데이터베이스 보안 프로젝트
암호 알고리즘

- 김윤희 -

본 프로젝트는 데이터베이스 보안 프로젝트 과목에서 진행한 것이며,
알고리즘의 정보는 모두 김명선 교수님께서 제공해 주셨습니다.

암호 알고리즘 작성자 : 김명선 교수님

Set up

p : prime
q : (p / 2 – 1) and prime
g_0 , g_1 , g_2 : q's generator

- p와 q는 Client 와 Server 만이 공유하고 있는 값이다.
- p와 q는 영지식 증명 프로토콜에서 쓰인다.
- p는 1024bit 이상이다.
- Client 와 Server 는 서로 공유한 상태에서 시작한다.
- Server 에서 p , q , g_0 , g_1 , g_2 값을 계산하여 소켓통신을 통해 Client에게 전달한다.

Client Algorithm

Client data : x_0 , x_1 , x_2 … x_n

1. $A \leftarrow 1$
2. for i in 0..n

   $A \leftarrow H(x_i) * A \bmod p$
3. RClient (RClient ∈ q , RClient ≠ 0)
4. $B \leftarrow g_0^{RClient} * A \bmod p$
5. for i in 0..n

   R2Client[i] (R2Client[i] ∈ q , R2Client[i] ≠ 0)

   $\alpha_i \leftarrow H(x_i) * g_1^{R2Client[i]} \bmod p$
6. $\delta_i \leftarrow A * H(x_i)^{-1} * g_2^{R2Client[i]} \bmod p$
7. $W \leftarrow B * \alpha_0^{-1} * \delta_0^{-1} \bmod p$
8. $h \leftarrow g_1 * g_2 \bmod p$
9. pi_c[3] ← Towprover(h, RClient, R2Client[0], W)
10. Client send Server <B, $\alpha_{0…n}$, $\delta_{0…n}$, pi_c[3]>
11. Receive < S, $\beta_{0..n}$, $U_{0..m}$, pi_s[3] >
12. if (EqualVerifier(S, β_0 , α_0 , pi_s[3]) = false) : exit
13. for I in 0..n

    $K_i \leftarrow S^{-R2Client[i]} * \beta_i \bmod p$

    $C_i \leftarrow SHA\_256(K_i \,||\, H(x_i) \,||\, x_i)$
14. $C_{0..n} \cup U_{0..m}$ /* 교집합 연산을 수행한다. */

Server Algorithm

Server data : Y_0 , Y_1 , Y_2 … Y_n

1. RServer (RServer ∈ q , RServer≠ 0)
2. for i in 0..m

   T ← $H(Y_i)^{RServer}$ mod p

   U_i ← SHA_256(T || $H(Y_i)$ || Y_i)

1. Receive <B, $\alpha_{0\ldots n}$, $\delta_{0\ldots n}$, pi_c[3]>
2. if (Twoverifer(B, α_0 , δ_0 , pi_c[3]) = false) : exit
3. $S \leftarrow g_1^{RServer} \ mod \ p$
4. for i in 0..n
5. $\beta_i \leftarrow \alpha_i^{RServer} \ mod \ p$
6. pi_s[3] ← EqualProver(S,R , β_0, α_0)
7. send client < S, $\beta_{0..n}$, $U_{0..n}$, pi_s[3] >

영지식 증명 – Client

Towprover(h, x_0 , x_1 , y)

1. RTowP0 (RTowP0 ∈ q , RTowP0 ≠ 0)
2. RTowP1 (RTowP1 ∈ q , RTowP1 ≠ 0)
3. K $\leftarrow g_0^{RTow0} * h^{RTowP1} \ mod \ p$
4. E $\leftarrow SHA\_256(\, p \,||\, \mathrm{y} \,||\, v\,)$
5. $Z_0 \leftarrow$ (RTowP0 − E ∗ x_0) mod q
6. $Z_1 \leftarrow$ (RTowP1 + E ∗ x_1) mod q
7. return [K , Z_0 , Z_1]

Twoverifer(B, α_0 , δ_0 , $pi\_c[3]$)

1. y $\leftarrow \alpha_0^{-1} * \delta_0^{-1} * B \ mod \ p$
2. $h \leftarrow g_1 * g_2 \ mod \ p$
3. E $\leftarrow SHA\_256(\, p \,||\, \mathrm{y} \,||\, pi\_c[0]\,)$
4. $v \leftarrow g_0^{pi\_c[1]} * h^{pi\_c[2]} y^E \ mod \ p$
5. $if \ v == pi\_c[0]$: return true
6. $else$ return false

영지식 증명 – Client

$$K = g_0^{RTow0} * g_1 g_2^{RTowP1} \mod p \quad (= pi\_c[0])$$

$$y = \alpha_0^{-1} * \delta_0^{-1} * B \mod p$$

$$= \alpha_0^{-1} * \delta_0^{-1} * g_0^{RClient} * A \mod p$$

$$= \frac{\cancel{H(x_0)} * \cancel{A} * g_0^{RClient}}{\cancel{A} * g_2^{R2Client[0]} * \cancel{H(x_0)} * g_1^{R2Client[0]}} \mod p$$

$$= g_2^{-R2Client[0]} * g_1^{-R2Client[0]} * g_0^{RClient} \mod p$$

$$v = g_0^{pi\_c[1]} * h^{pi\_c[2]} y^E \mod p$$

$$= \frac{g_0^{RTowP0 - \cancel{E * RClient}} * g_1 g_2^{RTowP1 + \cancel{E * R2Client[0]}} * \cancel{g_0^{E * RClient}}}{\cancel{g_1 g_2^{E * R2Client[0]}}} \mod p$$

$$= g_0^{RTowP0} * g_1 g_2^{RTowP1} \mod p$$

$$= K = pi\_c[0]$$

참고

$$B \leftarrow g_0^{RClient} * A \mod p$$

$$\delta_0 \leftarrow A * H(x_0)^{-1} * g_2^{R2Client[0]} \mod p$$

$$\alpha_0 \leftarrow H(x_0) * g_1^{R2Client[0]} \mod p$$

$$pi\_c[1] = (RTowP0 - E * x\_0) \mod q$$

$$pi\_c[2] = (RTowP1 + E * x\_1) \mod q$$

영지식 증명 – Server

Equalprover(S, R, β$_0$, α$_0$)

1. REqual (REqual ∈ q , REqual ≠ 0)
2. $K \leftarrow g_1^{\mathrm{REqual}}\ \ mod\ \ p$
3. $\mathrm{T} \leftarrow \alpha_0^{\mathrm{REqual}}\ \ mod\ \ p$
4. $ServerE \leftarrow$ SHA_256(p || S || β_0 || K || T)
5. $\mathrm{Z} \leftarrow (\mathrm{REqual}\ -\ ServerE * \mathrm{R})\ \ \mathrm{mod\ \ q}$
6. return [K , T , Z]

EqualVerifier (S, β$_0$, α$_0$, pi_s[3])

1. $ServerE \leftarrow$ SHA_256(p || S || β_0 || pi_s[0] || pi_s[1])
2. $v_0 \leftarrow\ g_1^{pi\_s[2]}\ *\ S^{ServerE}\ \ mod\ \ p$
3. $v_1 \leftarrow\ \alpha_0^{pi\_s[2]}\ *\ \beta_0^{SereverE}\ mod\ \ p$
4. if (pi_s[0] = v_0 ^ pi_s[1] = v_1) return true

   else return false

영지식 증명 – Server

$$v_0 = g_1^{pi\_s[2]} * S^{ServerE} \mod p$$
$$= g_1^{REqual - ServerE * RServer} * g_1^{ServerE * RServer} \mod p$$
$$= g_1^{REqual - ServerE * RServer + ServerE * RServer} \mod p$$
$$= g_1^{REqual} \mod p$$
$$= pi\_s[o]$$

$$v_1 = \alpha_0^{pi\_s[2]} * \beta_0^{SereverE} \mod p$$
$$= \alpha_0^{REqual - ServerE * RServer} * \alpha_0^{RServer * ServerE} \mod p$$
$$= \alpha_0^{REqual - ServerE * RServer + ServerE * RServer} \mod p$$
$$= \alpha_0^{REqual} \mod p$$
$$= pi\_s[1]$$

참고

$$pi\_s[0] = g_1^{REqual} \mod p$$
$$pi\_s[1] = \alpha_0^{REqual} \mod p$$
$$pi\_s[2] = (REqual - ServerE * RServer) \mod q$$
$$S = g_1^{RServer} \mod p$$