# О возможности стандартизации протоколов выработки общего ключа

Сергей Гребнев

ФСБ России
(при поддержке АК РФ)

РусКрипто 2014, Москва.

# Исходные положения

Процесс формирования общего секретного ключа двумя абонентами по открытому каналу связи (ВОК):

- Неотъемлемая часть сетевых протоколов (TLS/SSL, IPSEC и т.д.).
- Существующие решения (RFC 4357) представляются не вполне обоснованными.
- Нужна единообразная эффективная схема.

# Выход?...

Возможно ли разработать протокол, удовлетворяющий *всем* требованиям? Есть ли в этом необходимость?

- Не один протокол, а семейство;
- формализация и описание свойств;
- задание требований к криптографическим примитивам;
- выбор конкретного протокола – за разработчиком СКЗИ, в зависимости от модели нарушителя и требований к эксплуатационным характеристикам.

Переход от *примитивов* (ЭЦП, хэш, блочный шифр) к *протоколу* – композиции примитивов в контролирумой противником среде.

# Предложения: протоколы

**Протоколы типа Диффи-Хеллмана с единственной ключевой парой для каждого абонента:**

- статический;
- однораундовый;
- интерактивный.

**Протоколы с аутентификацией:**

- вариант схемы STS-MAC;
- вариант схемы MTI/A0 с использованием двух кривых (Матюхин, 2010).

# Предложения: базовый примитив

## Схема Диффи-Хеллмана с кофактором

- Группа точек эллиптической кривой над конечным простым полем, заданной
  1. в скрученной форме Эдвардса: $\overline{E}_E : ax^2 + y^2 = 1 + dx^2y^2$, самая быстрая реализация;
  2. в (краткой) форме Вейерштрасса: $E_W : y^2 = x^3 + ax + b$, совместимость и применение в ограниченных по объему программного кода устройствах вместе с ЭЦП;
- Базовая структура: $\langle P \rangle \subseteq E(GF(p)), \# \langle P \rangle = q, q|m = \#E(GF(p)), c = m/q.$
- Параметр стойкости: $\lambda \approx |q|/2$.
- Ключи абонента $A$: $s_A \in_R [1, q-1], S_A = s_A P, k_A \in_R [1, q-1], K_A = k_A P.$
- Операция: $K = ck_A K_B = ck_A k_B P = ck_b K_A.$

# Протоколы Диффи-Хеллмана

**Протокол Д-0 (статический)**

$$A, B: \qquad K = \left(H\left(cs_A s_B P, OI\right)\right)_{\lambda, 2\lambda-1}$$

**Протокол Д-1 (однораундовый)**

$$A \rightarrow B \qquad k_A P$$
$$A, B: \qquad K = \left(H\left(ck_A s_B P, OI\right)\right)_{\lambda, 2\lambda-1}$$

**Протокол Д-2 (интерактивный)**

$$A \rightarrow B \qquad k_A P$$
$$B \rightarrow A \qquad k_B P$$
$$A, B: \qquad K = \left(H\left(ck_A k_B P, OI\right)\right)_{\lambda, 2\lambda-1}$$

# Протоколы Диффи-Хеллмана: свойства

| Название | Д-0 | Д-1 | Д-2 |
|---|---|---|---|
| Номер в ISO/IEC 11770-3:2007 | 1 | 2 | 4 |
| Кол-во пересылок | 0 | 1 | 2 |
| Кол-во скаляр-ных умножений оффлайн | 2 | 1/1 | 0 |
| Кол-во скалярных умножений онлайн | 0 | 0/1 | 2 |
| Защита от чтения назад | - | *A* | *A* и *B* |
| Неявная аутенти-фикация ключа | взаимная *A* и *B* | *B* перед *A* | - |

# Протоколы аутентифицированной выработки общего ключа

**Протокол Э-3**

| | |
|---|---|
| $A \to B$ | $\mathtt{Cert}_A, k_A P$ |
| $B:$ | $K = \left(H\left(ck_B k_A P, \mathtt{Cert}_A, \mathtt{Cert}_B, OI\right)\right)_{\lambda, 2\lambda-1},$ |
| $B:$ | $M = \left(H\left(ck_B k_A P, \mathtt{Cert}_A, \mathtt{Cert}_B, OI\right)\right)_{0, \lambda-1}$ |
| $B \to A$ | $\mathtt{Cert}_B, k_B P, \mathtt{sign}_{s_B}\left(k_B P, k_A P, \mathtt{Cert}_A\right),$ $\mathtt{mac}_M\left(0, k_B P, k_A P, \mathtt{Cert}_B, \mathtt{Cert}_A\right)$ |
| $A:$ | если подпись или $\mathtt{mac}$ неверны, то разрывает сеанс |
| $A:$ | $K = \left(H\left(ck_A k_B P, \mathtt{Cert}_A, \mathtt{Cert}_B, OI\right)\right)_{\lambda, 2\lambda-1},$ |
| $A:$ | $M = \left(H\left(ck_A k_B P, \mathtt{Cert}_A, \mathtt{Cert}_B, OI\right)\right)_{0, \lambda-1}$ |
| $A \to B$ | $\mathtt{Cert}_A, \mathtt{sign}_{s_A}\left(k_A P, k_B P, \mathtt{Cert}_B\right),$ $\mathtt{mac}_M\left(1, k_A P, k_B P, \mathtt{Cert}_A, \mathtt{Cert}_B\right)$ |
| $B:$ | если подпись или $\mathtt{mac}$ неверны, то разрывает сеанс |

# Протоколы аутентифицированной выработки общего ключа

**Протокол Л-3**

| | |
|---|---|
| $A \to B$ | $\mathtt{Cert}_A, k_A P_B$ |
| $B:$ | $K = \left(H(c_A k_B S_A, c_B s_B k_A P_B, \mathtt{Cert}_A, \mathtt{Cert}_B, OI)\right)_{\lambda, 2\lambda-1}$ |
| $B:$ | $M = \left(H(c_A k_B S_A, c_B s_B k_A P_B, \mathtt{Cert}_A, \mathtt{Cert}_B, OI)\right)_{0, \lambda-1}$ |
| $B:$ | $tag_B = \mathtt{mac}_M(0)$ |
| $B \to A$ | $\mathtt{Cert}_B, K_B, tag_B$ |
| $A:$ | $M = \left(H(c_A s_A k_B P_A, c_B k_A S_B, \mathtt{Cert}_A, \mathtt{Cert}_B, OI)\right)_{0, \lambda-1}$ |
| $A:$ | если $tag_B \neq \mathtt{mac}_M(0)$, то $A$ разрывает сеанс. |
| $A:$ | $K = \left(H(c_A s_A k_B P_A, c_B k_A S_B, \mathtt{Cert}_A, \mathtt{Cert}_B, OI)\right)_{\lambda, 2\lambda-1}$ |
| $A:$ | $tag_A = \mathtt{mac}_M(1)$ |
| $A \to B$ | $tag_A$ |
| $B:$ | если $tag_A \neq \mathtt{mac}_M(1)$, то $B$ разрывает сеанс. |

# Протоколы аутентифицированной выработки общего ключа: свойства

| Название | Э-3 | Л-3 |
|---|---|---|
| Номер в ISO/IEC 11770-3: 2007 | 7 | 5 |
| Кол-во пересылок | 3 | 3 |
| Кол-во скалярных умножений онлайн | 2 | 3 |
| Кол-во мультискалярных умножений онлайн | 1 | 0 |
| Подтверждение ключа | неявное | неявное |
| Использование двух различных кривых | Нет | Да |
| Защита от чтения назад | $A$ и $B$ | $A$, $B$ |
| Док-во стойкости | 2 раунда, Canetti, Krawczyk, 2001 | Menezes, Ustaoglu, 2011; Lauter, Mityagin, 2006 |

# Строительные блоки: готовые

- Длина вырабатываемого общего секретного значения – 256 битов ($\lambda = 256$);
- базовый криптографический примитив – схема Диффи-Хеллмана с кофактором в подгруппе простого порядка $q$ группы точек эллиптической кривой над конечным простым полем, заданной в скрученной форме Эдвардса, где $2^{508} < q < 2^{512}$;
- хэш-функция согласно ГОСТ Р 34.11-2012 с длиной хэш-кода 512 битов;
- алгоритм выработки и проверки цифровой подписи согласно ГОСТ Р 34.10-2012;
- ключевая хэш-функция – HMAC на основе хэш-функции $h_{256}(\cdot)$ согласно ГОСТ Р 34.11-2012 с длиной хэш-кода 512 битов.

Спасибо за внимание.