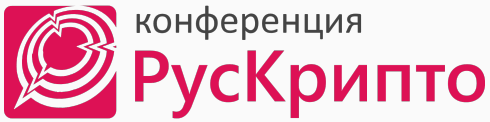
Криптография как реализация полезных интерфейсов

Сергей Агиевич
НИИ прикладных проблем математики и информатики
Белорусский государственный университет
2021-03-24, Минск — Солнечный



Содержание

Полезные интерфейсы

Несекретное засекречивание

J. H. Ellis (GCHQ/CESG Report, 1970) The Possibility Of Secure Non-Secret Digital Encryption

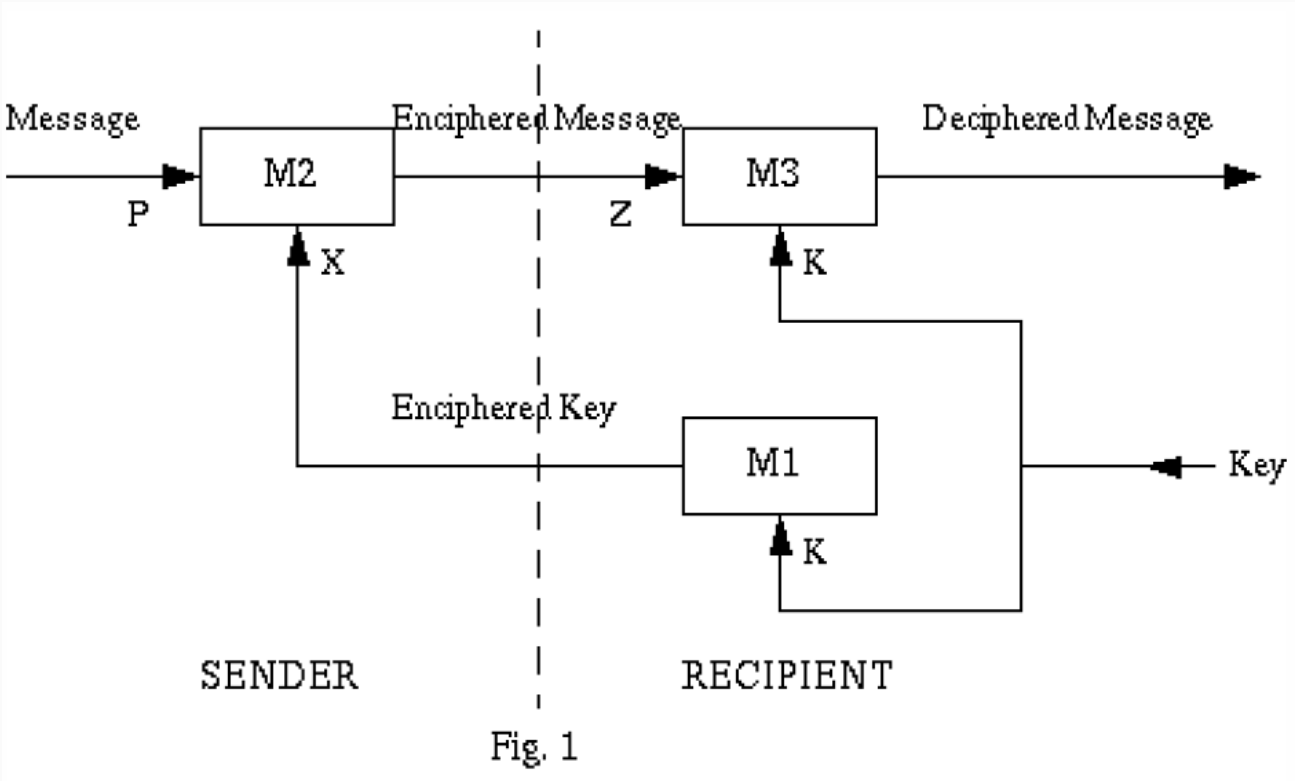
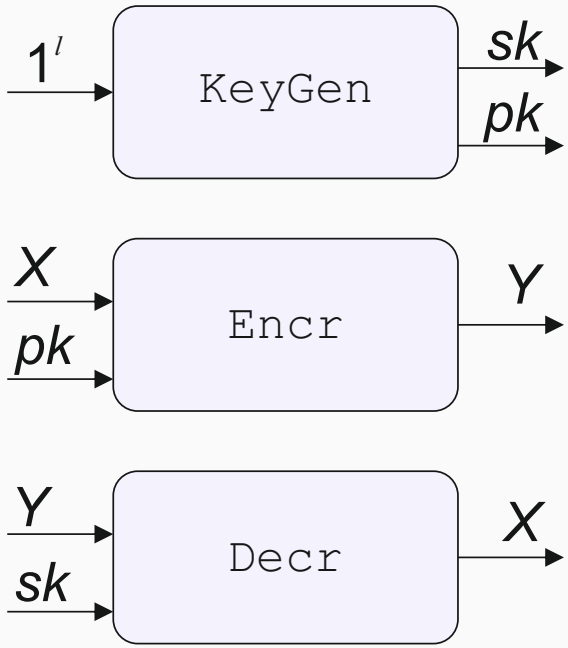


Fig. 1

Шифрование с открытым ключом



l — уровень стойкости

---

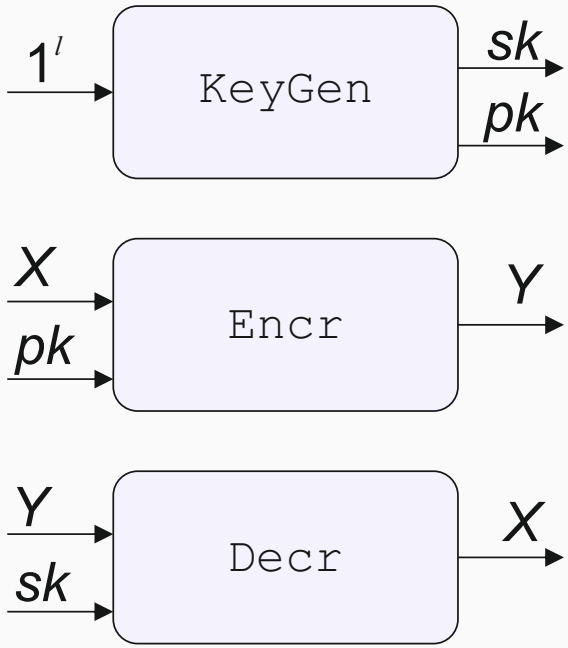
sk — личный ключ

pk — открытый ключ

X — открытый текст

Y — шифртекст

Шифрование с открытым ключом



l — уровень стойкости

---

sk — личный ключ

pk — открытый ключ

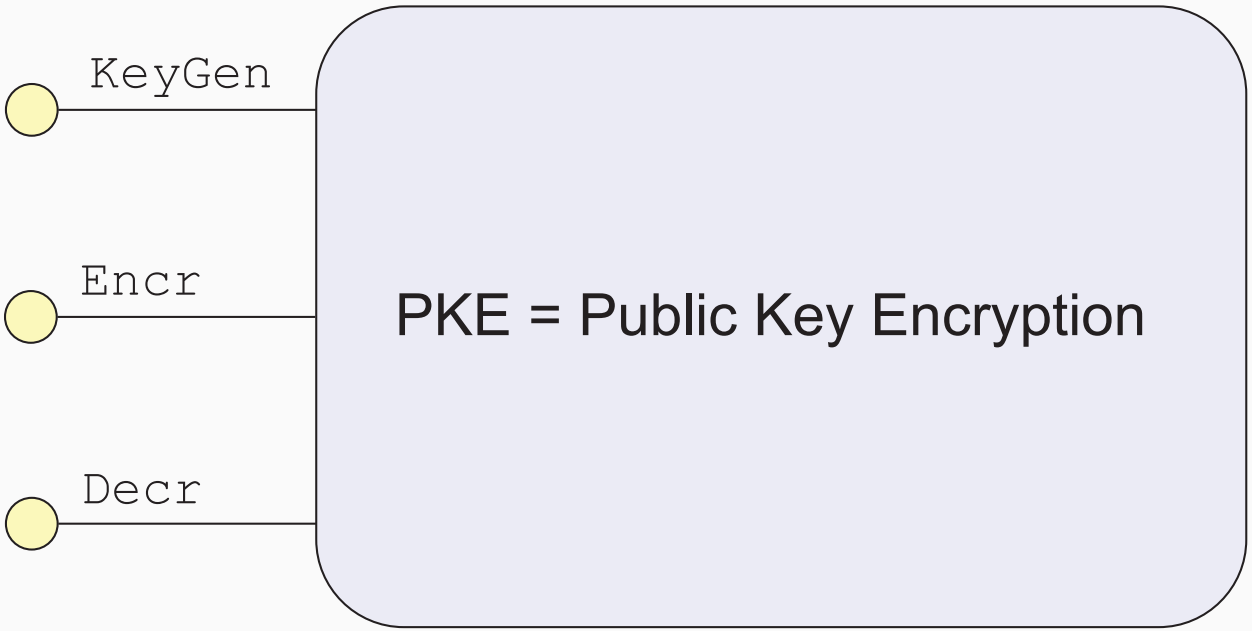
X — открытый текст

Y — шифртекст

Полезный интерфейс:

$$\texttt{Decr}(\texttt{Encr}(X, pk), sk) = X \quad \forall X, (sk, pk) \leftarrow \texttt{KeyGen}(1^l)$$

Шифрование с открытым ключом



Реализация интерфейсов

Шифрование с открытым ключом

- Концепция: Diffie, Hellman (1976) // Ellis (1970)
- Реализация: Rivest, Shamir, Adleman (1977) // Cocks (1973)

Реализация интерфейсов

Шифрование с открытым ключом

- Концепция: Diffie, Hellman (1976) // Ellis (1970)
- Реализация: Rivest, Shamir, Adleman (1977) // Cocks (1973)

Идентификационное шифрование

- Концепция: Shamir (1984)
- Реализация: Cocks (2001), Boneh, Franklin (2001)

Реализация интерфейсов

Шифрование с открытым ключом

- Концепция: Diffie, Hellman (1976) // Ellis (1970)
- Реализация: Rivest, Shamir, Adleman (1977) // Cocks (1973)

Идентификационное шифрование

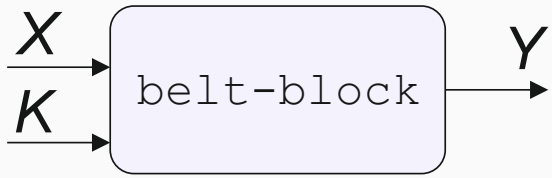
- Концепция: Shamir (1984)
- Реализация: Cocks (2001), Boneh, Franklin (2001)

(Полностью) гомоморфное шифрование

- Концепция: Rivest, Adleman, Dertouzos (1978)
- Реализация: Gentry (2009)

Собственный опыт

Шифрование блока (Belt, 2001)

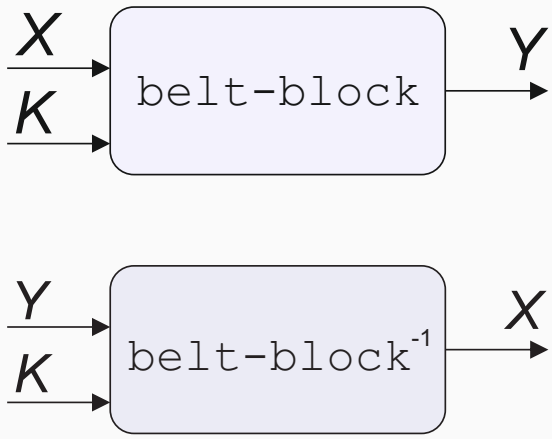


$X \in \{0,1\}^{128}$ (открытый текст)

$K \in \{0,1\}^{256}$ (ключ)

$Y \in \{0,1\}^{128}$ (шифртекст)

Шифрование блока (Belt, 2001)

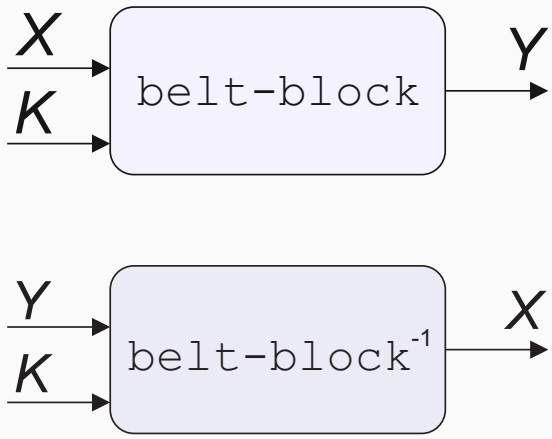


$X \in \{0,1\}^{128}$ (открытый текст)

$K \in \{0,1\}^{256}$ (ключ)

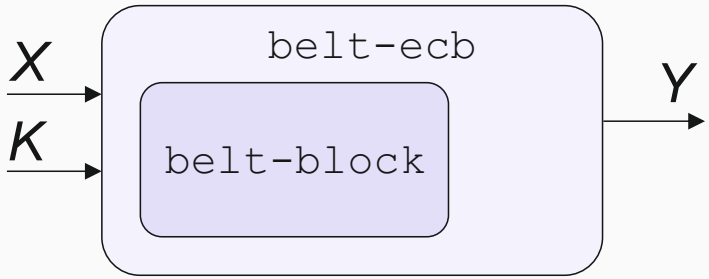
$Y \in \{0,1\}^{128}$ (шифртекст)

Шифрование блока (Belt, 2001)



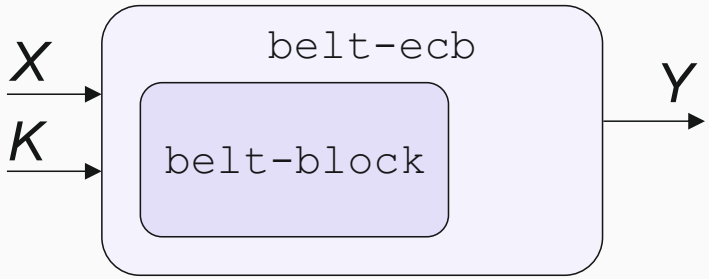
$$X \in \{0,1\}^{128} \text{ (открытый текст)}$$
$$K \in \mathcal{K} \in \{\{0,1\}^{128}, \{0,1\}^{192}, \{0,1\}^{256}\}$$
$$\overline{Y \in \{0,1\}^{128} \text{ (шифртекст)}}$$

Режимы шифрования

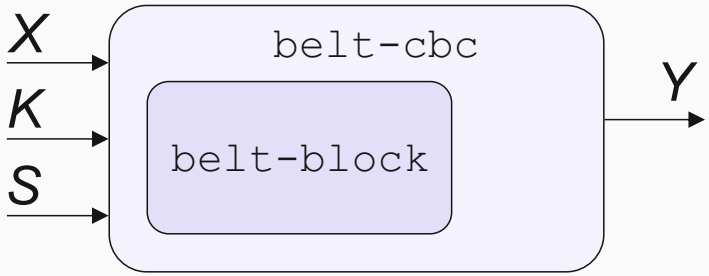


$$\frac{X \in \{0,1\}^{128*} \quad K \in \mathcal{K}}{Y \in \{0,1\}^{|X|}}$$

Режимы шифрования

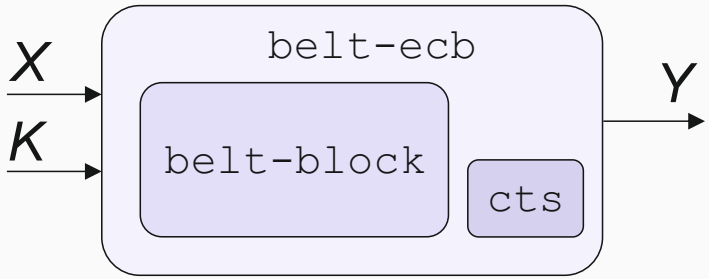


$$X \in \{0,1\}^{128*}$$
$$K \in \mathcal{K}$$
$$\hline$$
$$Y \in \{0,1\}^{|X|}$$

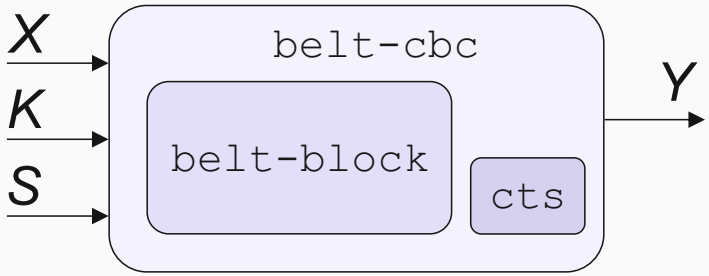


$$X \in \{0,1\}^{128*}$$
$$K \in \mathcal{K}$$
$$S \in \{0,1\}^{128} \text{ (синхропосылка)}$$
$$\hline$$
$$Y \in \{0,1\}^{|X|}$$

Режимы шифрования

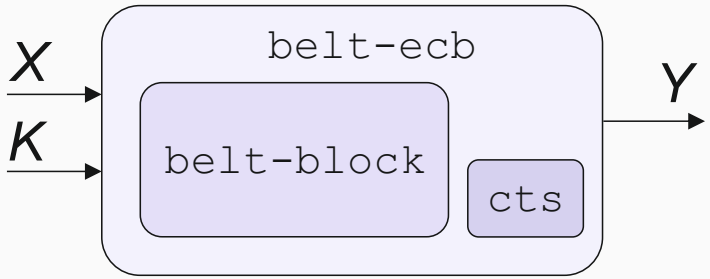


$$X \in \{0,1\}^{\geq 128}$$
$$K \in \mathcal{K}$$
$$\overline{Y \in \{0,1\}^{|X|}}$$

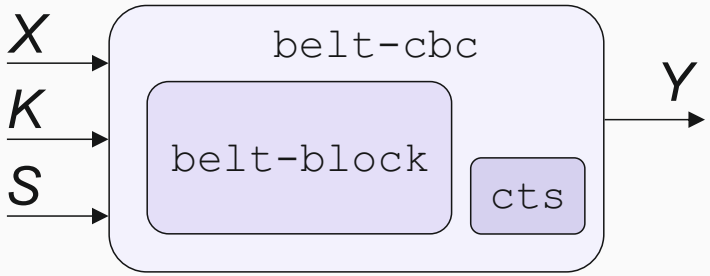


$$X \in \{0,1\}^{\geq 128}$$
$$K \in \mathcal{K}$$
$$S \in \{0,1\}^{128} \text{ (синхропосылка)}$$
$$\overline{Y \in \{0,1\}^{|X|}}$$

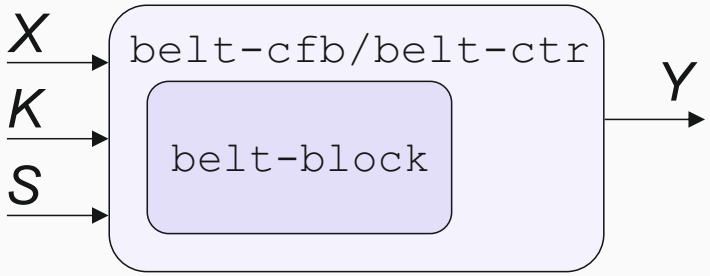
Режимы шифрования



$$X \in \{0,1\}^{\geq 128}$$
$$K \in \mathcal{K}$$
$$\overline{Y \in \{0,1\}^{|X|}}$$

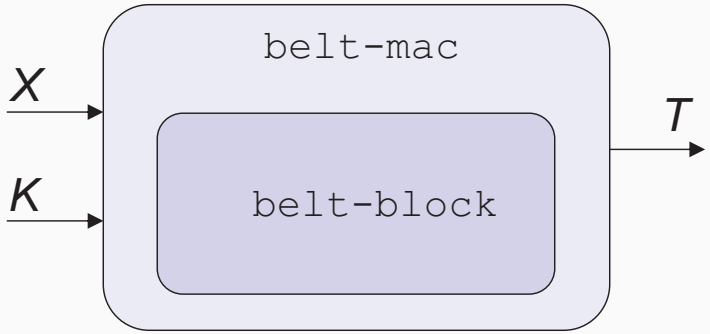


$$X \in \{0,1\}^{\geq 128}$$
$$K \in \mathcal{K}$$
$$S \in \{0,1\}^{128} \text{ (синхропосылка)}$$
$$\overline{Y \in \{0,1\}^{|X|}}$$



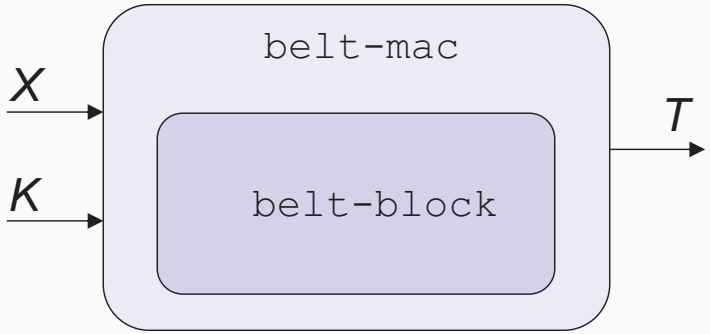
$$X \in \{0,1\}^{*}$$
$$K \in \mathcal{K}$$
$$S \in \{0,1\}^{128}$$
$$\overline{Y \in \{0,1\}^{|X|}}$$

Инкапсуляция

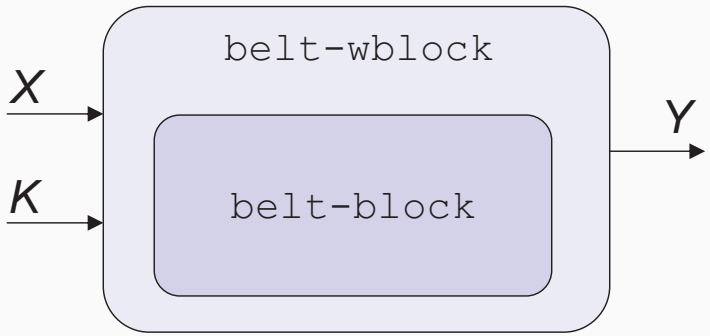


$$\frac{X \in \{0,1\}^* \quad K \in \mathcal{K}}{T \in \{0,1\}^{64} \text{ (имитовставка)}}$$

Инкапсуляция

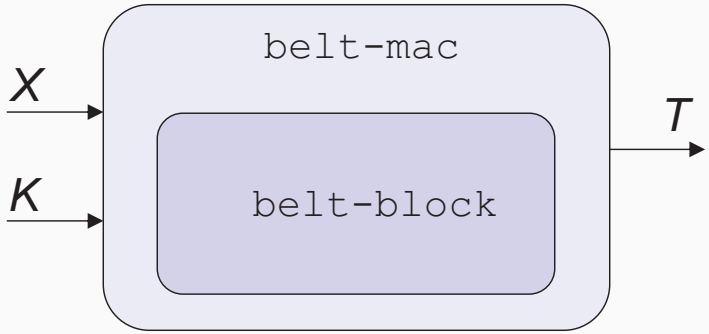


$$\frac{X \in \{0,1\}^* \quad K \in \mathcal{K}}{T \in \{0,1\}^{64} \text{ (имитовставка)}}$$

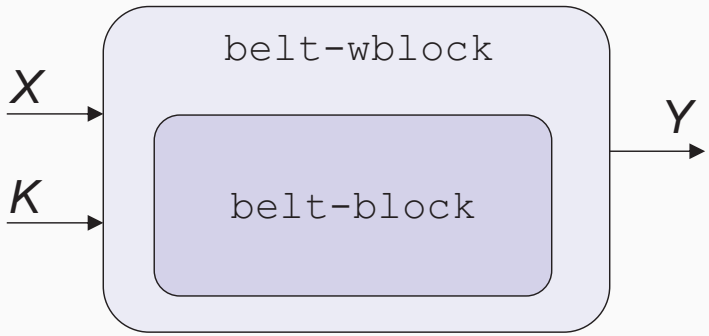


$$\frac{X \in \{0,1\}^{\geq 256} \text{ (широкий блок)} \quad K \in \mathcal{K}}{Y \in \{0,1\}^{|X|}}$$

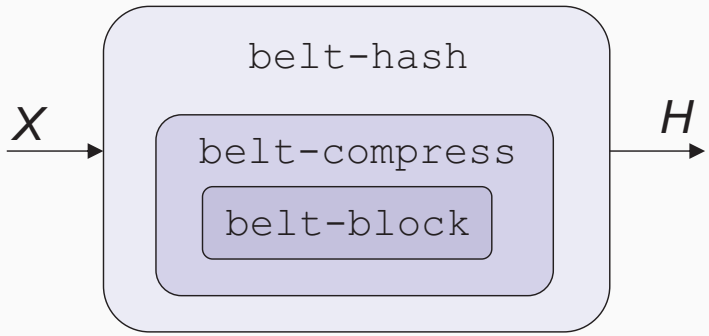
Инкапсуляция



$$X \in \{0,1\}^*$$
$$K \in \mathcal{K}$$
$$T \in \{0,1\}^{64} \text{ (имитовставка)}$$



$$X \in \{0,1\}^{\geq 256} \text{ (широкий блок)}$$
$$K \in \mathcal{K}$$
$$Y \in \{0,1\}^{|X|}$$



$$X \in \{0,1\}^*$$
$$H \in \{0,1\}^{256} \text{ (хэш-значение)}$$

Шифрование + имитозащита

$$\{\texttt{belt-cbc} \mid \texttt{belt-ctr} \mid \texttt{belt-cfb}\} + \texttt{belt-mac}$$

Шифрование + имитозащита

$\{\texttt{belt-cbc} \mid \texttt{belt-ctr} \mid \texttt{belt-cfb}\} + \texttt{belt-mac}$

совмещение ключей?

Шифрование + имитозащита

$\{\texttt{belt-cbc} \mid \texttt{belt-ctr} \mid \texttt{belt-cfb}\} + \texttt{belt-mac}$

~~совмещение ключей?~~ (опасно)

Шифрование + имитозащита

$\{\texttt{belt-cbc} \mid \texttt{belt-ctr} \mid \texttt{belt-cfb}\} + \texttt{belt-mac}$

~~совмещение ключей?~~ (опасно)

два отдельных ключа?

Шифрование + имитозащита

$\{\texttt{belt-cbc} \mid \texttt{belt-ctr} \mid \texttt{belt-cfb}\} + \texttt{belt-mac}$

~~совмещение ключей?~~ (опасно)

~~два отдельных ключа?~~ (неудобно)

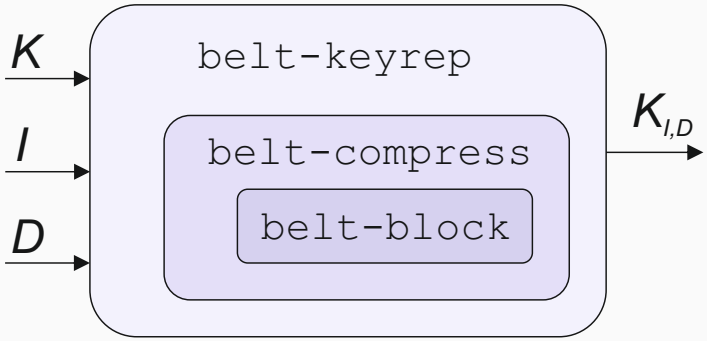
Шифрование + имитозащита

$\{\texttt{belt-cbc} \mid \texttt{belt-ctr} \mid \texttt{belt-cfb}\} + \texttt{belt-mac}$

~~совмещение ключей?~~ (опасно)

~~два отдельных ключа?~~ (неудобно)

Построение ключей:



$K \in \mathcal{K}$

$I \in \{0,1\}^{128}$ (заголовок / тип)

$D \in \{0,1\}^{96}$ (уровень / номер)

$K_{I,D}$

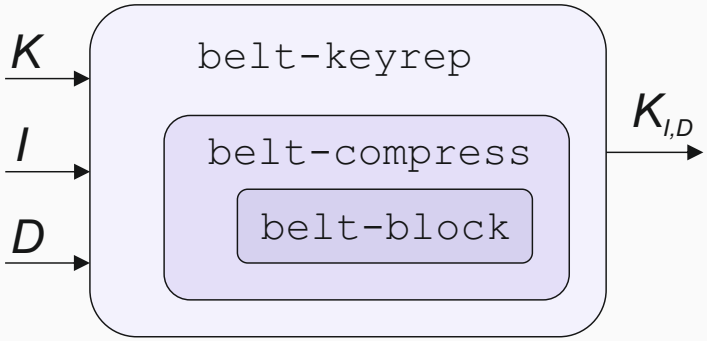
Шифрование + имитозащита

$\{\texttt{belt-cbc} \mid \texttt{belt-ctr} \mid \texttt{belt-cfb}\} + \texttt{belt-mac}$

~~совмещение ключей?~~ (опасно)

~~два отдельных ключа?~~ (неудобно)

Построение ключей:



$K \in \mathcal{K}$

$I \in \{0,1\}^{128}$ (заголовок / тип)

$D \in \{0,1\}^{96}$ (уровень / номер)

$K_{I,D}$

Обновление

$K_{I,1} \mapsto K_{I,2} \mapsto \ldots$

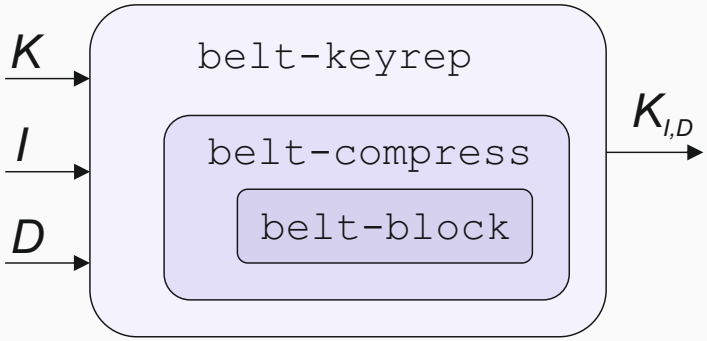
Шифрование + имитозащита

$\{\texttt{belt-cbc} \mid \texttt{belt-ctr} \mid \texttt{belt-cfb}\} + \texttt{belt-mac}$

~~совмещение ключей?~~ (опасно)

~~два отдельных ключа?~~ (неудобно)

Построение ключей:



$K \in \mathcal{K}$

$I \in \{0,1\}^{128}$ (заголовок / тип)

$D \in \{0,1\}^{96}$ (уровень / номер)

$K_{I,D}$

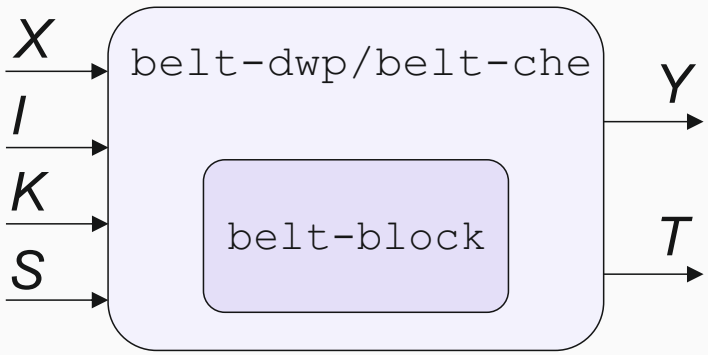
Обновление

$K_{I,1} \mapsto K_{I,2} \mapsto \ldots$

Диверсификация

$K \mapsto (K_{\texttt{ctr},0}, K_{\texttt{mac},0}, \ldots)$

Аутентифицированное шифрование



$X \in \{0,1\}^*$ (открытый текст)

$I \in \{0,1\}^*$ (ассоц. данные)

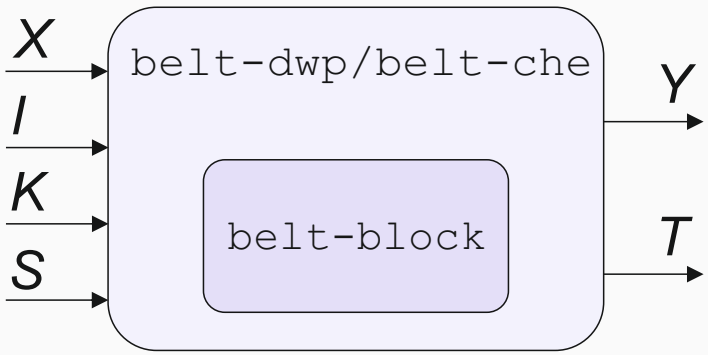
$K \in \mathcal{K}$ (ключ)

$S \in \{0,1\}^{128}$ (синхропосылка)

$Y \in \{0,1\}^{|X|}$ (шифртекст)

$T \in \{0,1\}^{64}$ (имитовставка)

Аутентифицированное шифрование



$X \in \{0,1\}^*$ (открытый текст)

$I \in \{0,1\}^*$ (ассоц. данные)

$K \in \mathcal{K}$ (ключ)

$S \in \{0,1\}^{128}$ (синхропосылка)

$Y \in \{0,1\}^{|X|}$ (шифртекст)

$T \in \{0,1\}^{64}$ (имитовставка)

Пакет:

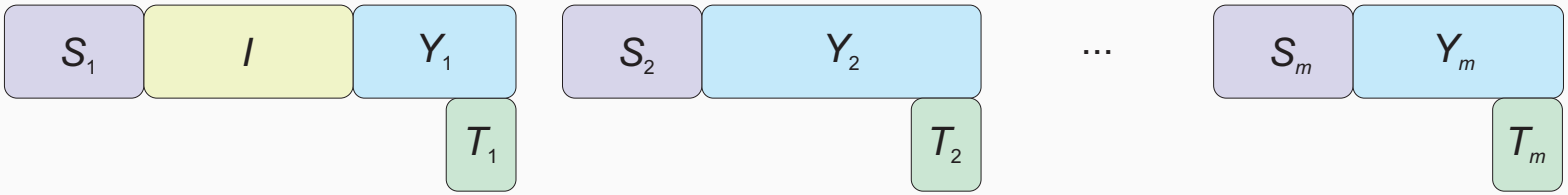
Аутентифицированное шифрование — II

Что делать при обработке большого текста X?

Аутентифицированное шифрование — II

Что делать при обработке большого текста X?

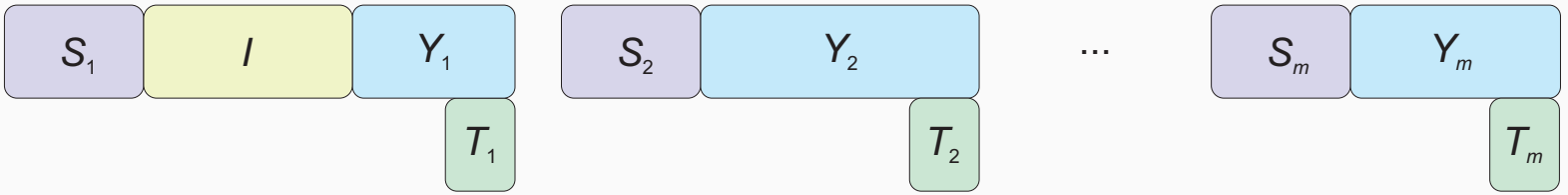
- Фрагментировать, своя синхропосылка для каждого фрагмента:



Аутентифицированное шифрование — II

Что делать при обработке большого текста X?

- Фрагментировать, своя синхропосылка для каждого фрагмента:

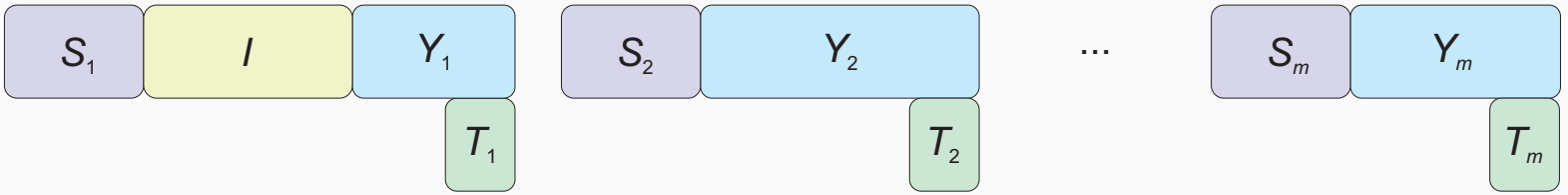


Недостаток: нет прямого контроля последовательности фрагментов (представим, что синхропосылки выбираются случайно).

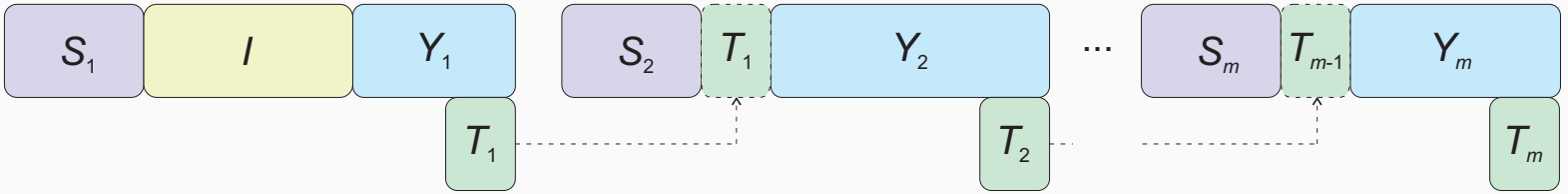
Аутентифицированное шифрование — II

Что делать при обработке большого текста X?

- Фрагментировать, своя синхропосылка для каждого фрагмента:



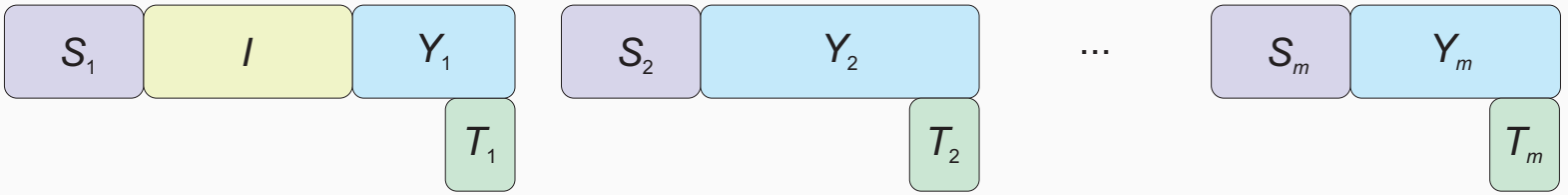
- Сцепленные фрагменты:



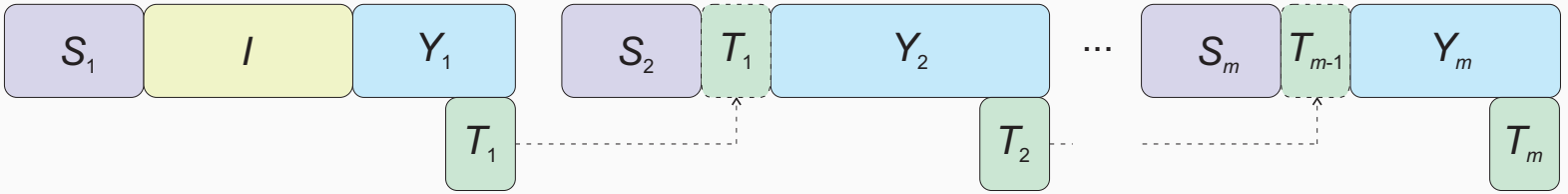
Аутентифицированное шифрование — II

Что делать при обработке большого текста X?

- Фрагментировать, своя синхропосылка для каждого фрагмента:



- Сцепленные фрагменты:

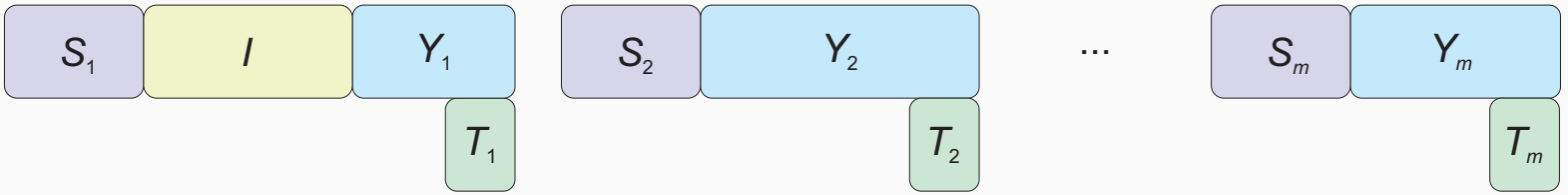


Недостаток: много дополнительных служебных данных.

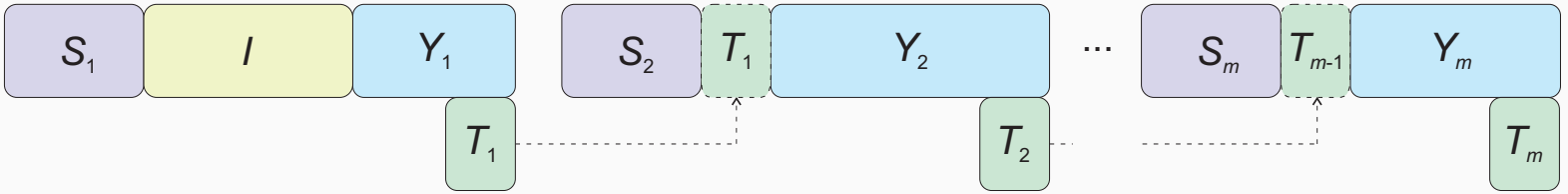
Аутентифицированное шифрование — II

Что делать при обработке большого текста X?

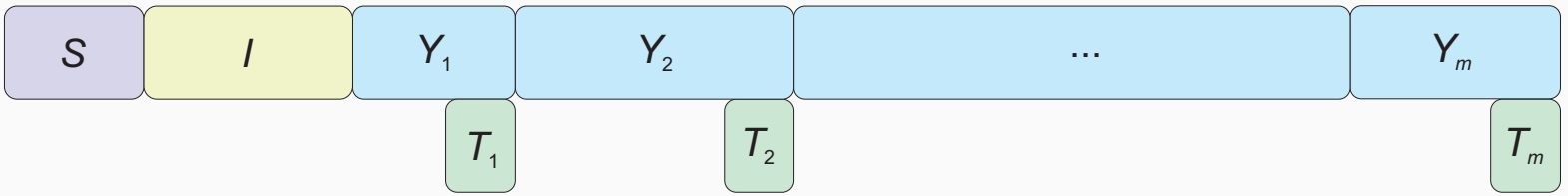
- Фрагментировать, своя синхропосылка для каждого фрагмента:



- Сцепленные фрагменты:



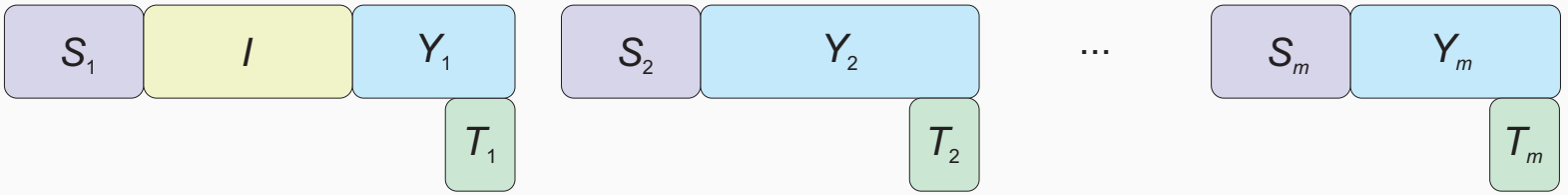
- Промежуточные имитовставки (без смены S):



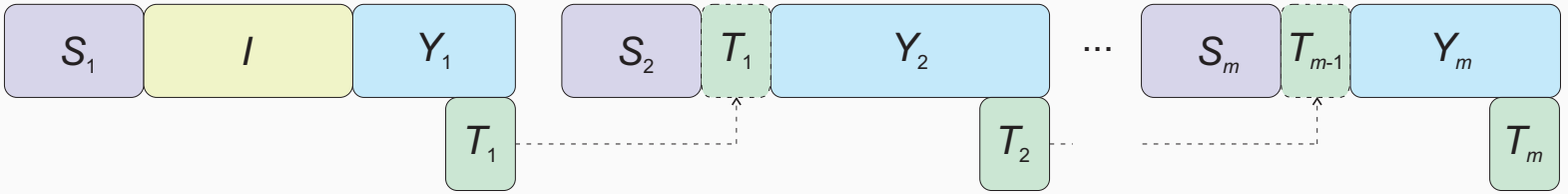
Аутентифицированное шифрование — II

Что делать при обработке большого текста X?

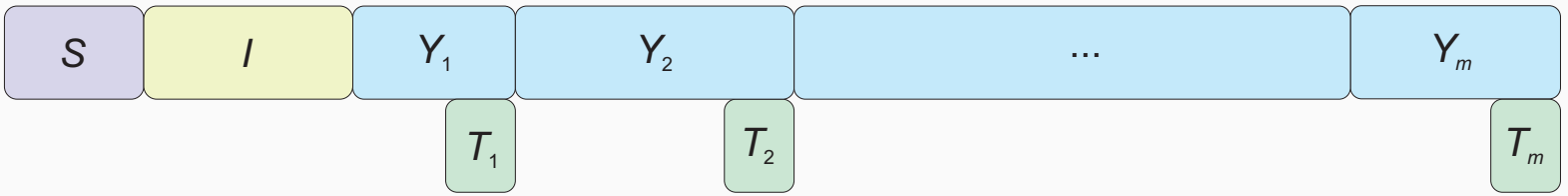
- Фрагментировать, своя синхропосылка для каждого фрагмента:



- Сцепленные фрагменты:



- Промежуточные имитовставки (без смены S):

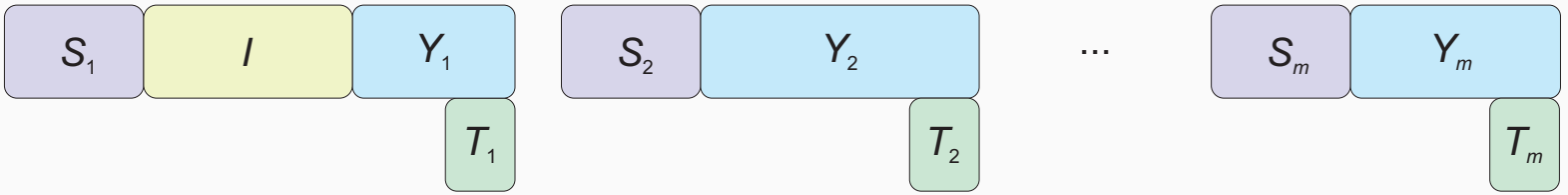


Безопасно?

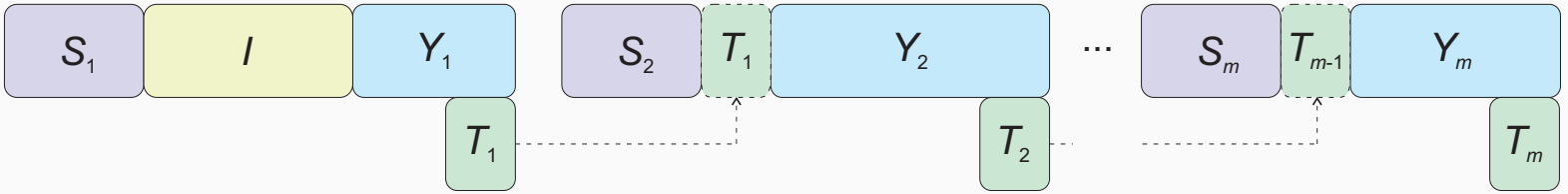
Аутентифицированное шифрование — II

Что делать при обработке большого текста X?

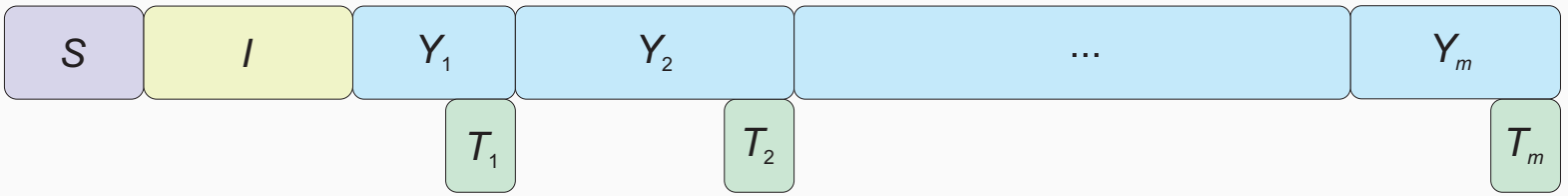
- Фрагментировать, своя синхропосылка для каждого фрагмента:



- Сцепленные фрагменты:



- Промежуточные имитовставки (без смены S):



Безопасно? Да.

Алгоритмы СТБ 34.101.31-2020

belt-block (шифрование блока)

belt-wblock (шифрование широкого блока)

belt-compress (сжатие)

belt-ecb, **belt-cbc**, **belt-cfb**, **belt-ctr** (режимы шифрования)

belt-mac (имитозащита)

belt-dwp, **belt-che** (аутентифицированное шифрование)

belt-kwp (аутентифицированное шифрование ключа)

belt-hash (хэширование)

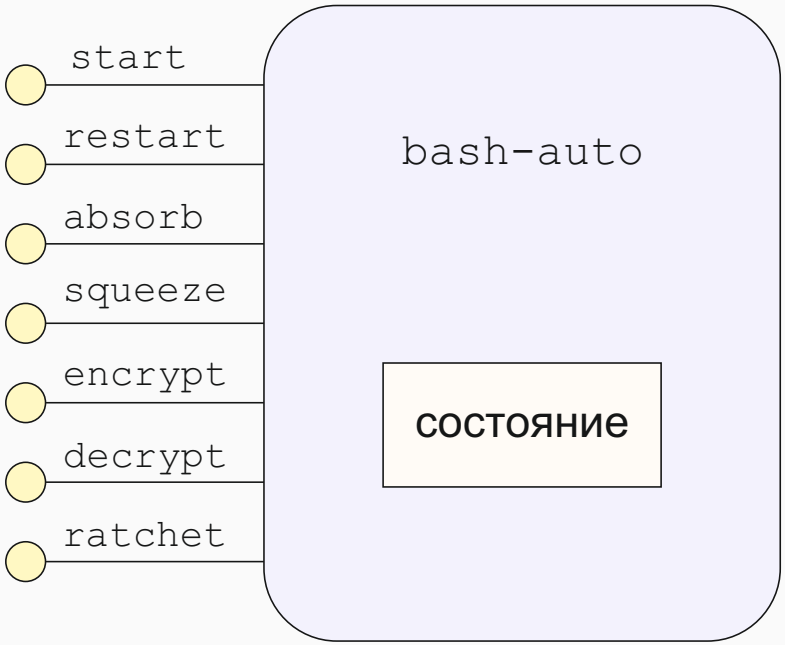
belt-bde, **belt-sde** (дисковое шифрование)

belt-fmt (шифрование с сохранением формата)

belt-keyexp (расширение ключа)

belt-keyrep (построение ключа)

Автомат bash-auto (СТБ 34.101.77-2020)



start — запуск

restart — перезапуск

absorb — загрузить данные

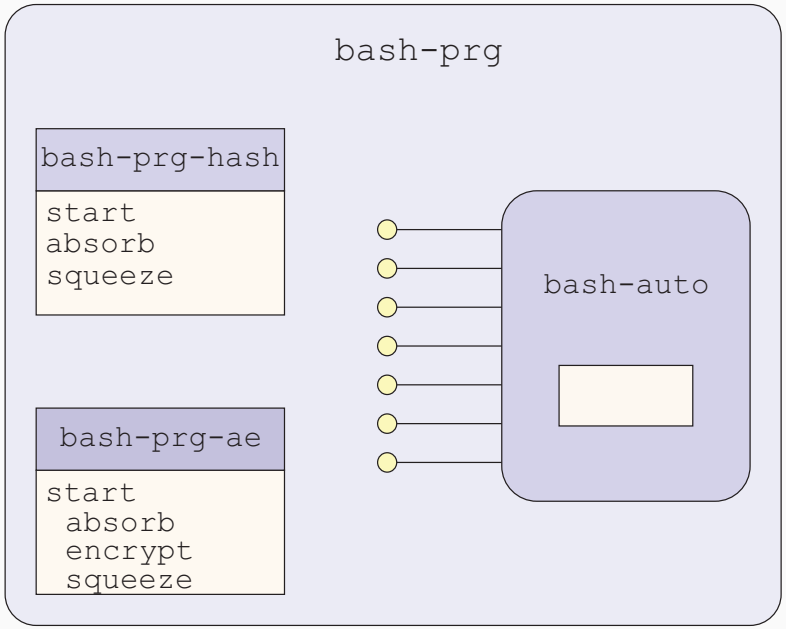
squeeze — выгрузить данные

encrypt — зашифровать

decrypt — расшифровать

ratchet — необратимо изменить

Программируемые алгоритмы



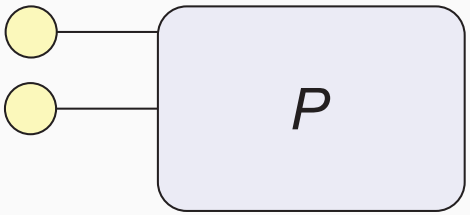
bash-prg-hash — хэширование (XOF)

bash-prg-ae — аутентифицированное шифрование

Противник как расширение интерфейса

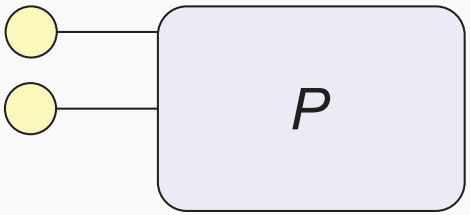
Обоснование стойкости...

Пусть требуется обосновать стойкость протокола (криптосистемы) P:



Обоснование стойкости...

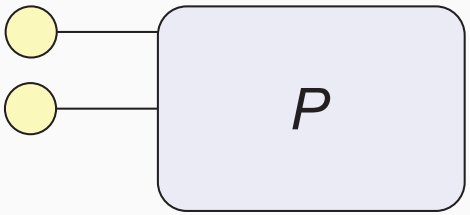
Пусть требуется обосновать стойкость протокола (криптосистемы) P:



Если P не является стойким, то существует противник (алгоритм) $\mathcal{A}$, который решает некоторую криптоаналитическую задачу относительно P.

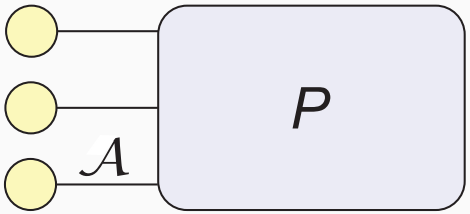
Обоснование стойкости...

Пусть требуется обосновать стойкость протокола (криптосистемы) P:



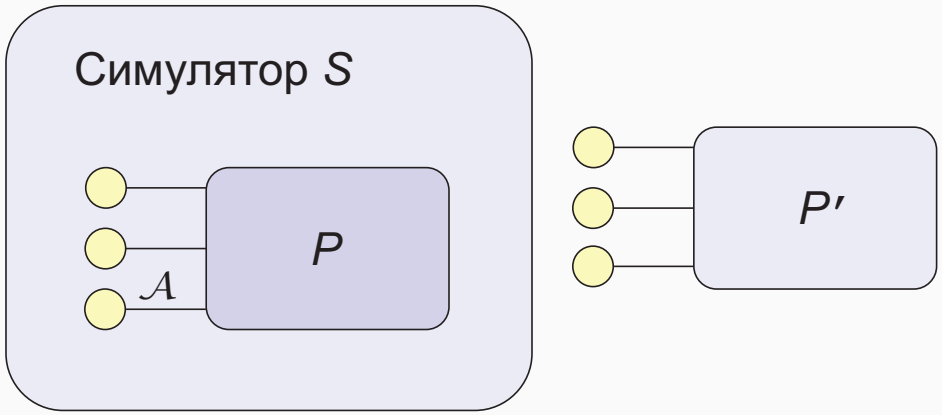
Если P не является стойким, то существует противник (алгоритм) $\mathcal{A}$, который решает некоторую криптоаналитическую задачу относительно P.

Можно считать, что $\mathcal{A}$ — это расширение интерфейса P:



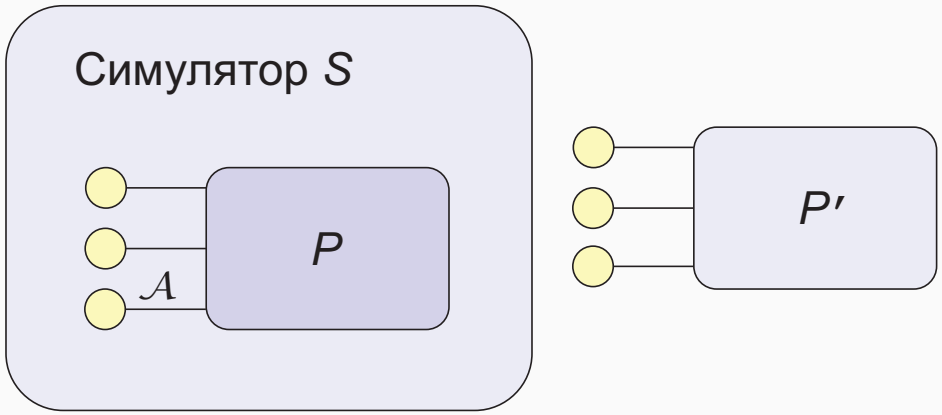
. . . от противного

Протокол P с (гипотетическим) расширением $\mathcal{A}$ может использовать симулятор $\mathcal{S}$ для атаки на протокол P':



. . . от противного

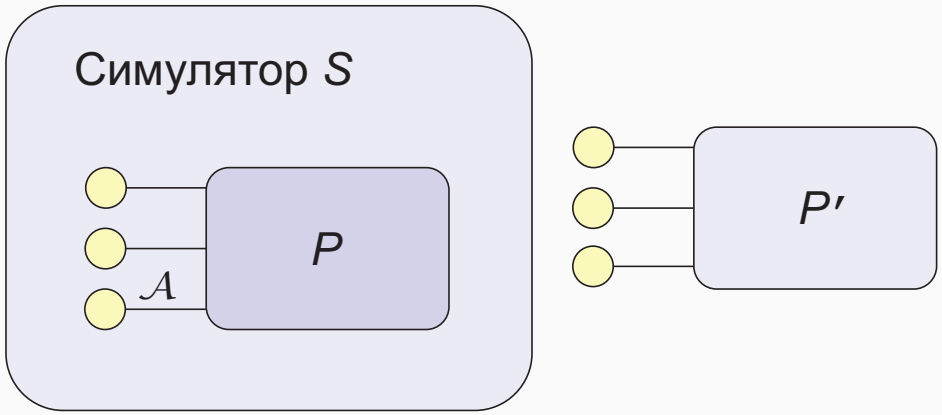
Протокол P с (гипотетическим) расширением $\mathcal{A}$ может использовать симулятор $\mathcal{S}$ для атаки на протокол P':



Если протокол P' признается стойким (соответствующие вычислительные задачи трудны), то $\mathcal{A}$ не может быть эффективным!

. . . от противного

Протокол P с (гипотетическим) расширением $\mathcal{A}$ может использовать симулятор $\mathcal{S}$ для атаки на протокол P':



Если протокол P' признается стойким (соответствующие вычислительные задачи трудны), то $\mathcal{A}$ не может быть эффективным!

Следовательно, P — стойкий протокол.

Ресурсы

- http://apmi.bsu.by/resources/std
- https://github.com/bcrypto/belt
- https://github.com/bcrypto/bash

Ресурсы

- http://apmi.bsu.by/resources/std
- https://github.com/bcrypto/belt
- https://github.com/bcrypto/bash

Спасибо за внимание!

До встречи офлайн!