BG ChVIII Bài 2. Giao thức Feige-Fiat-Shamir.

Giao thức xưng danh Feige-Fiat-Shamir mà ta sẽ giới thiệu trong tiết này thường được xem là một giao thức điển hình, trong đó một chủ thể tự xưng danh bằng cách chứng minh là mình biết một bí mật với việc dùng một kiểu chứng minh mà ta sẽ gọi là *chứng minh không lộ tri thức* (zero-knowledge proof), tức là trong chứng minh đó không tiết lộ bất cứ một thông tin dù nhỏ nào liên quan đến giá trị

bí mật của chủ thể xưng danh. ở đây,thuật ngữ "tri thức" chỉ được dùng với một nghĩa rất hạn chế để nói về việc **biết** một bí mật của một chủ thể**,** mà cái biết này thường khi chỉ là biết một bit (0 hoặc 1, đúng hoặc sai), không lộ tri thức là không tiết lộ cái biết về một bit đó. Trong tiết sau ta sẽ đề cập đến các "chứng minh không lộ tri thức" với một nghĩa rộng hơn, khi đó "tri thức" sẽ có nghĩa là biết chứng minh của một bài toán, và chứng minh không lộ tri thức sẽ có nghĩa là

thuyết phục một đối tác tin rằng mình biết cách chứng minh của bài toán đó, và ngoài việc bị thuyết phục đó ra thì đối tác không khai thác được bất cứ thông tin gì khác để có thể lặp lại chứng minh đó cả.

Bây giờ ta trở lại với việc trình bày giao thức xưng danh Feige-Fiat-Shamir.

ở bước chuẩn bị, trung tâm được uỷ thác (TA) công bố một môđuyn chung $n = pq$ cho mọi người tham gia, sau khi đã chọn và giữ bí mật hai số nguyên tố

lớn p và q , mỗi số này đều đồng dư với 3 theo mod4. Bài toán phân tích n thành thừa số được giả thiết là cực khó. Một số nguyên n như trên là số nguyên Blum, với -1 là một giả thặng dư bậc hai theo mod$n$ (tức là một bất thặng dư bậc hai có ký hiệu Jacobi bằng +1).

Mỗi người tham gia thực hiện các việc chuẩn bị như sau:

- Chọn k số nguyên ngẫu nhiên $s_1, s_2,...,s_k$ trong tập $\{1,...,n-1\}$, và k bit ngẫu nhiên $b_1, b_2,..., b_k$.

- Tính $v_i = (-1)^{b_i}(s_i^2)^{-1} \bmod n$ với mọi $1 \le i \le k$.

- Mỗi chủ thể A đăng ký với TA khoá công khai (v_1,..., v_k ; n) của mình, và giữ cho riêng mình khoá bí mật (s_1 ,...,s_k) .

Hoạt động của giao thức xưng danh sẽ gồm việc thực hiện t vòng hỏi-đáp sau đây; B sẽ chấp nhận danh tính của A nếu tất cả t vòng đó đều thành công. Giả thiết B có khoá công khai của A. Mỗi vòng gồm các bước :

(a) A chọn số nguyên ngẫu nhiên r $(1 \le r \le n-1)$, và một bit ngẫu nhiên b , tính $x = (-1)^b.r^2 \bmod n$; và gửi x cho B như một *bằng chứng*.

(b) B gửi cho A một vectơ gồm k bit ngẫu nhiên $(e_1,..., e_k)$ như một *câu hỏi* hay *lời thách đố*.

(c) A tính và gửi cho B $y = r.\prod_{j=1}^{k} s_j^{e_j} \bmod n$, như câu *trả lời*.

(d) B tính $z = y^2.\prod_{j=1}^{k} v_j^{e_j} \bmod n$, và *thử điều kiện* $z = \pm x$ và $z \neq 0$.

Chú ý rằng trong giao thức trên đây,các số k và t là các tham số an toàn như sẽ được giải thích trong một đoạn sau.

Thí dụ : Giả sử trung tâm TA chọn p =683 và q =811, và công bố $n = pq$ = 553913. Chọn các tham số k =3, t =1.

Giả sử A chọn s_1 =157, s_2 =43215, s_3 =4646, và 3 bit b_1=1, b_2=0, b_3=1. Tính ra v_1=441845, v_2=338402, v_3=124423.

Khoá công khai của A là (441845, 338402, 124423;

553913), khoá bí mật là (157, 43215, 4646).

Giao thức xưng danh của A có thể được thực hiện như sau:

a) A chọn r =1279, b =1, tính được x =25898, và gửi cho B,

b) B ra lời thách đố (e_1, e_2, e_3)=(0,0,1).

c) A trả lời lại bằng $y=rs_3 \bmod n$ = 403104.

d) B tính $z = y^2 v_3 \bmod n$ = 25898 và thử đúng $z = +x$ và $z \neq 0$.

Do đó B chấp nhận danh tính của A.

Đối với giao thức Feige-Fiat-Shamir, người ta chứng minh được rằng khả năng thành công của việc mạo xưng danh tính có xác suất nhiều lắm là 2^{-kt} , do đó nếu chọn k và t sao cho kt =20 chẳng hạn thì xác suất đó là khoảng 1 phần triệu, và nếu kt =40 thì xác suất đó là khoảng 1 phần triệu triệu, có thể coi là không thể xẩy ra. Tính an toàn của giao thức dựa trên độ khó của bài toán khai căn bậc hai

theo môđuyn là một hợp số lớn khó phân tích thành thừa số. Giao thức cũng có tính chất là một chứng minh không lộ tri thức theo nghĩa là nhờ biết khoá bí mật mà A thực hiện việc trả lời trong các vòng hỏi-đáp một cách trôi chảy, nhưng toàn bộ các trả lời của A không để lộ bất kỳ một chút bí mật nào để người khác (kể cả B) có thể khai thác nhằm phát hiện (khoá) bí mật của A.