РусКрипто XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Анализ применимости атак на протоколы аутентифицированной выработки ключа, основанные на механизме инкапсуляции ключа, к протоколу pqRTLS12

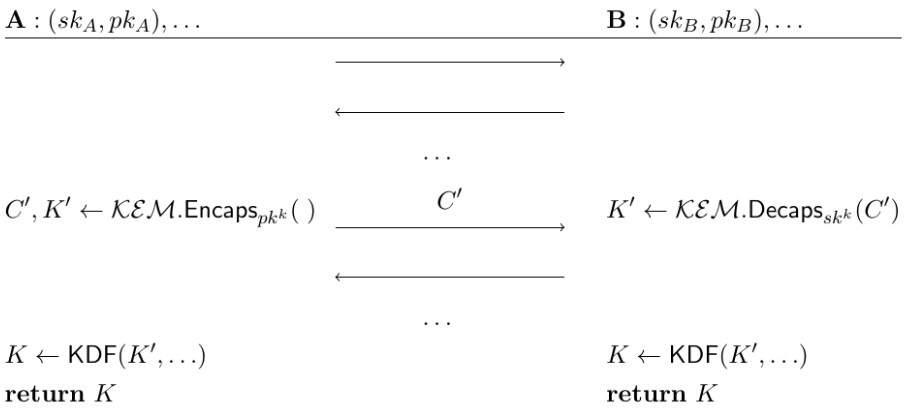
Мухортова Алена Андреевна, ООО «КРИПТО-ПРО»

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

Протокол pqRTLS12

- В 2024 году начат период предварительного изучения возможности встраивания постквантовых механизмов инкапсуляции ключа (KEM) в протокол TLS 1.2.
- Причины выбора именно TLS 1.2 обсуждались на заседаниях РГ СКАиП ТК26, а также на PKI-форуме в 2024 году в докладе «**Об одном подходе к внедрению постквантовых криптографических алгоритмов в протокол TLS**».
- На данный момент завершается этап формирования итогового облика протокола и оценки применимости к нему известных атак на родственные протоколы (основанные на KEM)
- Далее под pqRTLS12 будем понимать Handshake этого протокола.

AKE-протоколы



Угрозы для AKE-протоколов:

- **SEC** — нарушение секретности ключей.
- **PFS** — нарушение секретности ключей, выработанных до вскрытия долговременного ключа.
- **AUTH-I(R)** — ложная аутентификация перед инициатором (ответчиком).
- **KCI** — ложная аутентификация после вскрытия долговременного ключа проверяющего.
- **UUKS/BUKS** — два честных участника (A и B) выработали общий ключ, но один из них (оба) считает, что выработал его с другим участником (нарушителем или тоже честным участником).

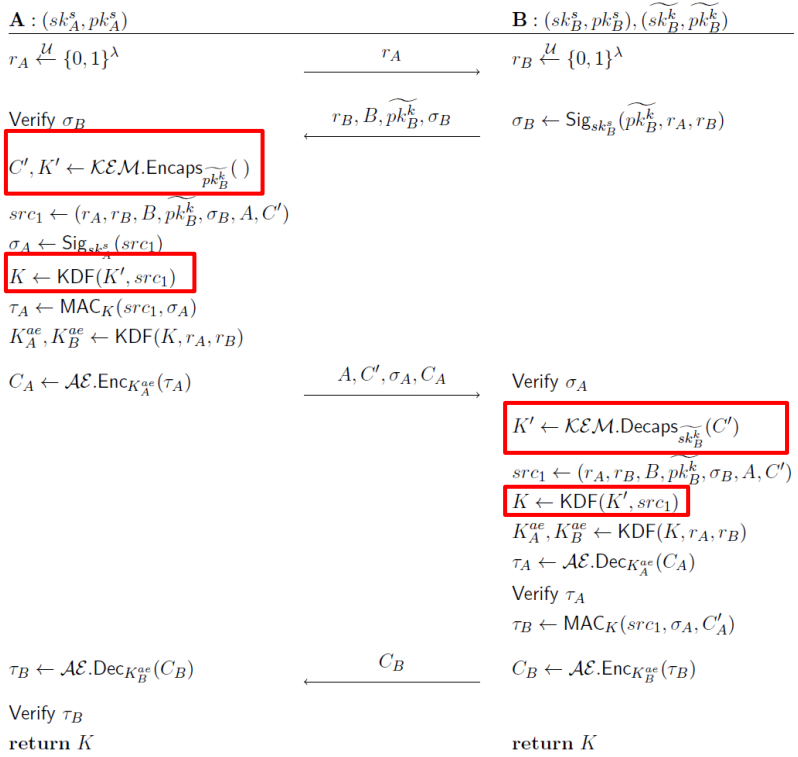
Протокол pqRTLS12. Схема Handshake

Особенность pqRTLS12:

- Способ формирования общего ключа K — инкапсуляция на кратковременном ключе сервера.

Задача:

- Оценить применимость к pqRTLS12 существующих атак на AKE-протоколы, основанные на механизме инкапсуляции или шифровании с открытым ключом.



Обзор атак на AKE-протоколы

В ходе обзора рассмотрено:

- 18 статей с атаками на существующие протоколы.
- Годы выпуска статей 1997-2024.
- 21 атака на 16 протоколов.
- Среди рассмотренных протоколов:
  - TLS-RSA
  - SSH
  - PQXDH
  - и др.

Статья	Год	Протокол	Угроза
[1]	2024	BKM-KK	BUKS
[2]	2024	Kyber-AKE	UUKS
[3]	2006	BGN	UUKS
[4]	1997	SSH	UUKS
[5]	2007	Oakley	BUKS
[6]	2024	PQXDH	SEC
[7]	2006	mMAKEP-JC	AUTH-I
[8]	2009	G2×KEM+DH	AUTH-R
[9]	1997	AKA	AUTH-I
[10]	2018	KF	KCI
[11]	2016	WC-MAKEP	AUTH-I
		WC-MAKEP-2	SEC
[12]	2015	π	AUTH-I
[13]	2015	π	KCI
[14]	2008	ES-MAKEP	SEC
[15]	2014	TLS-RSA	PFS
-	-	PQXDH	AUTH-R
[16]	2016	GC	SEC
[17]	2013	GC	AUTH-R
			AUTH-I
[18]	2024	BKM-KK	AUTH-I

Обзор атак на AKE-протоколы

Неприменимые атаки

Модельные неприменимые атаки

Применимые атаки, устранимые с помощью организационно-технических мер

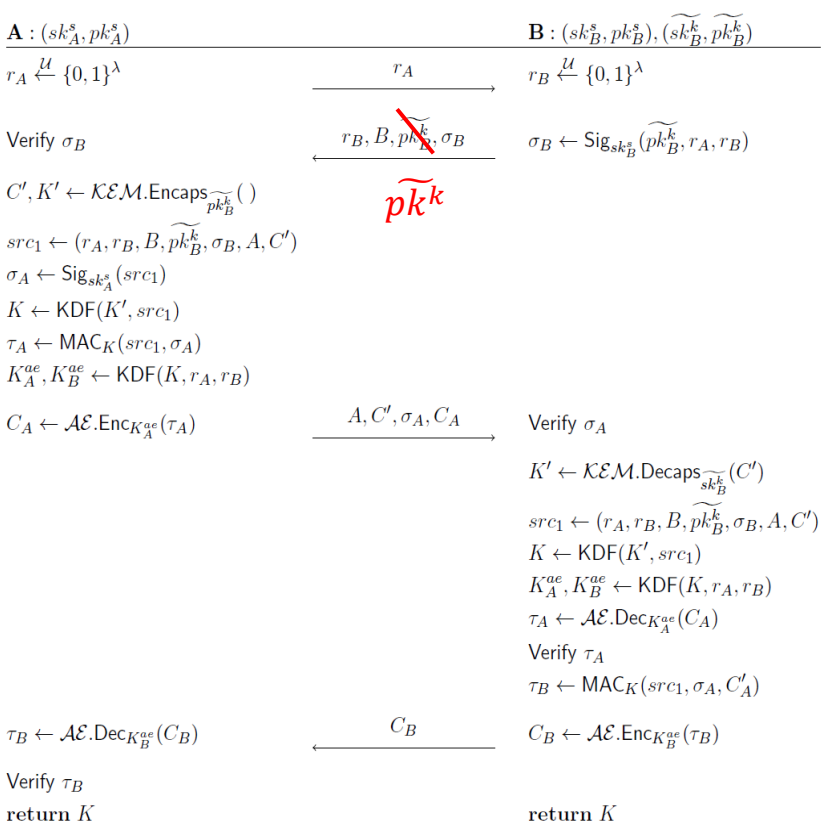
Применимые атаки, устранимые с помощью криптографических методов

Статья	Год	Протокол	Угроза
[1]	2024	BKM-KK	BUKS
[2]	2024	Kyber-AKE	UUKS
[3]	2006	BGN	UUKS
[4]	1997	SSH	UUKS
[5]	2007	Oakley	BUKS
[6]	2024	PQXDH	SEC
[7]	2006	mMAKEP-JC	AUTH-I
[8]	2009	G2×KEM+DH	AUTH-R
[9]	1997	AKA	AUTH-I
[10]	2018	KF	KCI
[11]	2016	WC-MAKEP	AUTH-I
		WC-MAKEP-2	SEC
[12]	2015	π	AUTH-I
[13]	2015	π	KCI
[14]	2008	ES-MAKEP	SEC
[15]	2014	TLS-RSA	PFS
-	-	PQXDH	AUTH-R
[16]	2016	GC	SEC
[17]	2013	GC	AUTH-R
			AUTH-I
[18]	2024	BKM-KK	AUTH-I

Атаки, не применимые к pqRTLS12

Атака на PQXDH

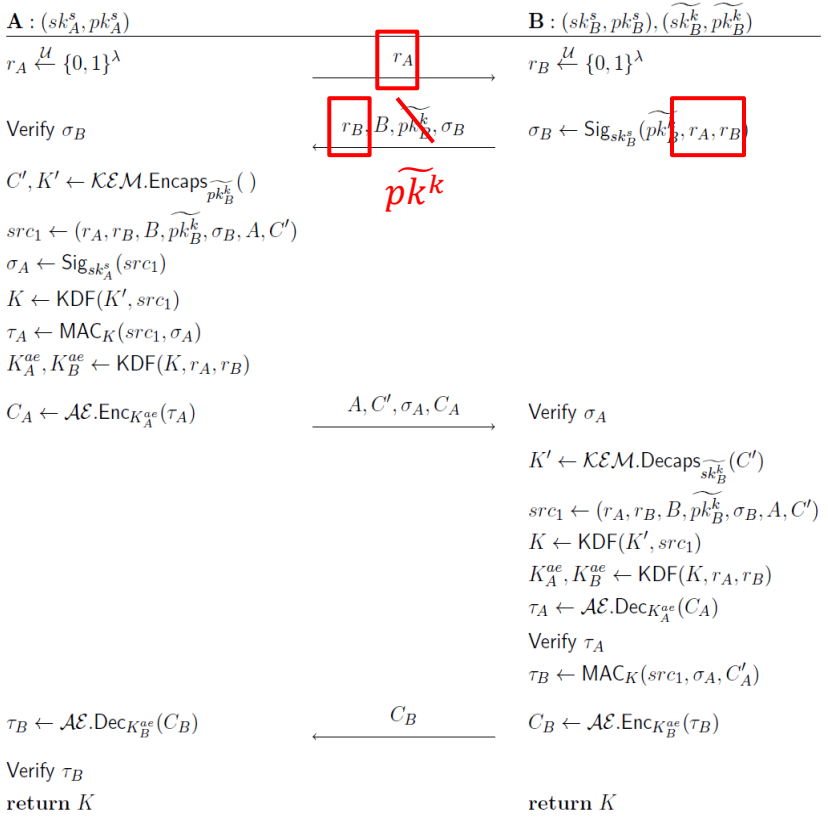
Статья	Протокол	Угроза
[6]	PQXDH	SEC



6. Bhargavan K., Jacomme C., Kiefer F., Schmidt R. Formal verification of the PQXDH Post-Quantum key agreement protocol for end-to-end secure messaging //USENIX Security. 2024.

Атака на PQXDH

Статья	Протокол	Угроза
[6]	PQXDH	SEC



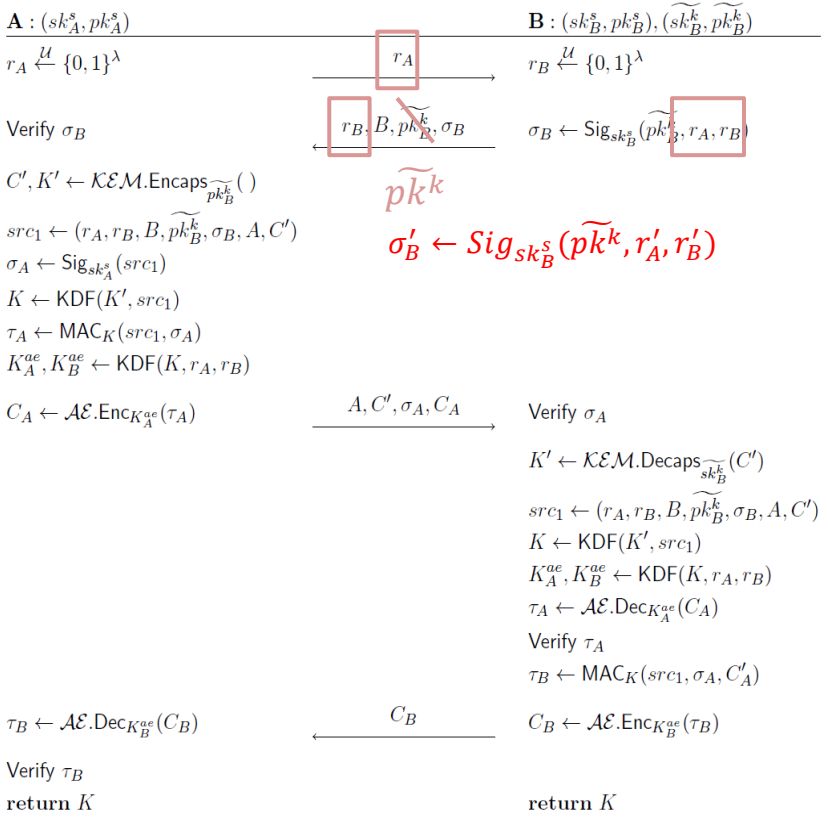
6. Bhargavan K., Jacomme C., Kiefer F., Schmidt R. Formal verification of the PQXDH Post-Quantum key agreement protocol for end-to-end secure messaging //USENIX Security. 2024.

Атака на PQXDH

Статья	Протокол	Угроза
[6]	PQXDH	SEC

Мера защиты:

- Привязка подписи к сеансу



6. Bhargavan K., Jacomme C., Kiefer F., Schmidt R. Formal verification of the PQXDH Post-Quantum key agreement protocol for end-to-end secure messaging //USENIX Security. 2024.

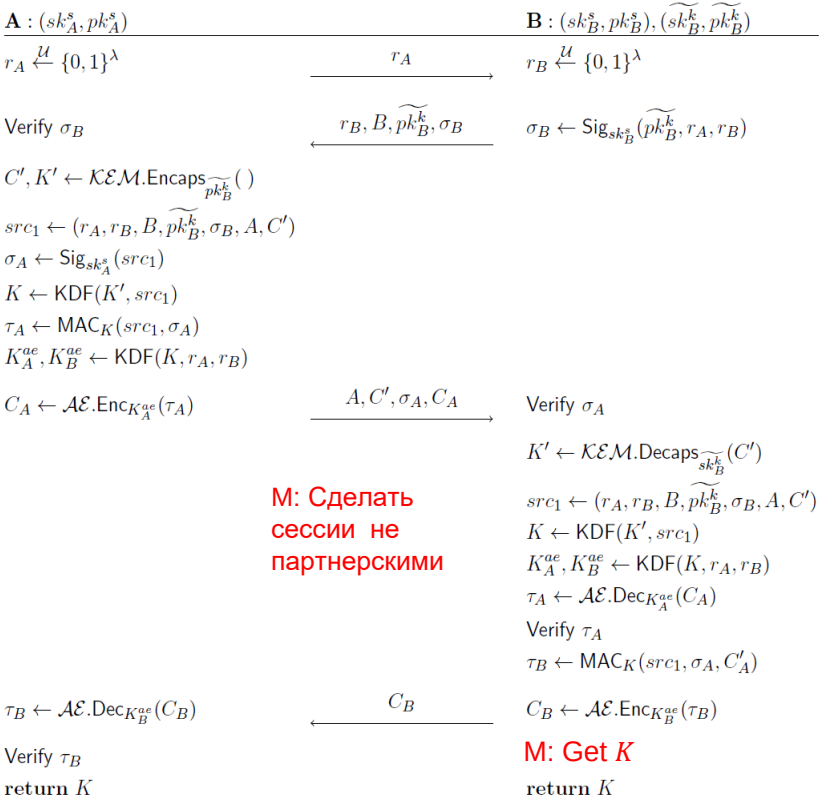
Атаки, не применимые к pqRTLS12

Протокол	Угроза	Меры защиты
BKM-KK	BUKS	KDF с идентификаторами
Kyber-AKE	UUKS	
BGN	UUKS	
SSH	UUKS	
Oakley	BUKS	
PQXDH	SEC	Привязка подписи к сеансу
mMAKEP-JC	AUTH-I	KDF с транскрипцией
G2×KEM+DH	AUTH-R	
AKA	AUTH-I	Подпись транскрипции
KF	KCI	IND-CCA стойкий KEM

Модельные атаки, не применимые к pqRTLS12

Атака на π

Статья	Протокол	Угроза	Идея
[12]	π	AUTH-I	Компрометация сеансового ключа второй стороны



12. Toorani M. (2015). On Continuous After-the-Fact Leakage-Resilient Key Exchange. 10.13140/RG.2.1.3064.6486.

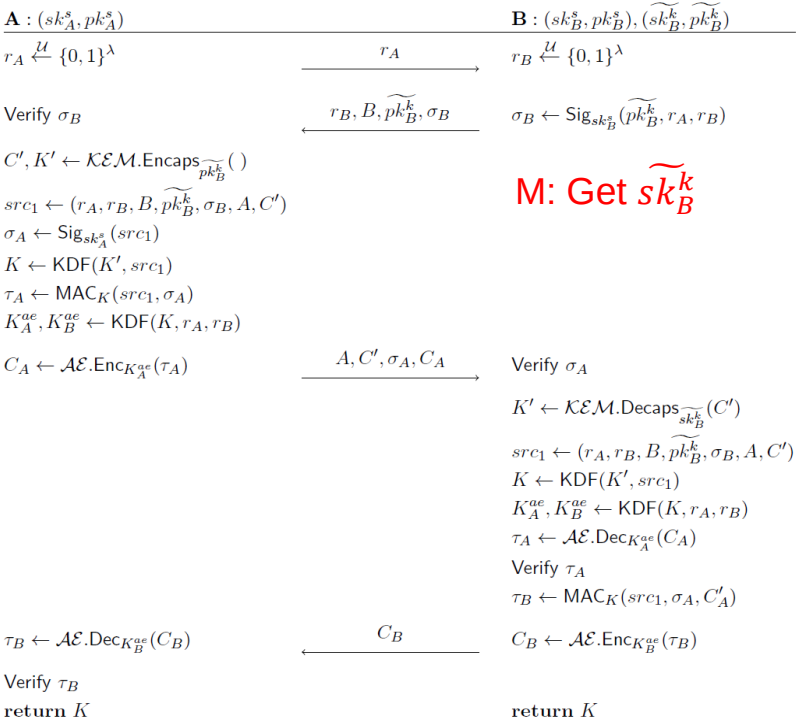
Модельные атаки, не применимые к pqRTLS12

Протокол	Угроза	Меры защиты
WC-MAKEP	AUTH-I	Модельная, неприменима
WC-MAKEP-2	SEC	
π	AUTH-I	

Атаки, применимые к pqRTLS12 и устранимые организационно-техническими мерами

Атаки, основанные на компрометации ключа шифрования

Статья	Протокол	Угроза	Идея
[13]	π	KCI	Компрометация долговременного закрытого ключа шифрования
[14]	ES-MAKEP	SEC	
[15]	TLS-RSA	PFS	
-	PQXDH	AUTH-R	Компрометация кратковременного ключа декапсуляции



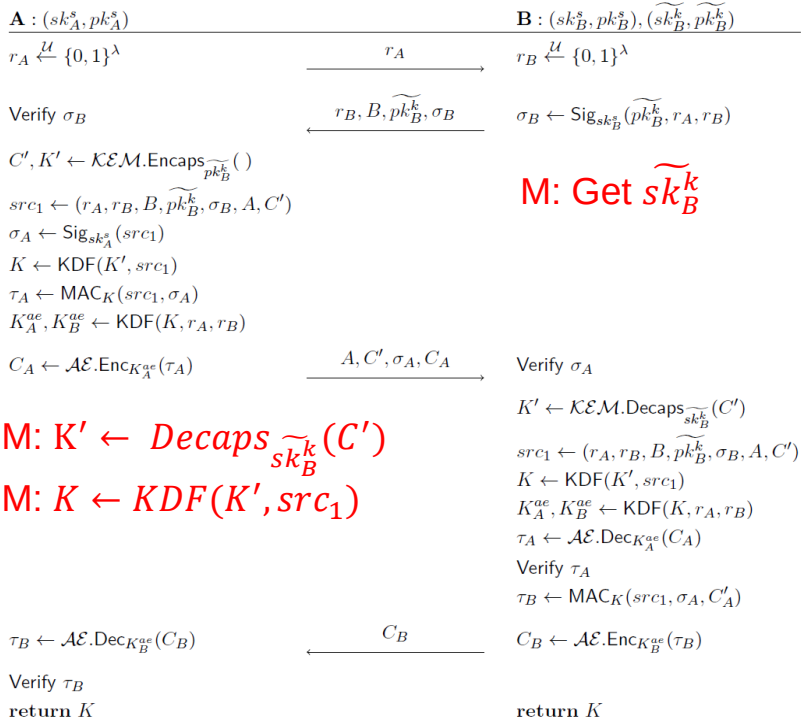
13. Li, Y. (2016). Design and analysis of cryptographic protocols (Doctoral dissertation, Bochum, Ruhr-Universit¨at Bochum, Diss., 2015).
14. He Y.J., Lee M.C. Towards a Secure Mutual Authentication and Key Exchange Protocol for Mobile Communications // 10.1109/WIOPT.2008.4586068., 225 - 231. 2008.
15. Basin D., Cremers C., Horvat M. Actor Key Compromise: Consequences and Countermeasures // Proceedings IEEE 27th Computer Security Foundations Symposium, 2014, pp. 244–258

Атаки, основанные на компрометации ключа шифрования

Статья	Протокол	Угроза	Идея
[13]	π	KCI	Компрометация долговременного закрытого ключа шифрования
[14]	ES-MAKEP	SEC	
[15]	TLS-RSA	PFS	
-	PQXDH	AUTH-R	Компрометация кратковременного ключа декапсуляции

Мера защиты:

- Защищенное хранение закрытых ключей



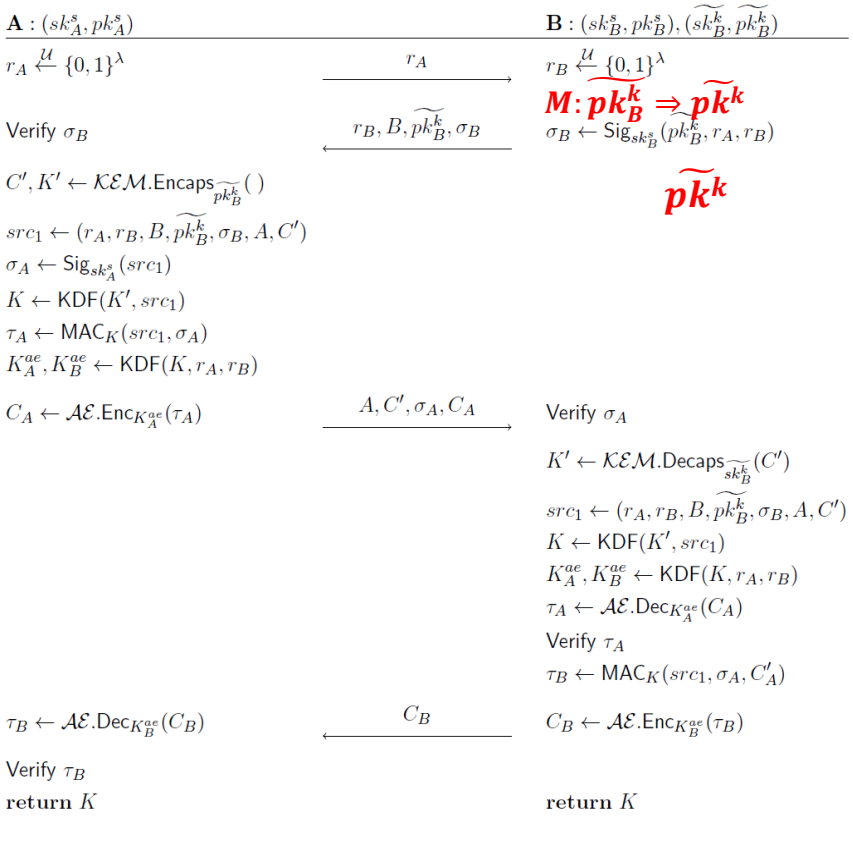
Атаки, применимые к pqRTLS12 и устранимые организационно-техническими мерами

Протокол	Угроза	Меры защиты
π	KCI	Защищенное хранение ключа
ES-MAKEP	SEC	
TLS-RSA	PFS	
PQXDH	AUTH-R	
GC	SEC	Защищенное хранение случайностей
GC	AUTH-R	Требования к аппаратной реализации
	AUTH-I	

Атаки, применимые к pqRTLS12 и устранимые криптографическими методами

Атака на BKM-KK

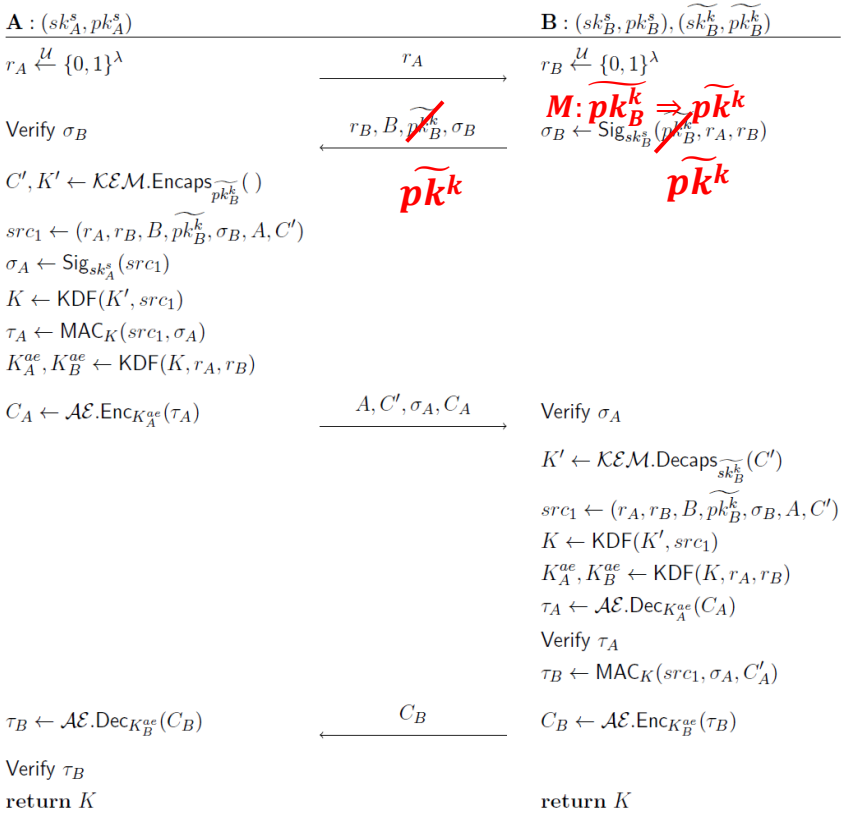
Статья	Протокол	Угроза	Идея
[18]	BKM-KK	AUTH-I	Навязывание эфемерного ключа инкапсуляции



18. Алексеев Е.К., Кяжин С.Н., Смышляев С.В. Атаки на протоколы аутентифицированной выработки общего ключа при навязывании будущих открытых эфемерных ключей // Прикладная дискретная математика. 2024. № 66. С. 60–77.

Атака на BKM-KK

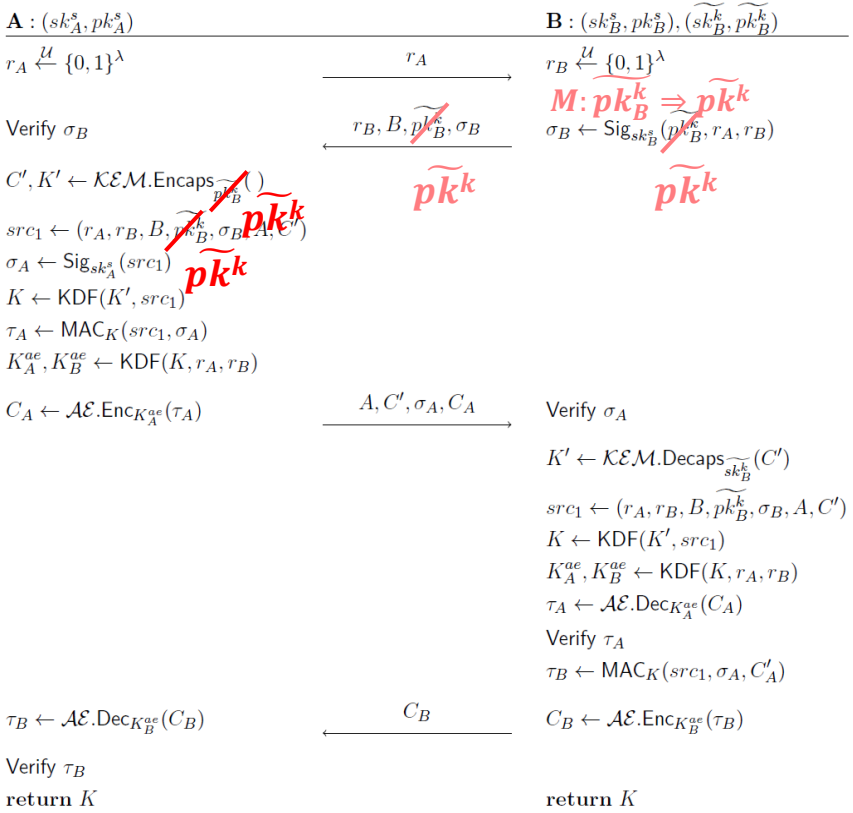
Статья	Протокол	Угроза	Идея
[18]	BKM-KK	AUTH-I	Навязывание эфемерного ключа инкапсуляции



18. Алексеев Е.К., Кяжин С.Н., Смышляев С.В. Атаки на протоколы аутентифицированной выработки общего ключа при навязывании будущих открытых эфемерных ключей // Прикладная дискретная математика. 2024. № 66. С. 60–77.

Атака на BKM-KK

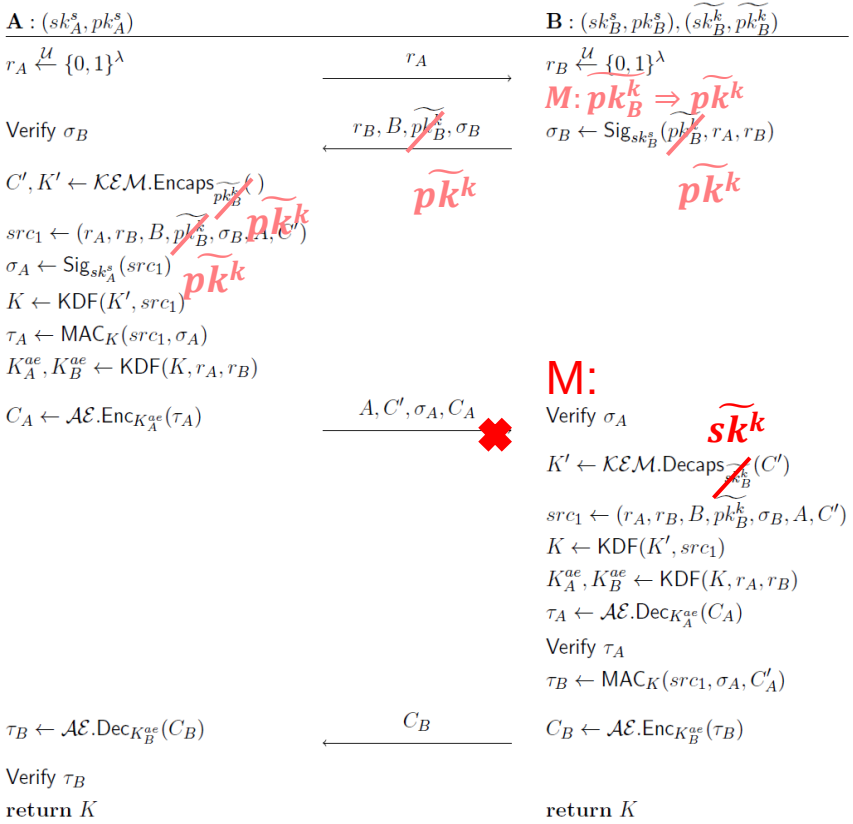
Статья	Протокол	Угроза	Идея
[18]	BKM-KK	AUTH-I	Навязывание эфемерного ключа инкапсуляции



18. Алексеев Е.К., Кяжин С.Н., Смышляев С.В. Атаки на протоколы аутентифицированной выработки общего ключа при навязывании будущих открытых эфемерных ключей // Прикладная дискретная математика. 2024. № 66. С. 60–77.

Атака на BKM-KK

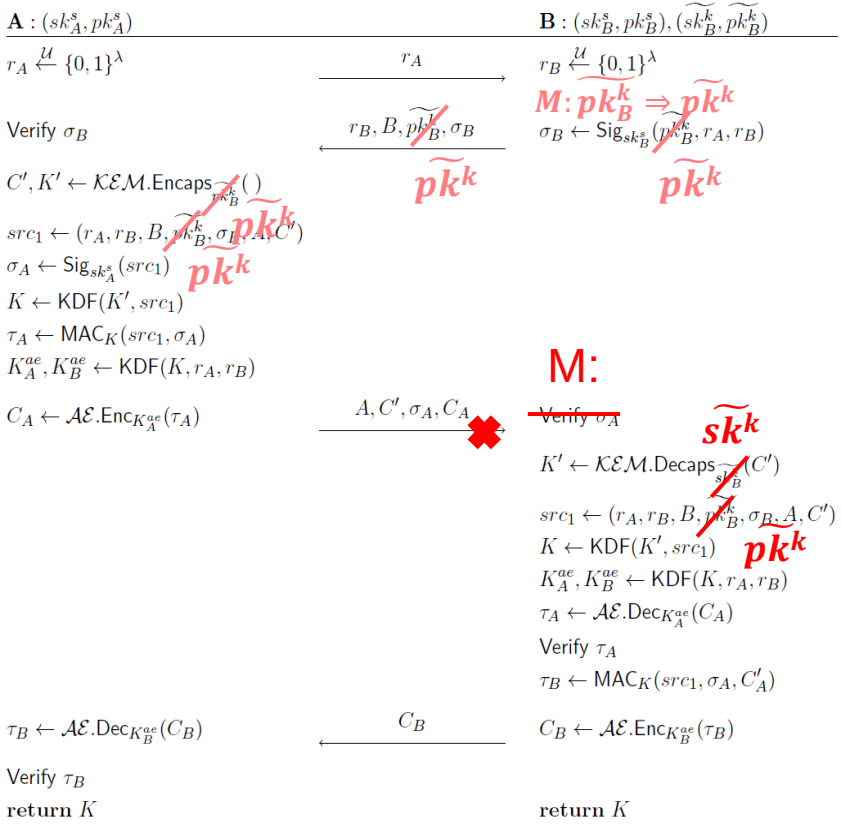
Статья	Протокол	Угроза	Идея
[18]	BKM-KK	AUTH-I	Навязывание эфемерного ключа инкапсуляции



18. Алексеев Е.К., Кяжин С.Н., Смышляев С.В. Атаки на протоколы аутентифицированной выработки общего ключа при навязывании будущих открытых эфемерных ключей // Прикладная дискретная математика. 2024. № 66. С. 60–77.

Атака на BKM-KK

Статья	Протокол	Угроза	Идея
[18]	BKM-KK	AUTH-I	Навязывание эфемерного ключа инкапсуляции



18. Алексеев Е.К., Кяжин С.Н., Смышляев С.В. Атаки на протоколы аутентифицированной выработки общего ключа при навязывании будущих открытых эфемерных ключей // Прикладная дискретная математика. 2024. № 66. С. 60–77.

Атака на BKM-KK. Меры защиты

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

1. Вычисление MAC:
   a. Подделка подписи

Атаки, применимые к pqRTLS12 и устранимые криптографическими методами

Протокол	Угроза	Меры защиты
BKM-KK	AUTH-I	Подпись в последней пересылке

Заключение

В ходе обзора рассмотрена 21 атака на 16 протоколов.

Среди рассмотренных атак:

- 10 атак не применимы к pqRTLS12;
- 3 атаки являются модельными;
- 6 атак применимы к pqRTLS12 и устранимы при помощи организационно-технических мер, идеи эти атак:
  - компрометация закрытого ключа шифрования или ключа декапсуляции;
  - компрометация промежуточного закрытого значения (результата декапсуляции или расшифрования);
- 1 атака применимы к pqRTLS12 и устранимы криптографическими методами:
  - внесением изменений в протокол (необходимо изменить способ формирования имитовставки).

Протокол	Угроза	Меры защиты
BKM-KK	BUKS	KDF с идентификаторами
Kyber-AKE	UUKS	
BGN	UUKS	
SSH	UUKS	
Oakley	BUKS	
PQXDH	SEC	Привязка подписи к сеансу
mMAKEP-JC	AUTH-I	KDF с транскрипцией
G2×KEM+DH	AUTH-R	
AKA	AUTH-I	Подпись транскрипции
KF	KCI	IND-CCA стойкий KEM
WC-MAKEP	AUTH-I	Модельная, неприменима
WC-MAKEP-2	SEC	
π	AUTH-I	
π	KCI	Защищенное хранение ключа
ES-MAKEP	SEC	
TLS-RSA	PFS	
PQXDH	AUTH-R	
GC	SEC	Защищенное хранение случайностей
GC	AUTH-R	Требования к аппаратной реализации
	AUTH-I	
BKM-KK	AUTH-I	Подпись в последней пересылке

Спасибо
за внимание!

РусКрипто
XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Мухортова Алена Андреевна
ООО «КРИПТО-ПРО»
mukhortova@cryptopro.ru

Источники литературы

1. Алексеев Е.К., Кяжин С.Н., Смышляев С.В, Мухортова А.А. Об угрозе UKS и влиянии на ее реализуемость возможности получения и навязывания будущих эфемерных ключей честных сторон // CTCrypt Pre-proceedings. 2026 (coming soon).
2. Cremers C., Dax A., Medinger N. Keeping Up with the KEMs: Stronger Security Notions for KEMs and automated analysis of KEM-based protocols. //CCS '24: Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. 2024. pp. 1046-1060
3. Choo K.K.R. Key establishment : proofs and refutations. PhD thesis, Queensland University of Technology. 2006.
4. Abadi M. Explicit communication revisited: two new attacks on authentication protocols // IEEE Transactions on Software Engineering. 1997, vol. 23, no. 3, pp. 185–186.
5. Chen L., Tang Q. Bilateral Unknown Key-Share Attacks in Key Agreement Protocols // Cryptology ePrint Archive. Paper 2007/209.
6. Bhargavan K., Jacomme C., Kiefer F., Schmidt R. Formal verification of the PQXDH Post-Quantum key agreement protocol for end-to-end secure messaging //USENIX Security. 2024.
7. Choo K.K.R., Boyd C., Hitchcock Y. The importance of proofs of security for key establishment protocols: Formal analysis of Jan–Chen, Yang–Shen–Shieh, Kim–Huh–Hwang–Lee, Lin–Sun–Hwang, and Yeh–Sun protocols // Computer Communications. 2006. Vol. 29, issue 15, pp. 2788–2797.
8. Chatterjee, S., Menezes, A., Ustaoglu, B. (2009, December). Reusing static keys in key agreement protocols. In International Conference on Cryptology in India (pp. 39-56). Berlin, Heidelberg: Springer Berlin Heidelberg.
9. Abadi M. Explicit communication revisited: two new attacks on authentication protocols // IEEE Transactions on Software Engineering. 1997, vol. 23, no. 3, pp. 185–186.
10. Yang Z., Chen Y., Luo S. Two-message Key Exchange with Strong Security from Ideal Lattices. // Cryptology ePrint Archive, Paper 2018/361, 2018.
11. Yoneyama, K. One-round authenticated key exchange without implementation tricks // Journal of Information Processing, 2016, 24(1), 9-19.
12. Toorani M. (2015). On Continuous After-the-Fact Leakage-Resilient Key Exchange. 10.13140/RG.2.1.3064.6486.
13. Li, Y. (2016). Design and analysis of cryptographic protocols (Doctoral dissertation, Bochum, Ruhr-Universit¨at Bochum, Diss., 2015).
14. He Y.J., Lee M.C. Towards a Secure Mutual Authentication and Key Exchange Protocol for Mobile Communications // 10.1109/WIOPT.2008.4586068., 225 - 231. 2008.
15. Basin D., Cremers C., Horvat M. Actor Key Compromise: Consequences and Countermeasures // Proceedings IEEE 27th Computer Security Foundations Symposium, 2014, pp. 244–258.
16. Yoneyama, K. One-round authenticated key exchange without implementation tricks // Journal of Information Processing, 2016, 24(1), 9-19.
17. Hu, X. X., Wei, J. H., Ye, M. (2013). Cryptanalysis of a strongly secure authenticated key exchange protocol. Journal of Electronics and Informatics 2278-2282.
18. Алексеев Е.К., Кяжин С.Н., Смышляев С.В. Атаки на протоколы аутентифицированной выработки общего ключа при навязывании будущих открытых эфемерных ключей // Прикладная дискретная математика. 2024. № 66. С. 60–77.