

Ежегодная международная научно-практическая конференция  
«РусКрипто'2019»

# Принципы построения отечественных криптонаборов для TLS 1.3

Докладчик:

Евгений Алексеев,

Начальник отдела криптографических исследований,

ООО «КРИПТО-ПРО»

# Протокол TLS

- Протокол установления аутентифицированного защищенного канала связи
- Работает поверх протокола TCP
- Имеет двухуровневую структуру: над TCP работает Record, над Record работают все остальные протоколы
- Основная криптографическая составляющая:
  - протокол **Record** – протокол обеспечения защищенного двустороннего канала связи
  - протокол **Handshake** – протокол аутентифицированной выработки общего ключа.



# Протокол TLS

- Определяется документами IETF (rfc)
- Версии:
  - TLS 1.0 – rfc 2246 (1999 год)
  - TLS 1.1 – rfc 4346 (2006 год)
  - TLS 1.2 – rfc 5246 (2008 год)
  - TLS 1.3 – rfc 8446 (2018 год) + контрольные примеры rfc 8448 («Example Handshake Traces for TLS 1.3», 2019 год)
- Фиксированный каркас, возможность уточнять порядок работы с различными криптопримитивами в рамках криптонаборов (ciphersuites): rfc 5289 определяет криптонабор на основе AES, режима GCM и хэш-функции SHA256.

# Криптонаборы TLS 1.2 с российскими криптоалгоритмами

- В 2019 году, криптонаборы для TLS 1.2, основанные на российских криптоалгоритмах получили официальные номера IANA!
- IANA Transport Layer Security (TLS) Parameters:
  - TLS\_GOSTR341112\_256\_WITH\_KUZNYECHIK\_CTR\_OMAC – 0xC1, 0x00
  - TLS\_GOSTR341112\_256\_WITH\_MAGMA\_CTR\_OMAC – 0xC1, 0x01
  - TLS\_GOSTR341112\_256\_WITH\_28147\_CNT\_IMIT – 0xC1, 0x02

# Криптонаборы TLS 1.2 с российскими криптоалгоритмами

- Преимущества наличия номеров IANA:
  - Устранение возможности блокировки TLS с ГОСТ-ми из-за захвата номеров другими криптонаборами;
  - Легитимизация поддержки российских криптонаборов в свободном ПО (например, в OpenSSL);
  - Снижение вероятности конфликтов с эволюционными изменениями в TLS;
  - Поддержка сторонним по отношению к реализациям TLS ПО (например, Wireshark).

# TLS 1.3

- Существенно переработан по сравнению с предыдущими версиями
- Учтены современные подходы к построения безопасных протоколов (возможность построения сведений к стойкости базовых криптопримитивов):
  - The key derivation functions have been redesigned. The new design allows easier analysis by cryptographers due to their improved key separation properties. The HMAC-based Extract-and-Expand Key Derivation Function (HKDF) is used as an underlying primitive.
- Особое внимание уделено обеспечению свойства Forward-Secrecy:
  - Static RSA and Diffie-Hellman cipher suites have been removed; all public-key based key exchange mechanisms now provide forward secrecy.

# Вариативность в TLS 1.3

**Блочный шифр**  
**ENTREE**

BABY COS SALAD  
WITH MARINATED CHICKEN STRIPS, TOASTED BREAD AND CLASSIC CAESAR DRESSING

SHREDDED DUCK SALAD  
WITH SHIITAKE MUSHROOMS, SPRING ONION AND BEAN THREAD NOODLES

**AEAD-режим**  
**MAINS**

SIRLOIN OF BEEF  
WITH ROASTED POTATOES, TOMATO, ONION, ROSEMARY AND GARLIC COMPOTE

GRILLED CHICKEN BREAST  
WITH CARAMELISED ONION, MASH POTATOES, TOMATOES, PEAS AND JUS

**Хэш-функция**  
**DESSERT**

STICKY DATE PUDDING  
WITH BUTTERSCOTCH SAUCE, VANILLA ICECREAM AND SWEET PASTRY

CHOCOLATE MACADAMIA BROWNIE  
WITH CHOCOLATE GARNISH AND COCONUT ICE CREAM

Криптонаборы в TLS 1.3

**AMERICAN DISH**

	Plain	w/ French Fried or Plain Fried Rice	w/ Roast pork or Chicken Fried Rice	w/ Beef or Shrimp Fried Rice
炸鸡翼 A1. Fried Chicken Wings(4)		5.95	6.25	7.35
炸鸡翼 A2. Buffalo Wings		6.25	6.75	7.55
炸鸡串 A4. Chicken Teriyaki(4)		4.95	5.95	6.75
炸鸡串 A5. Fried Baby Shrimp(12)		4.25	5.25	5.55
炸鸡块 A6. Fried Chicken Nuggets		3.95	4.95	5.75
薯条 A7. French Fries		(S)1.75 (L)2.95		

**APPETIZERS**

叉烧卷 1. Roast Pork Egg Roll(Each)	1.20
叉烧卷 2. Shrimp Egg Roll(Each)	1.35
叉烧卷 3. Vegetable Spring Roll(3)	2.50
叉烧卷 4. Beef Egg Roll(2)	2.50
炸春卷 5. Fried Pork Wonton(10)	2.75
炸春卷 6. B-B-Q Spare Ribs.....(S)1.95 (L)13.25	
炸春卷 7. Boneless Spare Rib.....(S)1.25 (L)9.95	
炸春卷 8. Pu Pu Platter.....	10.95
锅贴 9. Steamed or Fried Dumpling(10)	4.50
锅贴 10. Teriyaki Beef(4)	4.50
锅贴 11. Shrimp Toast(4)	2.95
锅贴 12. Fried Cheese Wonton(8)	2.95
锅贴 13. Fried Donuts(10)	10.95

**SOUP**

云吞汤 15. Wonton Soup	1.75 3.25
云吞汤 16. Egg Drop Soup	1.50 2.85
云吞汤 17. Chicken Rice (Hot) Soup	1.75 3.25
云吞汤 18. Wonton Soup	1.95 3.50
云吞汤 19. House Special Soup	2.15 4.15
云吞汤 20. House Special Soup	2.15 4.15
云吞汤 21. House Special Soup	1.75 3.25
云吞汤 22. House Special Soup	5.15

**CHOP SUEY**

鸡柳拼盘 23. Chicken Chop Suey	4.35 6.95
鸡柳拼盘 24. Beef Chop Suey	4.35 6.95
鸡柳拼盘 25. Beef Chop Suey	4.95 7.95
鸡柳拼盘 26. Shrimp Chop Suey	4.95 7.95
鸡柳拼盘 27. Vegetable Chop Suey	3.75 6.55
鸡柳拼盘 28. House Special Chop Suey	8.35

**FRIED RICE**

叉烧炒饭 29. Roast Pork Fried Rice	3.25 6.25
叉烧炒饭 30. Chicken Fried Rice	3.25 6.25
叉烧炒饭 31. Beef Fried Rice	3.95 7.15
叉烧炒饭 32. Shrimp Fried Rice	3.95 7.15
叉烧炒饭 33. Vegetable Fried Rice	3.50 6.50
叉烧炒饭 34. House Special Fried Rice	5.50
叉烧炒饭 35. Plain Fried Rice	1.95 3.95

**LO MEIN**

青菜捞面 36. Vegetable Lo Mein	3.05 5.95
青菜捞面 37. Plain Lo Mein	3.05 5.50
青菜捞面 38. Roast Pork Lo Mein	3.35 6.50
青菜捞面 39. Chicken Lo Mein	3.35 6.50
青菜捞面 40. Shrimp Lo Mein	3.95 7.25
青菜捞面 41. Beef Lo Mein	3.95 7.25
青菜捞面 42. House Special Lo Mein	4.50 7.55

**SEAFOOD**

什菜拼盘 78. Shrimp w. Mixed Veggies	8.25 10.25
什菜拼盘 79. Shrimp w. Lobster Sauce	6.25 10.25
什菜拼盘 80. Shrimp w. Black Beans	8.25 10.25
什菜拼盘 81. Shrimp w. Cashew Nuts	8.25 10.25
什菜拼盘 82. Shrimp w. Broccoli	8.25 10.25
什菜拼盘 83. Shrimp w. Broccoli	8.25 10.25
什菜拼盘 84. Curry Shrimp w. Onion	8.25 10.25
什菜拼盘 85. Szechuan Shrimp	(Order) 8.95
什菜拼盘 86. Kung Po Shrimp	(Order) 8.95
什菜拼盘 87. Shrimp w. Garlic Sauce	(Order) 8.95
什菜拼盘 88. Hunan Shrimp	(Order) 10.25

**EGG FOO YOUNG**

叉烧蛋卷 43. Roast Pork Egg Foo Young	6.95
叉烧蛋卷 44. Chicken Egg Foo Young	6.95
叉烧蛋卷 45. Shrimp Egg Foo Young	6.95
叉烧蛋卷 46. Beef Egg Foo Young	6.95
叉烧蛋卷 47. Vegetable Egg Foo Young	6.35

**SWEET & SOUR**

甜酸肉 48. Sweet & Sour Chicken	7.95
甜酸肉 49. Sweet & Sour Pork	7.95
甜酸肉 50. Sweet & Sour Shrimp	9.75

**PORK**

叉烧拼盘 51. Roast Pork w. Mixed Veggies	4.35 8.55
叉烧拼盘 52. Roast Pork w. Broccoli	4.35 8.55
叉烧拼盘 53. Pork w. Garlic Sauce	(Order) 8.55
叉烧拼盘 54. Szechuan Pork	(Order) 8.55
叉烧拼盘 55. Hunan Pork	(Order) 8.55
叉烧拼盘 56. Pork w. Cashew Nuts	(Order) 8.55

**BEEF**

什菜拼盘 57. Beef w. Mixed Veggies	4.85 8.75
什菜拼盘 58. Beef w. Mushrooms	4.85 8.75
什菜拼盘 59. Beef w. Broccoli	4.85 8.75
什菜拼盘 60. Pepper Steak w. Onion	4.85 8.75
什菜拼盘 61. Beef w. Broccoli	(Order) 8.75
什菜拼盘 62. Szechuan Beef	(Order) 8.75
什菜拼盘 63. Beef w. Garlic Sauce	(Order) 8.75
什菜拼盘 64. Hunan Beef	(Order) 8.75
什菜拼盘 65. Kung Po Beef	(Order) 8.75

**CHICKEN**

白菜鸡 66. Chicken w. Chinese Veg	4.55 8.55
白菜鸡 67. Chicken w. Cashew Nuts	4.55 8.55
白菜鸡 68. Moo Goo Gai Pan	4.55 8.55
白菜鸡 69. Chicken w. Black Bean Sc.	4.55 8.55
白菜鸡 70. Chicken w. Broccoli	4.55 8.55
白菜鸡 71. Chicken w. Broccoli	4.55 8.55
白菜鸡 72. Chicken w. Mixed Veggies	4.55 8.55
白菜鸡 73. Curry Chicken w. Onion	(Order) 8.55
白菜鸡 74. Chicken w. Broccoli	(Order) 8.55
白菜鸡 75. Kung Po Chicken	(Order) 8.55
白菜鸡 76. Chicken w. Garlic Sauce	(Order) 8.55
白菜鸡 77. Hunan Chicken	(Order) 8.55

**FREE**

2 Egg Rolls	3 Egg Rolls or Soda(2L)	4 Egg Rolls or Soda(2L)	General's Chicken
w. Order of \$20 or More only for dinner	w. Order of \$30 or More only for dinner	w. Order of \$40 or More only for dinner	w. Order of \$55 or More only for dinner

**COMBINATION PLATTER**

C 1. Chicken or Shrimp Chop Suey	7.15
C 2. Beef or Shrimp Lo Mein	7.25
C 3. Roast Pork or Chicken Egg Foo Young	7.15
C 4. Pepper Steak w. Onion	7.15
C 5. Roast Pork w. Mixed Vegetables	7.15
C 6. Chicken w. Cashew Nuts	7.15
C 7. Moo Goo Gai Pan	7.15
C 8. Bar-B-Q Spare Ribs	6.35
C 9. Shrimp w. Lobster Sauce	7.65
C 10. Sweet & Sour Pork or Chicken	7.15
C 11. Chicken w. Broccoli	7.15
C 12. Beef w. Broccoli	7.15
C 13. Shrimp w. Broccoli	7.65
C 14. Roast Pork or Chicken Lo Mein	7.15
C 15. Chicken or Beef w. Garlic Sauce	7.25
C 16. Shrimp w. Vegetables	7.65
C 17. Boneless Spare Ribs	7.65
C 18. Chicken or Beef w. Mixed Vegetables	7.15
C 19. General Tso's Chicken	7.35
C 20. Sesame Chicken	7.35
C 21. Hunan Chicken or Beef	7.35
C 22. Szechuan Chicken or Beef	7.35
C 23. Kung Pao Chicken	7.35
C 24. Hunan Triple Delight	7.75
C 25. Szechuan Shrimp	7.75
C 26. Orange Chicken	7.65
C 27. Shrimp w. Lobster Sauce	7.65
C 28. Hunan Shrimp	7.65
C 29. Mongolian Beef	7.55
C 30. House Special Lo Mein	7.55
C 31. Crispy Chicken	7.65
C 32. Honey Chicken	7.65

**CHOW MAI FUN**

豉汁炒粉 113. Chicken Chow Mai Fun	7.15
豉汁炒粉 114. Pork Chow Mai Fun	7.15
豉汁炒粉 115. Beef Chow Mai Fun	7.50
豉汁炒粉 116. Shrimp Chow Mai Fun	7.50
豉汁炒粉 117. Singapore Style Chow Mai Fun	7.95
豉汁炒粉 118. House Special Chow Mai Fun	7.95
豉汁炒粉 119. Vegetable Chow Mai Fun	6.25

**DIET SPECIAL**

D 1. Chicken Chow Mein	5.75
D 2. Steamed Chicken w. Mixed Vegetables	6.25
D 3. Steamed Shrimp w. Mixed Vegetables	7.25
D 4. Steamed Mixed Vegetables	5.25
D 5. Steamed Chicken w. Broccoli	6.50

**SEAFOOD**

海鲜大会 89. SEAFOOD DELIGHT	11.95
海鲜大会 90. CRISPY CHICKEN	8.95
全家福 91. HAPPY FAMILY	12.50
全家福 92. TRIPLE CROWN	9.95
全家福 93. HUNAN TRIPLE	9.95
全家福 94. HUNAN TRIPLE	9.95
全家福 95. SIZZLING STEAK & SCALLOPS	10.25
全家福 96. MONGOLIAN BEEF	9.25
全家福 97. MONGOLIAN BEEF	8.95
全家福 98. LEMON CHICKEN	7.50
全家福 99. FOUR SEASONS	9.75
全家福 100. DOUBLE DELIGHT	9.50
全家福 101. W. GARLIC SAUCE	10.25
全家福 102. SESAME SHRIMP	10.75
全家福 103. SESAME CHICKEN	9.25
全家福 104. ORANGE BEEF	9.25
全家福 105. HONEY CHICKEN	9.25
全家福 106. HONEY CHICKEN	8.95

**SIDE ORDER**

白饭 1. Steamed White Rice... (Pl.) 1.25 (Qt) 2.00	
粥 2. Fried Noodle..... (bag) 0.50	
甜品 3. Fortune Cookies(4)	0.50
热油 4. Hot Oil	0.20

Криптонаборы в TLS 1.2

# TLS 1.3 – строение и основные особенности

3 режима работы протокола Handshake:

- ECDHE-only
- PSK-only
- PSK-ECDHE

# TLS 1.3 – строение и основные особенности

Схема обмена сообщениями в режиме ECDHE-only протокола Handshake.

Клиент		Сервер
1-я фаза ключевого обмена		
ClientHello: • supported_versions • signature_algorithms • supported_groups • key_share	----->	
		ServerHello: supported_versions • key_share •
		EncryptedExtensions supported_groups* •
		CertificateRequest*: signature_algorithms •
		Certificate
		CertificateVerify
		Finished
	<-----	Application Data*
Certificate*		
CertificateVerify*		
Finished	----->	
Application Data	<----->	Application Data
	<-----	NewSessionTicket*
KeyUpdate*	<----->	KeyUpdate*

Используемая система обозначений:

-----*	– опциональные данные;
-----	– сообщения, защищенные на ключах, выработанных из секретного значения [sender]_handshake_traffic_secret (см. подробнее 8.4);
-----	– сообщения, защищенные на ключах, выработанных из секретного значения [sender]_application_traffic_secret_N (см. подробнее 8.4).

# TLS 1.3 – строение и основные особенности

Схема обмена сообщениями в режиме PSK-only протокола Handshake.

Клиент		Сервер
ClientHello <ul style="list-style-type: none"> <li>• supported_versions</li> <li>• [signature_algorithms]*</li> <li>• [key_share]*</li> <li>• [supported_groups]*</li> <li>• pre_shared_key</li> <li>• psk_key_exchange_modes</li> </ul>	----->	
		ServerHello <ul style="list-style-type: none"> <li>supported_versions •</li> <li>pre_shared_key •</li> </ul>
		EncryptedExtensions
		Finished
		Application Data*
Finished	----->	
Application Data	<-----	Application Data
	<-----	NewSessionTicket*
KeyUpdate*	<-----	KeyUpdate*

Используемая система обозначений:

*	– опциональные данные;
[]	– опциональное расширение, посылаемое клиентом в режиме восстановления соединения для обеспечения возможности перехода к Full Handshake;
■	– сообщения, защищенные на ключах, выработанных из секретного значения [sender]_handshake_traffic_secret (см. подробнее 8.4);
■	– сообщения, защищенные на ключах, выработанных из секретного значения [sender]_application_traffic_secret_N (см. подробнее 8.4).

# TLS 1.3 – строение и основные особенности

Схема обмена сообщениями в режиме PSK-ECDHE протокола Handshake.

Клиент		Сервер
ClientHello: <ul style="list-style-type: none"> <li>• supported_version</li> <li>• [signature_algorithms]*</li> <li>• key_share</li> <li>• supported_groups</li> <li>• pre_shared_key</li> <li>• psk_key_exchange_modes</li> </ul>	→	
		ServerHello: <ul style="list-style-type: none"> <li>• supported_versions</li> <li>• key_share</li> <li>• pre_shared_key</li> </ul>
		EncryptedExtensions: <ul style="list-style-type: none"> <li>• supported_groups*</li> </ul>
		Finished
	←	NewSessionTicket*
Finished	→	
Application Data	↔	Application Data
	←	NewSessionTicket*
KeyUpdate*	↔	KeyUpdate*

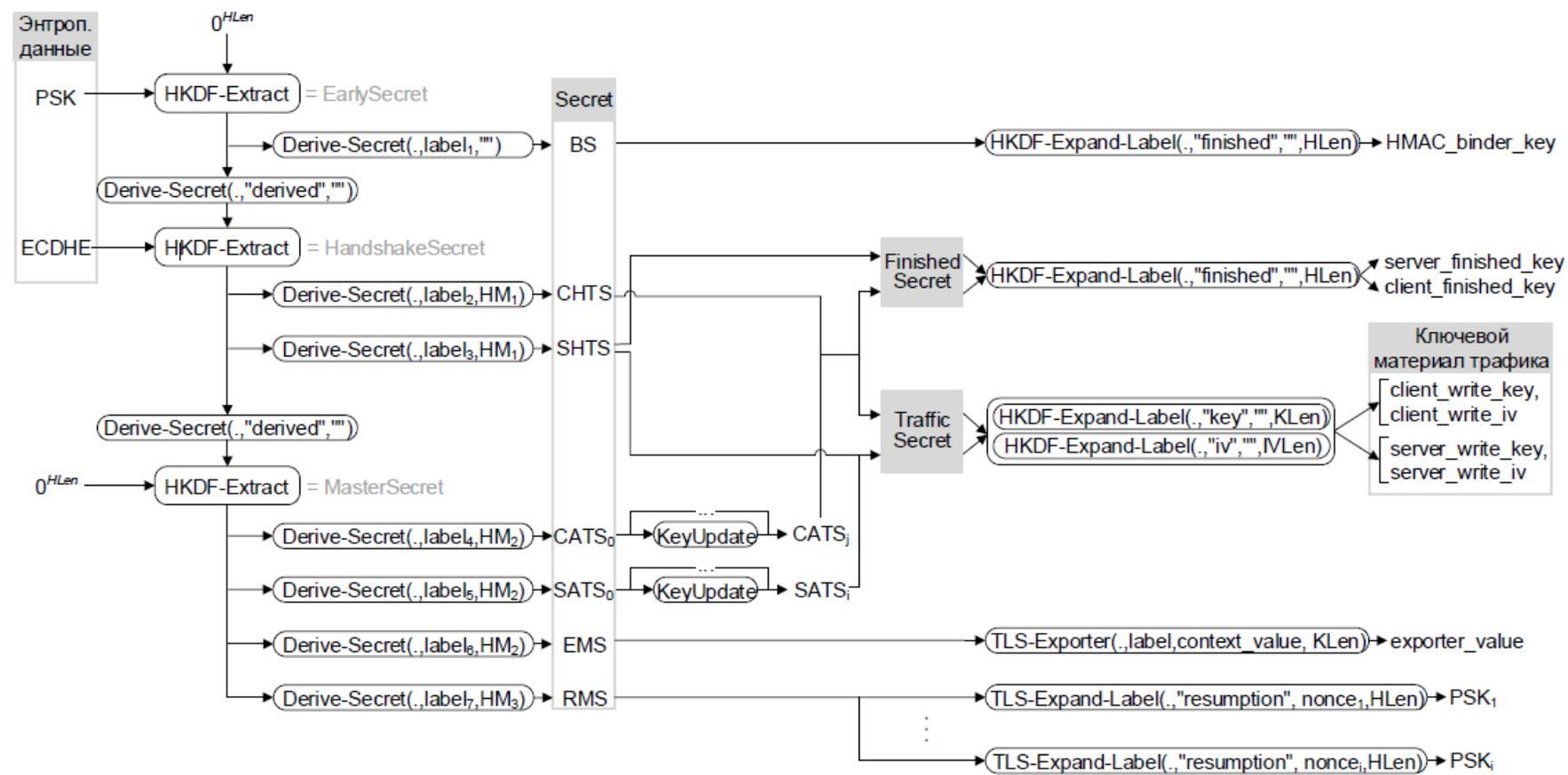
Используемая система обозначений:

*	– опциональные данные;
[]	– опциональное расширение, посылаемое клиентом в режиме восстановления соединения для обеспечения возможности перехода к Full Handshake;
■	– сообщения, защищенные на ключах, выработанных из секретного значения [sender]_handshake_traffic_secret (см. подробнее 8.4);
■	– сообщения, защищенные на ключах, выработанных из секретного значения [sender]_application_traffic_secret_N (см. подробнее 8.4).

# TLS 1.3 – строение и основные особенности

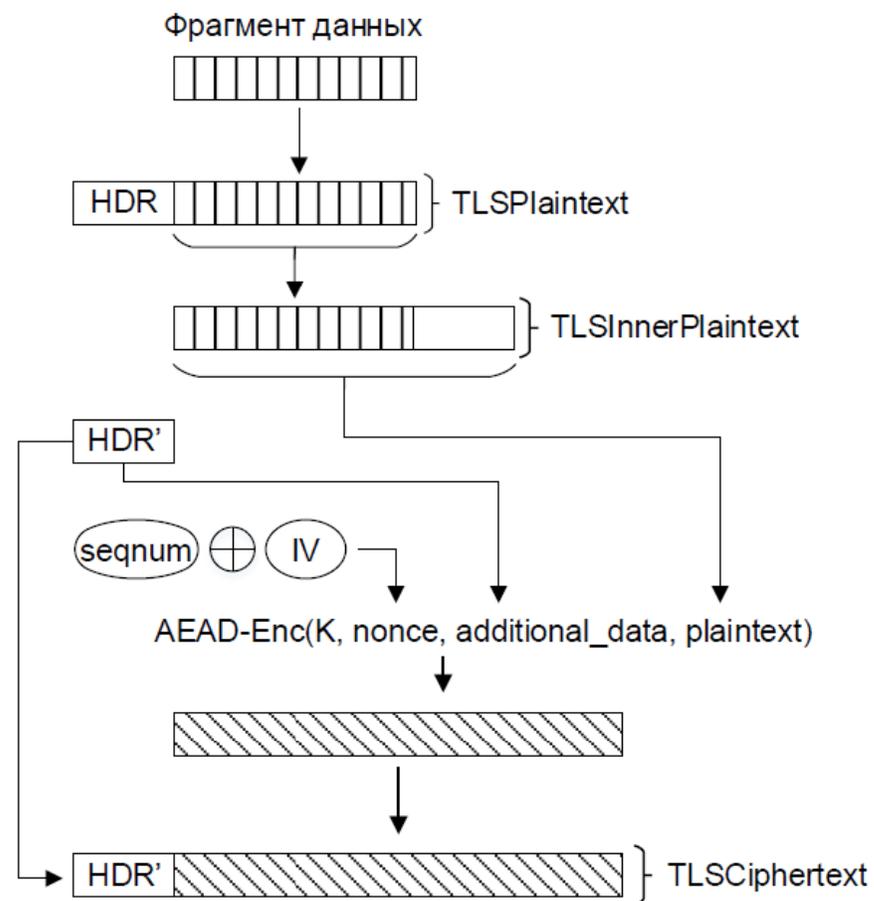
Дерево ключевого расписания в протоколе TLS 1.3:

Множество	Содержимое
$HM_1$	$\{ClientHello, \dots, ServerHello\}$
$HM_2$	$\{ClientHello, \dots, Finished \text{ со стороны сервера}\}$
$HM_3$	$\{ClientHello, \dots, Finished \text{ со стороны клиента}\}$



# TLS 1.3 – строение Record

Схема формирования защищенной записи в протоколе **Record**:



# TLS 1.3 – основные свойства Handshake

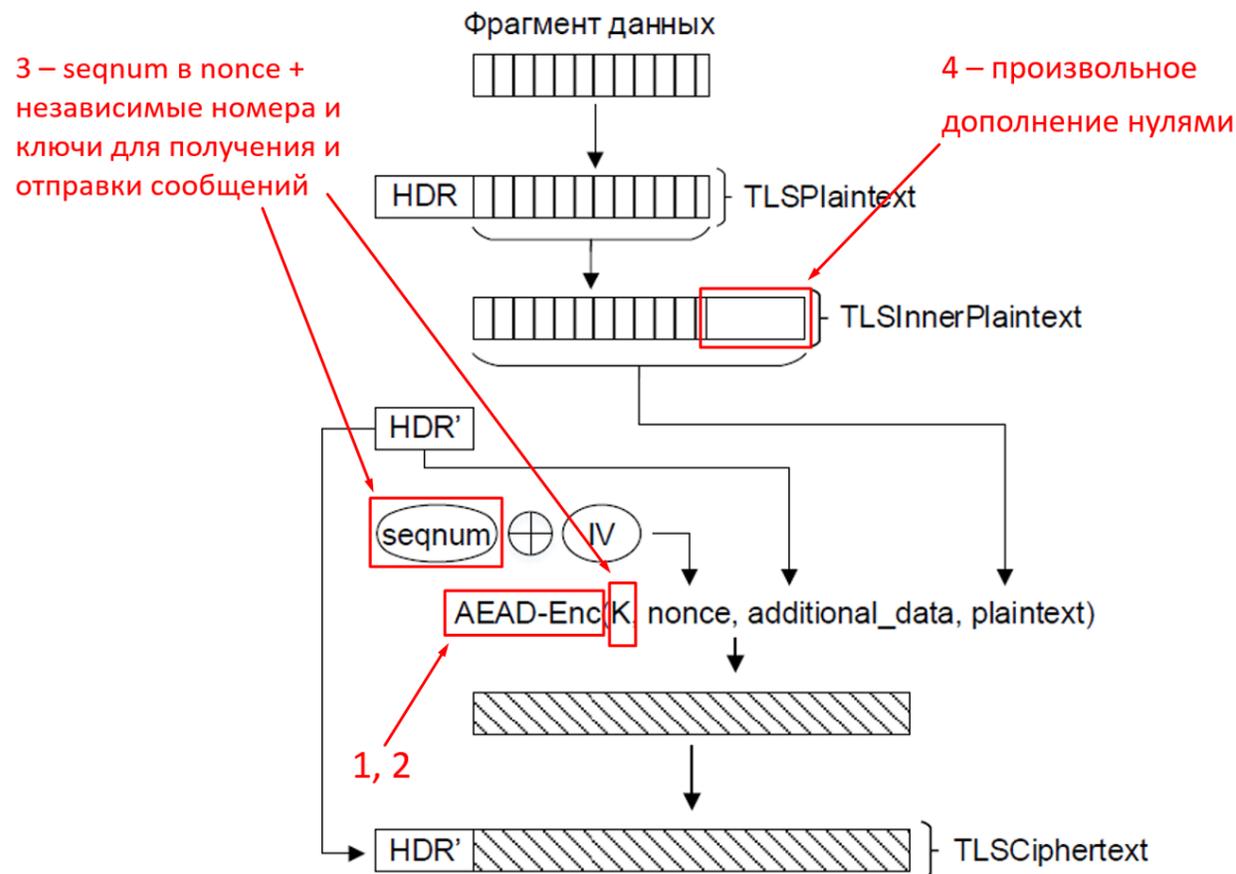
1. Установление одинаковых сессионных ключей
2. Секретность сессионных ключей
3. Аутентификация сторон
4. Уникальность и независимость ключей
5. Безопасность ранее установленных сессий при компрометации  
долговременных ключей (Forward Secrecy)
6. Стойкость в условиях KCI
7. Приватность

# TLS 1.3 – основные свойства Handshake

- 1, 2, 3 – стандартное свойство АКЕ-протоколов
- 4 – обеспечивается за счет структуры ключевого дерева («improved key separation properties»)
- 5, 6 – обеспечивается за счет использования долговременных ключей только для аутентификации вырабатываемых ключей (при подписи данных)
- 7 – обеспечивается за счет шифрование всех сообщений кроме ClientHello, ServerHello и HelloRetryRequest

# TLS 1.3 – основные свойства Record

1. Конфиденциальность
2. Целостность на уровне сообщений
3. Целостность на уровне потоков сообщений
4. Защита длины сообщений



# TLS 1.3 с российскими криптоалгоритмами

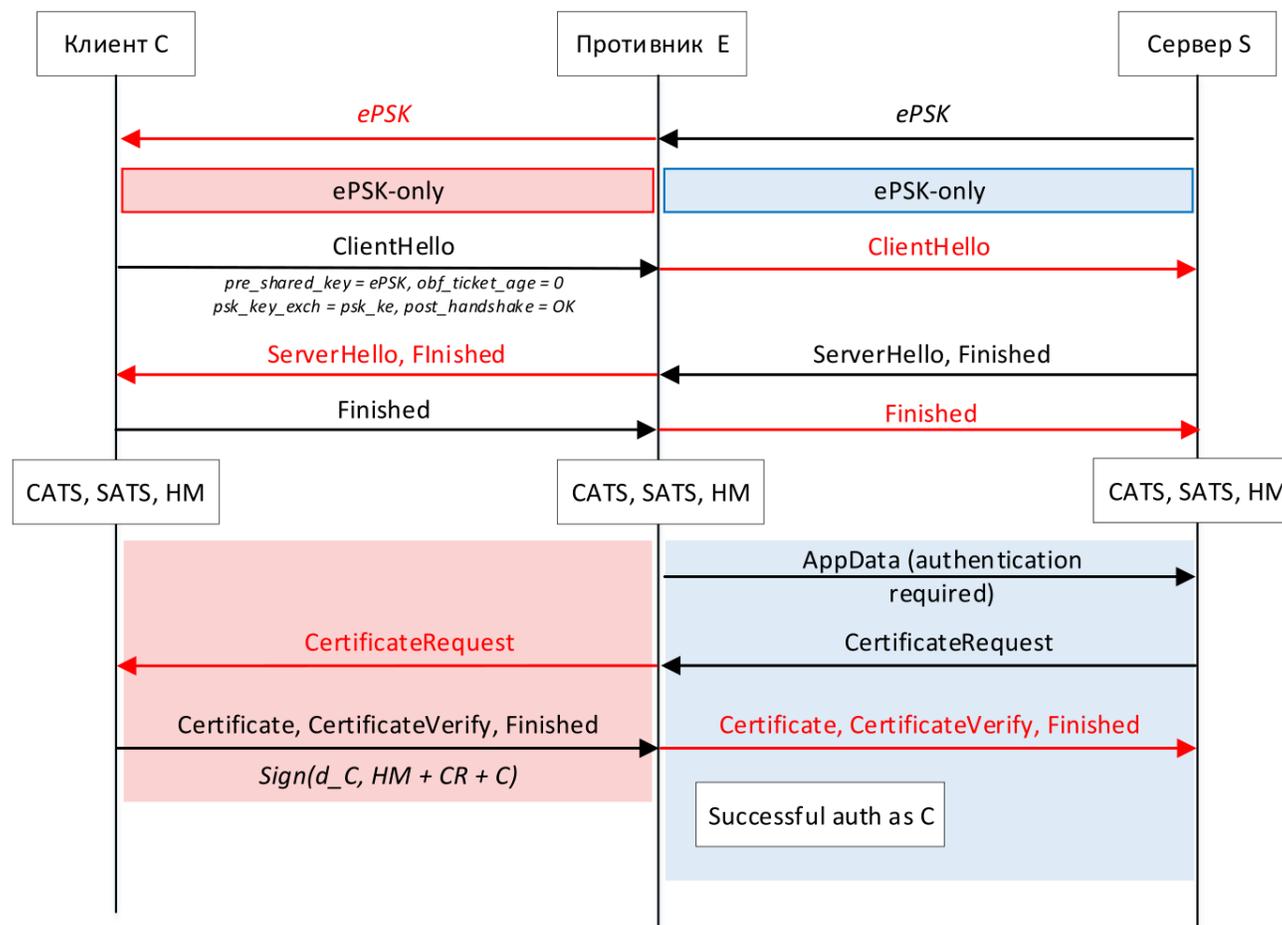
- Документ, определяющий криптонаборы на основе российских криптоалгоритмов, разрабатывается силами рабочей группы № 2.1 по сопутствующим криптографическим алгоритмам и протоколам (СКАиП) ТК26
- Планируемая дата окончания работы над документом: сентябрь 2019 года
- После завершения работы над документом планируется начать работу над rfc с целью получения номеров IANA и для этих криптонаборов

## RTLS 1.3 – основные особенности

- Использование внешнего PSK (ePSK) только в режиме с ECDHE
- Ограничение возможности пересылки прикладных данных клиентом и сервером до завершения протокола Handshake
- Ограничение возможностей «продления жизни» соединений с помощью вырабатываемых PSK (iPSK)
- Порядок защиты данных в протоколе Record

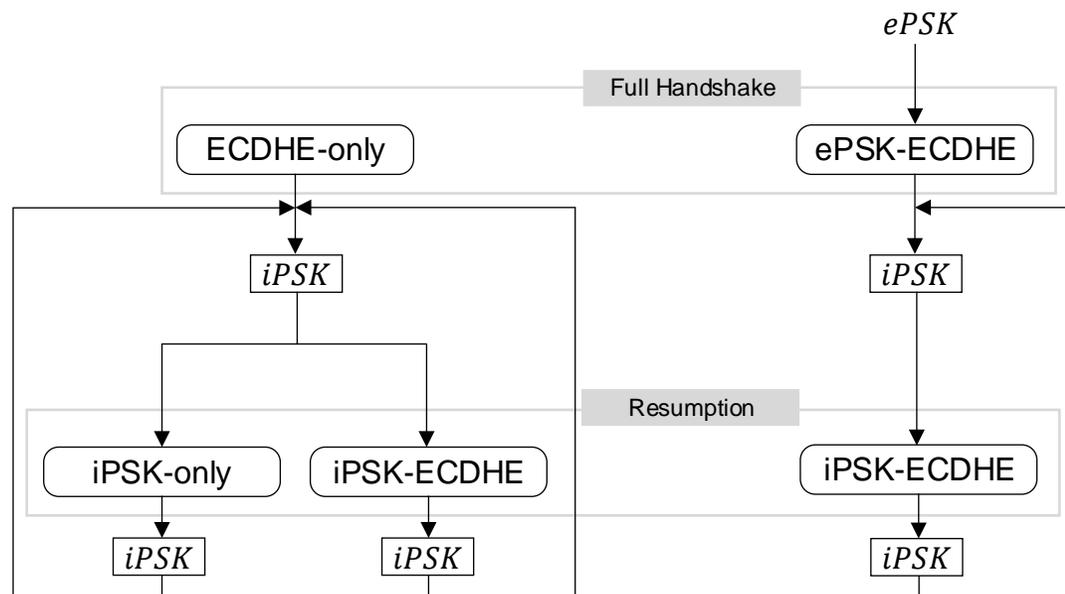
# RTLS 1.3 – ePSK только с ECDHE

- Возможность осуществления ложной аутентификации при некоторых условиях с использованием ePSK

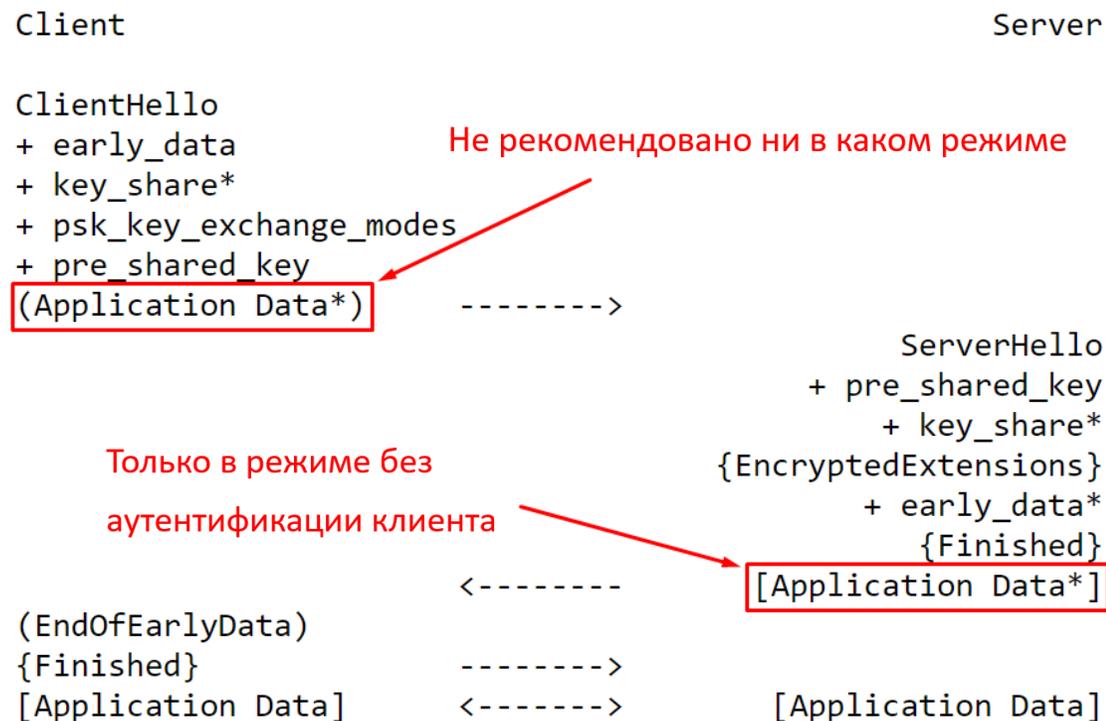


# RTLS 1.3 – ePSK только с ECDHE

Особенности взаимосвязи режимов работы протокола Handshake в RTLS



# RTLS 1.3 – прикладные данные до завершения Handshake



# RTLS 1.3 – жизнь соединения после ECDHE

- Режимы с PSK – аналог Session Resumption старых версий TLS
- Вводимые ограничения:
  - Один iPSK можно использовать только в рамках одного соединения
  - Сервер не должен отправлять более 1024 тикетов в рамках одного соединения
  - Срок жизни iPSK не должен превышать минимума из следующих значений:
    - 604800 секунд (7 дней) в соответствии с RFC 8446;
    - количество секунд с момента формирования тикета до момента, определяющегося датой, превышающей дату окончания действия сертификата на 604800 секунд (+ 7 дней);
    - количество секунд, продиктованное другими локальными политиками сервера. Например, если к моменту создания тикета сертификат клиента, с помощью которого устанавливалось базовое соединение, отозван, то сервер может принять решение о запрете создания новых тикетов.

# Модели для оценки стойкости подпротокола Record

- Эволюция моделей противника для конфиденциальности и целостности:
  - Конфиденциальность: LOR-CPA, ROR-CPA, IND-CPA, CPNA, SEM-CPA, ...
  - Целостность: EU-CMA, UU-CMA, SU-CMA, IND-CMA, ...
  - Совмещенные модели: DAE, IND-CCA, IND-CCA3, ...
  - Модели для защищенного канала: IND-sfCCA3, IND-sfCCSA

# Модель IND-sfCCSA для оценки стойкости подпротокола Record

$\text{Exp}_{\text{sfAEAD}}^{\text{IND-sfCCSA}-b}(A)$

```

 $K \xleftarrow{\$} \text{sfAEAD.K}()$ 
 $u \leftarrow 0, v \leftarrow 0$ 
 $\text{sent} \leftarrow \emptyset$ 
 $st \leftarrow A$ 
 $(st_E, st_D) \leftarrow \text{sfAEAD.Init}(st)$ 
 $b' \leftarrow A^{\text{Encrypt}^b, \text{Decrypt}^b}$ 
return  $b'$ 

```

Oracle Encrypt<sup>b</sup>(ad, m)

```

if  $b = 0$  then
   $m \xleftarrow{\mathcal{U}} \{0, 1\}^{|m|}$ 
 $c \leftarrow \text{sfAEAD.E}(K, ad, m, st_E)$ 
 $\text{sent} \leftarrow \text{sent} \cup (ad, c, u)$ 
 $st_E \leftarrow \text{sfAEAD.Upd}(st_E)$ 
 $u \leftarrow u + 1$ 
return  $c$ 

```

Oracle Decrypt<sup>1</sup>(ad, c)

```

 $m \leftarrow \text{sfAEAD.D}(K, ad, c, st_D)$ 
if  $(m \neq \perp)$  then
  if  $((ad, c, v) \in \text{sent})$  then
     $m \leftarrow \perp$ 
   $st_D \leftarrow \text{sfAEAD.Upd}(st_D)$ 
   $v \leftarrow v + 1$ 
return  $m$ 

```

Oracle Decrypt<sup>0</sup>(ad, c)

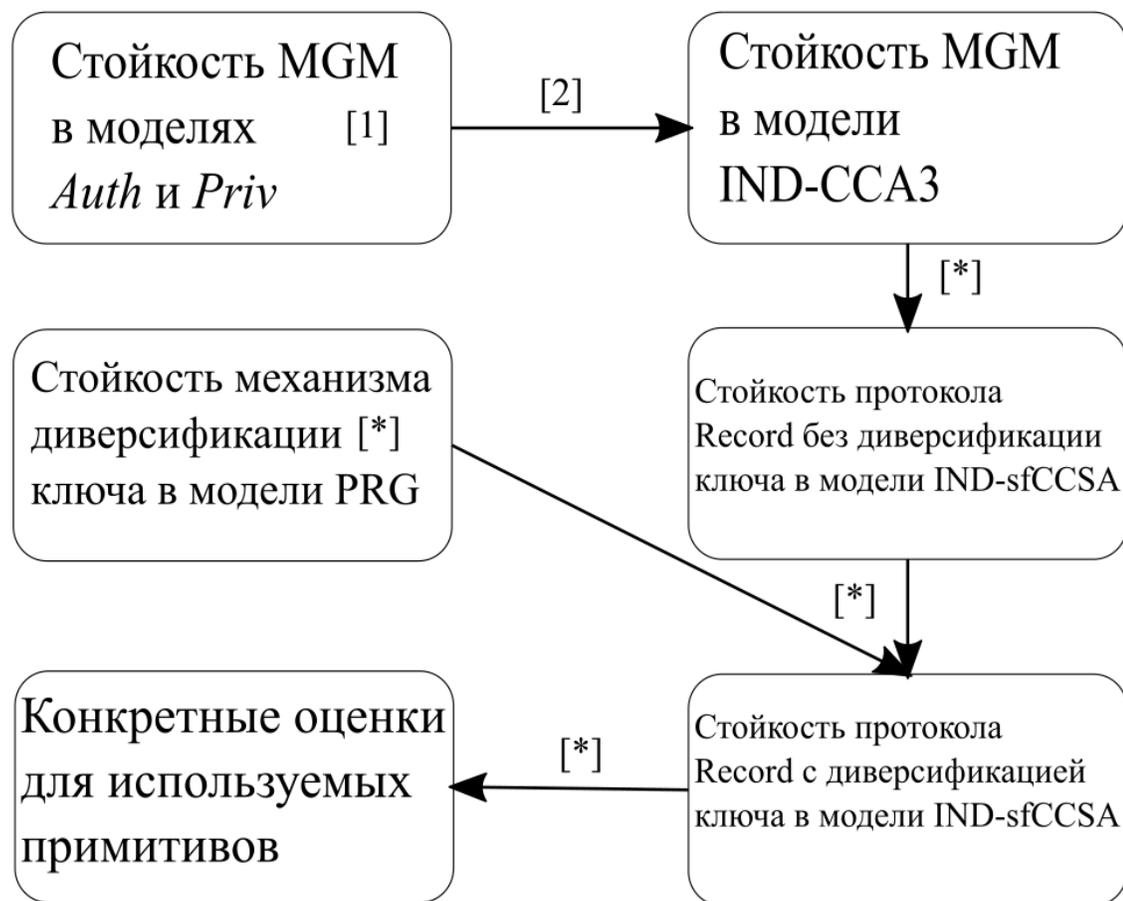
```

return  $\perp$ 

```

$$\text{Adv}_{\text{sfAEAD}}^{\text{IND-sfCCSA}}(A) = \Pr [\text{Exp}_{\text{sfAEAD}}^{\text{IND-sfCCSA}-1}(A) \rightarrow 1] - \Pr [\text{Exp}_{\text{sfAEAD}}^{\text{IND-sfCCSA}-0}(A) \rightarrow 1]$$

# Схема построения сведения



- [1] Akhmetzyanova L., Alekseev E., Karpunin G., Nozdrunov V. «*Security of Multilinear Galois Mode (MGM)*», 2019.
- [2] Shrimpton T. «*A characterization of authenticated-encryption as a form of chosen ciphertext security*», 2004.
- [\*] Доказано в ходе оценки стойкости Record.

# Доказанные теоремы

- Теорема о стойкости Record без диверсификации ключа:

$$\text{Insec}_{\text{RecordMGM}}^{\text{IND-sfCCSA}}(t, q, q_D, l) \leq \text{Insec}_{\text{MGM}}^{\text{IND-CCA3}}(t, q, q_D, l) \leq \frac{3(ql + 4q)^2}{2^n} + q_D \cdot \frac{3(ql + 4q + l + 3)^2 + 2}{2^n}.$$

- Теорема о стойкости схемы с диверсификацией ключа:

$$\text{Insec}_{(\text{RecordMGM}, \text{ExtKeyGen13})_h}^{\text{IND-sfCCSA}}(t, q, q_D, l) \leq 2 \cdot \text{Insec}_{\text{ExtKeyGen13}}^{\text{PRG}}\left(t, \left\lceil \frac{q}{h} \right\rceil\right) + \left\lceil \frac{q}{h} \right\rceil \cdot \text{Insec}_{\text{RecordMGM}}^{\text{IND-sfCCSA}}(t, h, q_D, l)$$

# Оценка стойкости в модели IND-sfCCSA

**Блочный шифр Кузнечик.** Для данного алгоритма  $l = 2^{10} + 1, n = 128$ . Тогда можно получить следующую оценку:

$$\begin{aligned}
 InSec_{(Record_{MGM}, ExtKeyGen13)_h}^{IND-sfCCSA}(t, q, 1, l) &\leq Insec_{ExtKeyGen13}^{PRG}\left(t, \left\lceil \frac{q}{h} \right\rceil\right) + \\
 &+ \left\lceil \frac{q}{h} \right\rceil \cdot \frac{3176523h^2 + 3173436h + 1585177}{170141183460469231731687303715884105728} \leq \\
 &\leq qh \cdot 2^{-105} \quad (1)
 \end{aligned}$$

**Блочный шифр Магма.** Для данного алгоритма  $l = 2^{11} + 1, n = 64$ . Тогда можно получить следующую оценку:

$$\begin{aligned}
 InSec_{(Record_{MGM}, ExtKeyGen13)_h}^{IND-sfCCSA}(t, q, 1, l) &\leq Insec_{ExtKeyGen13}^{PRG}\left(t, \left\lceil \frac{q}{h} \right\rceil\right) + \\
 &+ \left\lceil \frac{q}{h} \right\rceil \cdot \frac{12644427h^2 + 12638268h + 6316057}{9223372036854775808} \leq \\
 &\leq qh \cdot 2^{-39} \quad (2)
 \end{aligned}$$

Спасибо за внимание! Вопросы?



# Контактная информация

## Авторы доклада:

Алексеев Евгений

Ахметзянова Лилия

Седов Григорий

Смышляева Екатерина

## Электронная почта:

[alekseev@cryptopro.ru](mailto:alekseev@cryptopro.ru)

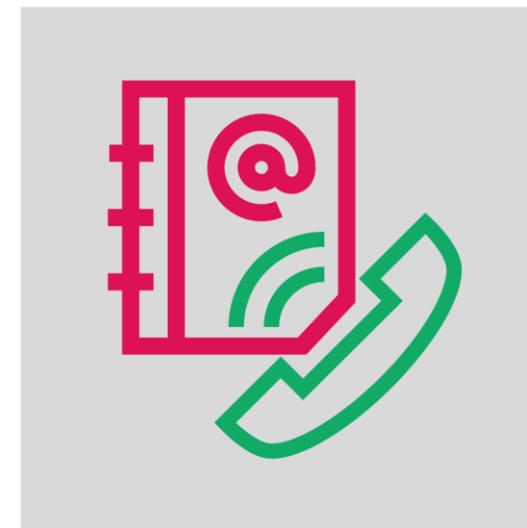
[lah@cryptopro.ru](mailto:lah@cryptopro.ru)

[sedovgk@cryptopro.ru](mailto:sedovgk@cryptopro.ru)

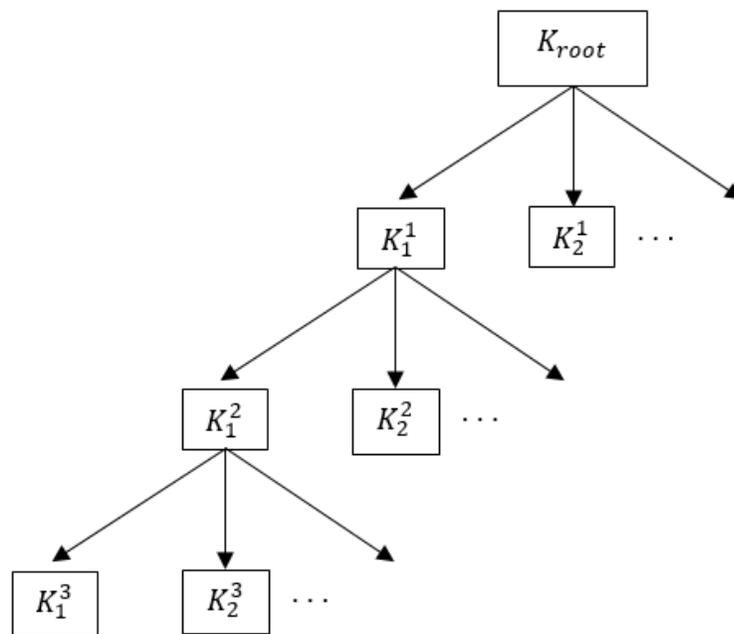
[ess@cryptopro.ru](mailto:ess@cryptopro.ru)

## Сайт:

[www.cryptopro.ru](http://www.cryptopro.ru)



# Ключевое дерево в Record



$$TLSTREE(K_{root}, i) = Divers_3(Divers_2(Divers_1(K_{root}, i \& C_1), i \& C_2), i \& C_3)$$