Ежегодная международная научно-практическая конференция
«РусКрипто’2021»

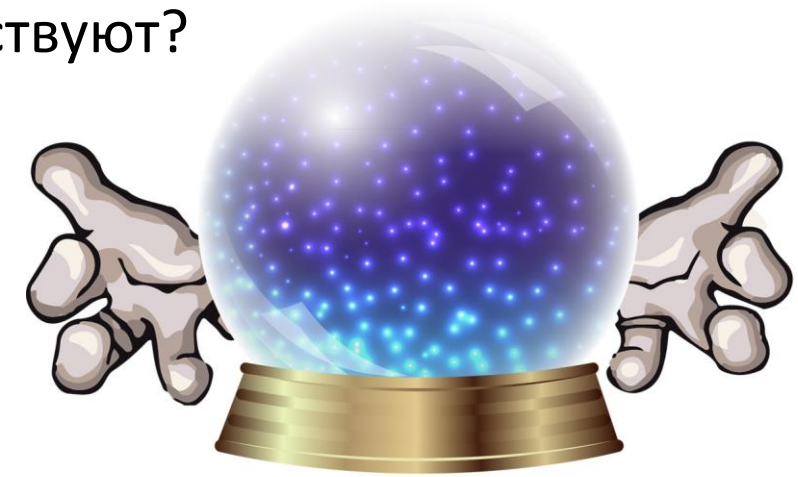
Шифрование, сохраняющее формат: задачи, подходы, схемы

Алексеев Е.К., к.ф.-м.н., начальник отдела криптографических исследований, КриптоПро
Ахметзянова Л.Р., зам. начальника отдела криптографических исследований, КриптоПро
Елистратов А.А., эксперт, ТК 26
Никифорова Л.О., инженер-аналитик, КриптоПро

Шифрование, сохраняющее формат – Format Preserving Encryption (FPE)

Ответим на вопросы:

- Что такое FPE-схемы и зачем они нужны?
- Какие криптографические свойства требуются от FPE-схемы?
- Какие базовые подходы к построению FPE-схемы существуют?
- Какие FPE-схемы существуют?



Исследование проведено в рамках НИР «Элемент», поставленного Академией криптографии РФ

Что такое FPE?

- FPE-схема – это семейство перестановок на произвольном множестве $\mathcal{M}$, индексируемое ключом K

$$\mathrm{FPE}_K: \mathcal{M} \to \mathcal{M}$$

- Блочный шифр – частный случай FPE-схемы, для которой $\mathcal{M} = \{0,1\}^n$, где n – длина блока

Зачем нужны FPE-схемы?

1. Шифрование базы данных, поля которой имеют фиксированных формат

2. Шифрование номеров банковских карт (финансовые операции)

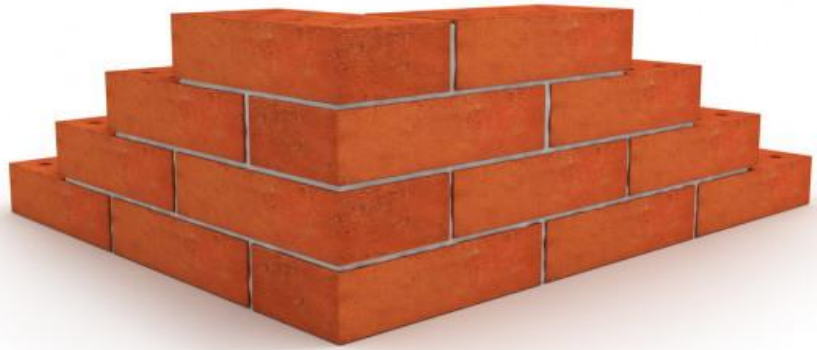
3. PAKE-протоколы, защита от появления критерия для ключа (см. [AAOS16] Раздел 4.5)

[AAOS16] Алексеев Е.К., Ахметзянова Л.Р., Ошкин И.Б., Смышляев С.В. "Обзор уязвимостей некоторых протоколов выработки общего ключа с аутентификацией на основе пароля и принципы построения протокола SESPAKE". Матем. вопр. криптогр., 2016, том 7, выпуск 4, 7–28.

Принцип построения схемы

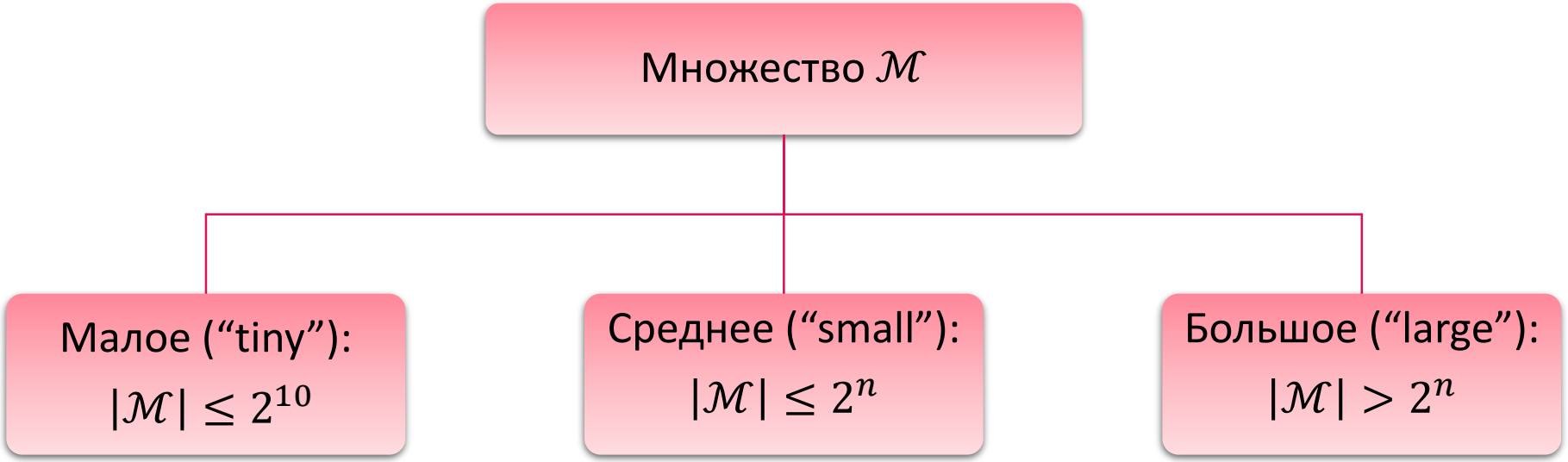
«С нуля»

На основе примитивов («из кирпичиков»)



Для FPE-схем «кирпичиком» обычно является блочный шифр

Зависимость от мощности множества $\mathcal{M}$ в случае построения FPE-схемы на основе блочного шифра с длиной блока n



Можно хранить полную таблицу отображений и/или относительно быстро ее вычислять

Full disk encryption (FDE)

Какие криптографические свойства требуются от FPE-схемы?

- **PRP-CPA** – PseudoRandom Permutation under Chosen Plaintext Attack

  Цель противника: «отличить» от случайной перестановки

  Возможности противника: накапливать пары (*открытый текст*, *шифртекст*) при адаптивном выборе *открытого текста*

- **PRP-CCA** – PseudoRandom Permutation under Chosen Ciphertext Attack

  Цель противника: «отличить» от случайной перестановки

  Возможности противника: накапливать пары (*открытый текст*, *шифртекст*) при адаптивном выборе *открытого текста* и *шифртекста*

Количество пар (*открытый текст*, *шифртекст*) определяется количеством запросов противника

Что такое настройка и зачем она нужна?

Проблема:

$\mathcal{M}$ малой мощности ⇒

⇒ накопить все пары (*открытый текст*, *шифртекст*) ⇒

⇒ восстановить перестановку

Решение:

- Рандомизация с помощью дополнительного несекретного параметра – настройки (tweak)
- Позволяет повысить стойкость схемы на множестве малой мощности

❖ Настраиваемая FPE-схема: $\mathcal{T} \times \mathcal{M} \to \mathcal{M}$

❖ Настраиваемый (tweakable) блочный шифр введен в работе [LRW02]

[LRW02] Liskov M., Rivest R., Wagner D. "Tweakable block ciphers". Advances in Cryptology – CRYPTO 2002, LNCS vol. 2442, Springer, pp. 31–46, 2002.

Какие криптографические свойства требуются от настраиваемой FPE-схемы?

Сильные модели

- **PRP-CPTA** – PseudoRandom Permutation under Chosen Plaintext and Tweak Attack
- **PRP-CCTA** – PseudoRandom Permutation under Chosen Ciphertext and Tweak Attack

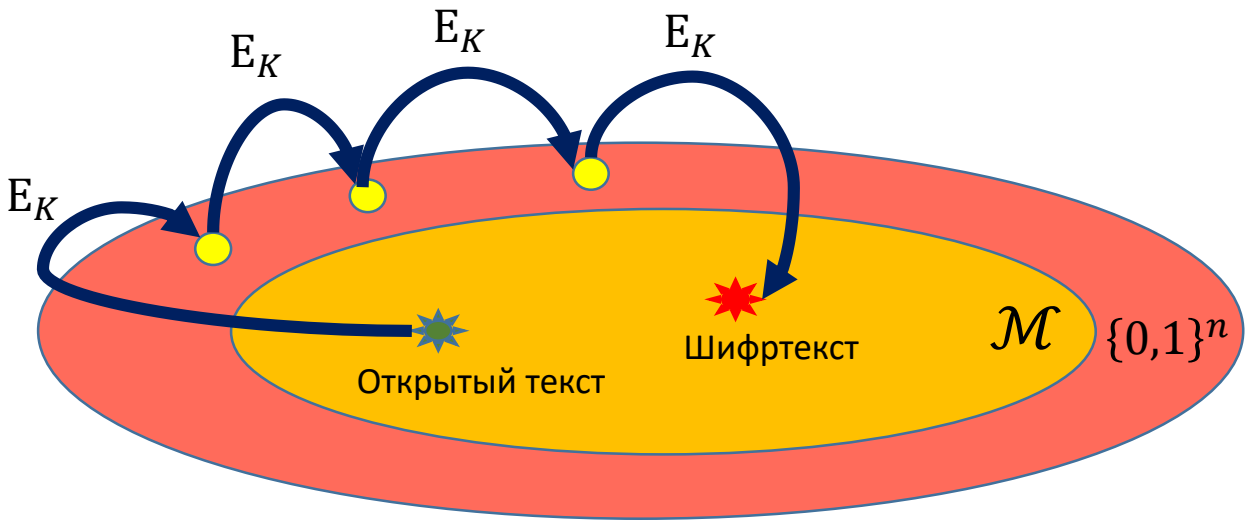
Более легкие цели противника:

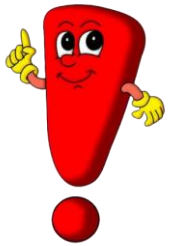
- **SPI** – Single Point Indistinguishability
- **MP** – Message Privacy
- **MR** – Message Recovery

Введены в работе:
Bellare M., Ristenpart T., Rogaway P., Stegers T. "Format-Preserving Encryption". In: Jacobson Jr., M.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol. 5867, pp. 295–312. Springer, Heidelberg (2009).

Какие базовые подходы существуют?

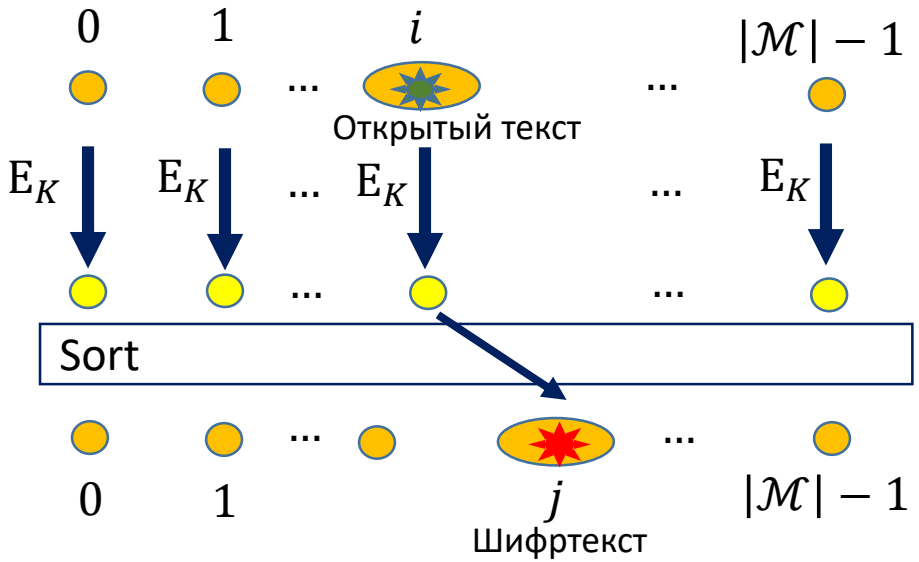
Кратное шифрование (cycle walking)

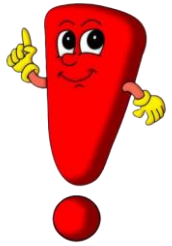




Эффективна для $|\mathcal{M}| \to 2^n$

Prefix-cipher





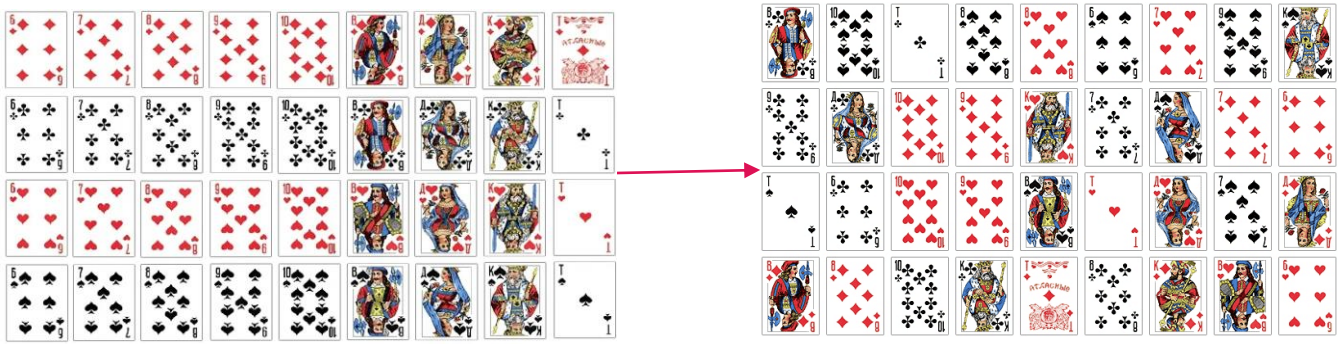
Эффективна для малых $|\mathcal{M}|$

Стойкость в моделях PRP-CPA и PRP-CCA совпадает со стойкостью блочного шифра E_K в данных моделях

Какие базовые подходы существуют?

«Забывчивые» перестановки (oblivious permutations)

В терминах колоды карт



- У карты в колоде есть порядковый номер
- Перемешать колоду – присвоить каждой карте новый номер

- «Забывчивый» способ перемешивания – узнать новый номер карты, не зная порядок карт в колоде после перемешивания

Какие базовые подходы существуют?

«Забывчивые» перестановки:

- Методы перемешивания (shuffling)
- Сеть Фейстеля

«Забывчивые» перестановки (oblivious permutations) позволяют узнавать результат применения перестановки к элементу множества, не узнавая результат применения данной перестановки к другим элементам множества

Методы перемешивания

Swap-or-Not (SoN)

- Многораундовая схема

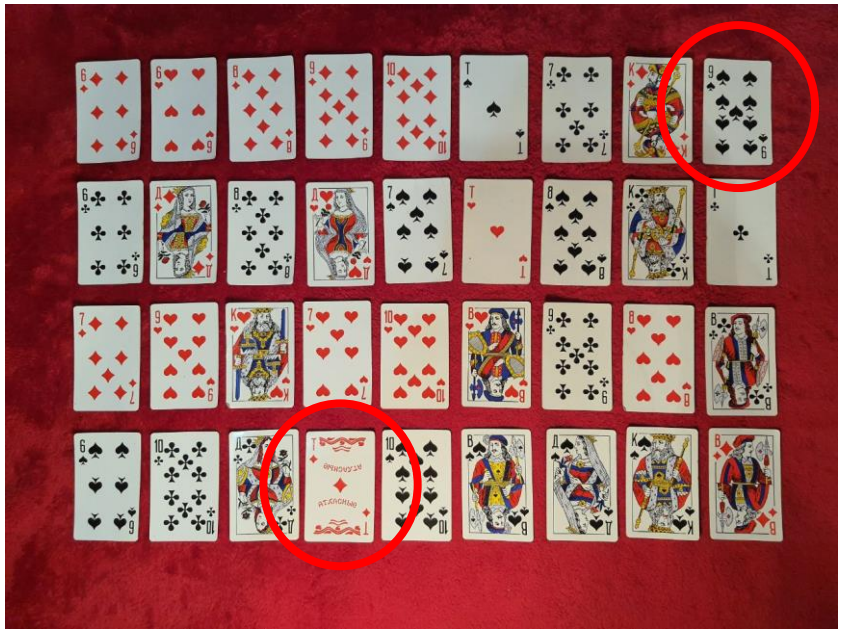
Текущее состояние колоды

Карты в колоде разбиваются на пары случайным образом

Методы перемешивания

Swap-or-Not (SoN)

Случайные пары



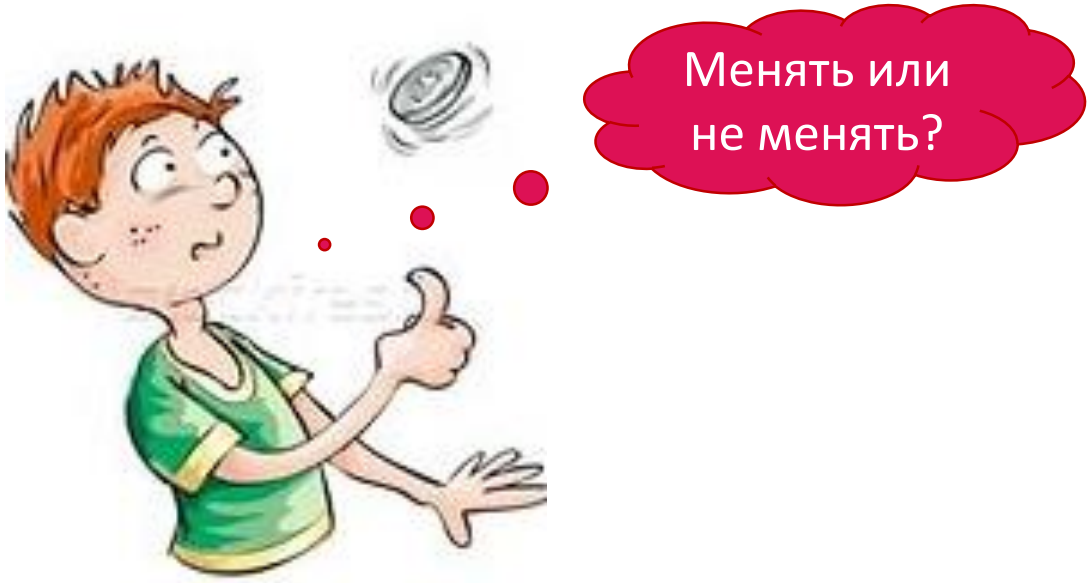
Случайным образом определяется переставляются местами в колоде карты из каждой пары или нет

Методы перемешивания

Swap-or-Not (SoN)

На каждом раунде $i = 1 \dots r$:

a. Карты в колоде разбиваются на пары.
b. Для каждой пары (x, y):
   1. Выбирается случайно $b \in \{0,1\}$.
   2. Если $b = 1$, то x и y меняются местами



«Забывчивая» перестановка

$\mathrm{SoN}(X)$

for $i = 1 \dots r$ **do**
  $Y \leftarrow X \oplus K_i$
  $X^* \leftarrow \max(X, Y)$
  if $F_i(X^*) = 1$ **then**
    $X \leftarrow Y$
return X

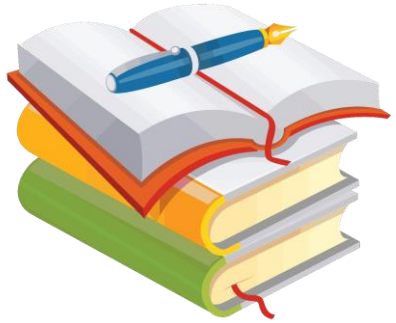
- $|\mathcal{M}| = 2^m$
- $X \in \{0, \dots, 2^m - 1\}$ – номер карты

a. K_i – раундовые ключи, разбивают колоду на пары
b. F_i - раундовые псевдослучайные функции, определяют меняются карты местами или нет

Методы перемешивания

Swap-or-Not (SoN)

- Можно добавить настройку, сделав настраиваемыми раундовые функции (см. [MR14])
- Оценки в модели PRP-CCA получены в работе [HMR12].
- Оценки в модели PRP-CCTA получены в работе [MR14]



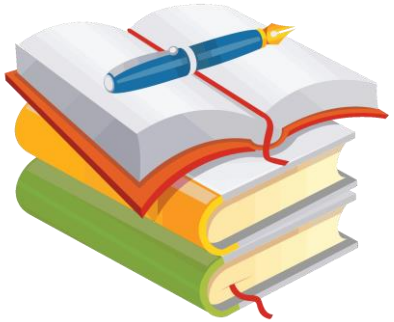
[HMR12] Hoang V.T., Morris B., Rogaway P. "An enciphering scheme based on a card shuffle". In R. Safavi-Naini and R. Canetti, editors, CRYPTO 2012, volume 7417 of LNCS, pages 1–13. Springer, Heidelberg, Aug. 2012.

[MR14] Morris B., Rogaway P. "Sometimes-recurse shuffle – almost-random permutations in logarithmic expected time". In EUROCRYPT 2014, volume 8441 of LNCS. Springer, Heidelberg, May 2014.

Методы перемешивания

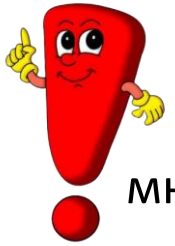
Улучшения SoN

- Mix-and-Cut (см. [RY13])
- Sometimes Recurse (SR) (см. [MR14])



[MR14] Morris B., Rogaway P. "Sometimes-recurse shuffle – almost-random permutations in logarithmic expected time". In EUROCRYPT 2014, volume 8441 of LNCS. Springer, Heidelberg, May 2014.

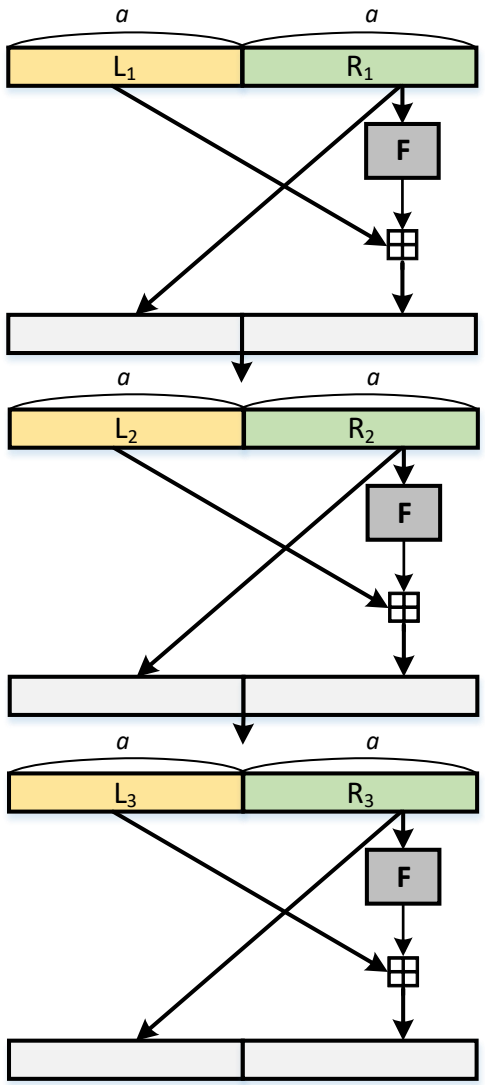
[RY13] Ristenpart T., Yilek S. "The mix-and-cut shuffle: Small-domain encryption secure against N queries". In R. Canetti and J. A. Garay, editors, CRYPTO 2013, Part I, volume 8042 of LNCS, pages 392–409. Springer, Heidelberg, Aug. 2013.

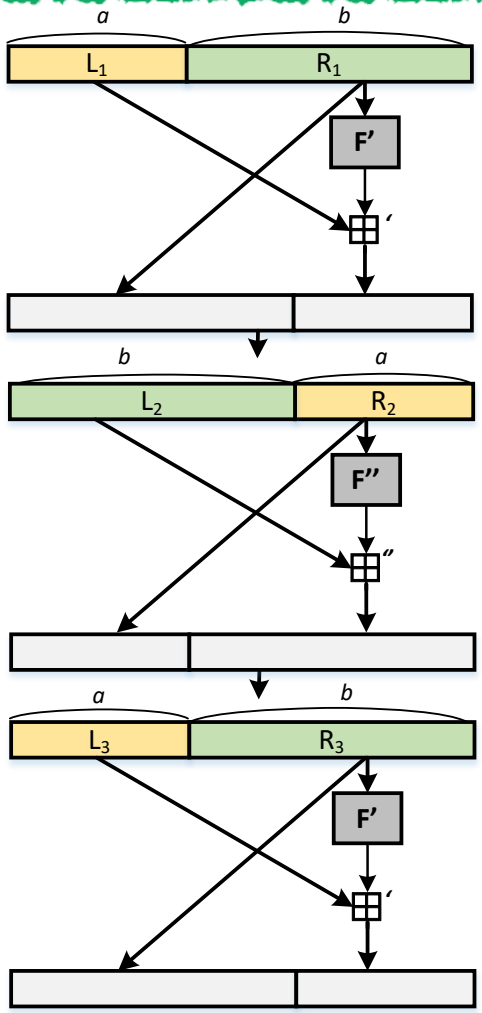


Методы перемешивания требует большого количества раундов при средней мощности множества $\mathcal{M}$

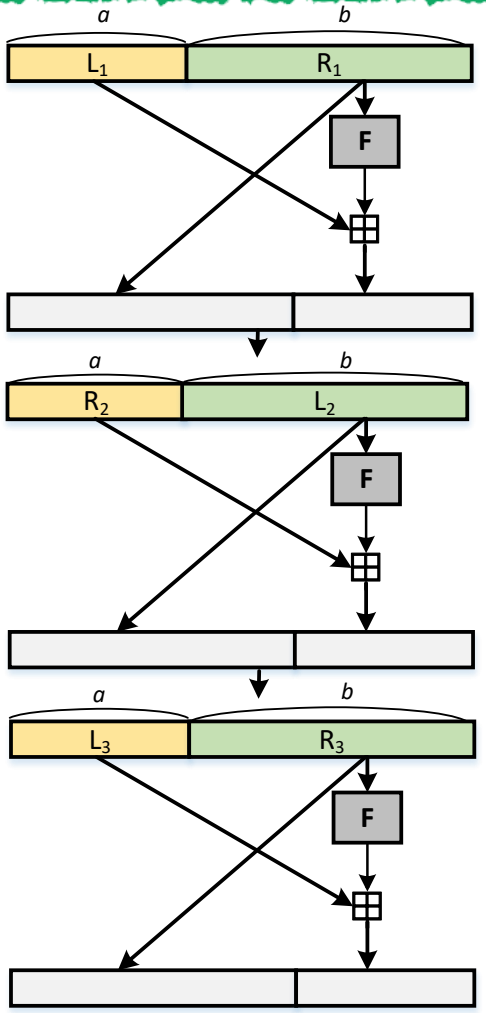
Сеть Фейстеля

– многораундовая конструкция, предназначенная для построения перестановок на множестве строк длины m: $\mathcal{M} = A^m$, где A – алфавит

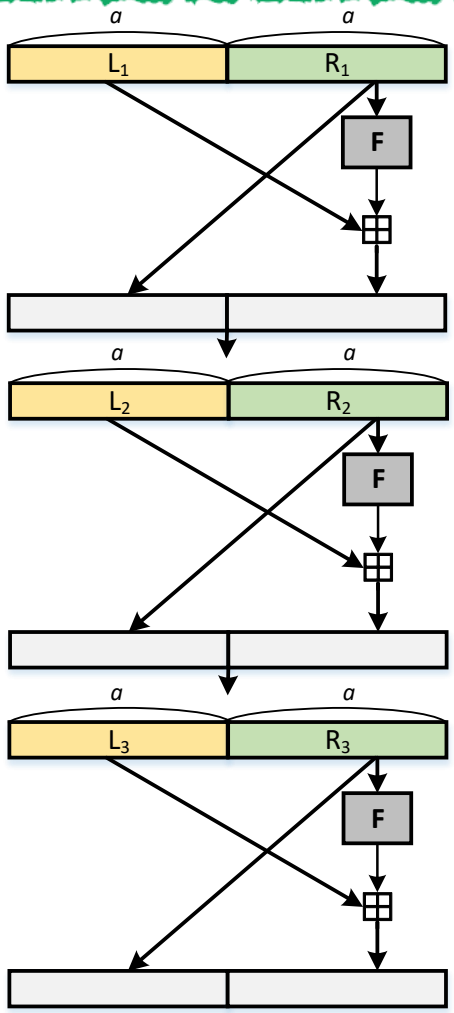




а



б



в

а) С чередованием (alternating)

б) Несбалансированная

в) Сбалансированная

Thorp shuffle

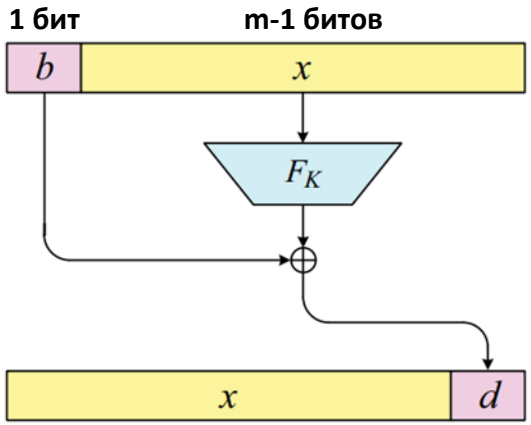
Тасование колоды «пролистыванием»

На каждом раунде:

Для всех $x \in \{0, \dots, |\mathcal{M}|/2 - 1\}$:

a. Выбирается случайно $c \in \{0,1\}$.
b. Если $c = 0$, карты x и $|\mathcal{M}|/2 + x$ переходят на позиции $2x$ и $2x + 1$ по модулю $|\mathcal{M}|$ соответственно.
c. Если $c = 1$, карты x и $|\mathcal{M}|/2 + x$ переходят на позиции $2x + 1$ и $2x$ по модулю $|\mathcal{M}|$ соответственно.

«Забывчивая» перестановка



$b \cdot |\mathcal{M}|/2 + x$

$d = c \oplus b$

$2x + d$

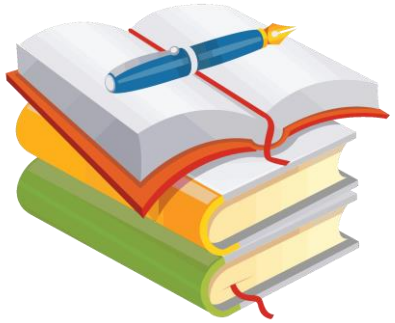
$|\mathcal{M}| = 2^m$

Номер карты – m битов

Максимально несбалансированная сеть Фейстеля

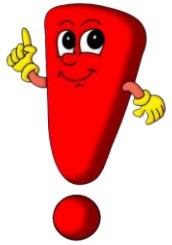
Сеть Фейстеля

- Оценки в модели PRP-CCA получены в работах [HR10] и [SGW20].



[HR10] Hoang V. T., Rogaway P. On generalized Feistel networks //Annual Cryptology Conference. – Springer, Berlin, Heidelberg, 2010. – С. 613-630.

[SGW20] Shen Y., Guo C., Wang L. Improved Security Bounds for Generalized Feistel Networks //IACR Transactions on Symmetric Cryptology. – 2020. – С. 425-457.

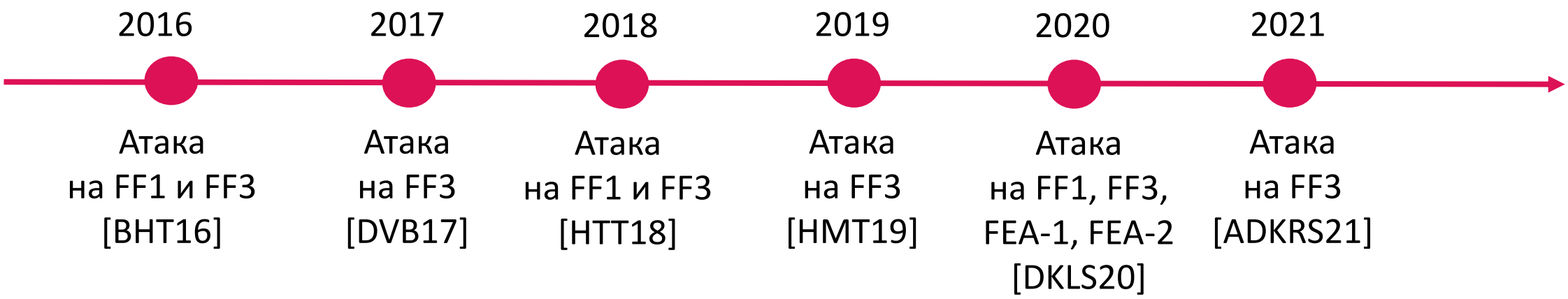


Нет оценок для сети Фейстеля с настраиваемыми раундовыми функциями

Какие схемы существуют?

FFX (format-preserving, Feistel-based) определяется набором параметров:		
▪ FF1	▪ FF2	▪ FF3
Стандартизирована NIST в 2016 году	Уязвимость в 2015 году	Стандартизирована NIST в 2016 году

FEA-1, FEA-2 – корейские стандарты



- Message Recovery (MR)
- Атака, описанная в [HMT19], позволяет построить соответствия между входами раундовых функций и их выходами для длины входа $m = 6$ за 2^{30} операций.

Стойкость схем

Эвристический метод

Появляются атаки

Мало раундов

Доказуемая стойкость

Много раундов

Спасибо за внимание! Вопросы?

Контактная информация

Электронная почта:

nikiforova@cryptopro.ru

Телефон:

+7 985 665-79-94

Facebook:

https://www.facebook.com/cryptopro

Сайт:

www.cryptopro.ru

Литература

[BHT16] Bellare M., Hoang V.T., Tessaro S. "Message-Recovery Attacks on Feistel-Based Format Preserving Encryption". Cryptology ePrint Archive: Report 2016/794.

[DVB17] Durak F. B., Vaudenay S. Breaking the FF3 format-preserving encryption standard over small domains //Annual international cryptology conference. – Springer, Cham, 2017. – С. 679-707.

[HTT18] Hoang V.T., Tessaro S., Trieu N. "The Curse of Small Domains: New Attacks on Format-Preserving Encryption". In: Shacham H., Boldyreva A. (eds) Advances in Cryptology – CRYPTO 2018. CRYPTO 2018. Lecture Notes in Computer Science, vol 10991. Springer, Cham. https://doi.org/10.1007/978-3-319-96884-1_8

[HMT19] Hoang V. T., Miller D., Trieu N. Attacks Only Get Better: How to Break FF3 on Large Domains //Annual International Conference on the Theory and Applications of Cryptographic Techniques. – Springer, Cham, 2019. – С. 85-116.

[DKLS20] Dunkelman, O., Kumar, A., Lambooij, E., Sanadhya, S. K. Cryptanalysis of Feistel-Based Format-Preserving Encryption.

[ADKRS21] Cryptanalysis of Feistel-Based Format-Preserving Encryption Orr Dunkelman1 , Abhishek Kumar2 , Eran Lambooij1 , and Somitra Kumar Sanadhya2