Conspect

Максим Крючков, M3339

31 октября 2018 г.

Wow

$k \leftarrow Gen(1^n)$
$((m_0, m_0'), (m_1, m_1')) \leftarrow Adv(1^n)$
$b \leftarrow \{0, 1\}$
$(c, c') = Enc_k(m_b, m_b')$
$b' \leftarrow Adv((c, c'), 1^n)$
$b = b'$
Вероятность того, что угадают, надо сравнивать с $\frac{1}{2} + negl(n)$

Взлом на основе выбранных текстов

Есть некий черный ящик, оракул - Enc_k в котором зашит ключ.
То, как он работает известно атакующему, неизвестен только ключ
$k \leftarrow Gen(1^n)$
$((m_0, m_1) \wedge |m_0| = |m_1| \leftarrow Adv(1^n, Enc_k)$
$b \leftarrow \{0, 1\}$
$c \leftarrow Enc_k(m_b)$
$b' \leftarrow Adv(c, 1^n, Enc_k)$
$b = b'$
Шифр является устойчивым к атакам на основе выбранных сообщений, если вероятность того, что угадают $\leq \frac{1}{2} + negl(n)$

Случайно распределенная функция

Возьмем функцию с ключом $F : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}^n$. Первый аргумент - это k, второй - x.
$k \leftarrow Gen(1^n)$
$F_k : \{0, 1\}^* \to \{0, 1\}^*$
Функция F случайно распределенная, если мы берем случайный ключ и получаем случайную функцию. F_k неотличима от случайной, если $|Pr[D^{(F_k, 1^n)} - Pr[D^{(f, 1^n)}]| \leq negl(n)$