Протоколы согласования ключей с аутентификацией на основе пароля: принципы обеспечения безопасности

Алексеев Евгений Константинович, к.ф.-м.н.,
ведущий инженер-аналитик

Смышляев Станислав Витальевич, к.ф.-м.н.,
начальник отдела защиты информации

РусКрипто'2016

«Протокол выработки общего ключа с аутентификацией на основе пароля»

Принят в 2015 году в ТК26 в качестве методических рекомендаций.

ТК26

SESPAKE (Полное описание: tc26.ru, раздел ”Методические документы”, «Протокол выработки общего ключа с аутентификацией на основе пароля»).

IETF

«The Security Evaluated Standardized Password Authenticated Key Exchange (SESPAKE) Protocol», draft-smyshlyaev-sespake-02.

КРИПТО ПРО

Задача

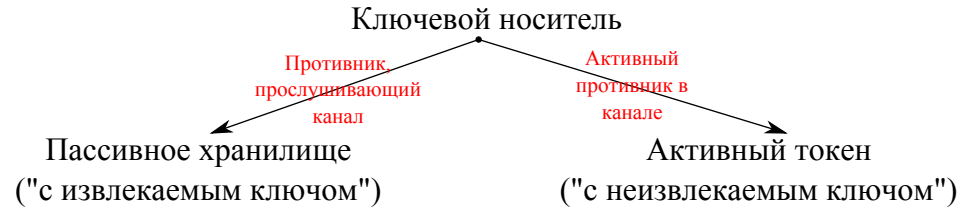
Безопасное хранение и использование криптографических ключей

Решение

Использование специальных ключевых носителей (токенов)

Проблема

Передача пароля по каналу в открытом виде



КРИПТО ПРО

1. 1992 год — первая работа — протокол EKE (Bellovin и Merritt);
2. 1993 год — первые «намеки» на модель противника (Bellare, Rogaway);
3. 2000 год — модели противника для протоколов семейства PAKE (Bellare, Pointcheval, Rogaway и Boyko, MacKenzie, Patel);
4. 2000 год — вместе с моделями были предложены варианты протоколов и доказательства их стойкости;
5. 2005 год — протокол SPAKE (Abdalla,Pointcheval), считающийся оптимальным (Abdalla).

КРИПТО ПРО

1. EKE (S. Bellovin, M. Merritt, «Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks», 1992)
2. PACE (J. Bender, M. Fischlin, D. Kugler, «Security Analysis of the PACE Key-Agreement Protocol», 2009)
3. SPAKE (M. Abdalla, D. Pointcheval, «Simple Password-Based Encrypted Key Exchange Protocols», 2005)
4. SPEKE (D. Jablon, «Strong Password-Only Authenticated Key Exchange», 1996)
5. DragonFly (D. Harkins. «Simultaneous authentication of equals: A secure, password-based key exchange for mesh networks», 2008)
6. AMP (T. Kwon, «Authentication and Key Agreement via Memorable Password», 2000)
7. AugPAKE (S. Shin, K. Kobara, «Most Efficient Augmented Password-Only Authentication and Key Exchange for IKEv2», 2010)
8. SESPAKE (Полное описание: tc26.ru, раздел ”Методические документы”, Протокол выработки общего ключа с аутентификацией на основе пароля)

КРИПТО ПРО

Public Information: EC parameters $\mathcal{G} = \{a, b, p, q, G, k\}$

A : PW		**B** : Q_{PW}
$Q_{PW}^A = F(PW, salt, 2000) \cdot Q_{ind}$	$\xrightarrow{A_{ID}}$	
	$\xleftarrow{(B_{ID}, ind, salt)}$	
$z_A = 0, \alpha \in_R \{1, \ldots, q-1\}$		
$u_1 = \alpha \cdot P - Q_{PW}^A$	$\xrightarrow{u_1}$	if $u_1 \notin E$, finish
		$Q_B = u_1 + Q_{PW}$
		$z_B = 0, \beta \in_R \{1, \ldots, q-1\}$
		if $\frac{m}{q} Q_B = 0_E$, than $Q_B = P$ and $z_B = 1$
		$src = (\frac{m}{q} \cdot \beta \mod q) Q_B$, $K_B = H_{256}(src)$
		$u_2 = \beta \cdot P + Q_{PW}$
if $u_2 \notin E$, finish	$\xleftarrow{u_2}$	
$Q_A = u_2 - Q_{PW}^A$		
if $\frac{m}{q} Q_A = 0_E$, than $Q_A = P$ and $z_A = 1$		
$src = (\frac{m}{q} \cdot \alpha \mod q) Q_A$, $K_A = H_{256}(src)$		
$M_A = \mathrm{HMAC}_{K_A}(T_A \Vert A_{ID} \Vert ind \Vert salt \Vert u_1 \Vert u_2)$	$\xrightarrow{M_A}$	
		Verify M_A and $z_B \stackrel{?}{=} 0$
		$M_B = \mathrm{HMAC}_{K_B}(T_B \Vert B_{ID} \Vert ind \Vert salt \Vert u_1 \Vert u_2)$
Verify M_B and $z_A \stackrel{?}{=} 0$	$\xleftarrow{M_B}$	

КРИПТО ПРО

Основные уязвимости/свойства

1. Шифрование структурированных данных
2. Атака со связанными ключами
3. Атака с одинаковыми порождающими
4. Атака с подгруппой малого порядка (DragonFly)
5. Атака со взломом сервера (augmented/balanced)
6. Атака отражения (PACE)
7. Impersonation Attack (SPEKE)
8. Атаки на неправильную работу со счетчиками

КРИПТО

Протокол EKE

A (Client): pw		B (Server): pw
$x \in_R \mathbb{Z}_q,\ T_x = E_{pw}(g^x)$	$\xrightarrow{T_x}$	$X = E_{pw}^{-1}(T_x)$
$Y = E_{pw}^{-1}(T_y)$	$\xleftarrow{T_y}$	$y \in_R \mathbb{Z}_q,\ E_{pw}(g^y)$
$K_A = \mathcal{H}(Y^x)$		$K_B = \mathcal{H}(X^y)$

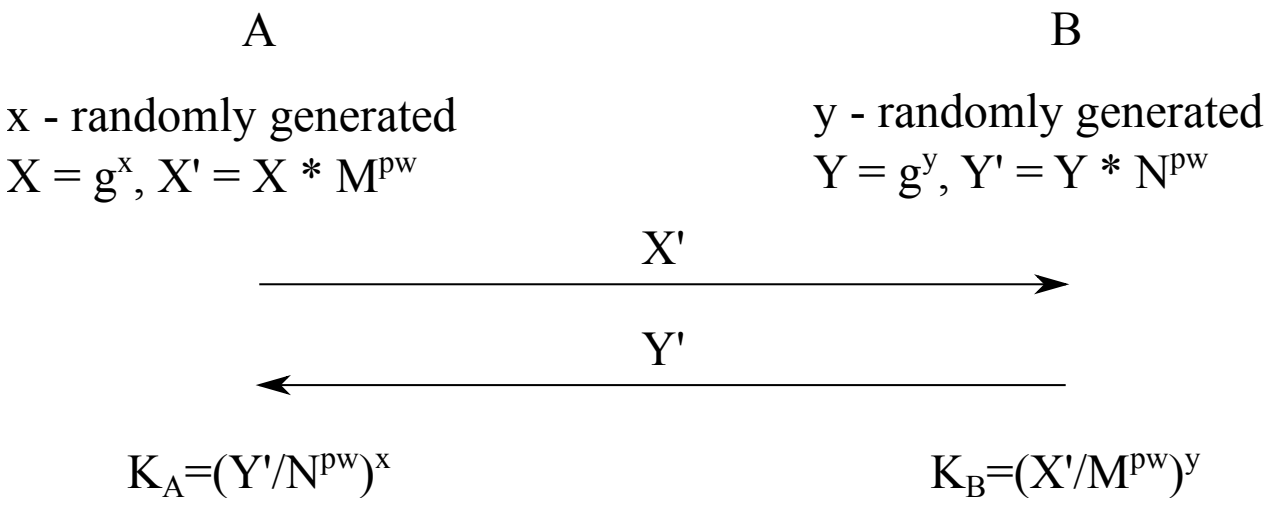
Шифрование g^x: $T = E_{pw}(g^x)$
$g^x \in \mathcal{K}$, $E_{pw} : V_m \to V_m$,
Необходимо $C : \mathcal{K} \to V_m$.

Если $C(\mathcal{K}) \ll |V_m|$, то
критерий для проверки пароля pw' на данных T:
$E_{pw'}^{-1}(T) \stackrel{?}{\in} C(\mathcal{K})$.

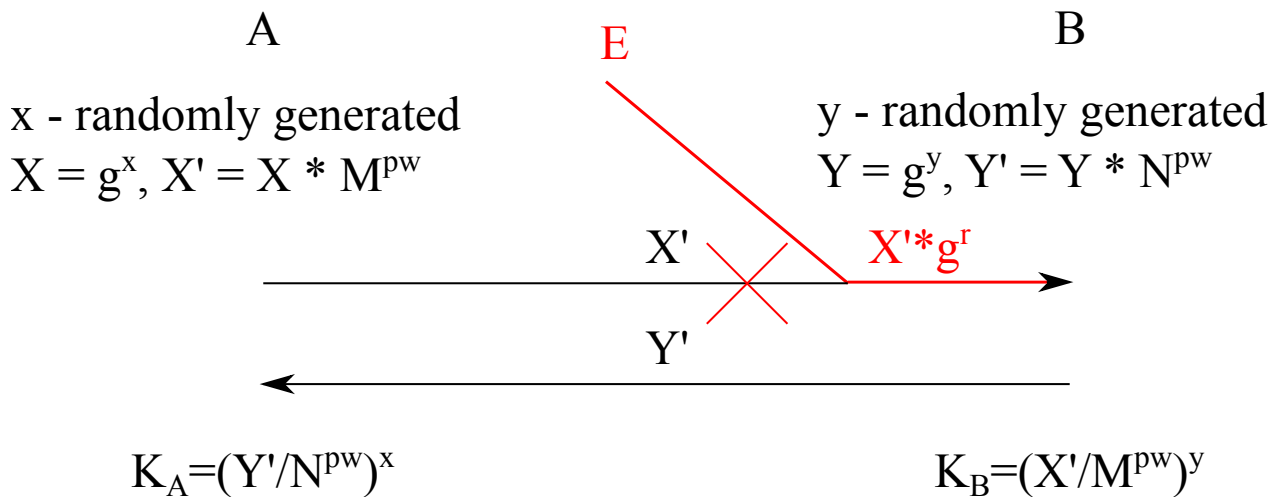
Пример плохого преобразования C:
$\mathcal{E}$ — группа точек эллиптической кривой,
$C : \mathcal{E} \to V_m$, $C(P) = INT(X) \| INT(Y)$.

RFC Draft, «Requirements for PAKE schemes», paragraph 4.2., Requirement R5:
«In case the PAKE scheme is intended to be used with ECC, the authors SHOULD discuss their requirements for a potential mapping or define a mapping to be used with the scheme»

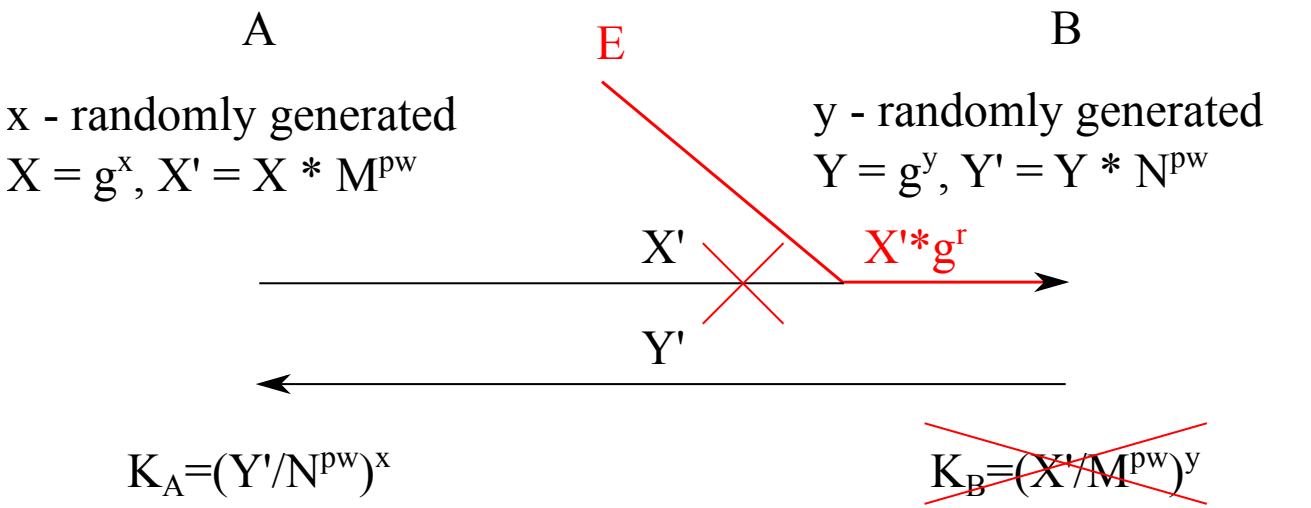
Password is used as ”gamma” to protect ephemeral Diffie-Hellman keys.
A session key does not depend on a password.
Toy protocol from Abdalla M., Pointcheval D.
«Simple Password-Based Encrypted Key Exchange Protocols», 2005.
Here: $G = \langle g \rangle = \langle M \rangle = \langle N \rangle$.



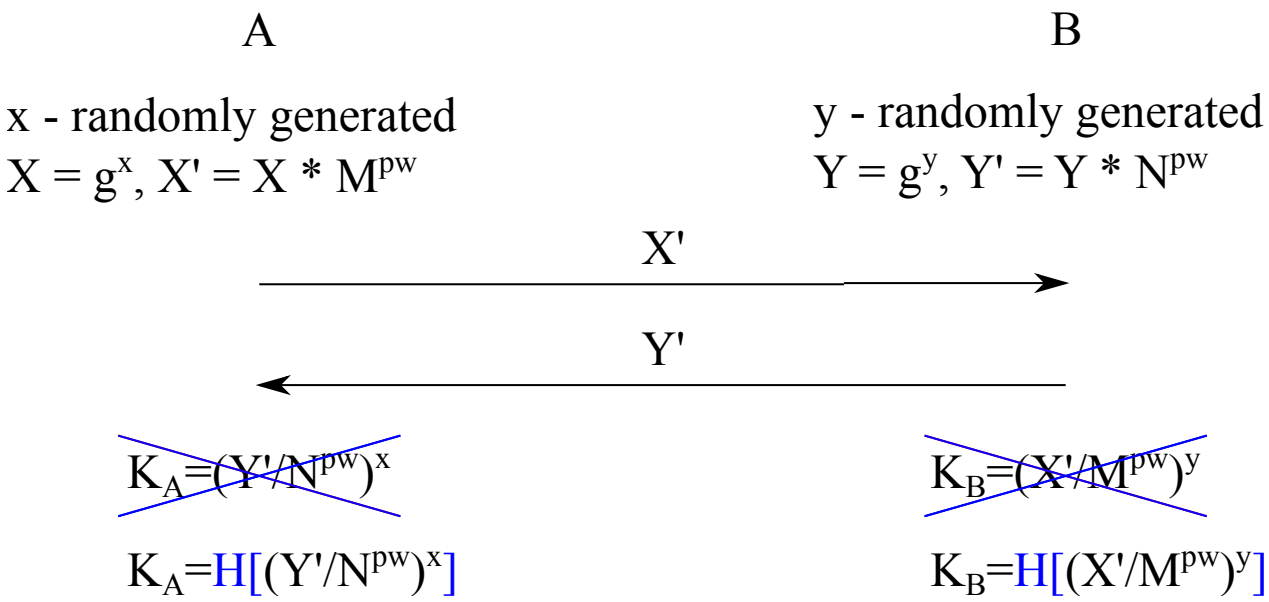
Password is used as ”gamma” to protect ephemeral Diffie-Hellman keys.
A session key does not depend on a password.
Toy protocol from Abdalla M., Pointcheval D.
«Simple Password-Based Encrypted Key Exchange Protocols», 2005.
Here: $G = \langle g \rangle = \langle M \rangle = \langle N \rangle$.



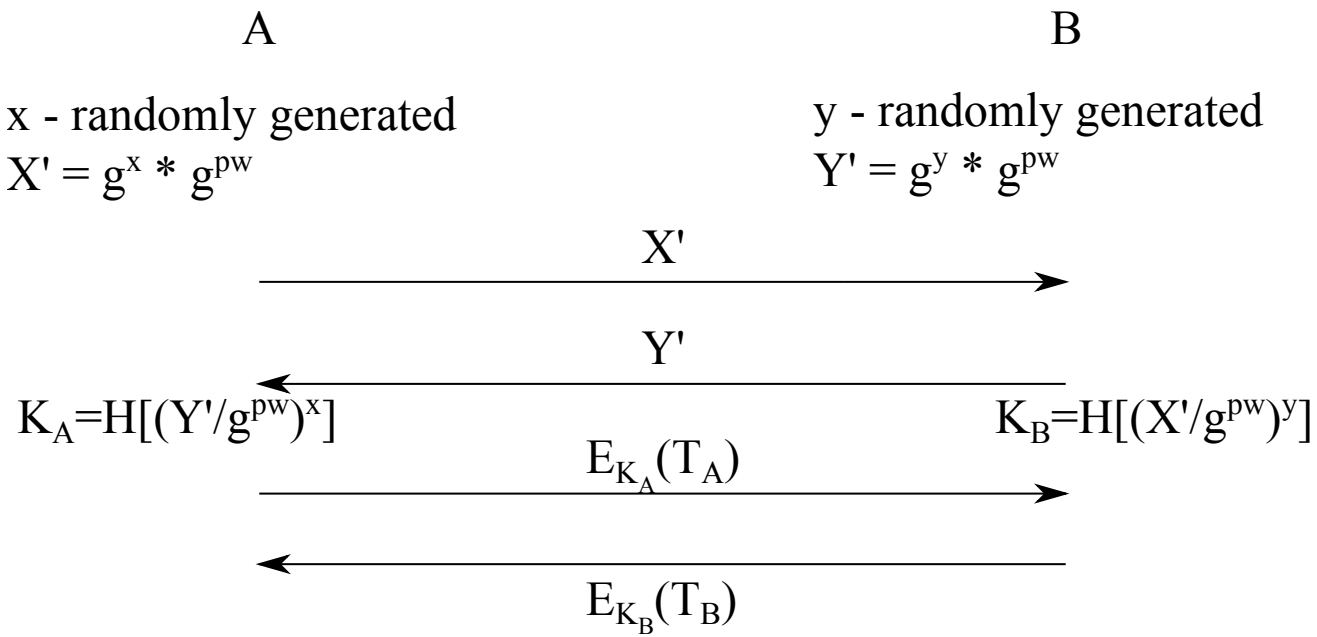
Password is used as ”gamma” to protect ephemeral Diffie-Hellman keys.
A session key does not depend on a password.
Toy protocol from Abdalla M., Pointcheval D.
«Simple Password-Based Encrypted Key Exchange Protocols», 2005.
Here: $G = \langle g \rangle = \langle M \rangle = \langle N \rangle$.



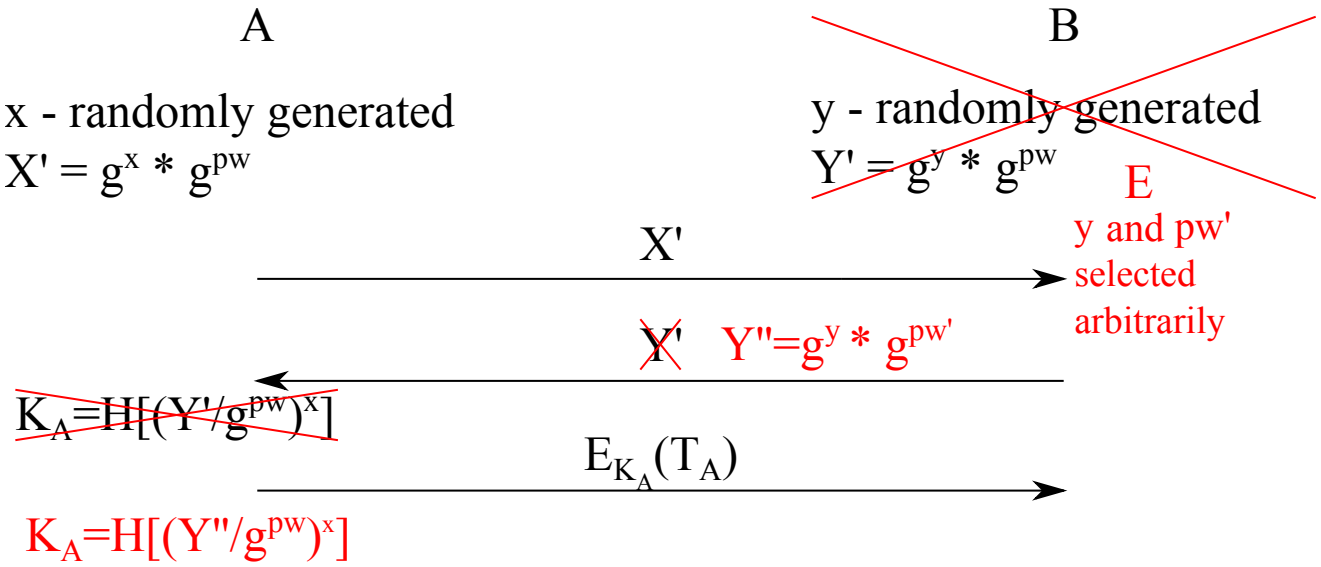
Password is used as ”gamma” to protect ephemeral Diffie-Hellman keys.
A session key does not depend on a password.
Toy protocol from Abdalla M., Pointcheval D.
«Simple Password-Based Encrypted Key Exchange Protocols», 2005.
Here: $G = \langle g \rangle = \langle M \rangle = \langle N \rangle$.



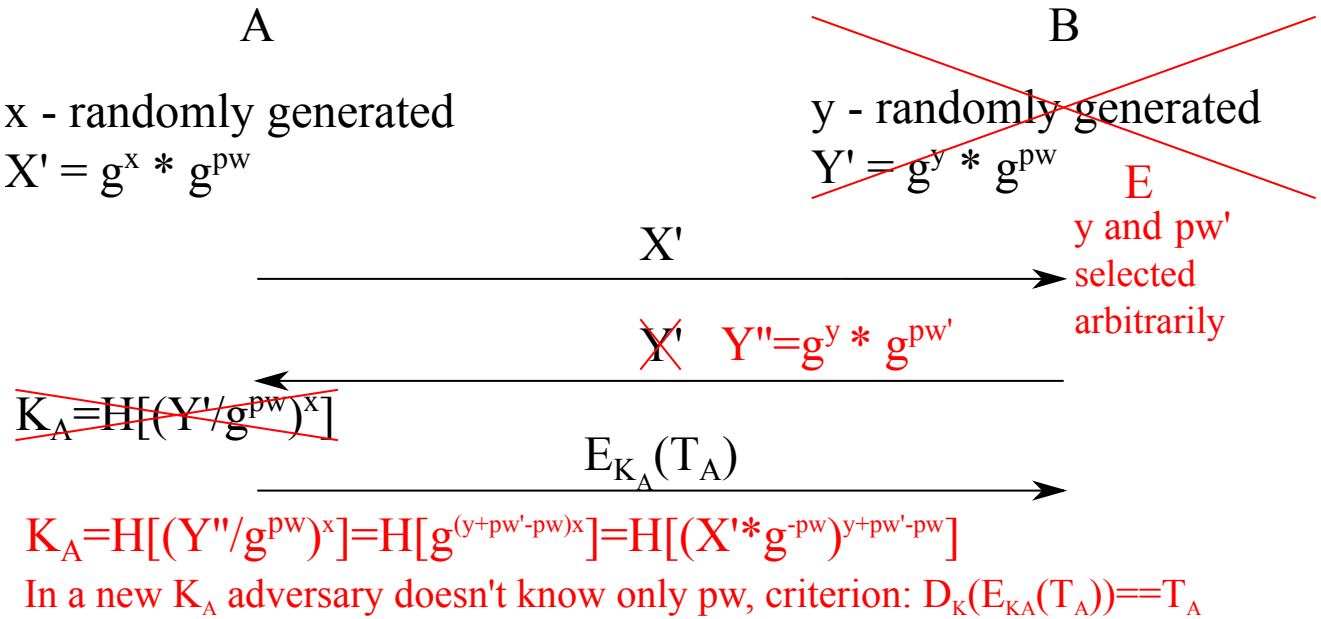
Toy protocol from Kobara K., Imai H. «Pretty-Simple Password-Authenticated Key-Exchange Under Standard Assumptions», 2003.



Toy protocol from Kobara K., Imai H. «Pretty-Simple Password-Authenticated Key-Exchange Under Standard Assumptions», 2003.



Toy protocol from Kobara K., Imai H. «Pretty-Simple Password-Authenticated Key-Exchange Under Standard Assumptions», 2003.



D. Clarke and F. Hao. Cryptanalysis of the Dragonfly key exchange protocol, 2014.

Public Information: Q, q		
A (Client): $P \in Q$ $r_A, m_A \in_R \{1, \ldots, q\}$ $s_A = r_A + m_A$ $E_A = P^{-m_A}$	$\xrightarrow{E_A, s_A}$	B (Server): $P \in Q$ $r_B, m_B \in_R \{1, \ldots, q\}$ $s_B = r_B + m_B$ $E_B = P^{-m_B}$
	$\xleftarrow{E_B, s_B}$	
$ss = (P^{s_B} E_B)^{r_A} = P^{r_A r_B}$		
$A = \mathcal{H}(ss \vert E_A \vert s_A \vert E_B \vert s_B)$	$\xrightarrow{A}$	Verify A $ss = (P^{s_A} E_A)^{r_B} = P^{r_A r_B}$
Verify B	$\xleftarrow{B}$	$T_B = \mathcal{H}(ss \vert E_B \vert s_B \vert E_A \vert s_A)$
$K = \mathcal{H}(ss \vert E_A \cdot E_B \vert (s_A + s_B) \bmod q)$		

Протоколы различают по тому, что хранит каждая из сторон:

- "balanced" – A и B хранят пароль pw;
- "augmented" – A хранит pw, B хранит $F(pw)$, где F — односторонняя.

- "balanced" – противник взламывает $B \Rightarrow$ он может аутентифицироваться на A и на B;
- "augmented" – противник взламывает $B \Rightarrow$ он может аутентифицироваться на A, но не на B (для этого нужно подобрать пароль);

- "nearly augmented" — противник взламывает $B \Rightarrow$ он может аутентифицироваться на A и на B, но он может получить значение пароля лишь после перебора по словарю;

КРИПТО ПРО

Примеры протоколов разных типов

- PACE – balanced
- AugPAKE – augmented
- SESPAKE – nearly augmented

RFC Draft, «Requirements for PAKE schemes», paragraph 3.1., Requirement R1:
«A PAKE scheme MUST clearly state its features regarding balanced/augmented versions.»

КРИПТО ПРО

Public Information: EC parameters $\mathcal{G} = \{a, b, p, q, G\}$		
A (Client): password π $K_\pi = \mathcal{H}(\pi \parallel 0)$ $s \in_R \mathbb{Z}_q$ $z = E_{K_\pi}(s)$	$\xrightarrow{\mathcal{G}, z}$	B (Server): password π $K_\pi = \mathcal{H}(\pi \parallel 0)$ abort if $\mathcal{G}$ incorrect $s = E^{-1}_{K_\pi}(z)$
$x_A \in_R \mathbb{Z}_q^*,\ X_A = x_A \cdot G$ $\widehat{G} = s \cdot G + x_A \cdot X_B$	$\xrightarrow{X_A}$ $\xleftarrow{X_B}$	$x_B \in_R \mathbb{Z}_q^*,\ X_B = x_B \cdot G$ $\widehat{G} = s \cdot G + x_B \cdot X_A$
$y_A \in_R \mathbb{Z}_q^*,\ Y_A = y_A \cdot \widehat{G}$ abort if $Y_B \notin \langle G \rangle \backslash \{0\}$ $K = y_A \cdot Y_B$ $K_{enc} = \mathcal{H}(K \parallel 1),\ K_{mac} = \mathcal{H}(K \parallel 2)$	$\xrightarrow{Y_A}$ $\xleftarrow{Y_B}$	$y_B \in_R \mathbb{Z}_q^*,\ Y_B = y_B \cdot \widehat{G}$ abort if $Y_A \notin \langle G \rangle \backslash \{0\}$ $K = y_B \cdot Y_A$ $K_{enc} = \mathcal{H}(K \parallel 1),\ K_{mac} = \mathcal{H}(K \parallel 2)$
$T_A = MAC_{K_{mac}}(Y_B, \widehat{G}, \mathcal{G})$ abort if T_B invalid	$\xrightarrow{T_A}$ $\xleftarrow{T_B}$	$T_B = MAC_{K_{mac}}(Y_A, \widehat{G}, \mathcal{G})$ abort if T_A invalid

Feng Hao, Siamak F. Shahandashti, «The SPEKE Protocol Revisited», 2014.

Работа с двумя параллельными сессиями;
Противник: E;
E блокирует сторону B в тот момент, когда A инициирует взаимодействие с B;
$Q = f(pw)$;
A_i — экземпляр субъекта A, работающий в i-ой сессии;

КРИПТО ПРО

1. A_1 посылает $X = x \cdot Q$ стороне B (реально, противнику E);
2. E посылает A_2 значение $z \cdot X$, инициируя начало второй сессии (при этом z выбирается случайно);
3. A_2 посылает B (реально — E) значение $y \cdot Q$ (y выбирается случайно);
4. E посылает A_1 значение $z \cdot Y$;

Выработанные A_1 и A_2 ключи совпадают и равны $K = H(xyz \cdot Q)$;
Подтверждение ключа производиться аналогично с чередованием пересылок между сессиями.

Результат: E удалось аутентифицироваться на A_1 и на A_2.

КРИПТО ПРО

Public Information: EC parameters $\mathcal{G} = \{a, b, p, q, G, k\}$

A : PW		**B** : Q_{PW}
$Q^A_{PW} = F(PW, salt, 2000) \cdot Q_{ind}$	$\xrightarrow{A_{ID}}$	
	$\xleftarrow{(B_{ID}, ind, salt)}$	
$z_A = 0, \alpha \in_R \{1, \ldots, q-1\}$		
$u_1 = \alpha \cdot P - Q^A_{PW}$	$\xrightarrow{u_1}$	if $u_1 \notin E$, finish
		$Q_B = u_1 + Q_{PW}$
		$z_B = 0, \beta \in_R \{1, \ldots, q-1\}$
		if $\frac{m}{q} Q_B = 0_E$, than $Q_B = P$ and $z_B = 1$
		$src = (\frac{m}{q} \cdot \beta \mod q) Q_B$, $K_B = H_{256}(src)$
		$u_2 = \beta \cdot P + Q_{PW}$
if $u_2 \notin E$, finish	$\xleftarrow{u_2}$	
$Q_A = u_2 - Q^A_{PW}$		
if $\frac{m}{q} Q_A = 0_E$, than $Q_A = P$ and $z_A = 1$		
$src = (\frac{m}{q} \cdot \alpha \mod q) Q_A$, $K_A = H_{256}(src)$		
$M_A = \mathrm{HMAC}_{K_A}(T_A \Vert A_{ID} \Vert ind \Vert salt \Vert u_1 \Vert u_2)$	$\xrightarrow{M_A}$	
		Verify M_A and $z_B \stackrel{?}{=} 0$
	$\xleftarrow{M_B}$	$M_B = \mathrm{HMAC}_{K_B}(T_B \Vert B_{ID} \Vert ind \Vert salt \Vert u_1 \Vert u_2)$
Verify M_B and $z_A \stackrel{?}{=} 0$		

Протокол, предложенный в ноябре 2015 года в TK26 в качестве альтернативы протоколу SESPAKE.

КРИПТО ПРО

Public Information: P, q

A (Client): PIN		B (Server): PIN
$d_A \in_R \{1, \ldots, q-1\}$		$d_B \in_R \{1, \ldots, q-1\}$
$Q_A = d_A P$	$\xrightarrow{Q_A}$	$Q_B = d_B P$
		$K_{SM} = H[H(H(PIN)) \cdot d_B \cdot Q_A]$
		$A_1, A_2 \in_R V_{n/2}$
$K_{SM} = H[H(H(PIN)) \cdot d_A \cdot Q_B]$	$\xleftarrow{Q_B, T_1 \| T_2}$	$T_1 \| T_2 = E^{CFB,0}_{K_{SM}}(A_1 \| A_2)$
$A'_1 \| A'_2 = D^{CFB,0}_{K_{SM}}(T_1 \| T_2)$		
$B_1, B_2 \in_R V_{n/2}$		
$U = E^{CFB,0}_{K_{SM}}(A'_1 \| B_1 \| A'_2 \| B_2)$	$\xrightarrow{U}$	$A''_1 \| B'_1 \| A''_2 \| B'_2 = D^{CFB,0}_{K_{SM}}(U)$
		$Check(A_1 == A''_1) and (A_2 == A''_2)$
$B''_1 \| B''_2 = D^{CFB,0}_{K_{SM}}(V)$	$\xleftarrow{V}$	$V = E^{CFB,0}_{K_{SM}}(B'_1 \| B'_2)$
$Check(B_1 == B''_1) and (B_2 == B''_2)$		

Атака: Противник выступает в роли стороны B.
Угроза: Противник получает критерий для offline-перебора пароля.
Метод: B получает от A точку Q_A. Генерирует случайный d_B, случайные A_1, A_2 и посылает стороне A значения $d_B P, A_1 \| A_2$.
Противник B принимает от A строку $U_1 \| U_2 \| U_3 \| U_4$. При этом выполнено

$$U_3 = A_2 \oplus E_{K_{SM}}(0)|_R \oplus E_{K_{SM}}(U_1 \| U_2)|_L .$$

Здесь индексы L и R указывают на левый и правый полублоки (для ГОСТ 28147-89 полублок — 32 бита).
Для ключа выполнено

$$K_{SM} = H\left[H(H(PIN)) \cdot d_B \cdot Q_A\right],$$

где противнику неизвестен лишь PIN. Вероятность ложного срабатывания критерия равна 2^{-32}.

Демонстрация того, что протокол стоек по отношению к известным методам осуществления различных угроз не достаточно.
Единственной гарантией того, что протокол является стойким в данной модели противника является строгое обоснование = сведение задачи осуществления угрозы к задаче, считающейся труднорешаемой (например, к вычислительной задаче Диффи-Хеллмана (CDH)).

RFC Draft, «Requirements for PAKE schemes», paragraph 4.0., Requirement R2:
«A PAKE scheme SHOULD come with a security proof and clearly state its assumptions and models.»

1. SPAKE — Abdalla M., Pointcheval D. «Simple Password-Based Encrypted Key Exchange Protocols», 2005;
2. AugPAKE — Shin S., Kobara K., Imai H. «Security Proof of AugPAKE», 2010;
3. PACE — Bender J., Fischlin M., Kugler D. «Security Analysis of the PACE Key-Agreement Protocol», 2009;
4. SESPAKE — Алексеев Е.К., Ахметзянова Л.Р., Ошкин И.Б., Смышляев С.В., 2015 (готовится к публикации);
5. and so on ...

КРИПТО ПРО

Спасибо за внимание! Вопросы?

КРИПТО ПРО

Public Information: $\mathcal{G} = \{G, g, p, q\}$		
A (Client): pw		B (Server): pw
$x \in_R \mathbb{Z}_q,\ T_x = E_{pw}(g^x)$	$\xrightarrow{T_x}$	$X = E_{pw}^{-1}(T_x)$
$Y = E_{pw}^{-1}(T_y)$	$\xleftarrow{T_y}$	$y \in_R \mathbb{Z}_q,\ E_{pw}(g^y)$
$K_A = \mathcal{H}(Y^x)$		$K_B = \mathcal{H}(X^y)$

КРИПТО ПРО

Public Information: EC parameters $\mathcal{G} = \{a, b, p, q, G\}$		
A (Client): password π $K_\pi = \mathcal{H}(\pi \parallel 0)$ $s \in_R \mathbb{Z}_q$ $z = E_{K_\pi}(s)$	$\xrightarrow{\mathcal{G}, z}$	B (Server): password π $K_\pi = \mathcal{H}(\pi \parallel 0)$ abort if $\mathcal{G}$ incorrect $s = E^{-1}_{K_\pi}(z)$
$x_A \in_R \mathbb{Z}_q^*,\ X_A = x_A \cdot G$ $\widehat{G} = s \cdot G + x_A \cdot X_B$	$\xrightarrow{X_A}$ $\xleftarrow{X_B}$	$x_B \in_R \mathbb{Z}_q^*,\ X_B = x_B \cdot G$ $\widehat{G} = s \cdot G + x_B \cdot X_A$
$y_A \in_R \mathbb{Z}_q^*,\ Y_A = y_A \cdot \widehat{G}$ abort if $Y_B \notin \langle G \rangle \backslash \{0\}$ $K = y_A \cdot Y_B$ $K_{enc} = \mathcal{H}(K \parallel 1),\ K_{mac} = \mathcal{H}(K \parallel 2)$	$\xrightarrow{Y_A}$ $\xleftarrow{Y_B}$	$y_B \in_R \mathbb{Z}_q^*,\ Y_B = y_B \cdot \widehat{G}$ abort if $Y_A \notin \langle G \rangle \backslash \{0\}$ $K = y_B \cdot Y_A$ $K_{enc} = \mathcal{H}(K \parallel 1),\ K_{mac} = \mathcal{H}(K \parallel 2)$
$T_A = MAC_{K_{mac}}(Y_B, \widehat{G}, \mathcal{G})$ abort if T_B invalid	$\xrightarrow{T_A}$ $\xleftarrow{T_B}$	$T_B = MAC_{K_{mac}}(Y_A, \widehat{G}, \mathcal{G})$ abort if T_A invalid

КРИПТО ПРО

Public Information: G, g, p, M, N

A (Client): $pw \in \mathbb{Z}_p$		B (Server): $pw \in \mathbb{Z}_p$
$x \in_R \mathbb{Z}_p,\ X = g^x$		$y \in_R \mathbb{Z}_p,\ Y = g^y$
$X^* = X \cdot M^{pw}$		$Y^* = Y \cdot N^{pw}$
	$X^* \longrightarrow$	
	$\longleftarrow Y^*$	
$K_A = (Y^*/N^{pw})^x$		$K_B = (X^*/M^{pw})^y$
$SK_A = \mathcal{H}(A, B, X^*, Y^*, pw, K_A)$		$SK_B = \mathcal{H}(A, B, X^*, Y^*, pw, K_B)$

КРИПТО ПРО

Public Information: G, p, q		
A (Client): pw $g = F(pw) \in G$ $x \in_R \{1, \ldots, q\},\ X \equiv g^x$		B (Server): pw $g = F(pw) \in G$ $y \in_R \{1, \ldots, q\},\ Y \equiv g^y$
	$\xrightarrow{X}$	
	$\xleftarrow{Y}$	
$K = \mathcal{H}(x \cdot Y)$		$K = \mathcal{H}(y \cdot X)$
$T_A = \mathcal{H}(\mathcal{H}(K))$	$\xrightarrow{T_A}$	Verify T_A
Verify T_B	$\xleftarrow{T_B}$	$T_B = \mathcal{H}(K)$

КРИПТО ПРО

Public Information: Q, q		
A (Client): $P \in Q$ $r_A, m_A \in_R \{1, \ldots, q\}$ $s_A = r_A + m_A$ $E_A = P^{-m_A}$	$\xrightarrow{E_A, s_A}$ $\xleftarrow{E_B, s_B}$	B (Server): $P \in Q$ $r_B, m_B \in_R \{1, \ldots, q\}$ $s_B = r_B + m_B$ $E_B = P^{-m_B}$
$ss = (P^{s_B} E_B)^{r_A} = P^{r_A r_B}$		
$T_A = \mathcal{H}(ss \mid E_A \mid s_A \mid E_B \mid s_B)$	$\xrightarrow{T_A}$	Verify T_A $ss = (P^{s_A} E_A)^{r_B} = P^{r_A r_B}$
Verify T_B	$\xleftarrow{T_B}$	$T_B = \mathcal{H}(ss \mid E_B \mid s_B \mid E_A \mid s_A)$
$K = \mathcal{H}(ss \mid E_A \cdot E_B \mid (s_A + s_B) \bmod q)$		

КРИПТО ПРО

Public Information: G, g, p, q		
A (Client): π		B (Server): g^π or π
$x \in_R \mathbb{Z}_q$, $G_1 \equiv g^x$		
	$\xrightarrow{id, G_1}$	$y \in_R \mathbb{Z}_q$
	$\xleftarrow{G_2}$	$G_2 = (G_1 g^\pi)^y$
$w = (x + \pi)^{-1} x \bmod q$		
$\alpha = (G_2)^w$		$\beta = (G_1)^y$
$K_A = \mathcal{H}_1(\alpha)$		$K_B = \mathcal{H}_1(\beta)$
$T_A = \mathcal{H}_2(G_1, K_A)$	$\xrightarrow{T_A}$	Verify T_A
Verify T_B	$\xleftarrow{T_B}$	$T_B = \mathcal{H}_3(G_2, K_B)$

КРИПТО ПРО

Public Information: G, g, p, q

A (Client): $pw \in \mathbb{Z}_q$		B (Server): $W \equiv g^{pw}$
$x \in_R \mathbb{Z}_q^*,\ X \equiv g^x$	$\xrightarrow{C, X}$	
	$\xleftarrow{S, Y}$	$r = \mathcal{H}(C, S, X),\ Y \equiv (X \cdot W^r)^y$
$r = \mathcal{H}(A, B, X),\ K' \equiv Y^{1/(x+pw \cdot r)}$		
$T_A = \mathcal{H}_1(A\|\|B\|\|X\|\|Y\|\|K')$	$\xrightarrow{T_A}$	if $T_A \neq \mathcal{H}_1(A\|\|B\|\|X\|\|Y\|\|K)$ reject
if $T_B \neq \mathcal{H}_2(A\|\|B\|\|X\|\|Y\|\|K')$ reject	$\xleftarrow{T_B}$	$T_B = \mathcal{H}_2(A\|\|B\|\|X\|\|Y\|\|K)$
$SK = \mathcal{H}_3(A\|\|B\|\|X\|\|Y\|\|K')$		$SK = \mathcal{H}_3(A\|\|B\|\|X\|\|Y\|\|K)$

КРИПТО ПРО

Public Information: EC parameters $\mathcal{G} = \{a, b, p, q, G, k\}$

A : PW		**B** : Q_{PW}
$Q^A_{PW} = F(PW, salt, 2000) \cdot Q_{ind}$	$\xrightarrow{A_{ID}}$	
	$\xleftarrow{(B_{ID}, ind, salt)}$	
$z_A = 0, \alpha \in_R \{1, \ldots, q-1\}$		
$u_1 = \alpha \cdot P - Q^A_{PW}$	$\xrightarrow{u_1}$	if $u_1 \notin E$, finish
		$Q_B = u_1 + Q_{PW}$
		$z_B = 0, \beta \in_R \{1, \ldots, q-1\}$
		if $\frac{m}{q} Q_B = 0_E$, than $Q_B = P$ and $z_B = 1$
		$src = (\frac{m}{q} \cdot \beta \mod q) Q_B$, $K_B = H_{256}(src)$
		$u_2 = \beta \cdot P + Q_{PW}$
if $u_2 \notin E$, finish	$\xleftarrow{u_2}$	
$Q_A = u_2 - Q^A_{PW}$		
if $\frac{m}{q} Q_A = 0_E$, than $Q_A = P$ and $z_A = 1$		
$src = (\frac{m}{q} \cdot \alpha \mod q) Q_A$, $K_A = H_{256}(src)$		
$M_A = \mathrm{HMAC}_{K_A}(T_A \Vert A_{ID} \Vert ind \Vert salt \Vert u_1 \Vert u_2)$	$\xrightarrow{M_A}$	
		Verify M_A and $z_B \stackrel{?}{=} 0$
		$M_B = \mathrm{HMAC}_{K_B}(T_B \Vert B_{ID} \Vert ind \Vert salt \Vert u_1 \Vert u_2)$
Verify M_B and $z_A \stackrel{?}{=} 0$	$\xleftarrow{M_B}$	