РусКрипто

XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

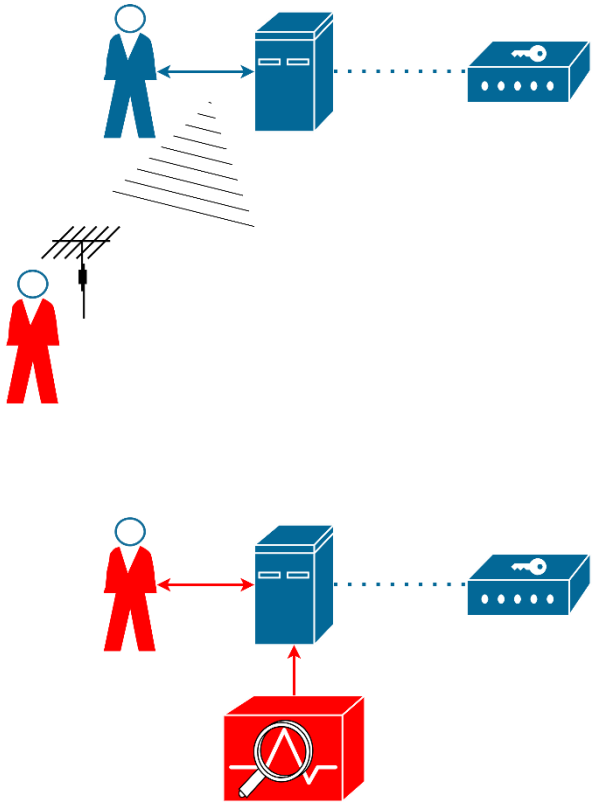
Об одной особенности формирования модели нарушителя из потенциально доступных ему возможностей на примере проекта протокола TLS 1.2 на основе механизма инкапсуляции ключа

Алексеев Евгений Константинович, ООО «КРИПТО-ПРО»
Кяжин Сергей Николаевич, НИЯУ МИФИ
Мухортова Алена Андреевна, ООО «КРИПТО-ПРО»

- Рабочая группа «Сопутствующие криптографические алгоритмы и протоколы» (СКАиП) в ТК26: период исследования порядка использования постквантовых KEM в протоколе TLS 1.2.
- Предложена первая версия протокола – pqRTLS12 (Handshake).
- Обзор известных атак и оценка их применимости. Атака на протокол GC в необычной модели нарушителя.
- Текущая версия pqRTLS12 уязвима к атаке при некоторых допущениях.
- **Меры противодействия атаке.**
- **Одно наблюдение о порядке формирования модели нарушителя.**

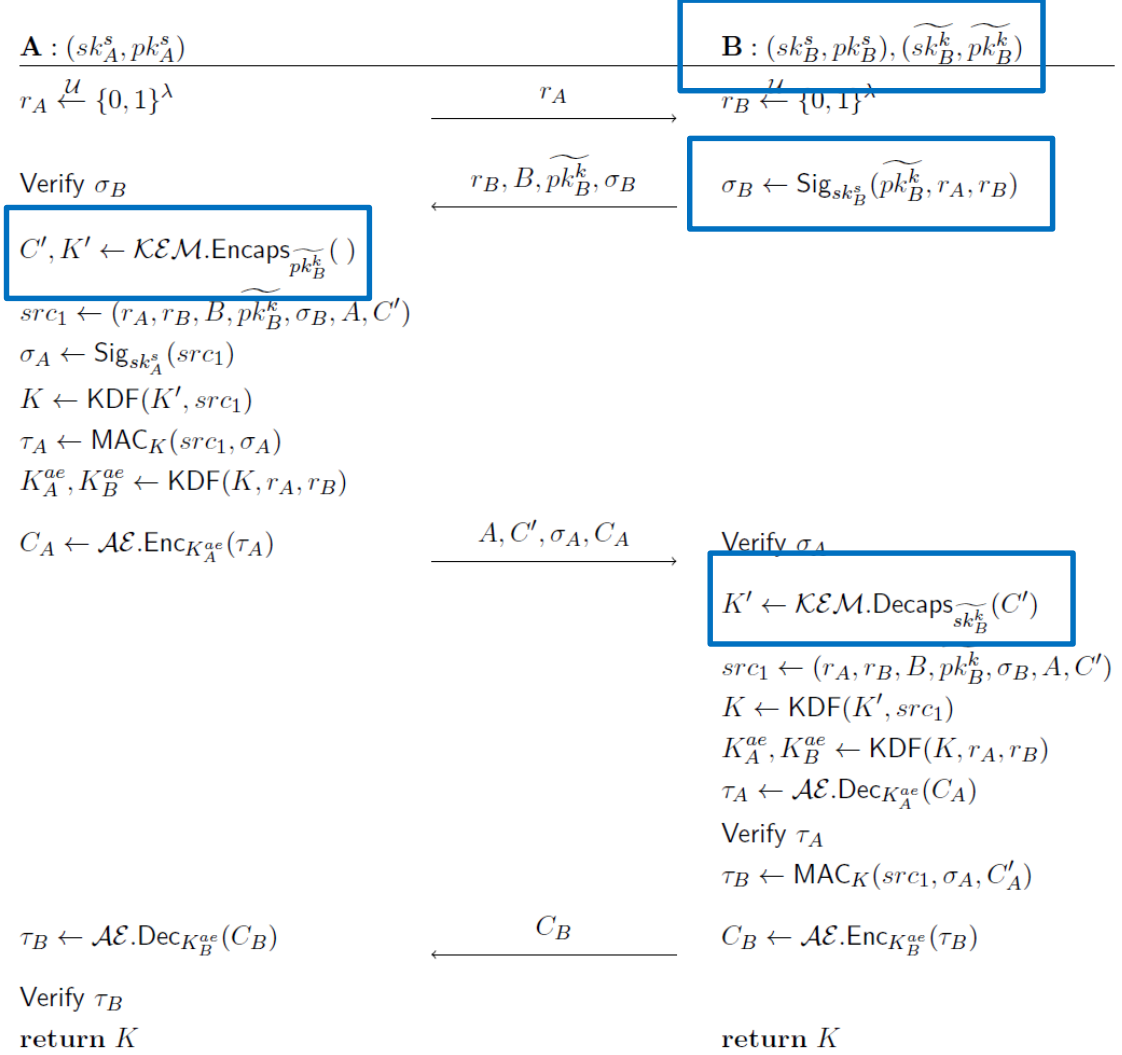
Модель нарушителя

- Протокол GC [1] и атака на него [2].
- Атака «модельная» – соответствующая практическая ситуация не описывается.
- Практическая ситуация вдохновлена текущими работами по ПВДНП
- Модель:
  - Если взаимодействуют честные, то только прослушивание
  - Если взаимодействует нарушитель, то может вскрывать промежуточные значения на честной стороне

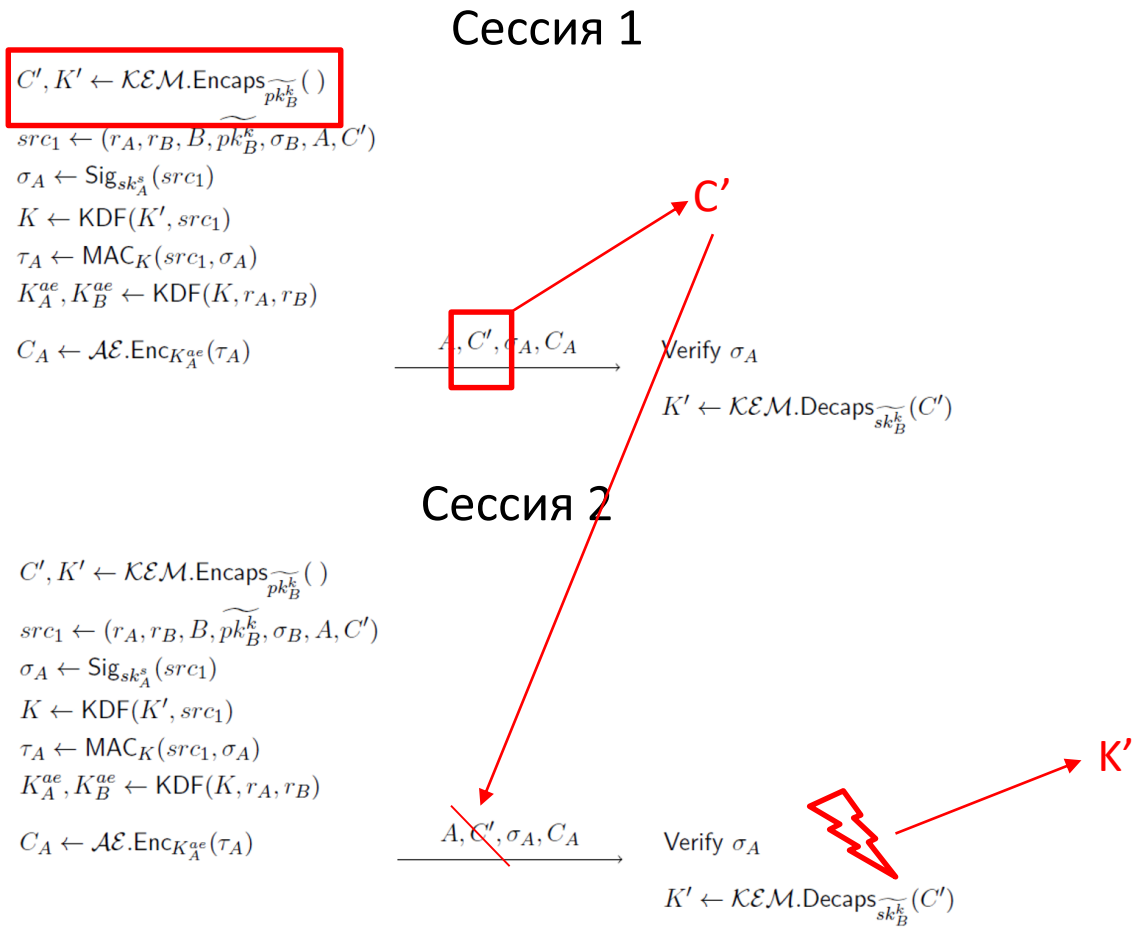


[1] «Strongly Secure Authenticated Key Exchange from Factoring, Codes, and Lattices», 2012.
[2] «Cryptanalysis of a strongly secure authenticated key exchange protocol», 2013.

pqRTLS12


$\mathbf{A} : (sk_A^s, pk_A^s)$
$\mathbf{B} : (sk_B^s, pk_B^s), (\widetilde{sk_B^k}, \widetilde{pk_B^k})$
$r_A \xleftarrow{\mathcal{U}} \{0,1\}^\lambda$
r_A
$r_B \xleftarrow{\mathcal{U}} \{0,1\}^\lambda$
Verify σ_B
$r_B, B, \widetilde{pk_B^k}, \sigma_B$
$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(\widetilde{pk_B^k}, r_A, r_B)$
$C', K' \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{\widetilde{pk_B^k}}(\,)$
$src_1 \leftarrow (r_A, r_B, B, \widetilde{pk_B^k}, \sigma_B, A, C')$
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(src_1)$
$K \leftarrow \mathsf{KDF}(K', src_1)$
$\tau_A \leftarrow \mathsf{MAC}_K(src_1, \sigma_A)$
$K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(K, r_A, r_B)$
$C_A \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_A^{ae}}(\tau_A)$
A, C', σ_A, C_A
Verify σ_A
$K' \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk_B^k}}(C')$
$src_1 \leftarrow (r_A, r_B, B, pk_B^k, \sigma_B, A, C')$
$K \leftarrow \mathsf{KDF}(K', src_1)$
$K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(K, r_A, r_B)$
$\tau_A \leftarrow \mathcal{AE}.\mathsf{Dec}_{K_A^{ae}}(C_A)$
Verify τ_A
$\tau_B \leftarrow \mathsf{MAC}_K(src_1, \sigma_A, C'_A)$
$\tau_B \leftarrow \mathcal{AE}.\mathsf{Dec}_{K_B^{ae}}(C_B)$
C_B
$C_B \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_B^{ae}}(\tau_B)$
Verify τ_B
return K
return K

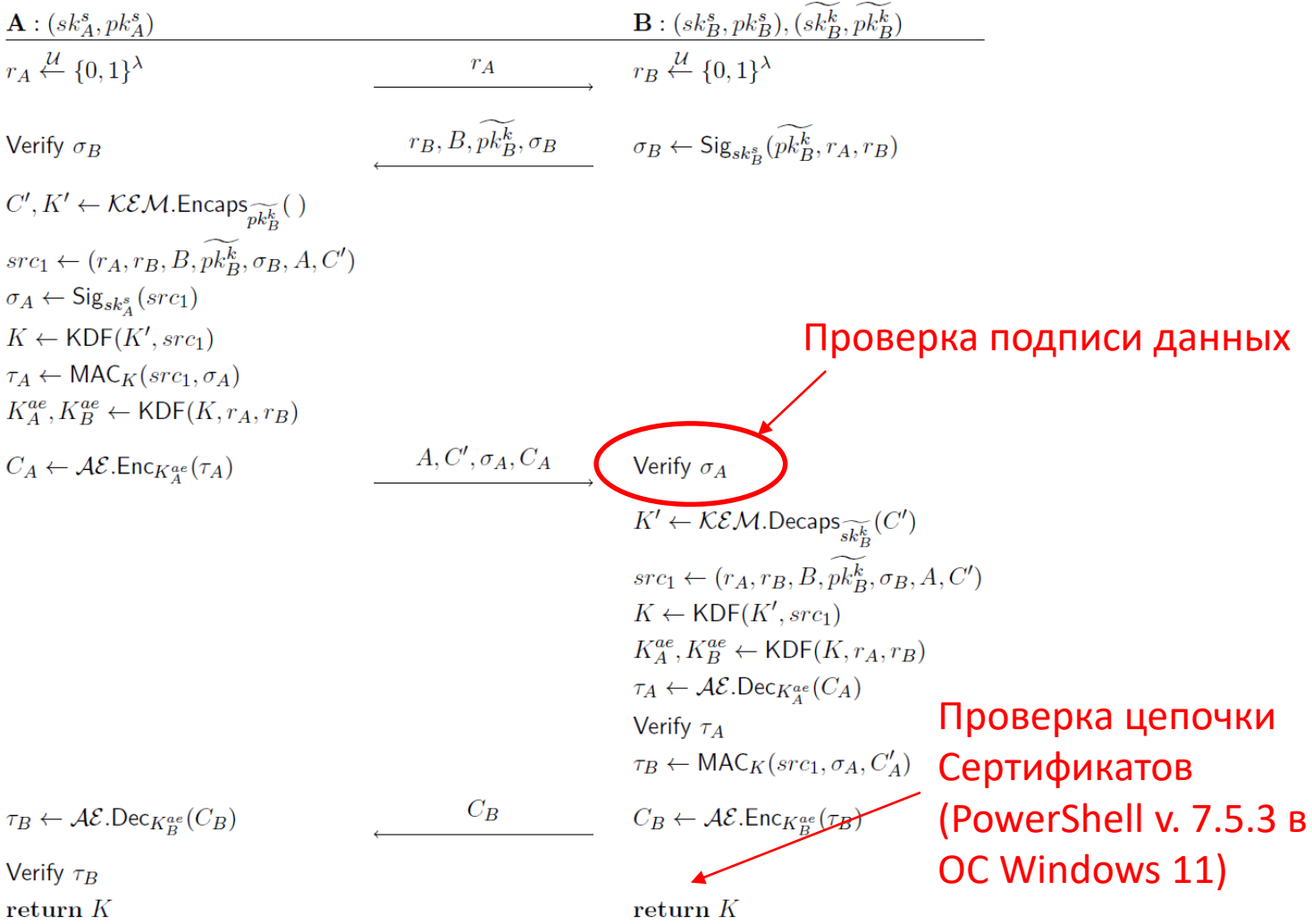
Идея атаки


Сессия 1
$C', K' \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{\widetilde{pk_B^k}}(\,)$
$src_1 \leftarrow (r_A, r_B, B, \widetilde{pk_B^k}, \sigma_B, A, C')$
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(src_1)$
$K \leftarrow \mathsf{KDF}(K', src_1)$
$\tau_A \leftarrow \mathsf{MAC}_K(src_1, \sigma_A)$
$K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(K, r_A, r_B)$
$C_A \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_A^{ae}}(\tau_A)$
C'
A, C', σ_A, C_A
Verify σ_A
$K' \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk_B^k}}(C')$
Сессия 2
$C', K' \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{\widetilde{pk_B^k}}(\,)$
$src_1 \leftarrow (r_A, r_B, B, \widetilde{pk_B^k}, \sigma_B, A, C')$
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(src_1)$
$K \leftarrow \mathsf{KDF}(K', src_1)$
$\tau_A \leftarrow \mathsf{MAC}_K(src_1, \sigma_A)$
$K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(K, r_A, r_B)$
$C_A \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_A^{ae}}(\tau_A)$
A, C', σ_A, C_A
Verify σ_A
$K' \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk_B^k}}(C')$
K'

Идея атаки

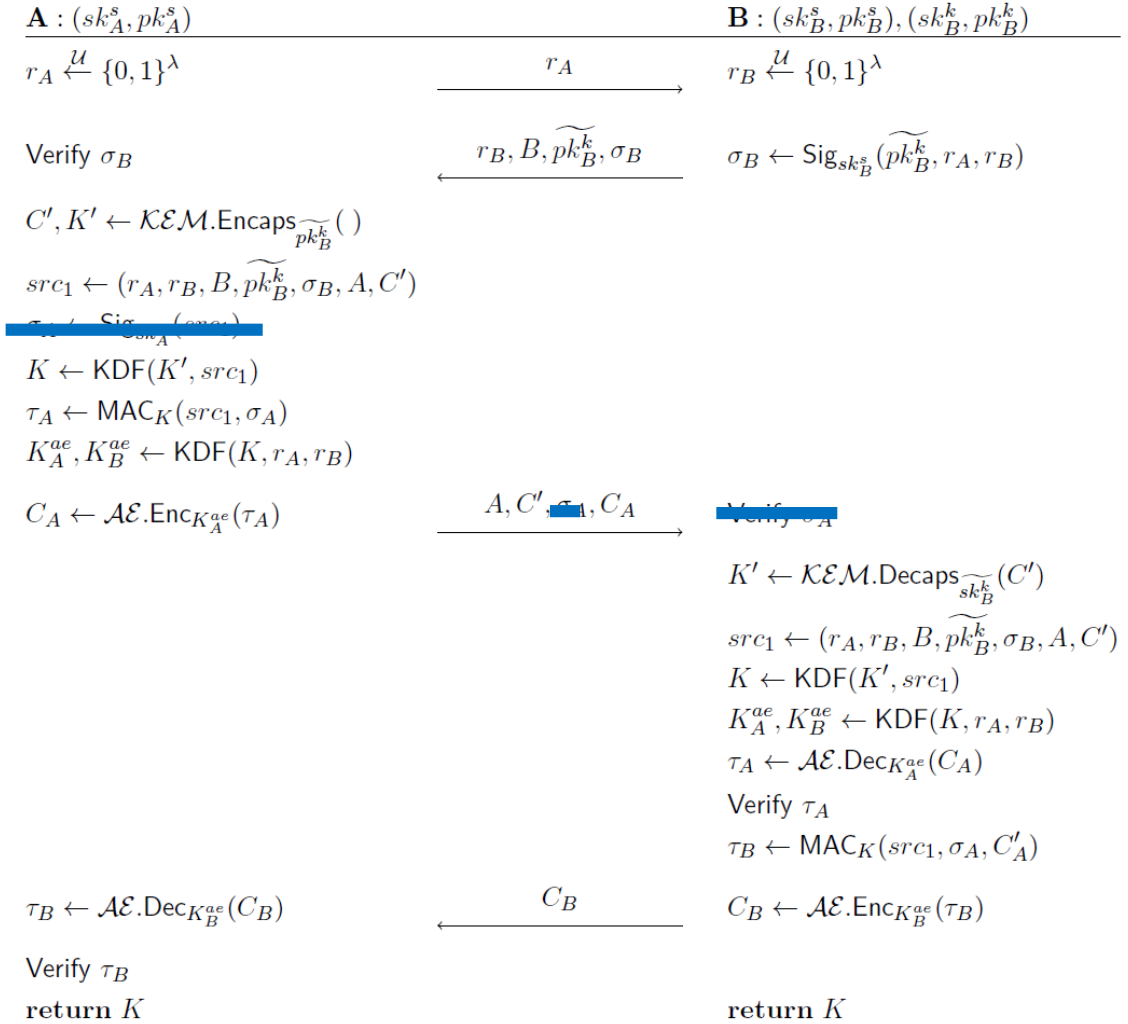

Сессия 1
$C', K' \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{\widetilde{pk_B^k}}(\,)$
$src_1 \leftarrow (r_A, r_B, B, \widetilde{pk_B^k}, \sigma_B, A, C')$
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(src_1)$
$K \leftarrow \mathsf{KDF}(K', src_1)$
$\tau_A \leftarrow \mathsf{MAC}_K(src_1, \sigma_A)$
$K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(K, r_A, r_B)$
$C_A \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_A^{ae}}(\tau_A)$
C'
A, C', σ_A, C_A
Verify σ_A
$K' \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk_B^k}}(C')$
Из-за подписи атака не проходит
Сессия 2
$C', K' \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{\widetilde{pk_B^k}}(\,)$
$src_1 \leftarrow (r_A, r_B, B, \widetilde{pk_B^k}, \sigma_B, A, C')$
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(src_1)$
$K \leftarrow \mathsf{KDF}(K', src_1)$
$\tau_A \leftarrow \mathsf{MAC}_K(src_1, \sigma_A)$
$K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(K, r_A, r_B)$
$C_A \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_A^{ae}}(\tau_A)$
A, C', σ_A, C_A
Verify σ_A
K'
$K' \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk_B^k}}(C')$

Отложенная проверка цепочки сертификатов



Вывод 1: При описании протоколов необходимо четко указывать, когда должна проверяться цепочка сертификатов. Момент проверки цепочки сертификатов нужно учитывать при криптографическом анализе. Изменение момента проверки цепочки при реализации может привести к появлению уязвимости.

pqRTLS12 с односторонней аутентификацией



Идея атаки

Сессия 1

$C', K' \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{\widetilde{pk_B^k}}(\,)$

$src_1 \leftarrow (r_A, r_B, B, \widetilde{pk_B^k}, \sigma_B, A, C')$

$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(src_1)$

$K \leftarrow \mathsf{KDF}(K', src_1)$

$\tau_A \leftarrow \mathsf{MAC}_K(src_1, \sigma_A)$

$K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(K, r_A, r_B)$

$C_A \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_A^{ae}}(\tau_A)$

C’

A, C', σ_A, C_A

Verify σ_A

$K' \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk_B^k}}(C')$

Сессия 2 с односторонней аутентификацией

$C', K' \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{\widetilde{pk_B^k}}(\,)$

$src_1 \leftarrow (r_A, r_B, B, \widetilde{pk_B^k}, \sigma_B, A, C')$

$K \leftarrow \mathsf{KDF}(K', src_1)$

$\tau_A \leftarrow \mathsf{MAC}_K(src_1, \sigma_A)$

$K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(K, r_A, r_B)$

$C_A \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_A^{ae}}(\tau_A)$

$A, C', \quad , C_A$

K’

$K' \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk_B^k}}(C')$

Требование к реализации pqRTLS12

$\mathbf{A}: (sk_A^s, pk_A^s)$		$\mathbf{B}: (sk_B^s, pk_B^s), (\widetilde{sk_B^k}, \widetilde{pk_B^k})$
$r_A \xleftarrow{\mathcal{U}} \{0,1\}^\lambda$	$\xrightarrow{r_A}$	$r_B \xleftarrow{\mathcal{U}} \{0,1\}^\lambda$
Verify σ_B	$\xleftarrow{r_B, B, \widetilde{pk_B^k}, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(\widetilde{pk_B^k}, r_A, r_B)$
$C', K' \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{\widetilde{pk_B^k}}(\,)$		
$src_1 \leftarrow (r_A, r_B, B, \widetilde{pk_B^k}, \sigma_B, A, C')$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(src_1)$		
$K \leftarrow \mathsf{KDF}(K', src_1)$		
$\tau_A \leftarrow \mathsf{MAC}_K(src_1, \sigma_A)$		
$K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(K, r_A, r_B)$		
$C_A \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_A^{ae}}(\tau_A)$	$\xrightarrow{A, C', \sigma_A, C_A}$	Verify σ_A
		$K' \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk_B^k}}(C')$
		$src_1 \leftarrow (r_A, r_B, B, \widetilde{pk_B^k}, \sigma_B, A, C')$
		$K \leftarrow \mathsf{KDF}(K', src_1)$
		$K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(K, r_A, r_B)$
		$\tau_A \leftarrow \mathcal{AE}.\mathsf{Dec}_{K_A^{ae}}(C_A)$
		Verify τ_A
		$\tau_B \leftarrow \mathsf{MAC}_K(src_1, \sigma_A, C'_A)$
$\tau_B \leftarrow \mathcal{AE}.\mathsf{Dec}_{K_B^{ae}}(C_B)$	$\xleftarrow{C_B}$	$C_B \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_B^{ae}}(\tau_B)$
Verify τ_B		
return K		**return** K

Нарушитель может вскрыть только K, но K уже привязан к сеансу за счет KDF

Требование к KEM

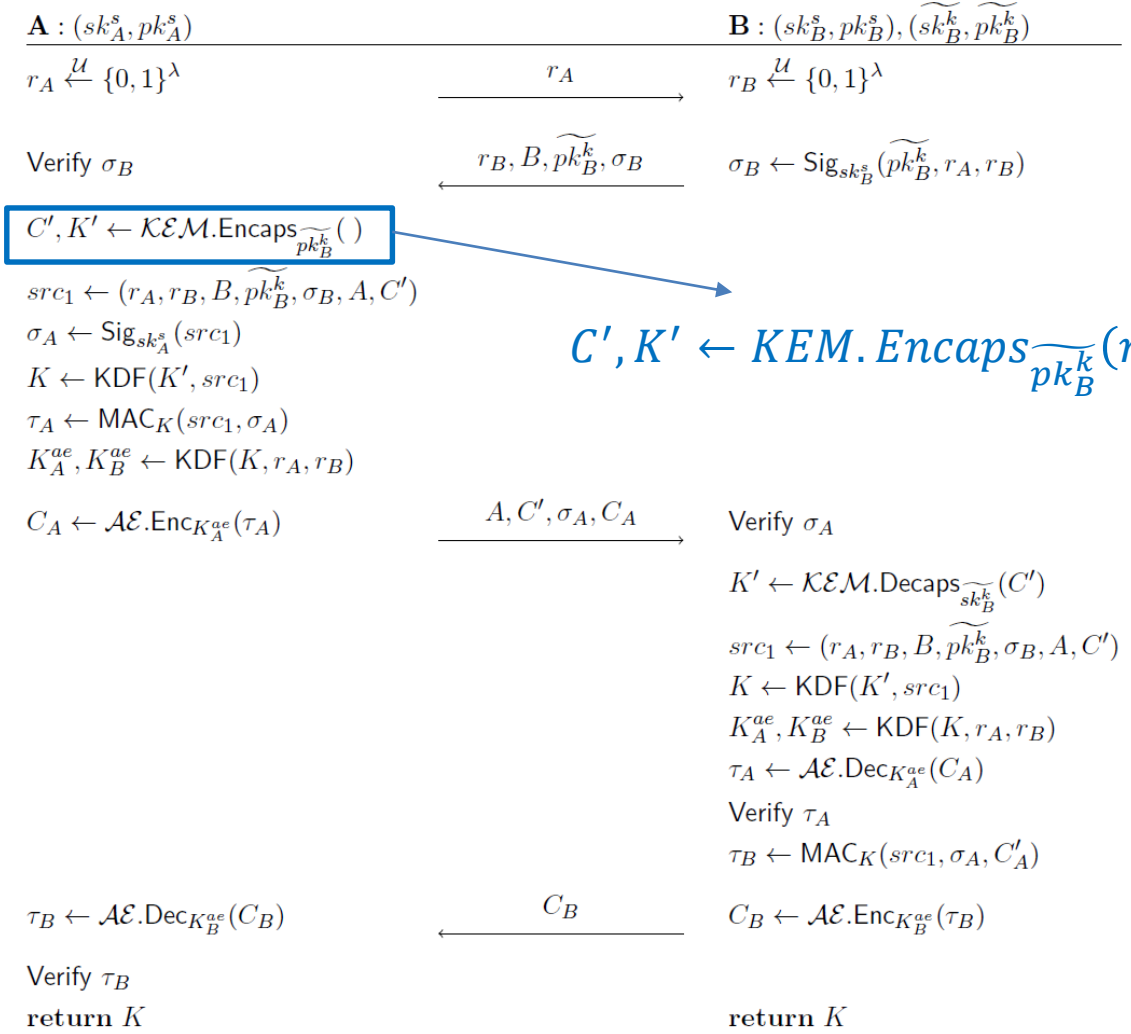
Но! KDF уже не задействует долговременный закрытый ключ, его перенос в защищенный модуль может породить дополнительные трудности

$\mathbf{A}: (sk_A^s, pk_A^s)$		$\mathbf{B}: (sk_B^s, pk_B^s), (\widetilde{sk_B^k}, \widetilde{pk_B^k})$
$r_A \xleftarrow{\mathcal{U}} \{0,1\}^\lambda$	$\xrightarrow{r_A}$	$r_B \xleftarrow{\mathcal{U}} \{0,1\}^\lambda$
Verify σ_B	$\xleftarrow{r_B, B, \widetilde{pk_B^k}, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(\widetilde{pk_B^k}, r_A, r_B)$
$C', K' \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{\widetilde{pk_B^k}}(\,)$		
$src_1 \leftarrow (r_A, r_B, B, \widetilde{pk_B^k}, \sigma_B, A, C')$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(src_1)$		
$K \leftarrow \mathsf{KDF}(K', src_1)$		
$\tau_A \leftarrow \mathsf{MAC}_K(src_1, \sigma_A)$		
$K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(K, r_A, r_B)$		
$C_A \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_A^{ae}}(\tau_A)$	$\xrightarrow{A, C', \sigma_A, C_A}$	Verify σ_A
		$K' \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk_B^k}}(C')$
		$src_1 \leftarrow (r_A, r_B, B, pk_B^k, \sigma_B, A, C')$
		$K \leftarrow \mathsf{KDF}(K', src_1)$
		$K_A^{ae}, K_B^{ae} \leftarrow \mathsf{KDF}(K, r_A, r_B)$
		$\tau_A \leftarrow \mathcal{AE}.\mathsf{Dec}_{K_A^{ae}}(C_A)$
		Verify τ_A
		$\tau_B \leftarrow \mathsf{MAC}_K(src_1, \sigma_A, C'_A)$
$\tau_B \leftarrow \mathcal{AE}.\mathsf{Dec}_{K_B^{ae}}(C_B)$	$\xleftarrow{C_B}$	$C_B \leftarrow \mathcal{AE}.\mathsf{Enc}_{K_B^{ae}}(\tau_B)$
Verify τ_B		
return K		**return** K

Нарушитель может вскрыть только K, но K уже привязан к сеансу за счет KDF

Требование к KEM

Вот бы привязать к сеансу сразу C’



$$C', K' \leftarrow KEM.Encaps_{\widetilde{pk_B^k}}(r_A \parallel r_B)$$

Вывод 2: Удобная мера защиты требует расширения интерфейса KEM путем добавления в функции инкапсуляции и декапсуляции открытых данных, к которым будет привязан ключ и результат инкапсуляции:

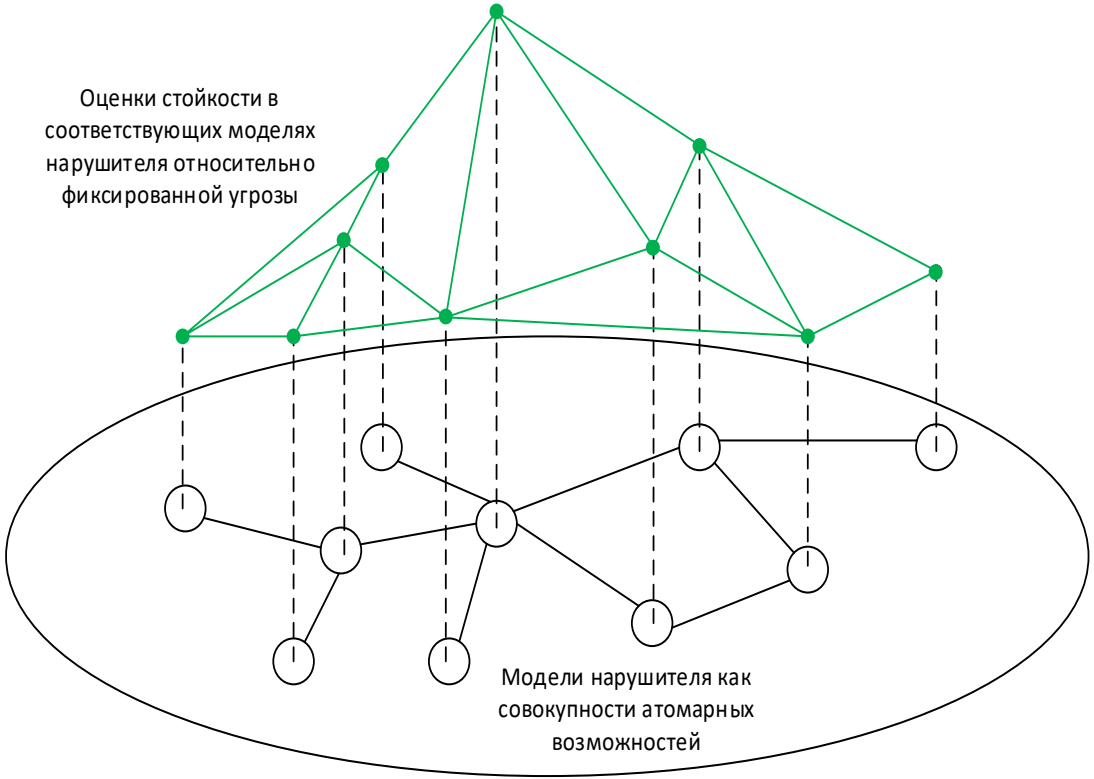
$$C, K \leftarrow KEM.Encaps_{\widetilde{pk_B^k}}(AD)$$

$$K \leftarrow KEM.Decaps_{\widetilde{sk_B^k}}(C, AD)$$

Формирование модели нарушителя и «ландшафта защищенности»

- CTCrypt 2023: «**Probing the security landscape for authenticated key establishment protocols**»
- Предложенная модель в терминах ландшафта:

  Если C1, то больше ничего, если C2, то еще UA7.



Вывод 3: Модель нарушителя может не описываться совокупностью «атомарных» возможностей, но иметь сложные зависимости, обоснованные исключительно условиями применения. Так что «ландшафта защищенности» может быть недостаточно для оценки стойкости протокола при встраивании.

Выводы:

1. Момент проверки цепочки сертификатов критически важен.
2. Предложение по расширению интерфейса KEM.
3. Модели нарушителя могут не описываться совокупностью атомарных возможностей.

РусКрипто
XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Спасибо за внимание!

Алексеев Евгений Константинович
ООО «КРИПТО-ПРО»
alekseev@cryptopro.ru