38 Идентификационное шифрование

38.1 Концепция

В системах шифрования с открытым ключом (Public Key Encryption, PKE) для организации шифрования используются 3 алгоритма:

$$\begin{aligned}\texttt{Gen}\colon 1^\ell &\mapsto (sk, pk),\\ \texttt{Enc}\colon (X, pk) &\mapsto Y,\\ \texttt{Dec}\colon (Y, sk) &\mapsto X.\end{aligned}$$

Здесь ℓ — уровень стойкости, sk — личный ключ (получателя), pk — открытый ключ.

Как мы уже неоднократно говорили, открытые ключи должны распространяться по аутентифицируемым каналам связи, т. е. с гарантиями целостности и подлинности. Для этого создаются инфраструктуры открытых ключей, обычно на основе сертификатов, которые выпускает доверенная сторона — Трент. Если создание и поддержание инфраструктуры оказывается затратным, то нужно искать альтернативные подходы к организации шифрования.

Одну из таких альтернатив предложил в 1985 г. А. Шамир. В предложении Шамира речь шла не о конкретной криптосистеме, а об общей схеме или концепции. Концепция получила название *идентификационное шифрование* (Identity-Based Encryption, IBE).

В IBE открытый ключ стороны с идентификатором Id не распространяется в форме сертификата, выпущенного Трентом, а вычисляется по идентификатору Id и открытому ключу Трента.

Алгоритмы IBE:

$$\begin{aligned}\texttt{Gen}\colon 1^\ell &\mapsto (sk_T, pk_T),\\ \texttt{Extract}\colon (Id, sk_T) &\mapsto sk,\\ \texttt{Enc}\colon (X, Id, pk_T) &\mapsto Y,\\ \texttt{Dec}\colon (Y, sk) &\mapsto X.\end{aligned}$$

Здесь ℓ, sk, X, Y имеют такой же смысл, как в PKE, Id — идентификатор получателя, sk_T, pk_T — личный и открытый ключи Трента.

Алгоритмы должны удовлетворять ограничению:

$$\texttt{Dec}(\texttt{Enc}(X, Id, pk_T), sk) = X$$

для всех допустимых X и Id и для sk и pk_T, вычисленных по схеме

$$(sk_T, pk_T) \leftarrow \texttt{Gen}(1^\ell), \quad sk \leftarrow \texttt{Extract}(Id, sk_T).$$

Интерфейс IBE может усложняться добавлением алгоритма генерации долговременных параметров $\texttt{Setup}\colon 1^\ell \mapsto par$ и включением сгенерированных параметров par в перечень входных данных остальных алгоритмов (в $\texttt{Gen}$ вместо 1^ℓ).

Обратим внимание, что проблема распространения открытых ключей в IBE не стоит — кроме pk_T других открытых ключей попросту нет. Однако если в PKE Трент заверяет открытые ключи, не зная личных, то в IBE Трент фактически генерирует личные ключи. Доверие к Тренту должно быть выше. Не случайно в инфраструктурах, обслуживающих IBE, Трента называют не “certificate authority”, а “trusted authority”.

Пример 38.1. При регистрации почтового адреса Id_A на сервере T Алиса получает по защищенному TLS соединению свой личный ключ sk_A. Боб, который хочет отправить защищенное письмо Алисы выполняет зашифрование, используя только адрес Id_A и долговременный открытый ключ pk_T. □

Долгое время IBE оставалась именно концепцией, поскольку не удавалось построить надежные наборы перечисленных алгоритмов. Наконец в 2001 году было предложено два решения — криптосистема Кокса и криптосистемы на основе билинейных отображений.

38.2 Билинейные отображения

Пусть $\mathbb{G}_1$ — аддитивная циклическая группа порядка q, $\mathbb{G}_1 = \langle G \rangle$, $\mathbb{G}_2$ — мультипликативная циклическая группа порядка q.

Определение 38.1. Отображение $e\colon \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ — *невырожденное билинейное*, если

1) $e(A + B, C) = e(A, C)e(B, C)$, $e(A, B + C) = e(A, B)e(A, C)$ для любых $A, B, C \in \mathbb{G}_1$ (билинейность);

2) $e(G, G) \neq 1$ (невырожденность). □

Будем предполагать, что имеется полиномиальный алгоритм вычисления значений e.

В 2000 А. Жу (Joux) предложил использовать билинейные отображения в криптографии. Стойкость соответствующих систем основывает на трудности следующей задачи.

Задача BDH$[\mathbb{G}_1, \mathbb{G}_2, e]$ **(билинейная задача Диффи – Хеллмана)**:

$$(G, aG, bG, cG) \mapsto e(G, G)^{abc},$$

где G — образующий $\mathbb{G}_1$, $a, b, c \in \mathbb{Z}_q$.

На сегодняшний день известны группы, в которых эта задача трудна. Во всех известных случаях $\mathbb{G}_1 \subseteq E(\mathbb{F}_p)$, $\mathbb{G}_2 \subseteq \mathbb{F}^*_{p^n}$, а e задается так называемыми *спариваниями* (Вейля и Тейта).

Криптографическая платформа, использующая билинейные отображения, так и называется — PBC (Pairing-Based Cryptography).

Свяжем **BDH** с уже изученными задачами.

Теорема 38.1. $\mathbf{BDH} \leqslant_P \mathbf{DL}[\mathbb{G}_1]$, $\mathbf{BDH} \leqslant_P \mathbf{CDH}[\mathbb{G}_1]$, $\mathbf{BDH} \leqslant_P \mathbf{CDH}[\mathbb{G}_2]$.

Доказательство. Если имеется алгоритм решения **DL** в $\mathbb{G}_1$, то можно определить $a = \mathbf{DL}[\mathbb{G}_1](G, aG)$, $b = \mathbf{DL}[\mathbb{G}_1](G, bG)$, $c = \mathbf{DL}[\mathbb{G}_1](G, cG)$, а затем найти abc и $e(G, G)^{abc}$.

Если имеется алгоритм решения **CDH** в $\mathbb{G}_1$, то можно определить $abG = \mathbf{CDH}[\mathbb{G}_1](G, aG, bG)$, а затем найти $e(G, G)^{abc} = e(abG, cG)$.

Если имеется алгоритм решения **CDH** в $\mathbb{G}_2$, то можно вычислить $g = e(G, G)$, $g^{ab} = e(aG, bG)$, $g^c = e(G, cG)$, а затем определить $e(G, G)^{abc} = g^{abc} = \mathbf{CDH}[\mathbb{G}_2](g, g^{ab}, g^c)$. □

Теорема означает, что трудность $\mathbf{CDH}[\mathbb{G}_1]$ является необходимым условием трудности **BDH**. Упрощенной формой $\mathbf{CDH}[\mathbb{G}_1]$ является распознавательная задача Диффи – Хеллмана $\mathbf{DDH}[\mathbb{G}_1]$:

$$(G, aG, bG, cG) \mapsto \begin{cases} 1, & c \equiv ab \pmod{q}, \\ 0, & \text{в противном случае.} \end{cases}$$

Оказывается, что если построено невырожденное билинейное отображение e, образы которого можно находить за полиномиальное время, то решения $\mathbf{DDH}[\mathbb{G}_1]$ также можно находить за полиномиальное время:

1) определить $\alpha = e(G, cG) = e(G, G)^c$;

2) определить $\beta = e(aG, bG) = e(G, G)^{ab}$.

3) если $\alpha = \beta \Rightarrow e(G, G)^c = e(G, G)^{ab} \Rightarrow c \equiv ab \pmod{q}$, то возвратить 1;

4) возвратить 0.

При этом факт существования e не означает автоматического ослабления $\mathbf{CDH}[\mathbb{G}_1]$. Отображение e в некотором смысле дифференцирует $\mathbf{CDH}[\mathbb{G}_1]$ и $\mathbf{DDH}[\mathbb{G}_1]$ по трудности.

38.3 Криптосистема Боне — Франклина

IBE-криптосистема, предложенная Боне и Франклином в 2001 году, задается следующими алгоритмами.

Алгоритм `Setup`. Трент генерирует долговременные параметры par следующим образом:

1. Построить группы $\mathbb{G}_1$, $\mathbb{G}_2$ простого порядка q и невырожденное билинейное отображение $e\colon \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. Битовая длина q определяется уровнем стойкости ℓ. Параметры $\mathbb{G}_1, \mathbb{G}_2, e$ выбираются так, чтобы задача $\mathbf{BDH}[\mathbb{G}_1, \mathbb{G}_2, e]$ была трудной.

2. Выбрать образующий G группы $\mathbb{G}_1$.

3. Построить функцию хэширования $h\colon \{0,1\}^* \to \mathbb{G}_1$.

4. Возвратить $par = (\mathbb{G}_1, \mathbb{G}_2, e, G, h)$.

Алгоритм `Gen`. Трент генерирует свой личный ключ d_T и соответствующий открытый ключ Q_T следующим образом:

$$d_T \xleftarrow{R} \mathbb{Z}_q, \quad Q_T \leftarrow d_T G.$$

Алгоритм `Extract`. Трент по идентификатору $Id \in \{0,1\}^*$ определяет личный ключ d его владельца:

$$d \leftarrow d_T \cdot h(Id).$$

Алгоритм `Enc`. Для зашифрования $X \in \mathbb{G}_2$ с целью передачи стороне с идентификатором Id выполняются следующие шаги:

1. $k \xleftarrow{R} \mathbb{Z}_q$.

2. $Y_1 \leftarrow kG$.

3. $Y_2 \leftarrow X \cdot e(h(Id), Q_T)^k$.

4. Возвратить (Y_1, Y_2) — шифртекст.

Алгоритм `Dec`. Получатель шифртекста $Y = (Y_1, Y_2)$ расшифровывает его следующим образом:

1. $X \leftarrow Y_2 \cdot e(d, Y_1)^{-1}$.

2. Возвратить X.

Корректность. Имеем

$$e(d, Y_1) = e(d_T h(Id), kG) = e(kh(Id), d_T G) = e(h(Id), Q_T)^k.$$

Поэтому

$$Y_2 \cdot e(d, Y_1)^{-1} = X \cdot e(h(Id), Q_T)^k \cdot e(h(Id), Q_T)^{-k} = X.$$

Стойкость. Противнику требуется по G, $Q_T = d_T G$, $Y_1 = kG$ и $h(Id) = mG$ определить $e(h(Id), Q_T)^k = e(G, G)^{d_T k m}$. Но это трудная задача **BDH**.