Криптографические протоколы

Лекция 6

Протоколы на основе техники доказательства знания

Деркач Максим Юрьевич

September 27, 2018

Ссылки

Протоколы на основе техники доказательства знания

Определение 1 Доказательство знания - это интерактивное доказательство, в котором доказывающий утверждает проверяющего в том, что он владеет секретной информацией.

Свойства протокола:

- полнота
- корректность
- нулевое разглашение

Протоколы на основе техники доказательства знания

Определение 2
Полнота - свойство означающее, что при выполнении честными участниками протокол решает задачу, для которой создан.

Определение 3
Корректность - свойство протокола противостоять угрозам со стороны злоумышленика, не располагающего секретной информацией, но пытающегося выполнить протокол вместо участника A, которой этой информацией владеет.

Определение 4
Нулевое разглашение - свойство протокола обеспечивающие, что никакая информация о доказываемом утверждение, не может быть получена нечестным проверяющим за полиномиальное время от длины переданных сообщений.

Протоколы на основе техники доказательства знания

1. $A- > B : \gamma$ (заявка - witness)
2. $B- > A : x$ (запрос - challenge)
3. $A- > B : y$ (ответ - response)

1. A : владеет секретом S.
2. A : генерирует случайное число r.
3. A : $\gamma = h(r, S)$

Шаг 3 могут повторять до тех пор пока B не примет решение, что протокол пройден.
Выполнение данного протокола t раз гарантирует, что A - подлинный участник.

$p,\ q$ - простые, $p \neq q,\ n = pq,\ |p|, |q| >= 512$
A : секретный ключ - $a \in Z_n^*,\ (a, n) = 1$
открытый ключ - $b = (a^{-1})^2\ (mod\ n)$

1. $A- > B : \gamma = r^2\ (mod\ n), 1 \leq r \leq n - 1,\ r-$ простое число
2. $B- > A : x \in \{0, 1\}$
3. $A- > B : y = ra^x\ (mod\ n)$

B проверяет $y^2 b^x \equiv \gamma(mod\ n)$
Шаги повторяются t раз.

Протоколы на основе техники доказательства знания

Протокол Фиата-Шамира

- Полнота:
  $y^2 b^x = r^2 a^{2x} a^{-2x} = r^2 \equiv \gamma (mod\ n)$
- Корректность:
  1. $\forall z, \gamma = z^2\ (mod\ n)$
     $x = 0- > y = z$: вероятность успеха 1
     $x = 1- > y = za,\ a = (\sqrt{b})^{-1}$: вероятность успеха $\frac{1}{n}$
     Вероятность успешного угадывания:
     $P = \frac{1}{2}(1 + \frac{1}{n})$
  2. Выберем r не случайно
     $r = za^{-1},\ \gamma = z^2 a^{-2} = z^2 b\ (mod\ n)$
     $x = 1- > y = z$: вероятность успеха 1
     $x = 0- > y = za^{-1}$: вероятность успеха $\frac{1}{n}$
     Вероятность успешного угадывания:
     $P = \frac{1}{2}(1 + \frac{1}{n})$

  $P = \frac{1}{2}(1 + \frac{1}{n}) \approx \frac{1}{2}$ и t повторов $\rightarrow P_{total} = 2^{-t}$
- Нулевое разглашение: (y, x, γ)

Протоколы на основе техники доказательства знания

Протокол Файге-Фиата-Шамира

$p,\ q$ - простые, $p \neq q,\ n = pq,\ |p|, |q| >= 512$
$A:$
секретный ключ -
$a = (s_1, ..., s_k),\ s_i \in\ Z_n^*,\ (s_i, n) = 1,\ \forall i \in \{1, ..., k\}$
открытый ключ -
$b = (v_1, ..., v_k),\ v_i = (s_i^2)^{-1}\ (mod\ \ n),\ \forall i \in \{1, ..., k\}$

1. $A- > B : \gamma = r^2\ (mod\ \ n), 1 \leq r \leq n - 1,\ r-$ простое число
2. $B- > A : x = (x_1, ..., x_i) \in \{0, 1\}^k$
3. $A- > B : y = r(s_1^{x_1} ... s_k^{x_k})\ (mod\ \ n)$

B проверяет $y^2(v_1^{x_1} ... v_k^{x_k}) \equiv \gamma(mod\ \ n)$
Шаги повторяются t раз.

$p, \ q$ - простые, $q|(p-1), \ \alpha \in Z_p, \ ord(\alpha) = q$
A : секретный ключ - $1 \le a \le q-2$
открытый ключ - $b = \alpha^{-a} \ (mod \ p)$

1. $A- > B : \gamma = \alpha^r \ (mod \ p), \ 1 \le r \le q-2$
2. $B- > A : 0 \le x \le q-1$
3. $A- > B : y = (r+ax) \ (mod \ q)$

B проверяет $\alpha^y b^x \equiv \gamma (mod \ p)$
Шаги повторяются t раз.

Протоколы на основе техники доказательства знания

Протокол Шнора

- Полнота:
  $\alpha^y b^x = \alpha^{r+ax}\alpha^{-ax} = \alpha^r \equiv \gamma (mod\ p)$
- Корректность: (для $x \in \{0, 1\}$)
  1. $\forall z, \gamma = \alpha^z\ (mod\ p)$
     $x = 0- > y = z$: вероятность успеха 1
     $x = 1- > y = z + a,\ a = -log_{\alpha} b$: вероятность успеха $\frac{1}{q}$
     Вероятность успешного угадывания:
     $P = \frac{1}{2}(1 + \frac{1}{q})$
  2. Выберем r не случайно
     $r = z - a,\ \gamma = \alpha^{z-a} = \alpha^z b\ (mod\ p)$
     $x = 1- > y = z$: вероятность успеха 1
     $x = 0- > y = z - a$: вероятность успеха $\frac{1}{q}$
     Вероятность успешного угадывания:
     $P = \frac{1}{2}(1 + \frac{1}{q})$

  $P = \frac{1}{2}(1 + \frac{1}{q}) \approx \frac{1}{2}$ и t повторов $\rightarrow P_{total} = 2^{-t}$
- Нулевое разглашение: (y, x, γ)

Протоколы на основе техники доказательства знания

Протокол Окамото

$p,\ q$ - простые, $q|(p-1),\ \alpha_1, \alpha_2 \in Z_p$
$ord(\alpha_1) = ord(\alpha_2) = q$
A : секретный ключ - $(a_1, a_2),\ 1 \leq a_1, a_2 \leq q-2$
открытый ключ - $b = \alpha_1^{-a_1} \alpha_2^{-a_2}\ (mod\ p)$

1. $A->B : \gamma = \alpha_1^{r_1} \alpha_2^{r_2}\ (mod\ p),\ 1 \leq r_1, r_2 \leq q-2$
2. $B->A : 0 \leq x \leq q-1,\ x < 2^t$
3. $A->B : y_1 = (r_1 + a_1 x)\ (mod\ q)$
   $y_2 = (r_2 + a_2 x)\ (mod\ q)$

B проверяет $\alpha_1^{y_1} \alpha_2^{y_2} b^x \equiv \gamma (mod\ p)$

- Полнота:
  $\alpha_1^{y_1} \alpha_2^{y_2} b^x = \alpha_1^{r_1 + a_1 x} \alpha_2^{r_2 + a_2 x} \alpha_1^{-a_1} \alpha_2^{-a_2} = \alpha_1^{r_1} \alpha_2^{r_2} \equiv \gamma (mod\ p)$
- Нулевое разглашение: (y_1, y_2, x, γ)

$p,\ q$ - простые, $n = pq,\ b \geq 3,\ (b,\ \varphi(n)) = 1$
$A:$ секретный ключ - $u \in Z_n^*,\ (u,\ n) = 1$
открытый ключ - $v = (u^{-1})^b\ (mod\ n)$

1. $A- > B: \gamma = r^b\ (mod\ n),\ 1 \leq r_1, r_2 \leq n-2$
2. $B- > A: 0 \leq x \leq b-1,\ x < 2^t$
3. $A- > B: y = ru^x\ (mod\ n)$

B проверяет $v^x y^b \equiv \gamma (mod\ n)$

- Полнота:
  $v^x y^b = u^{-bx} r^b u^{bx} = r^b \equiv \gamma (mod\ n)$
- Нулевое разглашение: (y, x, γ)

Протоколы на основе техники доказательства знания

Протокол GQ с ключами зависящими от индентификатора

$p,\ q$ - простые, $n = pq,\ b \geq 3,\ (b,\ \varphi(n)) = 1,\ ab \equiv 1\ (mod \varphi(n))$
A : секретный ключ - $u = (h(ID_A))^{-a} \in Z_n$
открытый ключ - $v = h(ID_A) = (u^{-1})^b\ (mod\ n)$

1. $A- > B : \gamma = r^b\ (mod\ n),\ 1 \leq r_1, r_2 \leq n - 2$
2. $B- > A : 0 \leq x \leq b - 1,\ x < 2^t$
3. $A- > B : y = ru^x\ (mod\ n)$

B проверяет $v^x y^b \equiv \gamma(mod\ n)$

- Полнота:
  $v^x y^b = u^{-bx} r^b u^{bx} = r^b \equiv \gamma(mod\ n)$
- Нулевое разглашение: (y, x, γ)