КРИПТОСИСТЕМЫ ГОЛЬВАССЕР – МИКАЛИ И БЛЮМА – ГОЛЬДВАССЕР

1 Криптосистема Гольвассер – Микали

Шифрсистема с открытым ключом называется *полиномиально* секретной, если ни один пассивный криптоаналитик не может за полиномиальное относительно длины шифртекста время выбрать два открытых сообщения $m_1 \in \Sigma^n$ и $m_2 \in \Sigma^n$ и затем с вероятностью, $\frac{1}{2} + \epsilon,\ \epsilon > 1/p(n)$, где $p(n)$ – любой полином, корректно различить шифробозначения $c_i = E(m_1)$ и $c_{3-i} = E(m_2)$ этих шифрвеличин.

Шифрсистема с открытым ключом называется *семантически* секретной, если при любых распределениях вероятностей на пространстве сообщений всё, что пассивный криптоаналитик может вычислить об открытом тексте за полиномиальное время, зная шифртекст, он может вычислить также за полиномиальное время без шифртекста.

Известно, что шифрсистема с открытым ключом семантически секретна тогда и только тогда, когда она полиномиально секретна.

Семантическая секретность может рассматриваться как полиномиально ограниченная совершенная секретность.

Рассмотрим криптосистему вероятностного шифрования Гольдвассер-Микали, обеспечивающую семантическую секретность.

Алгоритм генерации ключей в этой системе следующий.

Абонент A для обеспечения возможности передачи ему секретной информации на открытом ключе

1. Выбирает простые числа p и q, примерно одного размера.

2. Вычисляет $n = pq$.

3. Выбирает $y \in Z_n$, так, чтобы y было квадратичным невычетом по модулю n, а символ Якоби $\left(\frac{y}{n}\right) = 1$ (т.е. y является псевдоквадратом по модулю n : $\left(\frac{y}{p}\right) = \left(\frac{y}{q}\right) = -1$).

4. Открытым ключом объявляется (n, y), секретным ключом является пара (p, q).

Открытый ключ (n, y) публикуются через центр сертификации открытых ключей. [1]. Числа p и q составляют секретную *лазейку* и сохраняются как сек-

[1]Абонент A в центре сертификации открытых ключей проходит аутентификацию некриптографического характера, предъявляет открытый ключ и криптографическим методом доказывает, что владеет соответствующим ему секретным ключом. При этом возможно использование протокола доказательства с нулевым разглашением секрета. Центр сертификации публикует открытый ключ данного абонента в составе сертификата открытого ключа за своей цифровой подписью,ключ проверки которой известен всем абонентам компьютерной сети. Использование сертифицированного открытого ключа гарантирует,что зашифрованная на этом ключе информация может быть расшифрована только владельцем соответствующего секретного ключа, имя которого указывается в сертификате открытого ключа

ретный ключ абонента A. Любой отправитель B, получив от центра сертификации сертификат открытого ключа абонента A, имеет возможность зашифровать и безопасно передать абоненту A секретное сообщение в виде числа $m \in N$.

Сторона B зашифровывает сообщение m для стороны A, используя открытый ключ, по следующему алгоритму E_A зашифрования.

1. Получить и проверить сертификат открытого ключа стороны A.
2. Представить сообщение m в виде строки битов $m = m_1, \ldots, m_t$ длины t.
3. Для $i = 1, \ldots, t$

Выбрать случайно $x \in Z_n^*$.

Если $m_i = 1$, то присвоить $c_i := yx^2 \bmod n$, иначе $c_i := x^2 \bmod n$ (то есть $c_i = y^{m_i}x^2$).

Послать t-набор $c = (c_1, \ldots, c_t)$ стороне A.

Сторона A, получив t-набор от стороны B расшифровывает его с использованием своего секретного ключа по следующему алгоритму расшифрования:

Для $i = 1, \ldots, t$

Вычислить символ Лежандра $e_i = \left(\frac{c_i}{p}\right)$.

Если $e_i = 1$, то присвоить $m_i := 0$, иначе $m_i := 1$.

Расшифрованным сообщением является строка $m = m_1 m_2 \ldots m_t$.

Рассмотренные алгоритмы работают правильно.

Действительно, если сообщение $m_i = 0$, то $c_i = x^2 \bmod n$ является квадратичным вычетом по модулю n. При этом c_i является квадратичным вычетом по модулю n тогда и только тогда, когда c_i есть квадратичный вычет по модулю p, или, что эквивалентно, $\left(\frac{c_i}{p}\right) = 1$. Поскольку сторона A знает p, она может вычислить этот символ Лежандра и найти m_i.

Если же $m_i = 1$, то поскольку y является псевдоквадратом по модулю n, $c_1 = yx^2 \bmod n$ также является псевдоквадратом по модулю n. Признаком этого является равенство $\left(\frac{yx^2}{p}\right) = \left(\frac{y}{p}\right) = -1$ где символ Лежандра легко вычисляется.

Рассмотренная шифрсистема семантически секретна.

Действительно, поскольку x выбирается из Z_n^* случайно, то $x^2 \bmod n$ является случайным квадратичным вычетом по модулю n, а $yx^2 \bmod n$ является случайным псевдоквадратом по модулю n. Следовательно, криптоаналитик рассматривает случайно выбранные квадратичные вычеты и псевдоквадраты по модулю n. Учитывая трудность проблемы квадратичного вычета, криптоаналитику ничего не остаётся, как угадать значения каждого бита сообщения. То есть если проблема квадратичного вычета трудна, то шифрсистема Гольдвассер – Микали семантически секретна.

2 Шифрсистема Блюма – Гольдвассер

Система Блюма-Гольдвассер является системай вероятностного шифрования с минимальной избыточностью. Она семантически секретна, но не противостоит

атакам по выбираемому шифртексту. Посредством BBS-генератора[2] генерируется псевдослучайная последовательность, которая "складывается"по модулю два с открытым текстом. Аналогично шифруется и передается ее зерно. Это позволяет расшифровать ее легальному пользователю.

Для создания открытого и секретного ключей каждый пользователь

1. Выбирает два больших различных простых числа p и "q,"сравнимых с 3 по модулю 4.

2. Вычисляет $n = pq$.

3. Вычисляет числа a и b такие. что $ap + bq = 1$.

4. Открытый ключ есть n, секретный ключ есть p, q, a, b.

Для зашифрования сообщения m для A пользователь B

1. Получает аутентичный открытый ключ n пользователя A.

2. Представляет m строкой $m = m_1 m_2 \dots m_t$, где m_i есть бинарные строки длины $h = \lfloor \log_2 k \rfloor$, $k = \lfloor \log_2 n \rfloor$.

3. Выбирает зерно x_0 как случайный квадратичный вычет по модулю n (выбирает $r \in Z_n^*$ и вычисляет $x_0 = r^2 \bmod n$).

4. Для $i = 1 \dots t$ выполняет

4.1. $x_i = x_{i-1}^2 \bmod n$,

4.2. $c_i = p_i + m_i$, где p_i – младшие значащие биты числа x_i.

5. Вычисляет $x_{t+1} = x_t^2 \bmod n$.

6. Посылает к A шифртекст $c = c_1, c_2, \dots, c_t, x_{t+1}$.

Для извлечения открытого текста A выполняет следующие действия:

1. Вычисляет $d_1 = ((p+1)/4)^{t+1} \bmod (p-1)$, и $d_2 = ((q+1)/4)^{t+1} \bmod (q-1)$.

2. Вычисляет $u = x_{t+1}^{d_1} \bmod p$ и $v = x_{t+1}^{d_2} \bmod q$.

3. Вычисляет $x_0 = vap + ubq \bmod n$.

4. Для $i = 1 \dots t$ вычисляет

$x_i = x_{i-1}^2 \bmod n$; $m_i = p_i + c_i$, где p_i – младшие значащие биты числа x_i.

Доказательство правильности расшифрования следующее. Поскольку x_t является квадратичным вычетом по модулю n, x_t является квадратичным вычетом как по модулю p, так и по модулю q.

Заметим (принимая во внимание критерий Эйлера $x^{(p-1)/2} = \left(\frac{x}{p}\right)$, и, следовательно, если x есть квадратичный вычет, то $x^{(p-1)/2} = 1$), что

$$x_{t+1}^{(p+1)/4} \equiv (x_t^2)^{(p+1)/4} \equiv x_t^{(p-1)/2} x_t \equiv x_t (\bmod p)$$

Аналогично $x_t^{(p+1)/4} \equiv x_{t-1} \pmod p$.

[2]Такой генератор вырабатывает рекуррентную последовательность элементов кольца Z_n, где $n = pq$ – произведение двух различных простых чисел, сравнимых с 3 по модулю 4, определяемую рекуррентным уравнением

$$u_{n+1} = u_n^2 \bmod n$$

при некотором начальном состоянии («зерне») u_0, являющемся квадратичным вычетом по модулю n. Выходная последовательность BBS-генератора составляется из младших битов элементов этой рекуррентной последовательности.

Повторяя эти преобразования, получим

$$u \equiv x_{t+1}^{d_1} \equiv x_{t+1}^{((p+1)/4)^{t+1}} \equiv x_0 (\mathrm{mod}\ p).$$

Точно также получим

$$v \equiv x_{t+1}^{d_2} \equiv x_0 (\mathrm{mod}\ q).$$

Таким образом, имеем условия китайской теоремы об остатках:

$$x_0 \equiv u (\mathrm{mod} p).$$

$$x_0 \equiv v (\mathrm{mod} q).$$

Поскольку $ap + bq = 1$, по китайской теореме об остатках получаем

$$x_0 \equiv vap + ubq \equiv x_0\ (\mathrm{mod}\ n)$$

и A вычислит то же случайное зерно, что было использовано для зашифрования.

3 Контрольные вопросы

1. Почему криптосистемы Гольдвассер – Микали и Блюма – Гольдвассер называются криптосистемами вероятностного шифрования.

2. На каких трудных теоретико-числовых проблемах основана их криптографическая стойкость?

3. На каком основании криптосистема Гольдвассер – Микали считается семантически секретной,

4. С какой целью в криптограмму, получаемую в криптоситеме Блюма-Гольдвассер добавляется в конце шифртекста x_{t+1}?

Литература

Stinson D.R. Cryptography: theory and Practice. CRC Press LLC, Boca Raton, Florida, 1995.