Курс лекций по теоретической криптографии

Тема 7. **Криптосистемы с секретным ключом**

Шокуров А.В.

Определение

$n \in \mathbb{N}$ — параметр стойкости

$M_n \subseteq \mathbb{B}^*$ — пространство сообщений (открытых текстов)

Носитель случайной величины $\operatorname{supp}\xi = \{x \mid \Pr[\xi = x] \neq 0\}$

Определение

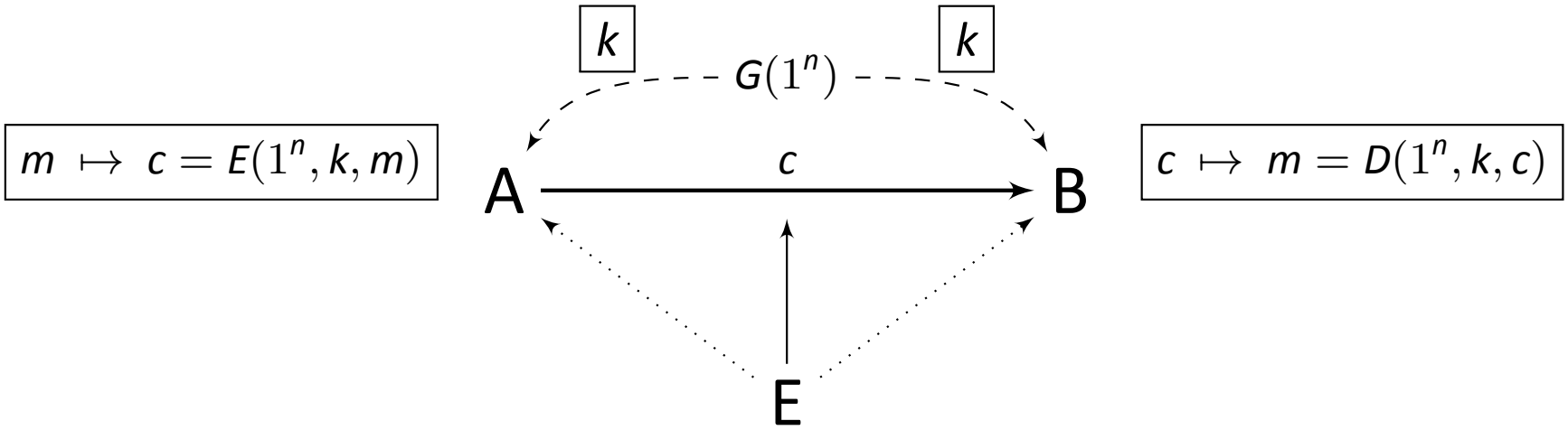
Система (вероятностного) шифрования[a] *с секретным ключом* (*private-key encryption system*) — это тройка алгоритмов (G, E, D):

- генератор ключей G — п. в. м. Т., $G(1^n) = k$ — *секретный ключ* (можно считать, что k выбирается из $K_n = \operatorname{supp} G(1^n)$ согласно вероятностному распределению $\mathcal{G}_n$, задаваемому случайной величиной $G(1^n)$);
- алгоритм шифрования E — п. (в.) м. Т., для $m \in M_n,\ k \in K_n$ $\quad E(1^n, k, m) = c$ — *криптограмма (шифртекст)* открытого текста m на ключе k;
- алгоритм дешифрования D — п. д. м. Т., $\forall n\ \forall m \in M_n\ \forall k \in K_n \quad D\big(1^n, k, E(1^n, k, m)\big) = m$ (с вероятностью 1).

---

[a] Синонимы: *криптосистема*, *шифр* (*cryptosystem*, *cipher*).

Схема применения и модель противника



Стойкость криптосистемы определяется относительно конкретного противника (против конкретной угрозы на основе конкретной атаки)

Модель противника (adversary model):

- *вычислительные ресурсы* = п. в. м. Т.
- *атака* (возможность получения исходных данных)
- *угроза* (цель противника)

Противник пытается реализовать угрозу, используя данные, полученные в ходе атаки.

Ему известна криптосистема, то есть алгоритмы G, E, D, и параметр стойкости n.

Параметр стойкости n и ключ k во время работы противника не меняются.

Основные типы атак

1. атака с известными шифртекстами (ciphertext-only / known ciphertext attack, **KCA**):
   $c_1, c_2, \ldots, c_l$;
2. атака с известными открытыми текстами (known plaintext attack, **KPA**):
   $(m_1, c_1), (m_2, c_2), \ldots, (m_l, c_l)$, где $c_i = E(1^n, k, m_i)$;
3. атака с выбором открытых текстов (chosen plaintext attack, **CPA**):
   $m_1, \ldots, m_l \rightsquigarrow (m_1, c_1), \ldots, (m_l, c_l)$, где $c_i = E(1^n, k, m_i)$;
4. атака с выбором шифртекстов (chosen ciphertext attack, **CCA**):
   $c_1, \ldots, c_l \rightsquigarrow (m_1, c_1), \ldots, (m_l, c_l)$, где $m_i = D(1^n, k, c_i)$;
5. атака с выбором текстов — комбинация 3 и 4.

$1 \leqslant i \leqslant l, \quad l \leqslant \mathrm{poly}(n)$

[1 — пассивный противник, 2—5 — активный противник]

Атаки 3—5 бывают

- *неадаптивными*, когда противник получает весь набор данных разом,
- *адаптивными*, когда пары к выбранным данным он получает последовательно по i, то есть выбор следующего запроса может зависеть от результата предыдущего.

NB Атаки, в которых по открытым текстам «выдаются» шифртексты, предполагают, что, вообще говоря, для каждого нового i вероятностная машина E использует новое заполнение своей «случайной» ленты.

Основные типы угроз

1. полное раскрытие (total breaking):
   найти использованный ключ[1];
2. извлечение открытого текста:
   по известной информации и случайному значению $E(1^n, k, m)$
   найти сообщение m;
3. извлечение частичной информации об открытом тексте:
   для некоторой функции $f : \mathbb{B}^* \to \mathbb{B}^*$
   по известной информации и случайному значению $E(1^n, k, m)$
   найти $f(m)$;
4. различение двух шифртекстов:
   при подходящем выборе $m^0, m^1 \in M_n \setminus \{m_1, \ldots, m_l\}$, $|m^0| = |m^1|$
   по криптограмме $E(1^n, k, m^b)$ для случайного $b \in_{\mathcal{U}} \{0, 1\}$
   определить b, то есть какое из двух сообщений было зашифровано.

---

[1] Сама по себе невозможность полного раскрытия не определяет стойкости, так как не исключает, что открытый текст всё же может быть получен (пример — система, передающая сообщения в открытую).

Основные типы угроз

Об *IND-стойкости* криптосистемы говорят, когда она удовлетворяет условию неразличимости двух шифртекстов (indistinguishability of encryptions), то есть
никакой противник не может осуществить угрозу 4 с вероятностью, существенно превосходящей вероятность случайного угадывания.

Понятие оракула для IND-CPA-стойкости

Определим IND-CPA-стойкость криптосистемы с секретным ключом — стойкость относительно пары *угроза* 4 / *атака* 3, — формализуя предположения о противнике с помощью специального оракула, к которому имеет доступ алгоритм противника.

Будем считать (без ограничения общности), что $m_i \in M_n \subseteq \mathbb{B}^n, \ \ 1 \leqslant i \leqslant l$.

Оракул $\mathcal{O}$, определяемый для криптосистемы (G, E, D),

- в начале работы выбирает секретный ключ $k \in_{\mathcal{G}_n} K_n$ $(k = G(1^n))$;
- после этого принимает запросы двух типов:
  1. $(1; x)$, где $x \in M_n$, в ответ на который возвращает $E(1^n, k, x)$,
  2. $(2; y^0, y^1)$, где $y^0, y^1 \in M_n$, получив который, проверяет, что y^0 и y^1 не появлялись ранее, выбирает случайный бит $b \in_{\mathcal{U}} \{0, 1\}$ и в зависимости от значения b возвращает либо $E(1^n, k, y^0)$, либо $E(1^n, k, y^1)$;
- ответив на *один* запрос второго типа, завершает свою работу.

? Какой вариант атаки здесь моделируется — адаптивный или нет?

Определение IND-CPA-стойкости

Предполагается, что «разумный» противник A, получая на вход 1^n,

- будет выбирать $m_i \in M_n$, $1 \leqslant i \leqslant l$, и делать l запросов $(1; m_i)$ к оракулу $\mathcal{O}$, чтобы набрать l пар $(m_1, c_1), \ \ldots, (m_l, c_l)$, где $c_i = E(1^n, k, m_i)$ (*атака*),
- потом выберет новые различные $m^0, m^1 \in M_n$ и сделает запрос $(2; m^0, m^1)$ к оракулу, а получив и проанализировав ответ c от оракула, выдаст некий бит и остановится (*угроза*).

Определение

Криптосистема (G, E, D) называется *IND-CPA-стойкой*, если для любой п. в. м. Т. A с вышеописанным оракулом $\mathcal{O}$

$$\Pr\left[A^{\mathcal{O}}(1^n) = b\right] \leqslant \frac{1}{2} + \operatorname{negl}(n).$$

NB Вероятность определяется выбором k, b, а также машинами A, E.

? Напишите определение стойкости для какой-нибудь другой пары *угроза* / *атака*.

Пример криптосистемы

Пусть g — псевдослучайный генератор, $g(\mathbb{B}^n) \subset \mathbb{B}^{q(n)}$ (q — полином)

$m_1, \ldots, m_t \in \mathbb{B}^n$ — сообщения[2], $t \cdot (n+1) < q(n)$

$\oplus$ — знак операции побитового сложения по модулю 2 (XOR)

Участники обмениваются по защищённому каналу секретным ключом $k \in_{\mathcal{U}} \mathbb{B}^n$

$g(k) = g_1 g_2 \ldots g_t \ldots \in \mathbb{B}^{q(n)}, \quad g_i \in \mathbb{B}^n, \quad 1 \leqslant i \leqslant t$

- Шифрование: $c_i = E(i, k, m_i) = m_i \oplus g_i$

  Отправитель посылает c_i по открытому каналу связи получателю
- Дешифрование: $D(i, k, c_i) = c_i \oplus g_i = m_i$

[2] Разбиение шифруемого сообщения на блоки фиксированной длины непринципиально, но так удобнее моделировать атаку CPA.

Пример криптосистемы

Эта система не вполне соответствует общему определению: для шифрования нескольких сообщений на одном ключе участники должны использовать счётчик этих сообщений, и значение счётчика у них должно быть синхронизированным. Другими словами, данный алгоритм шифрования имеет внутреннее состояние, изменяющееся после шифрования каждого нового сообщения.

Это пример т. н. *потокового шифра*. Большая часть потоковых шифров устроена именно так.

Стойкость криптосистемы из примера

Утверждение

Если g — псевдослучайный генератор, то

описанная криптосистема — IND-CPA-стойкая [a].

---

[a] В том смысле, который может иметь естественная формулировка понятия стойкости для случая криптосистем с внутренними состояниями (счётчиками).

Доказательство. Предположим, что существует такая п. в. м. Т. A, что $\Pr\left[A^{\mathcal{O}}(1^n) = b\right] > \frac{1}{2} + \frac{1}{p(n)}$ для некоторого полинома p и бесконечно многих n.

Построим п. в. м. Т. S, работающую на входе $(1^n, z)$, $z \in \mathbb{B}^{q(n)}$, следующим образом.

$z = z_1 z_2 \ldots z_t \ldots, \quad z_i \in \mathbb{B}^n, \quad 1 \leqslant i \leqslant t = \lfloor \frac{q(n)}{n} \rfloor$

1. S запускает машину A на входе 1^n и отвечает на её запросы к оракулу:
   - в ответ на $(1; m_i)$, $1 \leqslant i \leqslant l$, возвращает $c_i = m_i \oplus z_i$,
   - в ответ на $(2; m^0, m^1)$, выбирает $b \in_{\mathcal{U}} \{0, 1\}$ и возвращает $c = m^b \oplus z_{l+1}$,
   - получает выход машины A;
2. вычисляет выход — $S(1^n, z) = \begin{cases} 1, & \text{если } A^S(1^n) = b, \\ 0, & \text{если } A^S(1^n) \neq b. \end{cases}$

Стойкость криптосистемы из примера

- Если $z = g(\upsilon_n)$ $(\upsilon_n \in_{\mathcal{U}} \mathbb{B}^n)$, то A вычисляет b с вероятностью $> \frac{1}{2} + \frac{1}{p(n)}$, так как в этом случае S как оракул для A идентичен $\mathcal{O}$ $(k = \upsilon_n)$.

  Поэтому $\Pr\left[S(1^n, g(\upsilon_n)) = 1\right] > \frac{1}{2} + \frac{1}{p(n)}$.

- Если $z = \upsilon_{q(n)}$, то A угадывает b с вероятностью $\frac{1}{2}$ (c_i, c совпадают с υ_n как случайные величины).

  Поэтому $\Pr\left[S(1^n, \upsilon_{q(n)}) = 1\right] = \frac{1}{2}$.

  $\Rightarrow \quad \Pr\left[S(1^n, g(\upsilon_n)) = 1\right] - \Pr\left[S(1^n, \upsilon_{q(n)}) = 1\right] > \frac{1}{p(n)}$ для бесконечно многих n.

  Противоречие определению псевдослучайного генератора. □

Следствие

Если существует односторонняя функция,
то существуют и IND-CPA-стойкие криптосистемы с секретным ключом.