О некоторых свойствах схем выработки общего ключа, использующих инфраструктуру открытых ключей, в контексте разработки стандартизированных криптографических решений

Д. В. Матюхин

31 марта 2011 г.

Исходные положения

- Отечественные разработчики криптосредств испытывают потребность в стандартизированном криптографическом решении (национальном стандарте и/или рекомендациях) по выработке общего ключа двумя абонентами по открытому каналу связи (Key Agreement в терминологии международного стандарта ISO/IEC 11770-3)

- Такое решение должно быть реализовано в группе точек эллиптической кривой над конечным простым полем

- Вариант классической схемы Диффи-Хеллмана, в котором общий ключ зависит только от сеансовых ключей абонентов, подходит не для всех моделей нарушителя

Угрозы схемам с долговременными ключами

Пусть общий ключ K вырабатывают *инициатор* (initiator) A и *ответчик* (responder) B, имеющие долговременные (static) ключевые пары $(s_A, P_A), (s_B, P_B)$ (*не обязательно соответствующие одной кривой!*) и сертификаты $\mathrm{Cert}_A, \mathrm{Cert}_B$

- *Чтение назад* по отношению к A (B, A и B): зная s_A (s_B, s_A и s_B), определить ранее выработанные значения K
- *Key-compromise impersonation (KCI)*: зная $s_A(s_B)$, выдать себя за $B(A)$
- *Unknown key-share (UKS, source-substitution)*: A и B вырабатывают K, но B считает его общим с $E \neq A$

Свойства классической схемы Диффи-Хеллмана с долговременными ключами

- Используемые ключевые пары должны соответствовать одной эллиптической кривой
- Схема не обеспечивает защиту от чтения назад и KCI
- Схема не обеспечивает защиту от UKS, если при сертификации открытого ключа не проверяется знание абонентом соответствующего секретного ключа

Вывод: схема, стойкая к указанным угрозам, должна использовать и долговременные, и сеансовые ключевые пары!

Вариант 1: долговременные ключевые пары – ключи стандартизированной схемы ЭЦП

В этом случае $(s_A, P_A), (s_B, P_B)$ могут соответствовать разным эллиптическим кривым; K вырабатывается по классической схеме Диффи-Хеллмана с использованием только сеансовых ключей и, вообще говоря, еще одной кривой, которая должна быть предварительно согласована A и B. Получающиеся схемы – *station-to-station (STS)* (Diffie, van Oorschot, Wiener, 1992), рассмотрим схему *STS-MAC*, в которой A и B используют подгруппу $G = \langle P \rangle$ группы точек эллиптической кривой и *ключевую функцию хэширования* MAC

$$
\begin{array}{ll}
A \to B & A, k_A P \\
B \to A & \mathsf{Cert}_B, k_B P, \mathsf{Sign}_{s_B}(k_B P, k_A P), \mathsf{MAC}_K(\mathsf{Sign}_{s_B}(k_B P, k_A P)) \\
A \to B & \mathsf{Cert}_A, \mathsf{Sign}_{s_A}(k_A P, k_B P), \mathsf{MAC}_K(\mathsf{Sign}_{s_A}(k_A P, k_B P))
\end{array}
$$

UKS-атака на схему STS-MAC
(Blake-Wilson, Menezes, 1999)

Предположим, что используемая $X \in \{A, B\}$ схема ЭЦП Sign обладает свойством *duplicate-signature key selection*:
для сообщения M противник E может найти такую ключевую пару (s_E, P_E), что $\mathrm{Sign}_{s_E}(M) = \mathrm{Sign}_{s_X}(M)$. Это возможно для большинства реально используемых схем, включая ГОСТ Р 34.10-2001, где подпись $\mathrm{Sign}_{s_X}(M) = (r, s)$, соответствующая некоторой кривой и точке P' на ней простого порядка q, будет признана в качестве подписи $\mathrm{Sign}_{s_E}(M)$, соответствующей той же кривой и точке P'', если $(s - rs_E)P'' = sP' - rP_X$, откуда $P'' = ((s - rs_E)^{-1} \bmod q)(sP' - rP_X)$ при $s - rs_E \neq 0 \bmod q$. Таким образом, E достаточно выбрать такой s_E и $P_E = s_E P''$

Также предположим, что E может получить сертификат открытого ключа P_E в процессе BOK

UKS-атака на схему STS-MAC

($A \hookrightarrow B$ – сообщение перехвачено E и не дошло до B)

$A \hookrightarrow B$ $\quad A, k_A P$

$E \to B$ $\quad E, k_A P$

$B \to E$ $\quad \mathsf{Cert}_B, k_B P, \mathsf{Sign}_{s_B}(k_B P, k_A P), \mathsf{MAC}_K(\mathsf{Sign}_{s_B}(k_B P, k_A P))$

$E \to A$ $\quad \mathsf{Cert}_B, k_B P, \mathsf{Sign}_{s_B}(k_B P, k_A P), \mathsf{MAC}_K(\mathsf{Sign}_{s_B}(k_B P, k_A P))$

$A \hookrightarrow B$ $\quad \mathsf{Cert}_A, \mathsf{Sign}_{s_A}(k_A P, k_B P), \mathsf{MAC}_K(\mathsf{Sign}_{s_A}(k_A P, k_B P))$

E выбирает ключевую пару (s_E, P_E), такую, что
$\mathsf{Sign}_{s_E}(k_A P, k_B P) = \mathsf{Sign}_{s_A}(k_A P, k_B P)$ и получает Cert_E

$B \to E$ $\quad \mathsf{Cert}_E, \mathsf{Sign}_{s_A}(k_A P, k_B P), \mathsf{MAC}_K(\mathsf{Sign}_{s_A}(k_A P, k_B P))$

В результате B ошибочно считает K общим ключом с E!
Проверка знания E секретного ключа для P_E не спасает!

Модификация схемы STS-MAC для защиты от UKS-атаки

Идея: включить в подписываемые сообщения идентификаторы абонентов. Пример – *ISO-STS-MAC* (ISO/IEC 11770-3 Key agreement mechanism 7):

$A \to B$	$A, k_A P$
$B \to A$	$\mathsf{Cert}_B, k_B P, \mathsf{Sign}_{s_B}(k_B P, k_A P, A), \mathsf{MAC}_K(k_B P, k_A P, A)$
$A \to B$	$\mathsf{Cert}_A, \mathsf{Sign}_{s_A}(k_A P, k_B P, B), \mathsf{MAC}_K(k_A P, k_B P, B)$

Описанная выше атака не проходит, т. к. E получает $\mathsf{Sign}_{s_B}(k_B P, k_A P, E)$, а должен отправить $\mathsf{Sign}_{s_B}(k_B P, k_A P, A)$! Схема обеспечивает защиту от чтения назад по отношению к A и B и KCI-атаки. Недостаток: необходим выбор группы G

Вариант 2: долговременные ключевые пары вырабатываются специально для схемы BOK

В этом случае естественно построить схему BOK, «объединив» два варианта классической схемы Диффи-Хеллмана – с сеансовыми и долговременными ключами, т. е. A и B обмениваются сообщениями $k_A P, P_A$ и $k_B P, P_B$, где $P_A = s_A P', P_B = s_B P'$, $G = \langle P \rangle, G' = \langle P' \rangle$ – подгруппы групп точек в общем случае различных эллиптических кривых, и вычисляют

$$K = KDF(k_A k_B P, s_A s_B P'),$$

где KDF – некоторая функция. Получается схема *Full Unified Model* (стандарт ANS X9.63, рекомендации NIST SP800-56A). Она уязвима к KCI-атаке: E, зная $s_A(s_B)$, вырабатывает свое $k_B(k_A)$, отправляет $A(B)$ значение $k_B P(k_A P)$ и вычисляет

$K = KDF(k_B(k_A P), s_A P_B)$(соответственно $KDF(k_A(k_B P), s_B P_A)$)

Вариант 2, схемы с защитой от KCI: *MQV*

(Law, Menezes, Qu, Solinas, Vanstone, 1998;
ISO/IEC 11770-3 Key agreement mechanism 9)

$P_A = s_A P, P_B = s_B P$, где $G = \langle P \rangle$ – подгруппа группы точек эллиптической кривой. A и B обмениваются сообщениями $\mathrm{Cert}_A, k_A P$ и $\mathrm{Cert}_B, k_B P$, после чего A вычисляет

$$K = (k_A + \pi(k_A P) s_A)(k_B P + \pi(k_B P) P_B),$$

а B вычисляет

$$K = (k_B + \pi(k_B P) s_B)(k_A P + \pi(k_A P) P_A),$$

где $\pi : G \to \mathbb{Z}$ (в оригинале $\pi(Q) = x_P \bmod 2^{\frac{\lceil l(\#G) \rceil}{2}} + 2^{\frac{\lceil l(\#G) \rceil}{2}}$).

Модифицировать схему, чтобы P_A, P_B могли соответствовать разным кривым, не представляется возможным. Схема обеспечивает защиту от чтения назад по отношению к A и B.

UKS-атака на схему MQV
(Kaliski, 2000)

$$A \hookrightarrow B \quad \mathrm{Cert}_A, k_A P$$

E выбирает k, вычисляет $R = k_A P + \pi(k_A P) P_A - kP \neq O$, $s_E = \pi(R)^{-1} k \bmod \#G$, $P_E = s_E P$ и получает Cert_E

$$\begin{array}{ll} E \to B & \mathrm{Cert}_E, R \\ B \to E & \mathrm{Cert}_B, k_B P \end{array}$$

$$\begin{aligned} R + \pi(R) P_E &= k_A P + \pi(k_A P) P_A - kP + \pi(R) s_E P \\ &= (k_A - k + \pi(R)\pi(R)^{-1} k \bmod \#G) P + \pi(k_A P) P_A \\ &= k_A P + \pi(k_A P) P_A, \end{aligned}$$

поэтому B вычисляет ключ $(k_B + \pi(k_B P) s_B)(R + \pi(R) P_E) = K$ и ошибочно считает его общим с E. Проверка знания E секретного ключа для P_E не спасает!

Модификация схемы MQV для защиты от UKS-атаки

(Law, Menezes, Qu, Solinas, Vanstone, 1998; ISO/IEC 11770-3 Key agreement mechanism 10)

Идея: добавить подтверждение ключа (key confirmation), которое может быть реализовано, например, с помощью MAC:

$$\begin{array}{ll} A \to B & \mathrm{Cert}_A, k_A P \\ B \to A & \mathrm{Cert}_B, k_B P, MAC_{h(x_K)}(2, k_A P, k_B P) \\ A \to B & MAC_{h(x_K)}(3, k_A P, k_B P), \end{array}$$

где h – хэш-функция.

Описанная выше атака не проходит, т. к. E не сможет построить последнее сообщение

Вариант 2, схемы с защитой от KCI: схемы типа *MTI/A0*

(Matsumoto, Takashima, Imai, 1986;
Blake-Wilson, Johnson, Menezes, 1997;
ISO/IEC 11770-3 Key agreement mechanism 5)

$P_A = s_A P, P_B = s_B P$, где $G = \langle P \rangle$ – подгруппа группы точек эллиптической кривой. A и B обмениваются сообщениями $\mathrm{Cert}_A, k_A P$ и $\mathrm{Cert}_B, k_B P$, после чего A вычисляет

$$K = h(k_A P_B, s_A(k_B P)),$$

а B вычисляет

$$K = h(s_B(k_A P), k_B P_A),$$

где h – односторонняя функция (в оригинальном MTI/A0 $G \subset GF(p)^*$ и $h(x, y) = xy \bmod p$, в *KEA* используется $h(x \oplus y)$)

Свойства схем типа MTI/A0

Обеспечивают защиту от чтения назад по отношению к A, B (но не A и B!) и KCI

Не обеспечивают защиту от UKS, если при сертификации открытого ключа не проверяется знание абонентом соответствующего секретного ключа. Хотя такая проверка – обычная практика (см., напр., RFC 4210), можно обойтись без нее, вычисляя (Lauter, Mityagin, 2005 – *KEA+*):

$$K = h(k_A P_B, s_A(k_B P), A, B) = h(s_B(k_A P), k_B P_A, A, B)$$

Могут быть различными способами дополнены подтверждением ключа (см., напр., Lauter, Mityagin, 2005), количество пересылок при этом увеличивается на 1

Работают, если $(s_A, P_A), (s_B, P_B)$ получены на разных кривых!

Номер в ISO/IEC 11770-3	7	9	10	5
Тип схемы	STS-MAC	MQV	MQV	MTI/A0
Количество пересылок	3	2	3	2
Работает, если P_A и P_B на разных кривых	да*	нет	нет	да**
Защита от чтения назад	A и B	A и B	A и B	A, B
Защита от KCI	да	да	да	да
Защита от UKS	да	нет***	да	нет****

*требуется еще одна кривая, согласованная A и B

**в литературе не встречается, требуется *доказать* свойства

***если противник E может получить Cert_E в процессе BOK

****если при получении Cert_E нет проверки знания E соответствующего секретного ключа; защиту без проверки обеспечивает модификация с тем же количеством пересылок

Вывод

Среди стандартизированных на международном уровне схем выработки общего ключа, в которых абоненты используют как сеансовые, так и долговременные ключи, наиболее предпочтительными для разработки отечественного стандартизированного решения с точки зрения рассмотренных свойств представляются схемы типа STS и MTI/A0