Криптография.

1 апреля 2017 г.

1 Разделение секрета

Теорема 1.1 (Csirmaz'94)**.** *Существуют структуры доступа* Γ *на* n *участниках, такие что для любой схемы разделения секрета* $\max_i \frac{H(S_i)}{H(S_0)} \geq \Omega(n/\log n)$.

Доказательство. Выберем n и k такие, что $n = 2^k + k + 1$, и два множества участников

$$A = \{a_1, a_2, \ldots, a_k\},$$
$$B = \{b_1, b_2, \ldots, b_{2^k-1}\}.$$

Для определения структуры доступа нам потребуются два семейства множеств. Пусть $\{A_0, A_1, A_2, \ldots, A_{2^k-1}\}$ — это все подмножества A, причём $A_0 = A$ и для любых $i < j$ выполняется $A_i \not\subseteq A_j$ (например, можно их упорядочить по уменьшению размера). Построим множества $\{B_0, B_1, B_2, \ldots, B_{2^k-1}\}$ следующим образом: $B_0 = \emptyset$, $B_i = \{b_1, b_2, \ldots, b_i\}$. Теперь мы готовы определить структуру доступа Γ: $\Gamma = \{U_i\}_{i=0}^{2^k-1}$, где $U_i = A_i \cup B_i$.

Как и в предыдущих утверждениях обозначим $H(S_0)$ за h. В дальнейших рассуждениях мы будем использовать следующую нотацию: под энтропией некоторого множества участников $X = \{x_1, x_2, \ldots, x_t\} \subset A \cup B$, мы будем понимать энтропию секретов, которые принадлежат участникам этого множества, т.е. $H(X) = H(S_{x_1}, S_{x_2}, \ldots, S_{x_t})$.

Лемма 1.1. *Для* $i = \{0, 1, 2, \ldots, 2^k - 2\}$

$$H(A \cup B_i) - H(B_i) \geq H(A \cup B_{i+1}) - H(B_{i+1}) + h.$$

Упражнение 1.1. *Покажите, что из леммы 1.1 следует, что* $H(A) \geq (2^k - 1) \cdot h$.

Упражнение 1.2. *Докажите, что из предыдущего упражнения следует теорема.*

Осталось доказать лемму 1.1.

Доказательство леммы 1.1. Докажем два неравенства:

1. $H(A_{i+1} \cup B_i) + H(B_{i+1}) \geq H(A_{i+1} \cup B_{i+1}) + H(B_i)$.
2. $H(A \cup B_i) + H(A_{i+1} \cup B_{i+1}) \geq H(A \cup B_{i+1}) + H(A_{i+1} \cup B_i) + h$.

Упражнение 1.3. *Из двух неравенств выше получите утверждение леммы.*

Упражнение 1.4. *Докажите неравенство 1. [Hint: $I(x : y \mid z) \geq 0$.]*

Упражнение 1.5. *Докажите второе неравенство аналогично лемме 5.3 из конспекта лекций(конспект скоро появится если еще не). Рассмотрите условное распределение при известном $A_? \cup B_?$(подставьте вместо вопросиков нужное).*

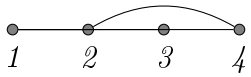
□

Упражнение 1.6. *Соберите доказательство теоремы из леммы и упражнений (записывать не надо).*

□

2 Другие задачи

Упражнение 2.1. *Доказать, что для любой схемы разделения секреты для этой структуры* $\max_i \frac{H(S_i)}{H(S_0)} \geq 3/2$.



Упражнение 2.2. *Случайные функции a и b принимают значения в 3-элементном множестве, и $a = b$ с вероятностью $2/3$. Докажите, что $H(a \mid b) \leq \frac{4}{3}$. [Hint: Чуть улучшите неравенство, которое напрашивается быть здесь примененным.]*