorr và Okamoto kể trên, nhưng bài toán khó mà ta dựa vào ở đây không phải là bài toán tính lôgarit rời rạc mà là bài toán RSA.

Sơ đồ cũng cần có sự tham gia của một cơ quan uỷ thác TA để cấp chứng chỉ cho các người tham gia. TA chọn hai số nguyên

tố lớn p và q và tính tích $n = pq$, giữ bí mật p ,q và công khai n. Các tham số đó được chọn sao cho bài toán phân tích n thành thừa số là rất khó. TA cũng chọn thêm một số b là số nguyên tố có độ lớn khoảng 2^{40} như là một tham số an toàn. Số b cũng được xem là số mũ thoả mãn điều kiện RSA, nghĩa là việc tính $v = u^b \bmod n$ là dễ, nhưng việc tính ngược u từ v là rất khó, nếu không biết p,q.

Thủ tục cấp chứng chỉ cho một người tham gia A được tiến hành như sau:

1.TA xác lập các thông tin về danh tính của A dưới dạng một dãy ký tự mà ta ký hiệu là I_A hay $ID(A)$.

2. A chọn bí mật một số ngẫu nhiên u ($0 \le u \le n-1$), tính

$$v = (u^{-1})^b \bmod n,$$

và chuyển số v cho TA.

3. TA tạo chữ ký $s = sig_{TA}(I_A, v)$ và cấp cho A chứng chỉ

$$C(A) = (ID(A), v, s).$$

Như vậy, chứng chỉ mà TA cấp cho A gồm (I_A, v) và chữ ký của TA trên thông tin (I_A, v) đó. Chú ý rằng TA cấp chứng chỉ cho A mà có thể không biết gì về thông tin bí mật của A là số u.

Bây giờ, với chứng chỉ C(A) đó, A có thể xưng danh với bất kỳ đối tác B nào bằng cách cùng B thực hiện một giao thức xác nhận danh tính như sau:

1. A chọn thêm một số ngẫu nhiên k ($0 \le k \le n$-1), tính

$$\gamma = k^b \bmod n,$$

và gửi cho B các thông tin C(A) và γ.

2. B kiểm thử chữ ký của TA trong chứng chỉ C(A) bởi hệ thức $ver_{TA}(ID(A), v, s)$ =đúng. Kiểm thử xong, B chọn một số ngẫu nhiên r $(1 \leq r \leq b-1)$ và gửi r cho A.

3. A tính $y = k.u^r \bmod n$ và gửi y cho B.

4. B thử điều kiện

$$\gamma \equiv v^r y^b \pmod{n}$$

và nếu điều kiện đó được thoả mãn thì xác nhận danh tính của A.

Cũng như các trường hợp trước, việc chứng minh tính *đầy đủ* của sơ đồ là rất đơn giản:

$$\begin{aligned} v^r y^b &\equiv (u^{-b})^r (ku^r)^b \pmod{n} \\ &\equiv u^{-br} k^b u^{br} \pmod{n} \\ &\equiv k^b \equiv \gamma \pmod{n}. \end{aligned}$$

Một người khác A, do không biết số bí mật u , nên không thể tính đúng được số y ở bước 3 của giao thức để được B xác nhận (như là A) ở bước 4, tức không

thể mạo nhận mình là A; đó là tính *đúng đắn* của sơ đồ.

Giả sử có một người O có thể thực hiện thông suốt giao thức xác nhận để có thể được mạo nhận là A, chẳng hạn ít nhất hai lần. Điều đó có nghĩa là O biết được hai số $r_1 \neq r_2$ và hai số y_1, y_2 sao cho

$$\gamma \equiv v^{r_1} y_1^b \equiv v^{r_2} y_2^b \pmod{n}.$$

Giả thiết $r_1 > r_2$, khi đó ta có

$$v^{r_1 - r_2} \equiv (y_2 / y_1)^b \pmod{n}.$$

Do $0< r_1 - r_2 < b$ và b là số nguyên tố nên $\gcd(r_1 - r_2, b) = 1$, có thể tính được dễ dàng

$t = (r_1 - r_2)^{-1} \bmod b$, và có

$$v^{(r_1 - r_2)t} \equiv (y_2 / y_1)^{bt} \pmod{n}.$$

Do $t = (r_1 - r_2)^{-1} \bmod b$ nên ta có

$$(r_1 - r_2)t = lb + 1$$

với l là một số nguyên dương nào đó, vì vậy,

$$v^{lb+1} \equiv (y_2 / y_1)^{bt} \pmod{n},$$

hay là

$$v \equiv (y_2 / y_1)^{bt} (v^{-1})^{lb} \pmod{n}.$$

Nâng cả hai về lên luỹ thừa bậc $b^{-1} \bmod \phi(n)$, ta được

$$u^{-1} \equiv (y_2 / y_1)^t (v^{-1})^l \pmod{n}.$$

cuối cùng, tính nghịch đảo của hai vế theo mod$n$ ta được

$$u = (y_1 / y_2)^t v^l \bmod n .$$

Như vậy, O tính được số bí mật u trong thời gian đa thức! Theo giả thiết, điều đó không thể xẩy ra, vì vậy, giả thiết về việc O có

thể thực hiện thông suốt giao thức xác nhận để được mạo nhận danh tính là A là không đúng; sơ đồ xưng danh được chứng minh là *an toàn*.

Thí dụ: Giả sử TA chọn p =467, q =479, như vậy n =223693, TA cũng chọn thêm b =503.

Giả sử A chọn số bí mật u =101576, và tính

$$v=(101576^{-1})^{503} \bmod 223693$$
$$= 89888.$$

TA tạo chữ ký $s = sig_{TA}(ID(A), v)$ và cấp cho A chứng chỉ

$$C(A) = (ID(A), v, s).$$

Giả thiết A muốn xưng danh với B, A chọn $k = 187485$, và gửi cho B giá trị $\gamma = 187485^{503} \bmod 223693 = 24412$. B dùng thuật toán kiểm thử ver_{TA} để thử điều kiện $ver_{TA}(ID(A), v, s) =$ đúng, sau đó gửi đến A câu hỏi $r = 375$. A sẽ trả lời lại bằng

$$y = 187485.101576^{375} \bmod 223693$$

$$= 93725.$$

B thử điều kiện $\gamma \equiv v^r y^b$ (mod$n$), trong trường hợp này là

$$24412 \equiv 89888^{375}.93725^{503} (\text{mod } 223693),$$

đồng dư thức đó đúng. Vậy B xác nhận danh tính của A.

Bây giờ ta lại giả thiết là O biết được hai số r_1=401, r_2=375 và các số tương ứng y_1=103386 và y_2=93725. O biết rằng

$$v^{401}.103386^b \equiv v^{375}.93725^b (\text{mod}n).$$

O sẽ tính

$t = (r_1 - r_2)^{-1} \bmod b = (401-375)^{-1} \bmod 503 = 445,$

sau đó tính được

$$l = \frac{(r_1 - r_2)t - 1}{b} = \frac{(401-375)445 - 1}{503} = 23.$$

Cuối cùng, O sẽ tìm được giá trị bí mật u là

$$u = (y_1 / y_2)^t v^l \bmod n$$

$$= (103386/93725)^{445}.89888^{23} \bmod 223693$$

$$= 101576,$$

là số bí mật của A.

Chú ý: Sơ đồ xưng danh Guillou-Quisquater, cũng như các sơ đồ Schnorr và Okamoto

trước đó, đều cần có chứng chỉ của TA cho mỗi người tham gia. Ta có thể thay đổi chút ít để biến sơ đồ xưng danh đó thành một **sơ đồ xưng danh dựa vào danh tính** mà không cần có chứng chỉ như sau: Sơ đồ dùng một hàm băm công khai h , và thay cho việc cấp chứng chỉ C(A) cho người tham gia A, TA sẽ cấp cho A danh tính ID(A) cùng một số u được tính bởi công thức

$$u = (h(ID(\mathrm{A}))^{-1})^{a} \bmod n .$$

(a là một số mũ bí mật của TA). Số u được A giữ riêng cho mình.

Khi A cần xưng danh với B, A và B cùng thực hiện một giao thức xác nhận danh tính sau đây:

1. A chọn một số ngẫu nhiên k, $0 \le k \le n-1$, và tính

$$\gamma = k^b \bmod n ,$$

rồi gửi ID(A) và γ cho B.

2. B tính $v = h(ID(\text{A}))$; chọn một số ngẫu nhiên r ($0 \le r \le 1$) và gửi r cho A.

3. A tính $y = ku^r \bmod n$ và gửi y cho B.

4. B thử điều kiện $\gamma \equiv v^r y^b \pmod n$ để xác nhận danh tính của A.

Khi xưng danh theo giao thức nói trên với B, A chỉ cần biết giá trị *u* là một giá trị được tính bởi TA (và chỉ TA tính được giá trị đó). O không thể giả mạo danh tính của A vì O không biết giá trị *u*.