Способы интеграции квантовых ключей в протоколы IPsec, TLS 1.3 и IPlir

Бородин Михаил Алексеевич

АНО «НТЦ ЦК»*, АО «ИнфоТеКС»

*Работа выполнена коллективом авторов по заказу АНО «НТЦ ЦК»

infotecs

РусКрипто 2025

Первый этап

(Постановка задачи. Предварительные результаты)

АКТУАЛЬНОСТЬ ЗАДАЧИ

Неотъемлемой частью большинства криптографических протоколов являются секретные ключи.

Секретные ключи в протоколе

Распределены заранее

- Требуется физическая доставка ключей на устройство, что существенно сужает список сценариев применения.
- Высокая безопасность, но требуется доверие к администратору/курьеру.

Выработаны в процессе выполнения протокола

- Безопасность большинства протоколов с выработкой ключа опирается на предположение о вычислительной трудоемкости (в классической модели вычислений) некоторых математических задач. В случае появления достаточно мощного квантового вычислителя решение таких задач станет возможным за обозримое время.
- Постквантовые алгоритмы имеют эксплуатационные ограничения, связанные с размером ключей и/или с требуемыми объемом вычислений. Кроме того, нуждаются во всесторонних криптографических исследований.

АКТУАЛЬНОСТЬ ЗАДАЧИ

Возможной альтернативой упомянутым способам является использование в криптографических протоколах ключей, полученных по технологии КРК (далее КЗК – квантовозащищенные ключи).

Предпосылки использования КРК:

- Распределение ключей может происходить в автоматическом режиме, без участия администратора/курьера.
- КЗК являются независимыми, между ними отсутствует математическая связь. Полезно для организации «защиты от чтения назад» (PFS).
- Способ устойчив против «классического» и «квантового» нарушителя. В предельном случае возможно использование теоретико-информационно стойких криптографических методов.

Для интеграции КЗК были выбраны стандартизованные в России протоколы:

- IPsec, документы Р 1323565.1.035–2021 и Р 1323565.1.048–2023;
- TLS 1.3, документ Р 1323565.1.030-2020;
- IPlir, документ Р 1323565.1.034–2020.

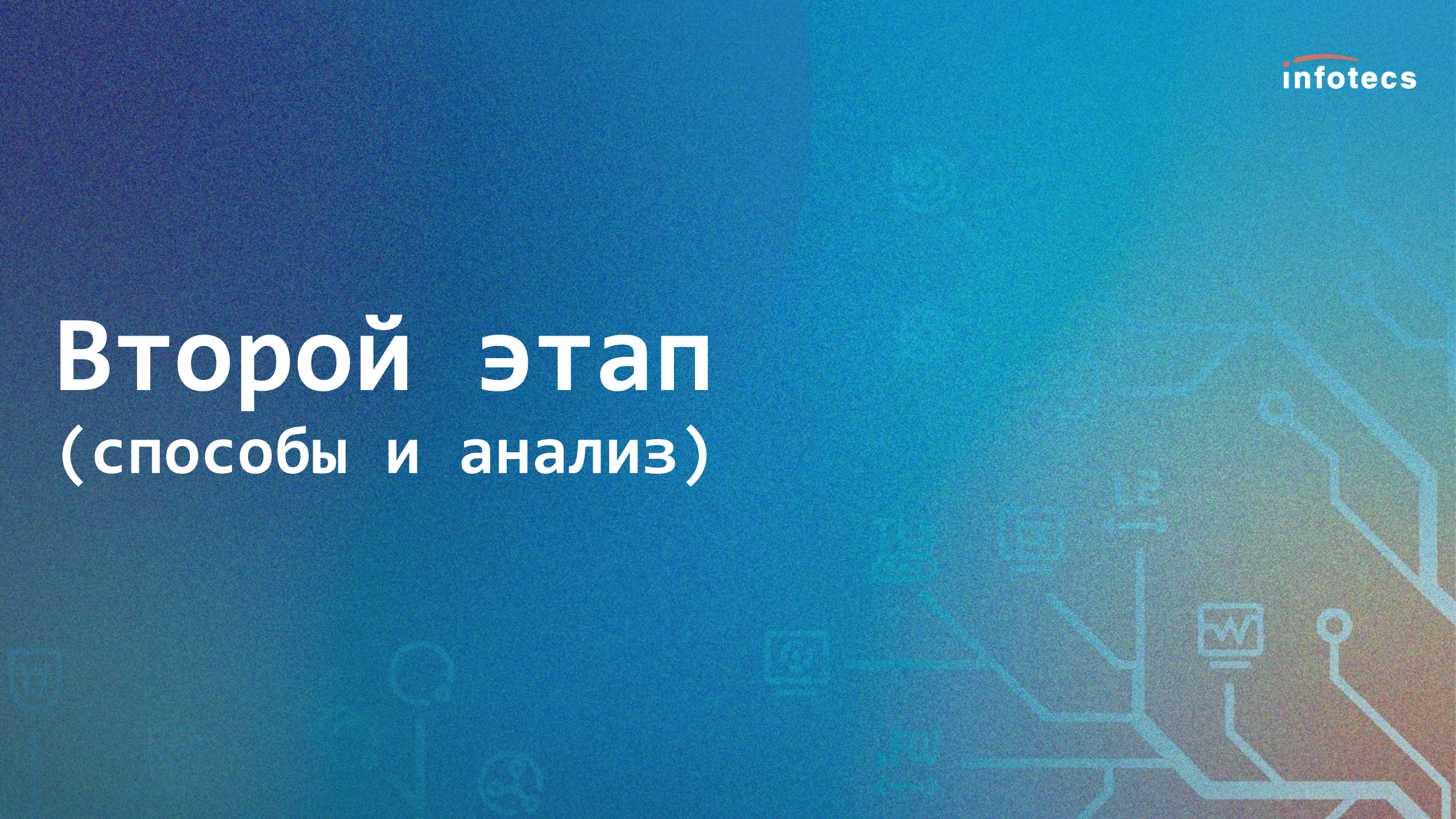
Результаты первого этапа

На первом этапе изучалась целесообразность интеграции КЗК в протоколы. Были рассмотрены доступные материалы о добавлении дополнительных ключей в протоколы: патенты, стандарты, рекомендации, статьи.

- Найденные способы были проанализированы на качественном уровне: исследованы криптографические качества и эксплуатационные свойства.
- Была отобрана группа наиболее перспективных способов с целью дальнейшей проработки на втором этапе.
- Подробнее о результатах докладывалось на РусКрипто 2024: «Подходы к интеграции технологии квантового распределения ключей в протоколы сетевой защиты данных».

В результате для выбранных способов было показано, что интеграция КЗК в протоколы позволяет улучшить криптографические качества этих протоколов и не приводит к существенной деградации их эксплуатационных свойств.

Второй этап
(способы и анализ)



Разработка предложений. IPsec

IKE_SA_INIT(SPI_i, SA_{i1}, KE_i, N_i) →	
	← **IKE_SA_INIT**($SPIr_r$, SA_{r1}, KE_r, N_r)
$SKEYSEED = prf(N_i \| \| N_r, K_{ir})$; $SK_d \| \| SK_{ai} \| \| SK_{ar} \| \| SK_{ei} \| \| SK_{er} \| \| SK_{pi} \| \| SK_{pr} = prf+(SKEYSEED, N_i \| \| N_r \| \| SPI_i \| \| SPI_r)$.	
$BLOB_i = MSG_i \| \| N_r \| \| prf(SK_{pi}, ID_i)$; либо $AUTH_i = SIGN_{Ki}(BLOB_i)$, либо $AUTH_i = prf(prf(PSK, "Key\ Pad\ for\ IKEv2"), BLOB_i)$.	$BLOB_r = MSG_r \| \| N_i \| \| prf(SK_{pr}, ID_r)$; либо $AUTH_r = SIGN_{Kr}(BLOB_r)$, либо $AUTH_r = prf(prf(PSK, "Key\ Pad\ for\ IKEv2"), BLOB_r)$.
IKE_AUTH ({ID_i, [CERT,] [ID_r,] $AUTH_i$, SA_{i2}}) →	
	← **IKE_AUTH** ({ID_r, [CERT,] $AUTH_r$, SA_{r2}})
Соединения IKE SA и IPsec SA созданы	
CREATE_CHILD_SA ({SA_i, N_i, [KE_i]}) →	
	← **CREATE_CHILD_SA** (SA_r, N_r, [KE_r])
либо $SKEYSEED = prf(SK_d, K_{ir} \| \| N_i \| \| N_r)$, либо $KEYMAT = prf+(SK_d, [K_{ir}] \| \| N_i \| \| N_r)$.	

Разработка предложений. IPsecQ

IKE_SA_INIT(SPI_i, SA_{i1}, KE_i, N_i, КЗК?) →	
	← **IKE_SA_INIT**(SPI_r, SA_{r1}, KE_r, N_r, КЗК!)
SKEYSEED = *prf* (N_i||N_r, K_{ir});	SK_d||SK_{ai}||SK_{ar}||SK_{ei}||SK_{er}||SK_{pi}||SK_{pr} = prf+(SKEYSEED, N_i||N_r||SPI_i||SPI_r).
PPK_Conf($КЗК_j$) = msb_{64}(prf($КЗК_j$,N_i||N_r||SPI_i||SPI_r)); **IKE_INTERMEDIATE**({Список КЗК_ID, Список PPK_Conf}) →	
	Проверка значений PPK_Conf; ← **IKE_INTERMEDIATE**({идентификатор КЗК})
SKEYSEED_TEMP = prf+(КЗК, SK_d);	SK_d||SK_{ai}||SK_{ar}||SK_{ei}||SK_{er}||SK_{pi}||SK_{pr} = prf+(SKEYSEED_TEMP, N_i||N_r||SPI_i||SPI_r).
$IntAuth_i$ = prf(SK_{pi}, 0||IKE_INTER_i), $IntAuth_r$ = prf(SK_{pr}, 0||IKE_INTER_r), $BLOB_i$ = MSG_i||N_r||prf(SK_{pi}, 1||ID_i)||$IntAuth_i$||$IntAuth_r$||MSGID, либо $AUTH_i$ = $SIGN_{Ki}$($BLOB_i$), либо $AUTH_i$ = prf (prf (PSK, "*Key Pad for IKEv2*"), $BLOB_i$).	$IntAuth_i$ = prf(SK_{pi}, 0||IKE_INTER_i), $IntAuth_r$ = prf(SK_{pr}, 0||IKE_INTER_r), $BLOB_r$ = MSG_r||N_i||prf(SK_{pr}, 1||ID_r)||$IntAuth_i$||$IntAuth_r$||MSGID либо $AUTH_r$ = $SIGN_{Kr}$($BLOB_r$), либо $AUTH_r$ = prf (prf (PSK, "*Key Pad for IKEv2*"), $BLOB_r$).
IKE_AUTH ({ID_i, [CERT,] [ID_r,] $AUTH_i$, SA_{i2}}) →	
	← **IKE_AUTH** ({ID_r, [CERT,] $AUTH_r$, SA_{r2}})
Соединения IKE SA и IPsec SA созданы	
CREATE_CHILD_SA ({SAi, Ni, [KEi], Список КЗК_ID, PPK_Conf}) →	
	← **CREATE_CHILD_SA** ({SAr, Nr, [KEr], идентификатор КЗК})
SK_d_TEMP = prf+(КЗК, SK_d), либо SKEYSEED = prf(SK_d_TEMP, K_{ir} || N_i||N_r), либо KEYMAT = prf+(SK_d_TEMP, [K_{ir}] || N_i||N_r).	

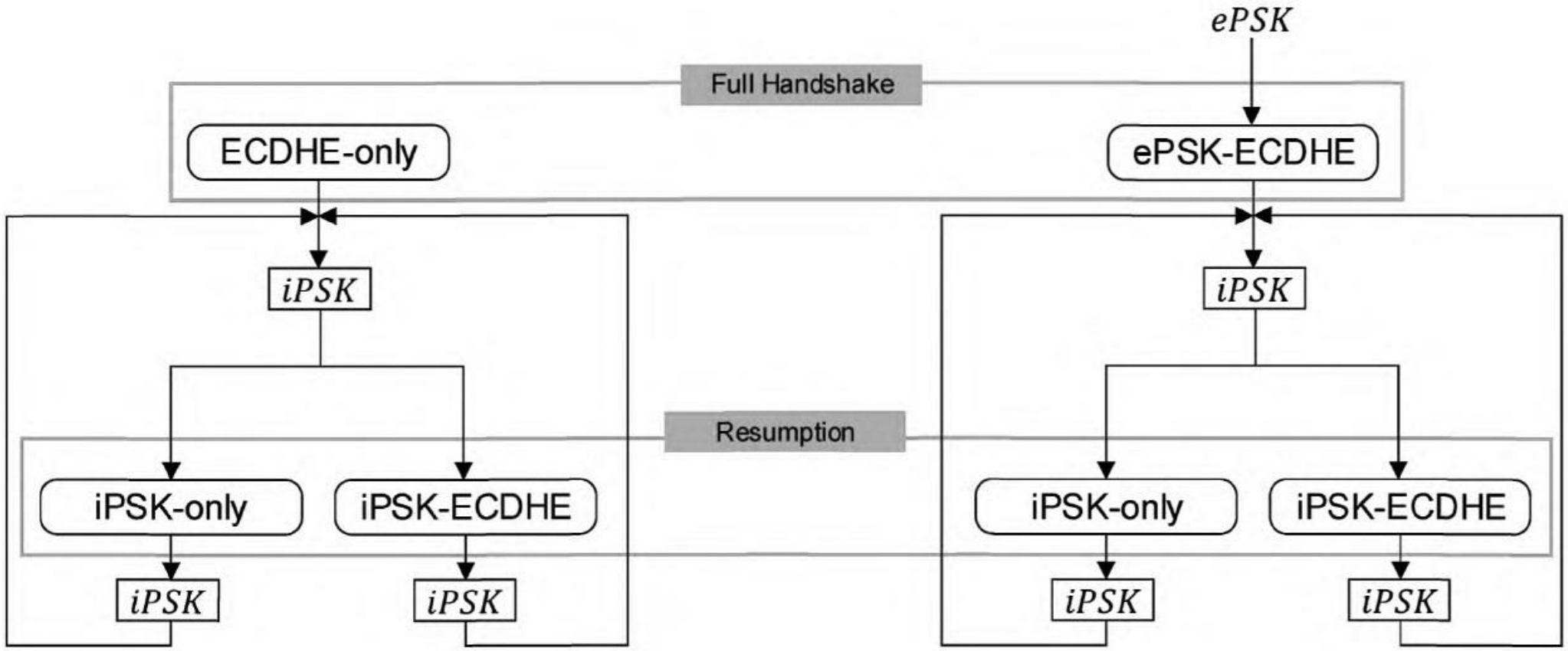
Разработка предложений. IPsecQ*

Требования по идентификации КЗК

- В рамках предлагаемого способа каждому участнику известен свой идентификатор.
- Каждому КЗК, используемому в протоколе, сопоставлены:
  - идентификаторы пары участников (ID_i и ID_r),
  - уникальный идентификатор КЗК в рамках пары участников (ppkid).
- Для каждой из сторон протокола ppkid однозначно задает другого участника (ID_i, ppkid) → ID_r и (ID_r, ppkid) → ID_i.

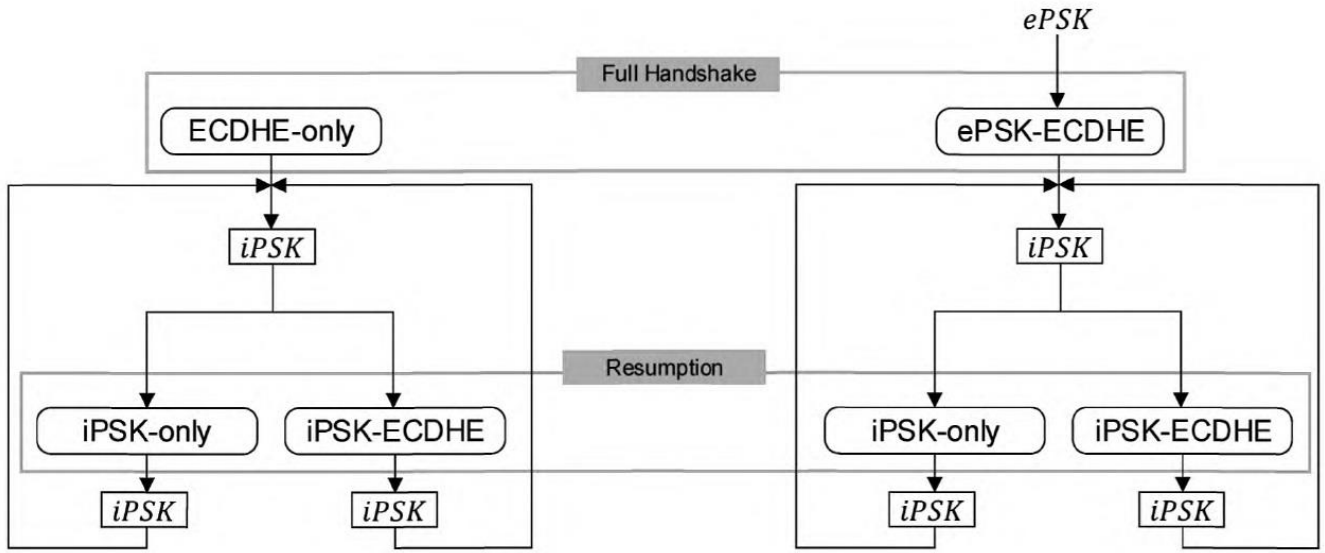
*Способ основан на draft-ietf-ipsecme-ikev2-qr-alt-06

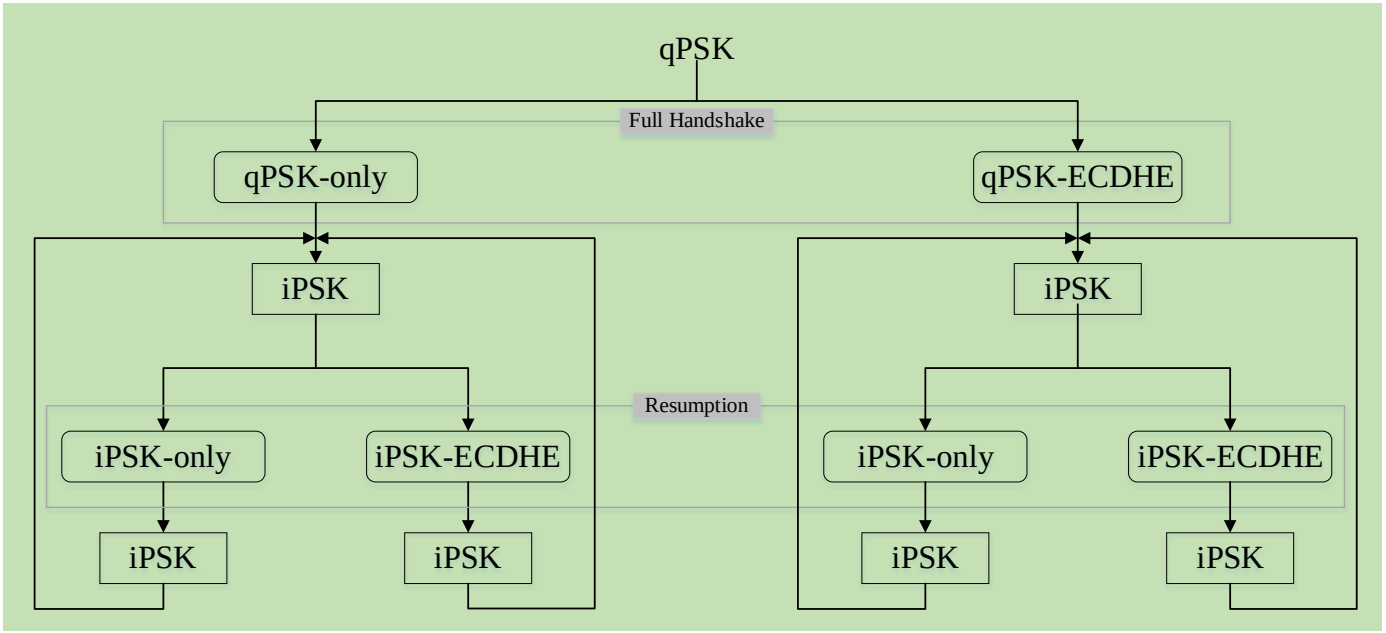
Разработка предложений. TLS 1.3



Режим **ePSK-only** в **Р 1323565.1.030 - 2020** отсутствует (запрещен в виду возможных атак).

Разработка предложений. TLSQ 1.3





qPSK (КЗК) – «ключ со справкой о благородном происхождении».

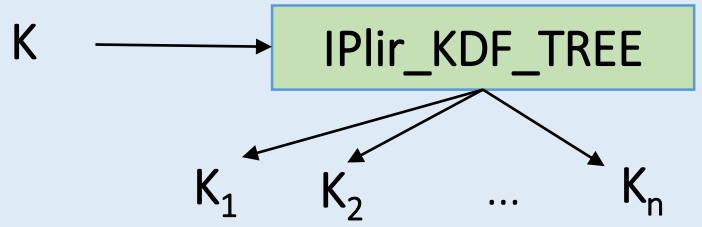
Требования к qPSK:

- каждому qPSK однозначно сопоставляется пара участников протокола и qPSK известен только этой паре участников;
- для каждого qPSK фиксируется роль каждого участника в протоколе (клиент или сервер);
- в рамках пары участников и их ролей qPSK соответствует уникальный идентификатор.

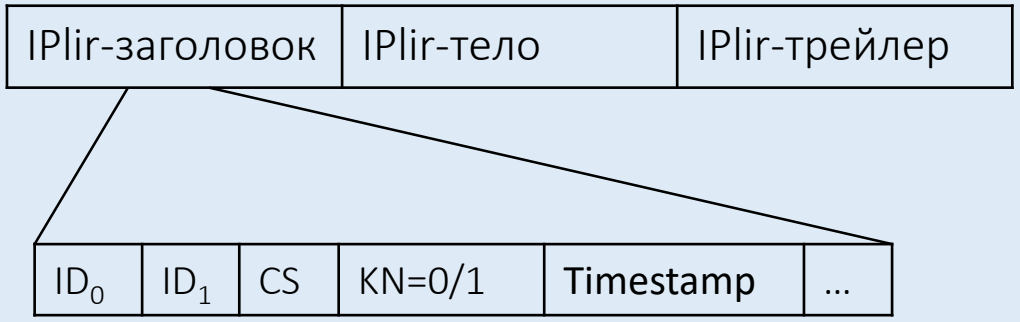
Разработка предложений. IPlir и IPlirQ

IPlir

Вычисление ключей:

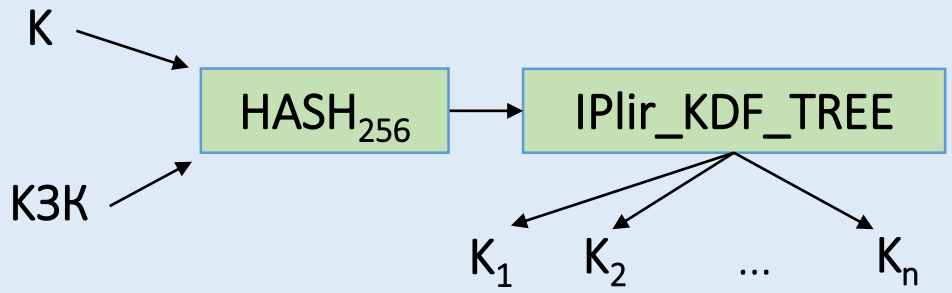


Защищенное сообщение:



IPlirQ

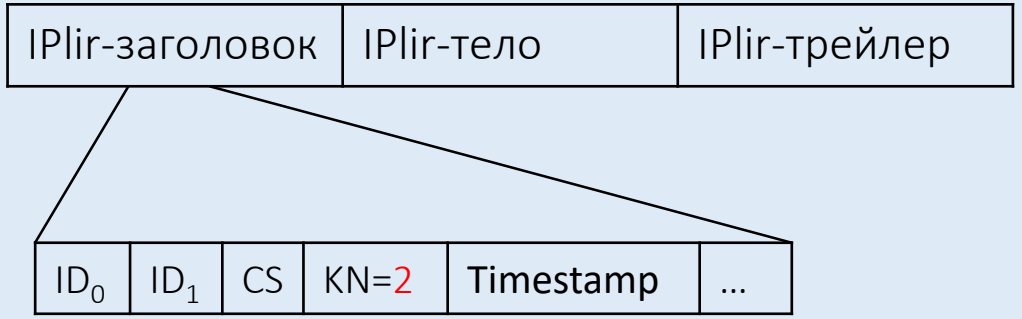
Вычисление ключей:



$Hash_{256}(K||КЗК||"HYBKEY"||ID_0||ID_1||CS||QKStartTime)$

Размер K и КЗК – 256 бит

Защищенное сообщение:



Анализ разработанных способов

Эксплуатационные свойства

- Все предложенные способы требуют своевременную доставку КЗК обоим участникам протокола. В протоколах IPsecQ и TLSQ 1.3 допускается использование одного и того же КЗК в разных соединениях, что несколько аннигилирует указанную зависимость. Для протокола IPlirQ указанная зависимость выражается в необходимости получить новый КЗК до установленного времени.
- В предложенных способах предусмотрен режим работы совместимый с оригинальными протоколами.
- Предложенные способы имеют схожую вычислительную сложность с оригинальными протоколами.

Анализ разработанных способов

Криптографические качества. (t, ε)-секретность

- Ключ является (t, ε)-секретным, если для любого противника **с вычислительными ресурсами t** величина преобладания в задаче различения этого ключа от «идеального» не превосходит ε.
- Ключ является ε-секретным, если для любого противника **с любыми вычислительными ресурсами** величина преобладания в задаче различения этого ключа от «идеального» не превосходит ε.

Анализ разработанных способов

Криптографические качества. Гибридизация

- Если не накладывать требование о «совместимости», то в качестве функции гибридизации рекомендовано использовать однократное хэширование алгоритмом ГОСТ 34.11-2018.
- Показано, что HMAC-Стрибог и HKDF-Стрибог (из IPsec и TLS 1.3) являются (с некоторыми ограничениями) двойственными псевдослучайными функциями (dualPRF) и могут использоваться для гибридизации двух ключей.

Анализ разработанных способов

Криптографические качества. Анализ IPsecQ, TLSQ 1.3 и IPlirQ

Рассматриваемые протоколы состоят из двух частей:

- Протокол аутентифицированной выработки общего ключа для протоколов IPsecQ и TLSQ. Некая «надстройка» реализующая гибридизацию «классического» ключа и КЗК для IPlirQ.
- Протокол защиты целостности и секретности канала связи с использованием выработанного общего ключа – оригинальные протоколы ESP, Record и IPlir.

Доказательство стойкости проведено по каждой части каждого протокола.

Анализ разработанных способов

Криптографические качества. Протоколов ESP, Record и IPlir

- Доказательство стойкости протоколов проведено не только для «идеального» секретного ключа, но и для ключа, обладающим лишь свойством «(t, ε)-секретности».
- В итоге показано, что все три протокола обеспечивают свойства конфиденциальности и целостности.
  - Протоколы IPlir и ESP могут обеспечивать также защиту от повторного навязывания при реализации у получателя соответствующих механизмов проверки.
  - Протокол TLS 1.3 Record в обязательном порядке предоставляет защиту повторного навязывания, переупорядочивания и удаления сообщений.

Анализ разработанных способов

Криптографические качества. Протокол IKEv2Q

В ходе анализа IKEv2Q, рассматривались два случая:

- в первом допускалась компрометация КЗК;
- во втором допускалась компрометация ключей подписи/имитозащиты, а задача Диффи-Хеллмана не предполагалась сложной.

В обоих случаях показано, что предложенный способ **обеспечивает целевые свойства безопасности**, в частности:

- секретность сессионных ключей и их независимость от ключей иных сессий;
- явную взаимную аутентификацию сторон и ключей;
- анонимность (секретность) передаваемых в рамках трех обменов идентификаторов ключей и сторон.

Анализ разработанных способов

Криптографические качества. Протокол HandshakeQ

В результате анализа протокола HandshakeQ было показано, что

- обеспечивается взаимная аутентификация пары участников;
- вырабатываемые у участников сессионные ключи одинаковы, секретны и независимы от ключей, сформированных в иных сессиях и на иных этапах сессии;
- так как КЗК в схеме qPSK-only используется однократно или ограниченное число раз, то это позволяет сократить потенциальный ущерб от его компрометации. В этом смысле использование КЗК частично обеспечивает свойство «forward secrecy».

Анализ разработанных способов

Криптографические качества. Протокол IPlirQ

В результате анализа протокола IPlirQ было показано, что

- При использовании КЗК протокол обеспечивает конфиденциальность, целостность и защиту от повторов;
- Протокол «приобрел» устойчивость к раскрытию/навязыванию ключевого материала.
  - Протокол остается стойким при навязывании или «классического» ключа, или последовательности КЗК.
  - Навязывание одновременно «классического» ключа и КЗК, приводит к потере свойств безопасности, в то же время, протоколом обеспечивается защита сообщений, которые были или будут сформированы с использованием иных секретных КЗК (при том же раскрытом/навязанном «классическом» ключе). Таким образом, в указанном выше смысле протокол обеспечивает «forward secrecy» и «backward secrecy».

Заключение

В результате была подтверждена целесообразность интеграция КЗК в протоколы IPsec, TLS 1.3 и IPlir, указанными способами.

Спасибо за внимание

Подписывайтесь
на наши соцсети,
там много интересного

infotecs

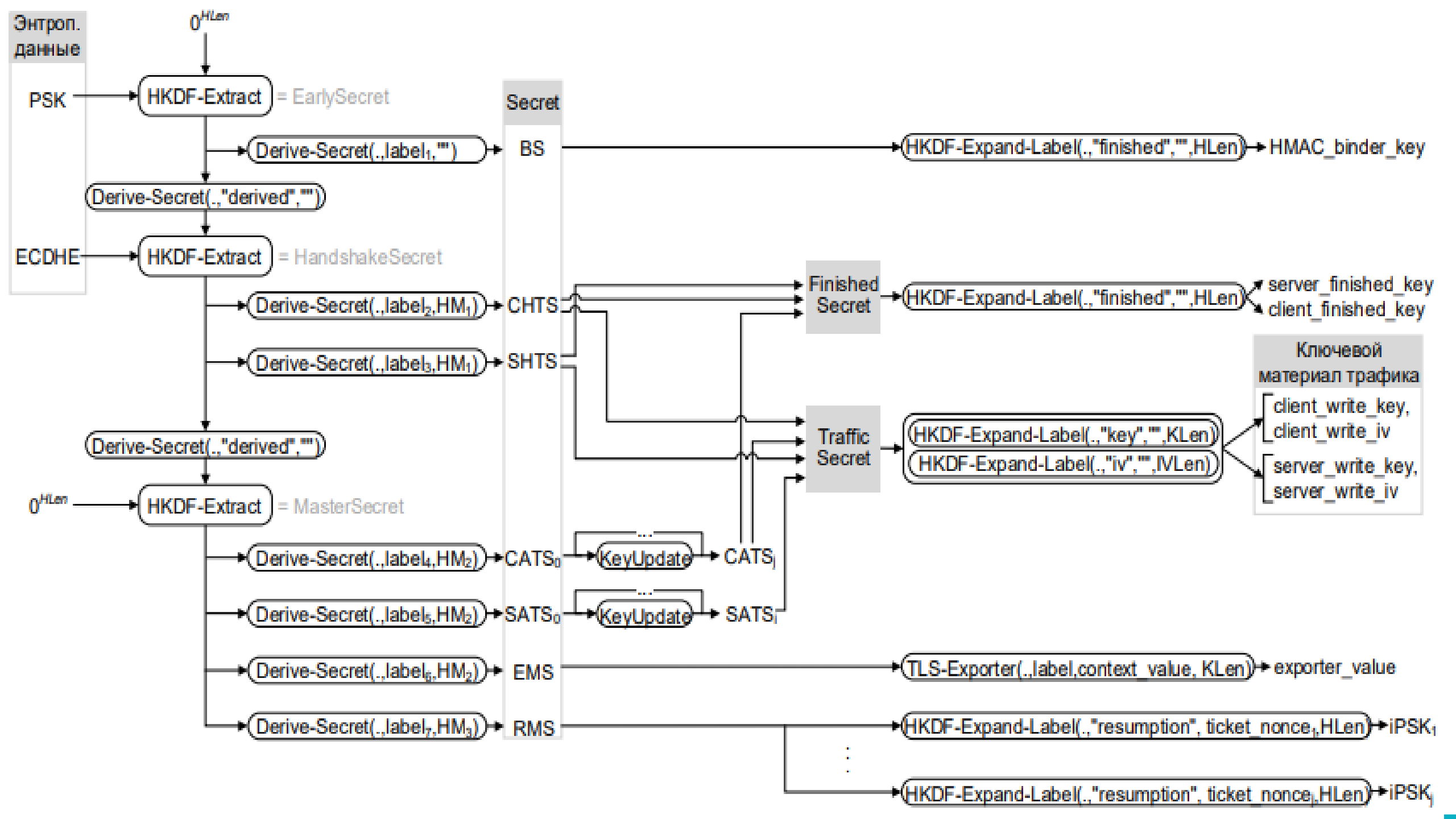
Mikhail.Borodin@infotecs.ru

Направление дальнейших исследований

В качестве дальнейших направлений исследований можно выделить следующие:

- исследование криптографических качеств предложенных способов в «классических» расширенных моделях безопасности, например, в модели MultiStage;
- разработка предложений по использованию постквантовых алгоритмов распределения ключей в представленных способах.

Модель				Решение
HYB	OT	1	KMA	XOR
	OT	1	CMA	XOR
	OT	N	KMA	XOR-then-PRF
	OT	N	CMA	XOR-then-PRF
	LT	1	KMA	HybHash
	LT	1	CMA	HybHash
	LT	N	KMA	HybHash
	LT	N	CMA	HybHash


Энтроп. данные
0^{HLen}
PSK
HKDF-Extract
= EarlySecret
Secret
Derive-Secret(.,label$_1$,"")
BS
HKDF-Expand-Label(.,"finished","",HLen)
HMAC_binder_key
Derive-Secret(.,"derived","")
ECDHE
HKDF-Extract
= HandshakeSecret
Derive-Secret(.,label$_2$,HM$_1$)
CHTS
Finished Secret
HKDF-Expand-Label(.,"finished","",HLen)
server_finished_key
client_finished_key
Derive-Secret(.,label$_3$,HM$_1$)
SHTS
Ключевой материал трафика
Traffic Secret
HKDF-Expand-Label(.,"key","",KLen)
HKDF-Expand-Label(.,"iv","",IVLen)
client_write_key, client_write_iv
server_write_key, server_write_iv
Derive-Secret(.,"derived","")
0^{HLen}
HKDF-Extract
= MasterSecret
Derive-Secret(.,label$_4$,HM$_2$)
CATS$_0$
KeyUpdate
CATS$_j$
Derive-Secret(.,label$_5$,HM$_2$)
SATS$_0$
KeyUpdate
SATS$_j$
Derive-Secret(.,label$_6$,HM$_2$)
EMS
TLS-Exporter(.,label,context_value, KLen)
exporter_value
Derive-Secret(.,label$_7$,HM$_2$)
RMS
HKDF-Expand-Label(.,"resumption", ticket_nonce$_1$,HLen)
iPSK$_1$
HKDF-Expand-Label(.,"resumption", ticket_nonce$_j$,HLen)
iPSK$_j$

Анализ разработанных способов

Определение. Вариационным (статистическим) расстоянием между распределениями D_0 и D_1, определенными на конечном множестве X, назовем величину

$$SD(D_0, D_1) = \frac{1}{2}\sum_{x \in X} |D_0(x) - D_1(x)| .$$

Наиболее важным случай, когда одно из распределений является равномерным (U).

Каждому распределению D на множестве X однозначным образом сопоставляем вероятностный алгоритм, заключающийся в выборе элемента $x \in X$ согласно распределению D.

Лемма. Преобладание любого противника *A* (в т.ч. с неограниченными вычислительными ресурсами), пытающегося различить распределение D_0 от распределения D_1, ограничено

$$Adv^{IND}_{D_0,D_1}(A) = \Pr\left(x \xleftarrow{R} D_0; A(x) \Rightarrow 1\right) - \Pr\left(x \xleftarrow{R} D_1; A(x) \Rightarrow 1\right) \leq SD(D_0, D_1).$$

Определение. Распределение D на множестве X, а равно порождаемые элементы $x \in X$, называем «ε-неотличимым» («ε-секретным»), если $SD(D, U) \leq \varepsilon$.

Аналогичным образом произвольный вероятностный алгоритм Alg называем «(t, ε)-неотличимым» (а результаты его работы «(t, ε)-секретными»), если преобладание любого противника с вычислительными ресурсами t ограничено $Adv^{IND}_{Alg,U}(t) \leq \varepsilon$.