конференция
РусКрипто'2011

МАТЕМАТИЧЕСКИЕ МОДЕЛИ КРИПТОГРАФИИ

"Cryptography is communication in the presence of adversaries."

Ron Rivest

"Cryptography is communication in the presence of adversaries."

Ron Rivest

Определение. Криптография является разделом прикладной математики, связанным со схемами, механизмами, устройствами и протоколами, выполняющими определенные задачи по обеспечению информационной безопасности, несмотря на усилия злоумышленника (нарушителя).

ЗАДАЧИ КРИПТОГРАФИИ

- Обеспечение секретности (конфиденциальности) (*confidentiality, secrecy, privacy*)
- Обеспечение целостности (*data integrity*)
- Аутентификация (проверка подлинности) (*authentication*)
  - *Идентификация* (*entity authentication*)
  - *Проверка подлинности данных* (*data origin authentication*)
- *Прочие криптографические сервисы :*
  - Неотказуемость (*nonrepudiation*)
  - *Анонимность* (*anonymity*)
  - *Нулевое разглашение* (*zero-knowledge*)
  - *Электронные платежи* (*electronic payment*)
  - и т.д. и т.п.

ВСЯ криптография базируется на понятии однонаправлен-ности

ОДНОНАПРАВЛЕННЫЕ ФУНКЦИИ

$f: X \to Y$ – ***однонаправленная функция*** (***one-way function***), если

- для всех $x \in X$ можно легко вычислить значение $f(x)$,
- для почти всех элементов $y \in \mathrm{Im}(f)$ трудно найти $x \in X$: $f(x)=y$.

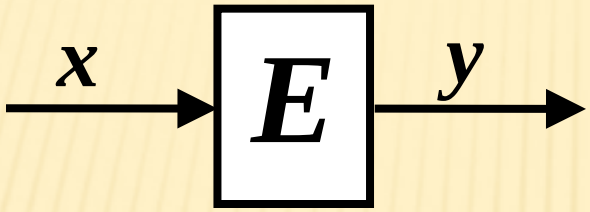
ОДНОНАПРАВЛЕННЫЕ ФУНКЦИИ

Однонаправленной функцией с лазейкой (*trapdoor one-way function*) называется однонаправленная функция $f: X \to Y$ со следующим дополнительным свойством: если известна некоторая дополнительная информация, называемая ***лазейкой*** (*trapdoor*), то для любого элемента $y \in \mathrm{Im}(f)$, можно эффективно найти такой элемент $x \in X$, что $f(x)=y$.

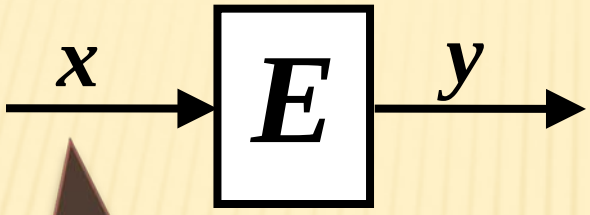
ВСЯ

криптография держится на использовании преобразований трех основных типов.

ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ



ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ

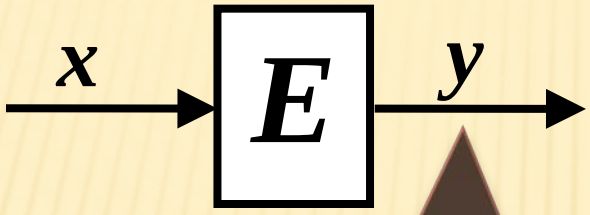


$x \in P$

P – *пространство открытых текстов*

шифрующее преобразование, преобразование шифрования или просто *шифр*

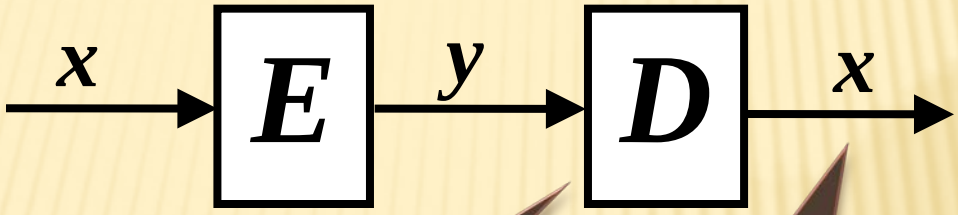
ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ



$E(x) = y \in C$

C – *пространство шифртекстов*

ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ

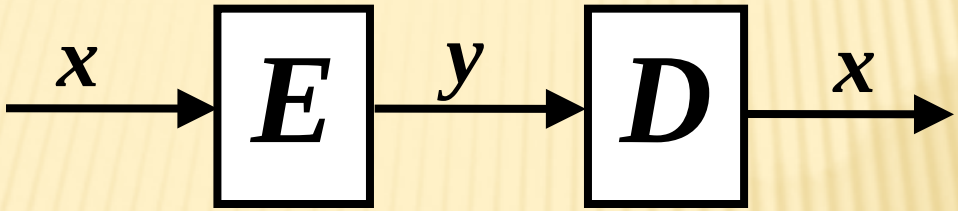


преобразование расшифрования

при этом $D=E^{-1}$:

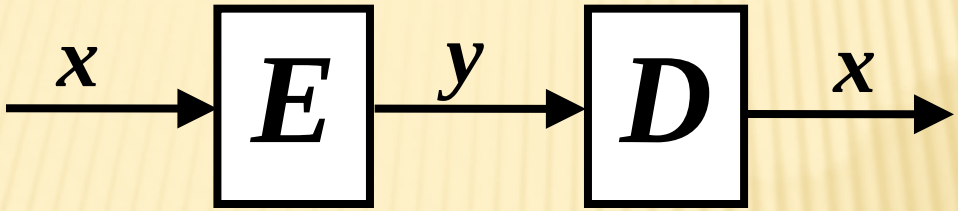
$x = D(y) = E^{-1}(y)$

ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ



Основным требованием к преобразованию E является то, что оно должно быть ***однонаправленной функцией***. В этом случае преобразование E называется ***обратимым криптографическим преобразованием***.

ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ



Основным требованием к преобразованию E является то, что оно должно быть ***однонаправленной функцией***. В этом случае преобразование E называется ***обратимым криптографическим преобразованием***.

ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ С КЛЮЧОМ

$$E: P \times K \rightarrow C$$

ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ С КЛЮЧОМ

$$E: P \times K \rightarrow C$$

$$\{E_e: P \rightarrow C,\ e \in K\}$$

ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ С КЛЮЧОМ

$$E: P \times K \rightarrow C$$

ключевое пространство

$$\{E_e: P \rightarrow C,\ e \in K\}$$

обратимые отображения

ключ шифрования

ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ С КЛЮЧОМ

$$E: P \times K \rightarrow C$$

$$\{E_e: P \rightarrow C,\ e \in K\}$$

ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ С КЛЮЧОМ

$$E: P \times K \rightarrow C$$

$$\{E_e: P \rightarrow C,\ e \in K\}$$

$$\{D_d: C \rightarrow P,\ d \in K'\}$$

ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ С КЛЮЧОМ

$$E: P \times K \to C$$

$\forall\, e \;\; \exists!\, d :$
$D_d = (E_e)^{-1}$

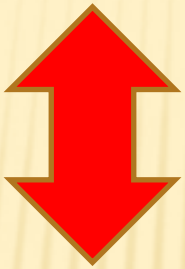
$P \to C,$

ключ расшифрования

$$\{D_d: C \to P,\ d \in K'\}$$

ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ С КЛЮЧОМ

$$\{E_e: P \to C,\ e \in K\}$$



$$\{D_d: C \to P,\ d \in K'\}$$

(e,d) – (*ключ шифрования, ключ расшифрования*)

ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ С КЛЮЧОМ

$$\{E_e: P \to C, e \in K\}$$

Преобразование E_e должно быть *однонаправленной функцией с лазейкой* относительно преобразования x в y, роль лазейки исполняет ключ расшифрования d.

В этом случае преобразование E_e называется *обратимым криптографическим преобразованием с ключом*.

ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ С КЛЮЧОМ

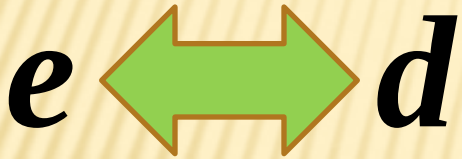
$$\{E_e: P \to C, e \in K\}$$

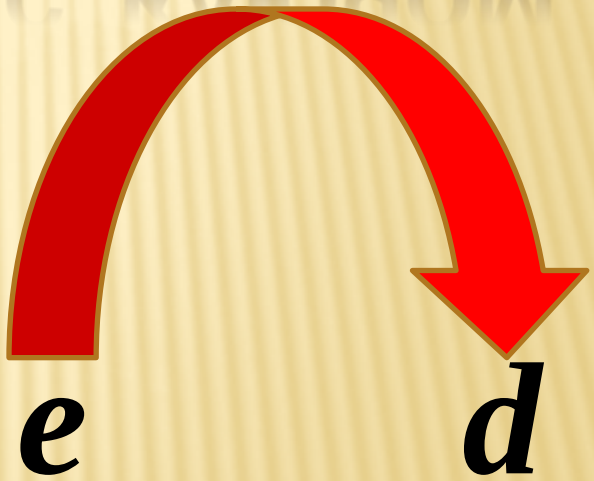
Преобразование E_e должно быть *однонаправленной функцией с лазейкой* относительно преобразования x в y, роль лазейки исполняет ключ расшифрования d.

В этом случае преобразование E_e называется *обратимым криптографическим преобразованием с ключом*.

СИММЕТРИЧНЫЕ И АСИММЕТРИЧНЫЕ ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ С КЛЮЧОМ

СИММЕТРИЧНЫЕ И АСИММЕТРИЧНЫЕ ОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ С КЛЮЧОМ





симметричное криптографическое преобразование

Симметричные и асимметричные обратимые криптографические преобразования с ключом

$e \Leftrightarrow d$

Асимметричное криптографическое преобразование

НЕОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ

$$h: A^* \rightarrow H = A^n$$

(1) ***Однонаправленность*** (***one-wayness, preimage resistance***): для почти всех значений выхода $y \in H$ вычислительно трудно найти хотя бы один вход $x' \in A^*$ такой, что $h(x') = y$ (заметим, что y может быть получен из неизвестного нам x не обязательно совпадающего с x').

НЕОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ

$$h: A^* \rightarrow H = A^n$$

(2) ***Слабая устойчивость к коллизиям*** (***weak collision resistance***, ***2nd-preimage resistance***) если задан произвольный элемент $x \in A^*$, вычислительно трудно найти еще один вход $x' \in A^*$, $x' \neq x$, такой, что $h(x') = h(x)$.

НЕОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ

$$h: A^* \rightarrow H = A^n$$

(3) ***Сильная устойчивость к коллизиям*** (***strong collision resistance***, ***collision resistance***): **вычислительно трудно найти два различных входа** x, $x' \in A^*$, $x' \neq x$, **для которых** $h(x)=h(x')$ **(заметим, что здесь, в отличии от предыдущего пункта, мы независимы в выборе обоих входов** x **и** x'**).**

НЕОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ

$$h: A^* \rightarrow H = A^n$$

Отображение называется ***необратимым криптографическим отображением***, если оно в обязательном порядке удовлетворяет свойству (1), т.е. является однонаправленной функцией, и, желательно, удовлетворяет свойствам (2) и (3).

НЕОБРАТИМЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ

$$h: A^* \rightarrow H = A^n$$

Отображение называется ***необратимым криптографическим отображением***, если оно в обязательном порядке удовлетворяет свойству (1), т.е. является **однонаправленной функцией**, и, желательно, удовлетворяет свойствам (2) и (3).

КРИПТОГРАФИЧЕСКИЕ ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

$$R: A^k \rightarrow A^T$$

КРИПТОГРАФИЧЕСКИЕ ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

$$R: A^k \rightarrow A^T$$

Вход генератора псевдослучайных битов (seed)

Псевдослучайная последовательность $(T >> k)$

КРИПТОГРАФИЧЕСКИЕ ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Генератор псевдослучайных последовательностей R называется ***криптографическим генератором псевдослучайных последовательностей*** если он удовлетворяет следующим свойствам:

- Его выходная последовательность должна «выглядеть случайной». Это означает, что генератор проходит все известные статистические «тесты на случайность».

КРИПТОГРАФИЧЕСКИЕ ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

- Генератор является «непредсказуемым». Это означает, что вычислительно невозможно предсказать значение очередного знака его выходной последовательности с вероятностью существенно большей ½ даже зная сам алгоритм выработки выходной последовательности и зная значения предыдущих знаков выходной последовательности.

КРИПТОГРАФИЧЕСКИЕ ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Из последнего свойства следует, что отображение R является однонаправленной функцией.

КРИПТОГРАФИЧЕСКИЕ ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Из последнего свойства следует, что отображение R является **однонаправленной функцией**.

"...after almost thirty years of public-key cryptography, there is still no proof that trapdoor one-way functions, which are the fundament to the theory, exist."

Jim Massey, January 2002.

ВСЯ

криптография держится на «практической» однонаправленности тех или иных функций.

ПРИМИТИВЫ С СЕКРЕТНЫМ КЛЮЧОМ

Симметричные шифры

ПРИМИТИВЫ С СЕКРЕТНЫМ КЛЮЧОМ

Симметричные шифры

«практические» однонаправленные функции

БЛОЧНЫЕ ШИФРЫ

$$E: K \times \{0,1\}^n \rightarrow \{0,1\}^n$$

БЛОЧНЫЕ ШИФРЫ

ключевое пространство

$$E\colon K\times\{0,1\}^n \to \{0,1\}^n$$

отображение $E_e = E(e,\cdot)$ для всех $e \in K$ является подстановкой на множестве $\{0,1\}^n$.

БЛОЧНЫЕ ШИФРЫ

- Как задавать подстановки на множестве $\{0,1\}^n$,
  где n = 64, 128 или 256,
  т.е. имеет порядок 10^{19}–10^{77}?
- Отбор подстановок указанного порядка по их свойствам

БЛОЧНЫЕ ШИФРЫ

- *P-блоки* (*P-box, permutation box*) и *S-блоки* (*S-box, substitution box*).

БЛОЧНЫЕ ШИФРЫ

- *m*-битовые наборы – как элементы алгебраических систем:
  - линейного пространства $(Z_2)^n$,
  - кольца вычетов Z_{2^n},
  - конечного поля F_{2^n},
  - мультипликативной группы поля F_{2^n+1} (последнее – при условии, что 2^n+1 – простое число)

СХЕМЫ БЛОЧНЫХ ШИФРОВ

- ***Схема Фейстеля*** (***Feistel scheme***)

Подстановка, реализуемая схемой Фейстеля с R раундами обычно обозначается через $\Psi(f_1, \ldots, f_R)$,

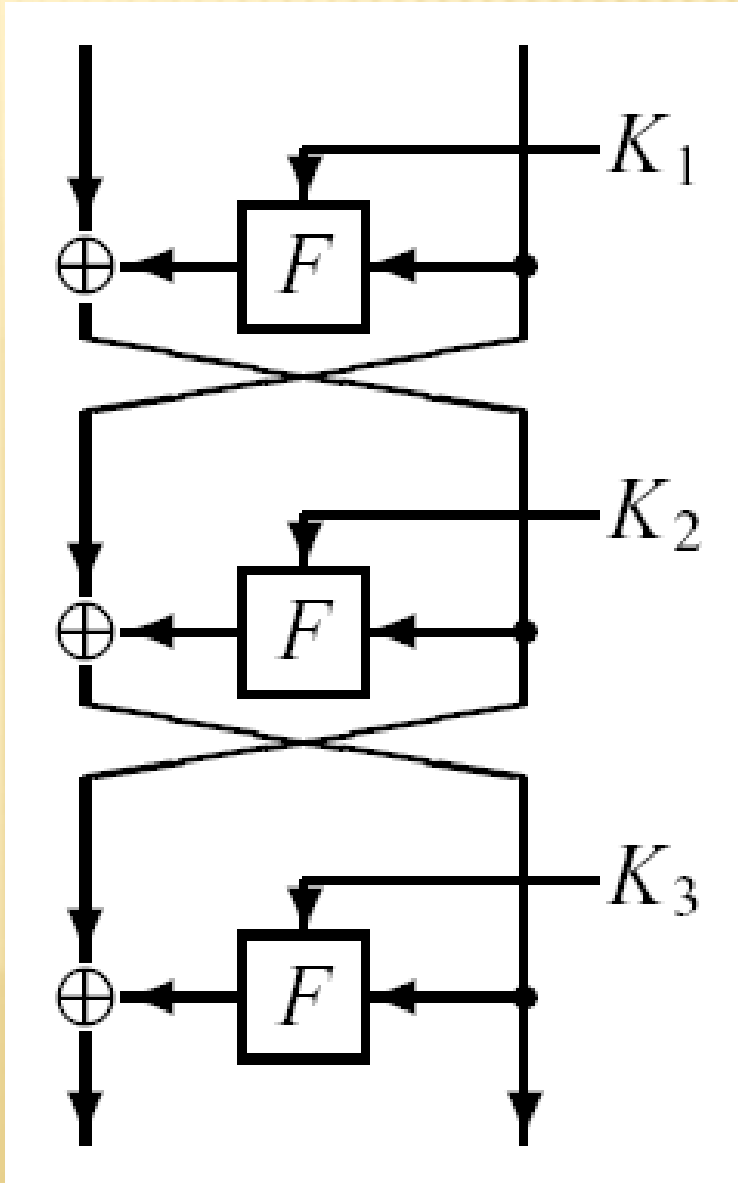


СХЕМА ФЕЙСТЕЛЯ

Подстановки вида $\Psi(f_1, \ldots, f_R)$ являются в определенном смысле «очень хорошими» с криптографической точки зрения:

- $\Psi(f_1, f_2, f_3)$ реализует псевдослучайную подстановку
- $\Psi(f_1, f_2, f_3, f_4)$ – суперпсевдослучайная подстановка

СХЕМА ФЕЙСТЕЛЯ

Подстановки вида $\Psi(f_1, f_2, f_3, f_4)$, $\Psi(f_1, f_1, f_1, f_2)$, $\Psi(f_1, f_2, f_2, f_2)$, $\Psi(f_1, f_1, f_2, f_2)$, $\Psi(f_1, f_2, f_1, f_2)$, $\Psi(f_1, f_1, f_2, f_1)$, $\Psi(f_1, f_2, f_1, f_1)$, а также $\Psi(f_1, 1, f_2, f_1, 1, f_2)$ и $\Psi(f_1, 1, f_1^2, f_1, 1, f_1^2)$ реализуют суперпсевдослучайные подстановки

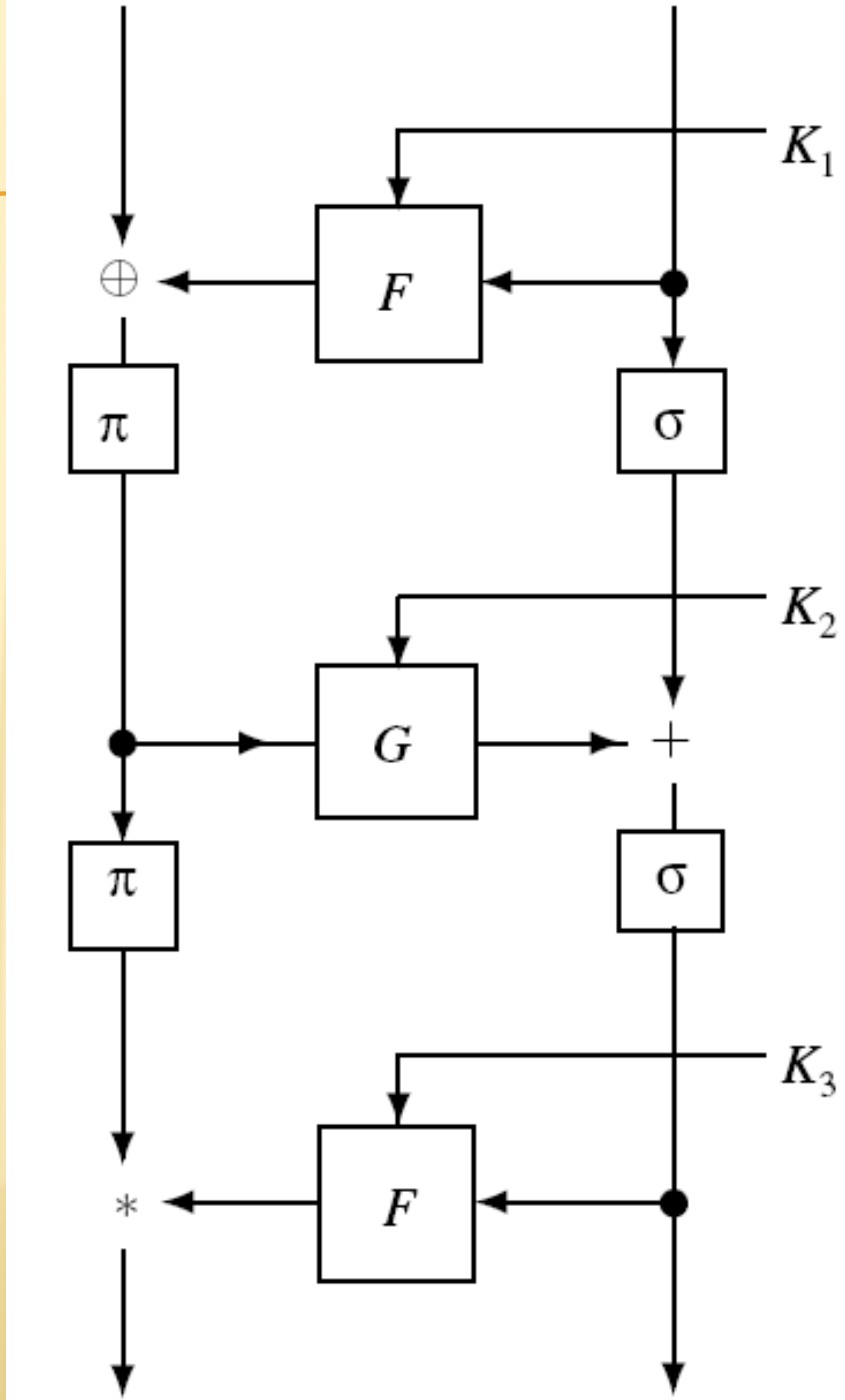
СХЕМА ФЕЙСТЕЛЯ

Подстановки вида

- $\Psi(f_1, f_2, f_3)$,
- $\Psi(f_1, f_1, f_2)$,
- $\Psi(f_1, f_2, f_2)$,
- $\Psi(f_1, f_1, f_1, f_1^k)$

– реализуют псевдослучайные но не суперпсевдослучайные подстановки.

ОБОБЩЕНИЯ СХЕМЫ ФЕЙСТЕЛЯ



СХЕМЫ БЛОЧНЫХ ШИФРОВ

- ***Схема Лая-Месси*** (***Lai-Massey***).

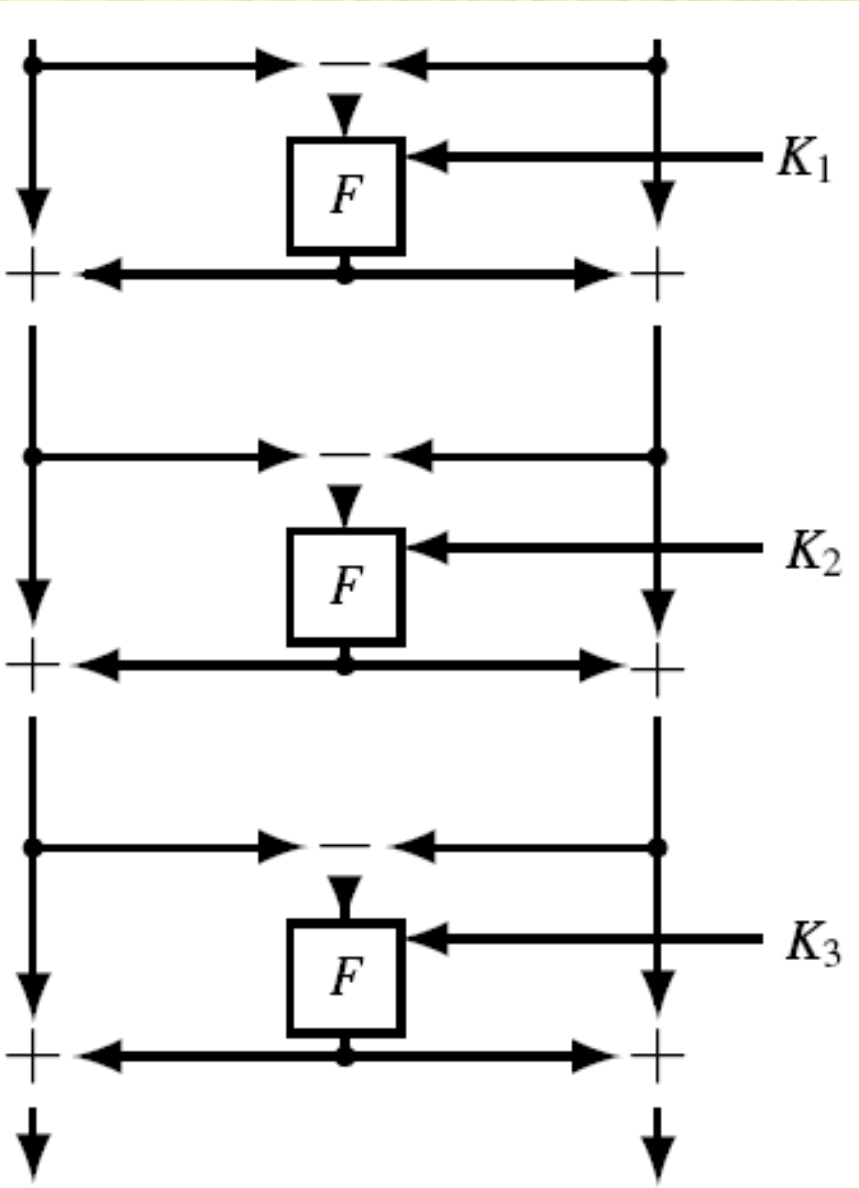
Вход: (x_L , x_R);

$$t = F(x_L - x_R),$$

$$y_L = x_L + t,$$

$$y_R = x_R + t;$$

Выход: (y_L , y_R).



СХЕМЫ БЛОЧНЫХ ШИФРОВ

- ***Схема Лая-Месси (Lai-Massey).***

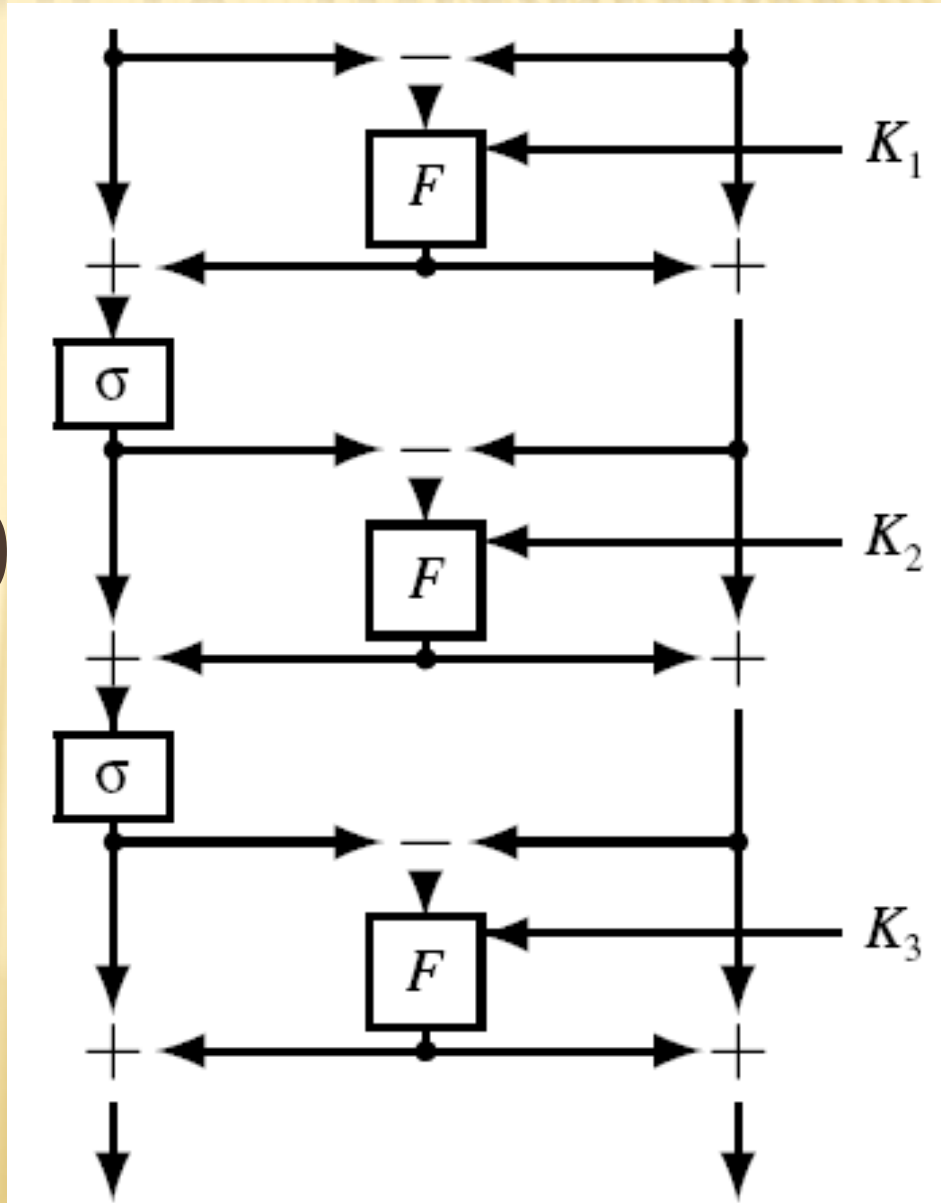
Вход: (x_L , x_R);

$$t = F(x_L - x_R)$$

$$y_L = \sigma(x_L + t),$$

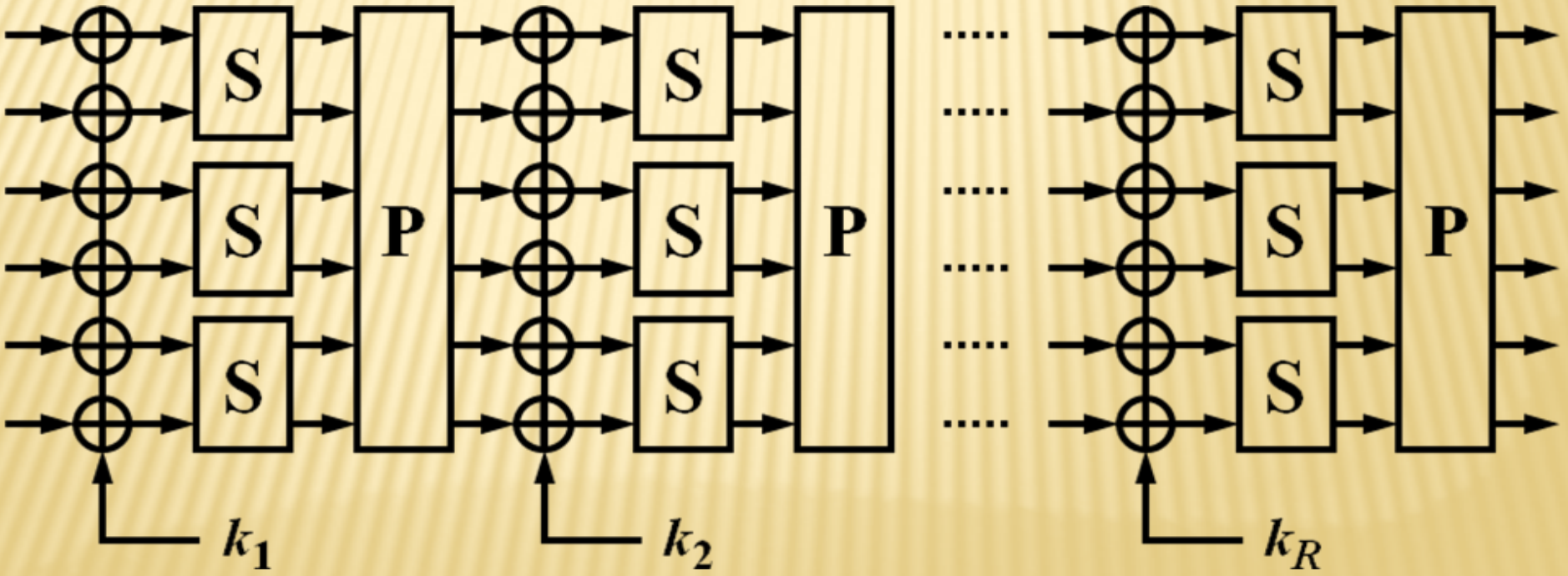
$$y_R = x_R + t;$$

Выход: (y_L , y_R).



СХЕМЫ БЛОЧНЫХ ШИФРОВ

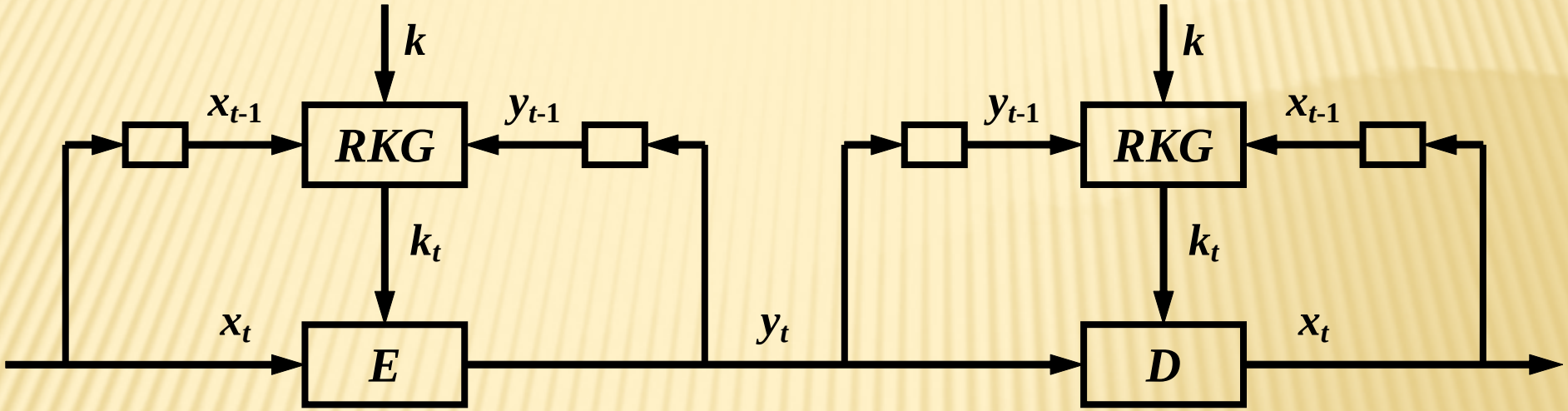
- ***SP-сеть (SP-net, Substitution-Permutation Network)***



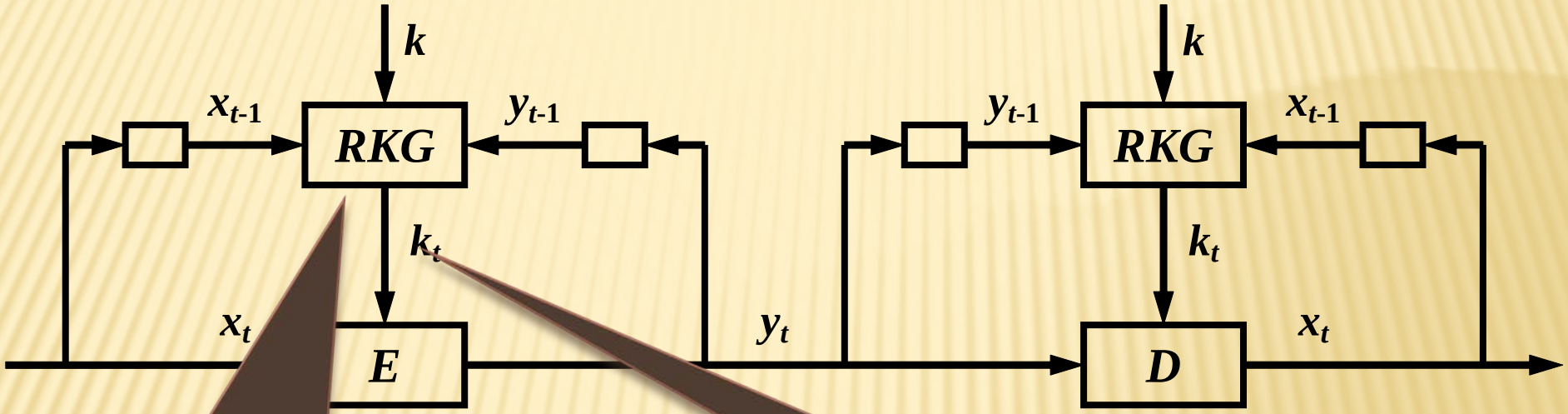
ПОТОЧНЫЕ ШИФРЫ

Поточный шифр (***stream cipher***) — симметричный шифр, который обрабатывает открытый текст посимвольно (побитно, побайтно, бинарными словами длины 32, 64 или 128 битов), причем преобразование, которому подвергаются последовательные знаки открытого текста, ***все время изменяется во времени***.

ПОТОЧНЫЕ ШИФРЫ



ПОТОЧНЫЕ ШИФРЫ

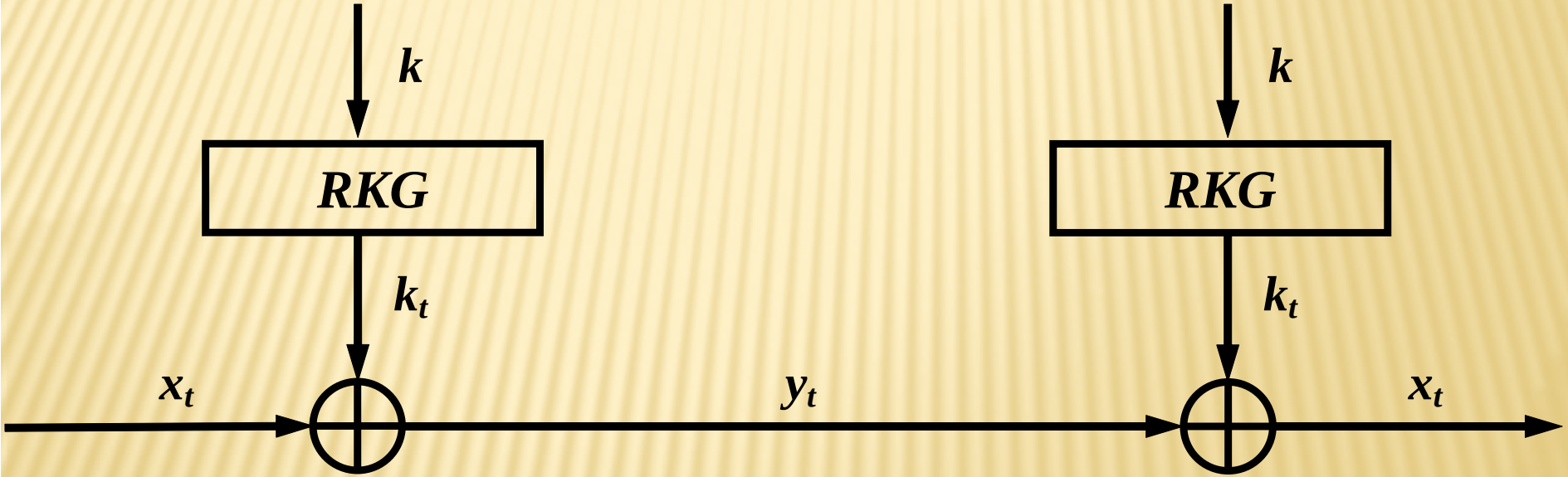


генератор ключевого потока

ключевой поток

ПОТОЧНЫЕ ШИФРЫ

Аддитивный синхронный поточный шифр (шифр гаммирования)



наиболее распространенный тип поточного шифра

ПОТОЧНЫЕ ШИФРЫ

Генераторы ключевого потока – криптографические генераторы псевдослучайных последовательностей

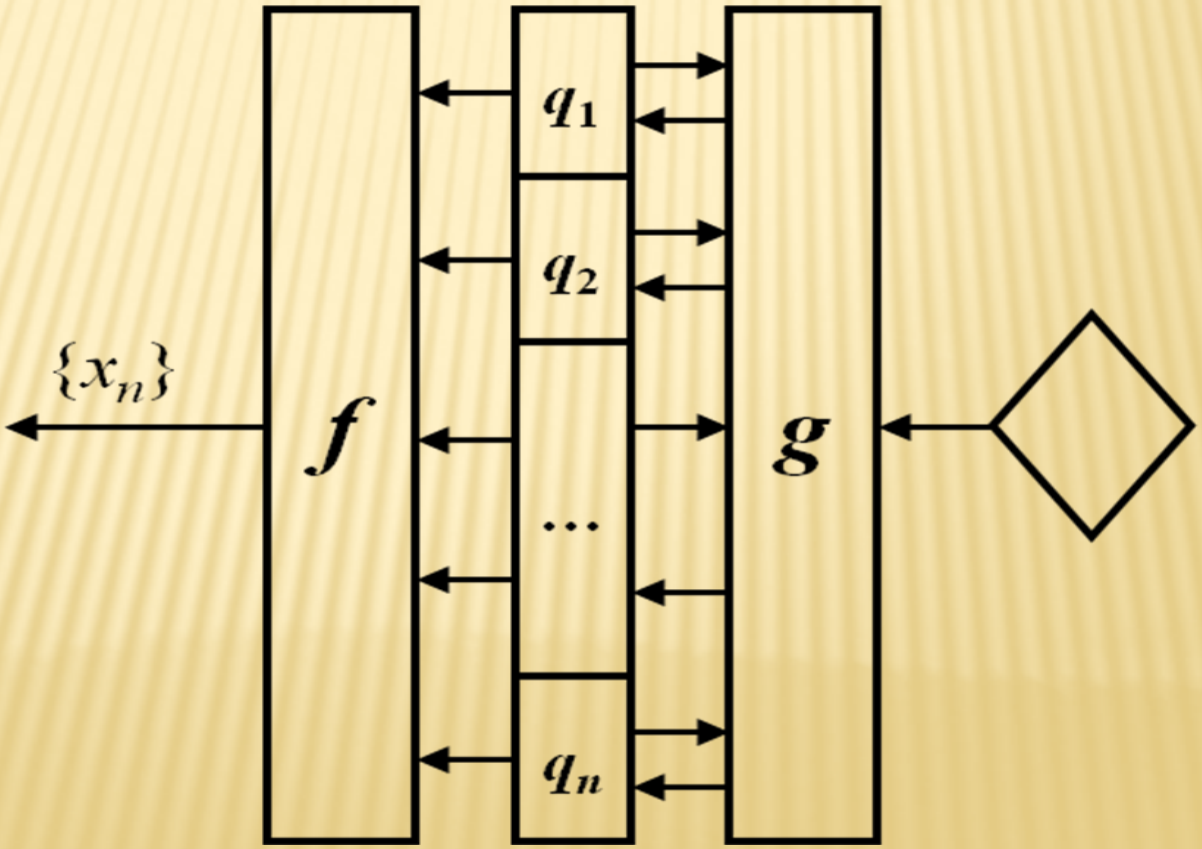
- ***Управляющая часть (Driving Part)***
- ***Комбинационная часть (Combining Part)***

УПРАВЛЯЮЩАЯ ЧАСТЬ

- Регистры сдвига с линейной обратной связью (*Linear Feedback Shift Register* – LFSR).
- Регистры сдвига с управляемым движением (*Jump Controlled LFSR*).
- Регистры сдвига с нелинейной обратной связью (*Nonlinear Feedback Shift Register* – NFSR).

УПРАВЛЯЮЩАЯ ЧАСТЬ

- **Динамические массивы памяти (*Dynamic Memory Array*).**



УПРАВЛЯЮЩАЯ ЧАСТЬ

- **Динамические массивы памяти (*Dynamic Memory Array*).**
  - **Клеточные автоматы (*cellular automata*).**
- **Счетчики (*Counter*).**

КОМБИНАЦИОННАЯ ЧАСТЬ

- Нелинейные функции.
- Прореживание последовательности, выработанной управляющей частью (*Decimating of the intermediate sequence*).
- Конечные автоматы (*finite-state machine*).
- Отдельные узлы блочных шифров.

ПРИМИТИВЫ С ОТКРЫТЫМ КЛЮЧОМ

Асимметричные шифры

ПРИМИТИВЫ С ОТКРЫТЫМ КЛЮЧОМ

Асимметричные шифры

«практические» однонаправленные функции

КРИПТОСИСТЕМА RSA

RSA (Rivest-Shamir-Adleman Cryptosystem)

- Задача факторизация модуля системы RSA (*RSA Factorization Problem* – RSAFP)

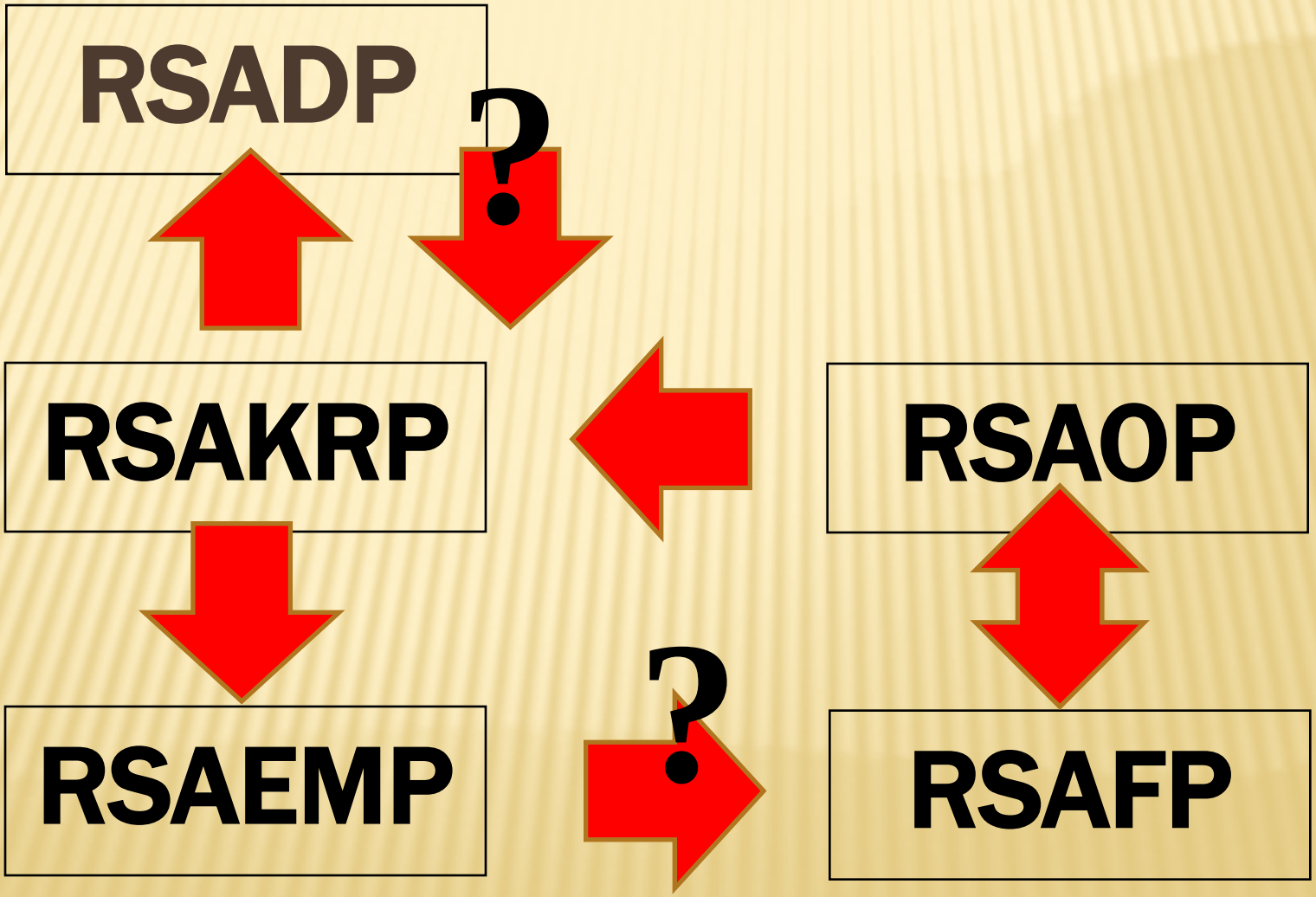
КРИПТОСИСТЕМА RSA

- Задача раскрытия системы RSA (*RSA Decryption Problem* – RSADP)
- Задача нахождения кратного экспоненты системы RSA (*RSA Exponent Multiple Problem* – RSAEMP)

КРИПТОСИСТЕМА RSA

- Задача нахождения секретного ключа системы RSA (*RSA Key Recovery Problem* – RSAKRP)
- Задача нахождения порядка мультипликативной группы системы RSA (*RSA Order Problem* – RSAOP)

КРИПТОСИСТЕМА RSA



ДИСКРЕТНЫЕ ЛОГАРИФМЫ

- Задача дискретного логарифмирования (*discrete logarithm problem* – DLP):

Дано: $G = \langle g \rangle$,

$\forall y \in G$ *найти* x: $y = g^x$.

$$x = \log_g y$$

ДИСКРЕТНЫЕ ЛОГАРИФМЫ

- Порядок группы G может быть известен или неизвестен.
- Элемент y не обязательно лежит в группе G. В этом случае появляется задача, как отличать элементы группы G от других элементов.

ДИСКРЕТНЫЕ ЛОГАРИФМЫ

- *Discrete Logarithm Problem* – DLP
- *Discrete Logarithm with Known Order Problem* – DLKOP
- *Discrete Logarithm with Known Order Factorization Problem* DLKOFP

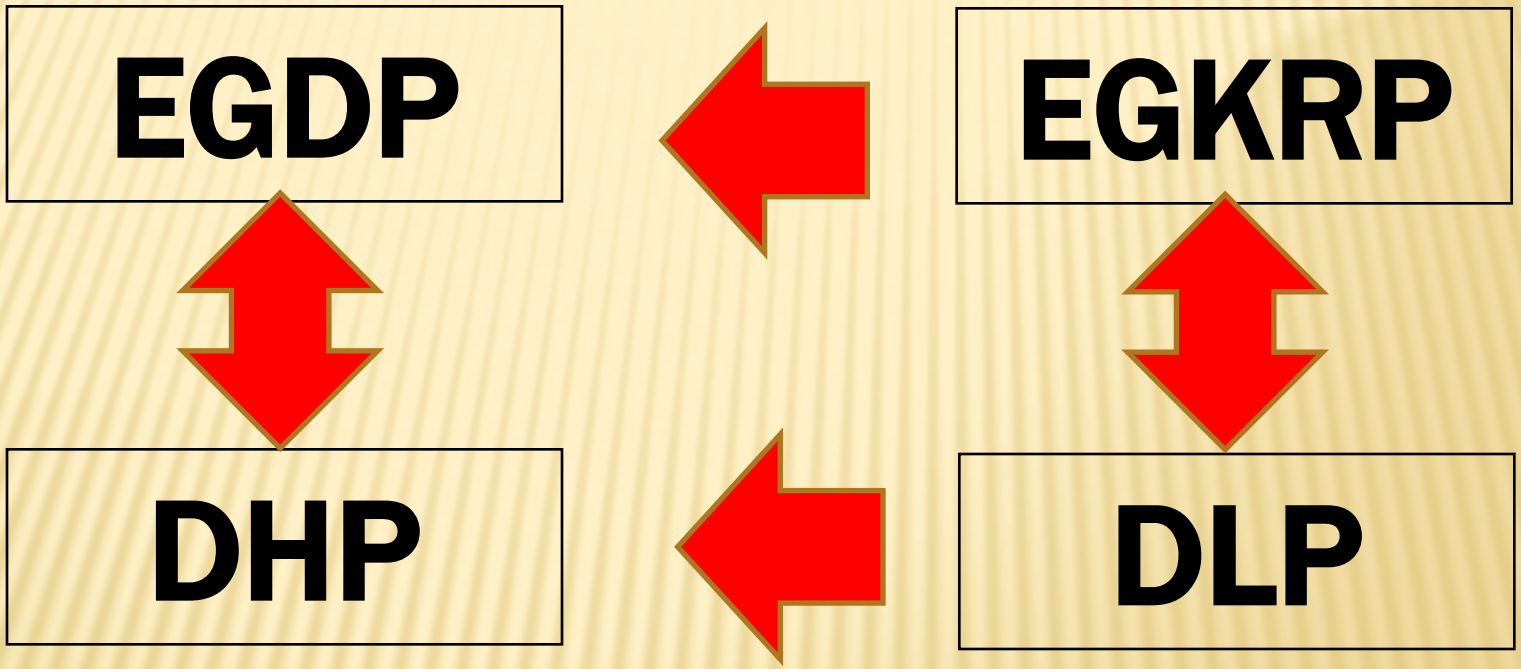
ПРОТОКОЛ ДИФФИ-ХЕЛЛМАНА

- ***Diffie-Hellman Problem*** **– DHP**
- ***Decisional Diffie-Hellman Problem*** **– DDHP**

АЛГОРИТМ ШИФРОВАНИЯ ЭЛЬ-ГАМАЛЯ

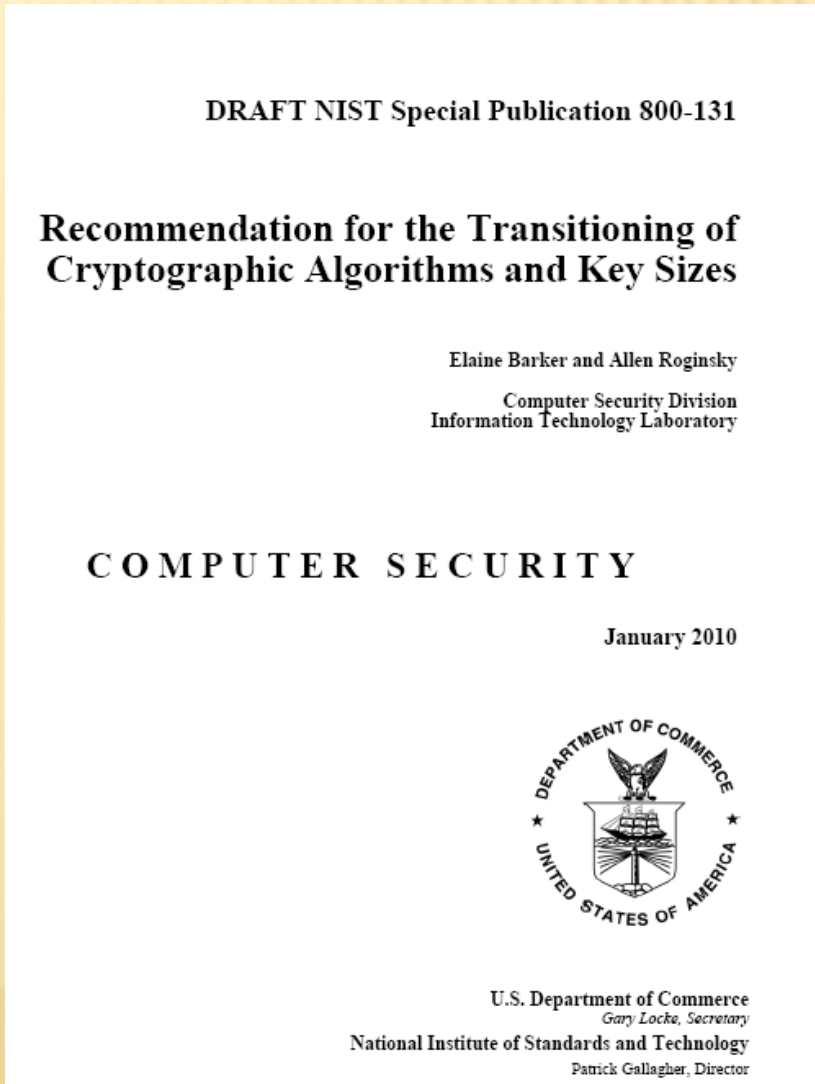
- *ElGamal Decryption Problem* – EGDP
- *ElGamal Key Recovery Problem* – EGKRP

ДИСКРЕТНЫЕ ЛОГАРИФМЫ



SP 800-131

RECOMMENDATION FOR THE TRANSITIONING OF CRYPTOGRAPHIC ALGORITHMS AND KEY SIZES



DRAFT NIST Special Publication 800-131

Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes

Elaine Barker and Allen Roginsky

Computer Security Division
Information Technology Laboratory

COMPUTER SECURITY

January 2010

U.S. Department of Commerce
Gary Locke, Secretary
National Institute of Standards and Technology
Patrick Gallagher, Director

СРАВНИТЕЛЬНАЯ СТОЙКОСТЬ КРИПТОАЛГОРИТМОВ И СРОКИ ИХ ДЕЙСТВИЯ

Bits of security	Symmetric key algorithms	FFC (DSA, D-H, MQV)	IFC (RSA)	ECC (ECDSA)
80 (до 2010 г.)	2TDEA, SKIPJACK,	$L = 1024$ $N = 160$	$k = 1024$	$f = 160-223$
112 (до 2030 г.)	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224-255$
128 (после 2030 г.)	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256-383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384-511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ И НЕЧИСЛОВЫЕ АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ

Так как для алгебраических объектов теоретико-числовой природы разработаны сравнительно хорошие алгоритмы, для построения новых систем с открытым ключом можно попробовать уход в алгебраические системы с элементами нечисловой природы, например, в неабелевые группы – группы заведомо нечисловой природы.

ТРУДНЫЕ ЗАДАЧИ В ТЕОРИИ ГРУПП

При использовании таких групп в криптосистеме с открытым ключом прежде всего возникают следующие вопросы:

ТРУДНЫЕ ЗАДАЧИ В ТЕОРИИ ГРУПП

- Как представить сообщение в виде элемента группы G;
- Существует ли единственное представление для элементов группы G. Если элементы представляются не единственным образом, открытый текст и расшифрованный могут не совпасть.
- Возможно ли эффективное вычисление такого представления.

ТРУДНЫЕ ЗАДАЧИ В ТЕОРИИ ГРУПП

- **Проблема сопряженности:**

  Дано: $x, y \in G$

  Определить: $x \sim y$?

- **Проблема поиска сопрягающего элемента:**

  Дано: $x, y \in G, x \sim y$

  Определить: $a \in G$: $y = axa^{-1}$

ТРУДНЫЕ ЗАДАЧИ В ТЕОРИИ ГРУПП

- **Обобщенная проблема поиска сопрягающего элемента:**

  Дано: $x, y \in G$, $y = bxb^{-1}$, $b \in H \subset G$,

  b — *неизвестен*

  Определить: $a \in G$: $y = axa^{-1}$

ТРУДНЫЕ ЗАДАЧИ В ТЕОРИИ ГРУПП

- **Проблема сопряженной разрешимости:**

  Дано: $x, y \in G,\ \ y = bxb^{-1},\ b \in H \subset G$

  Определить: $a_1, a_2 \in G$: $a_1 x a_2 = y$

- **Проблема извлечения корня:**

  Дано: $y \in G, y = x^p,\ x - неизвестен$

  Определить: $z \in G$: $y = z^p$

"...after almost thirty years of public-key cryptography, there is still no proof that trapdoor one-way functions, which are the fundament to the theory, exist."

Jim Massey, January 2002.

ВЫЧИСЛИТЕЛЬНЫЕ МОДЕЛИ

- Машины Тьюринга
- Равнодоступные адресные машины (PAM)
- Схемы из функциональных элементов
- Конечные автоматы
- И т.д. и т.п.

ВЫЧИСЛИТЕЛЬНЫЕ МОДЕЛИ

- Машины Тьюринга
- Равнодоступные адресные машины (PAM)
- Схемы из функциональных элементов
- Конечные автоматы
- И т.д. и т.п.

ВЫЧИСЛИТЕЛЬНЫЕ МОДЕЛИ

- Машины Тьюринга
- Равнодоступные адресные машины (PAM)
- Схемы из функциональных элементов
- Конечные автоматы
- И т.д. и т.п.

НОВЫЙ ПОДХОД К ОДНОНАПРАВЛЕННОСТИ

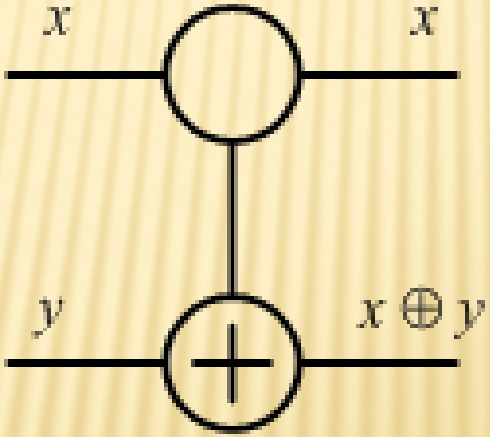
В качестве меры сложности того или иного преобразования будем рассматривать сложность минимальной булевой схемы, реализующей данное преобразование и обозначаемой через $C(f)$. В качестве модели однонаправленной функции будем рассматривать *вычислительно асимметричное преобразование*, т.е. такое обратимое преобразование, сложность которого отличается от сложности обратного преобразования.

ВЫЧИСЛИТЕЛЬНО АСИММЕТРИЧНЫЕ ПРЕОБРАЗОВАНИЯ

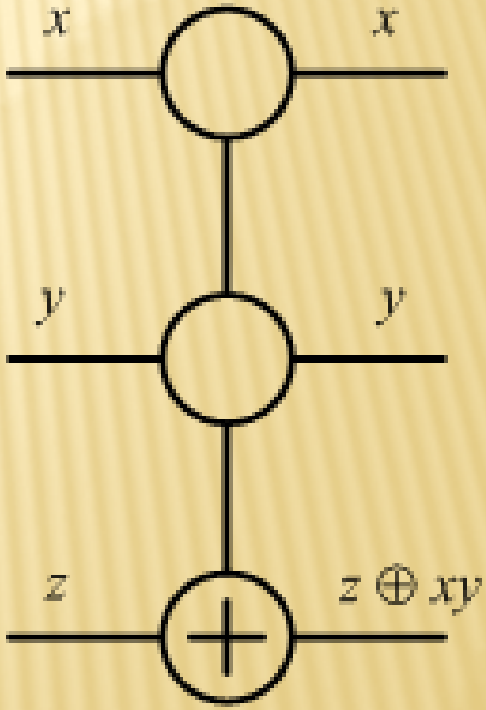
- Boppana R.B., Lagarias J.C. *One-way functions and circuit complexity.* Information and Computation, v. 74 (1987), pp. 226-240
- Hiltgen A.P. *Constructions of feebly-one-way families of permutations.* AUSCRYPT'92, LNCS v.718 (1993), pp. 422-434
- Hiltgen A.P. *Cryptographically Relevant Contributions to Combinatorial Complexity Theory.* ETH Series in Information Processing, vol. 3 (1993)

ОБРАТИМЫЕ ЛОГИЧЕСКИЕ ЭЛЕМЕНТЫ

Элемент NOT

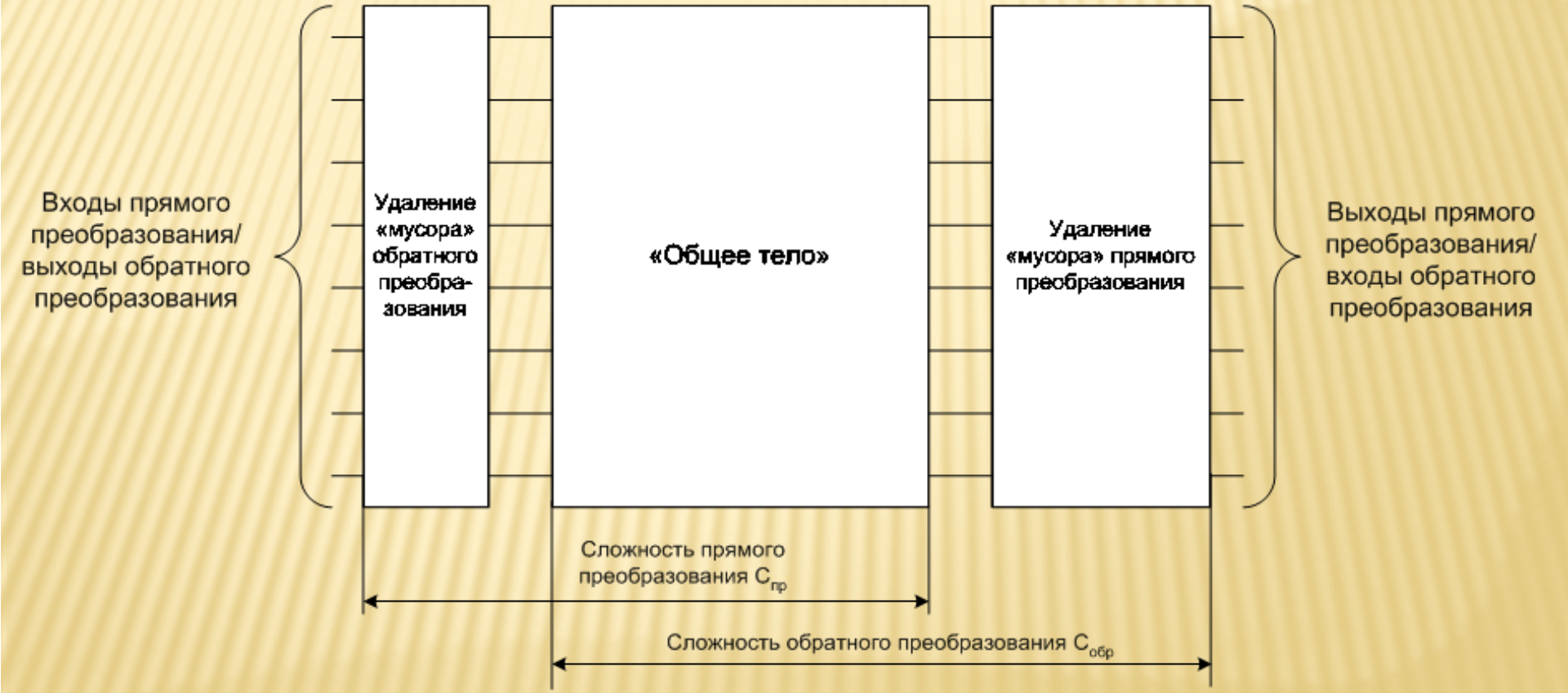


Элемент CNOT



Элемент CCNOT

ОБРАТИМЫЕ СХЕМЫ



НОВЫЙ ПОДХОД К ОДНОНАПРАВЛЕННОСТИ

В отличии от предыдущих подходов, когда рассматривались *две отдельные схемы* – для f и для f^{-1}, при новом подходе эти схемы связаны внутри одной схемы и являются *подсхемами одной и той же схемы* – построенной из обратимых логических элементов обратимой схемы для обратимого преобразования f.


КОНЕЦ