Выпуск промежуточных имитовставок при аутентифицированном шифровании

Сергей Агиевич
НИИ прикладных проблем математики и информатики
Белорусский государственный университет

20 октября 2020 г. [Минск]

Международная научная конференция «Теоретическая и прикладная криптография»

Аутентифицированное шифрование

Интерфейс

$\texttt{Wrap}\colon (X, I, K, S) \mapsto (Y, T)$

$\texttt{Unwrap}\colon (Y, I, T, K, S) \mapsto X \mid \perp$

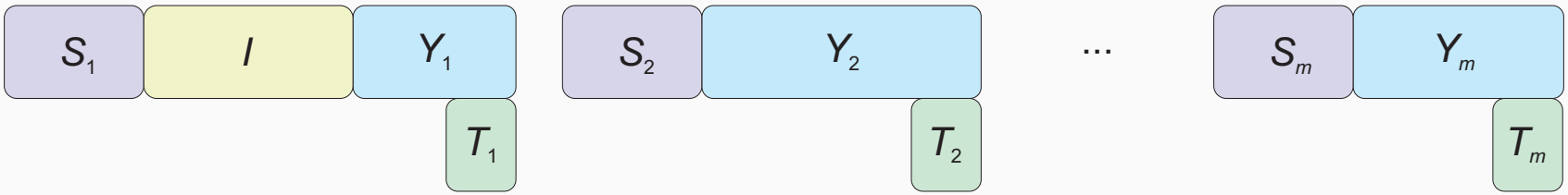
- X — открытый текст
- I — ассоциированные данные
- Y — шифртекст
- K — ключ
- S — синхропосылка (нонс)
- $\perp$ — ошибка (контроля целостности)

Защищенный контейнер

Проблема

О нарушении целостности (Y, I) мы узнаем только в конце обработки данных. Как быть, если речь идет о больших потоках, которые нужно обрабатывать в реальном времени? Видео?

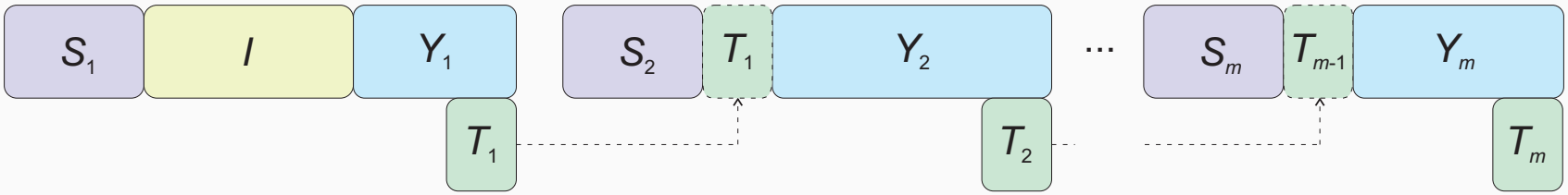
Поток данных: пакеты



Недостаток

Нет прямого контроля целостности последовательности пакетов (представим, что синхропосылки выбираются случайно).

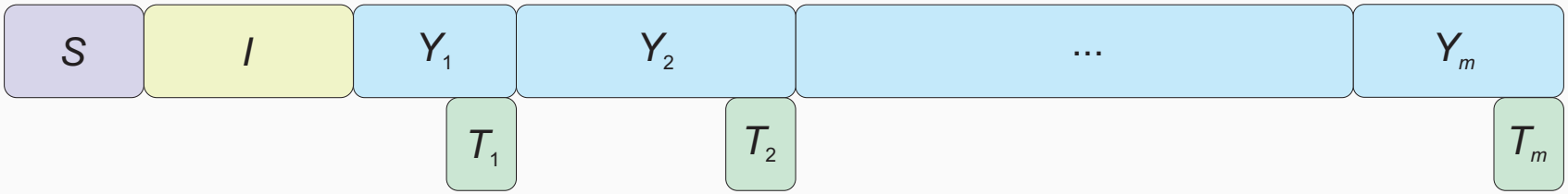
Поток данных: сцепленные пакеты



Недостаток

Много дополнительных служебных данных в каждом пакете.

Поток данных: промежуточные имитовставки



Вопрос

Безопасно ли это?

Безопасно?

GCM	**нет** (повтор синхропосылок!)
sponge-режимы	**да** (обычное дело)
CHE, DWP (СТБ 34.101.31)	**да** (объясняется далее)

Режим CHE

Название:

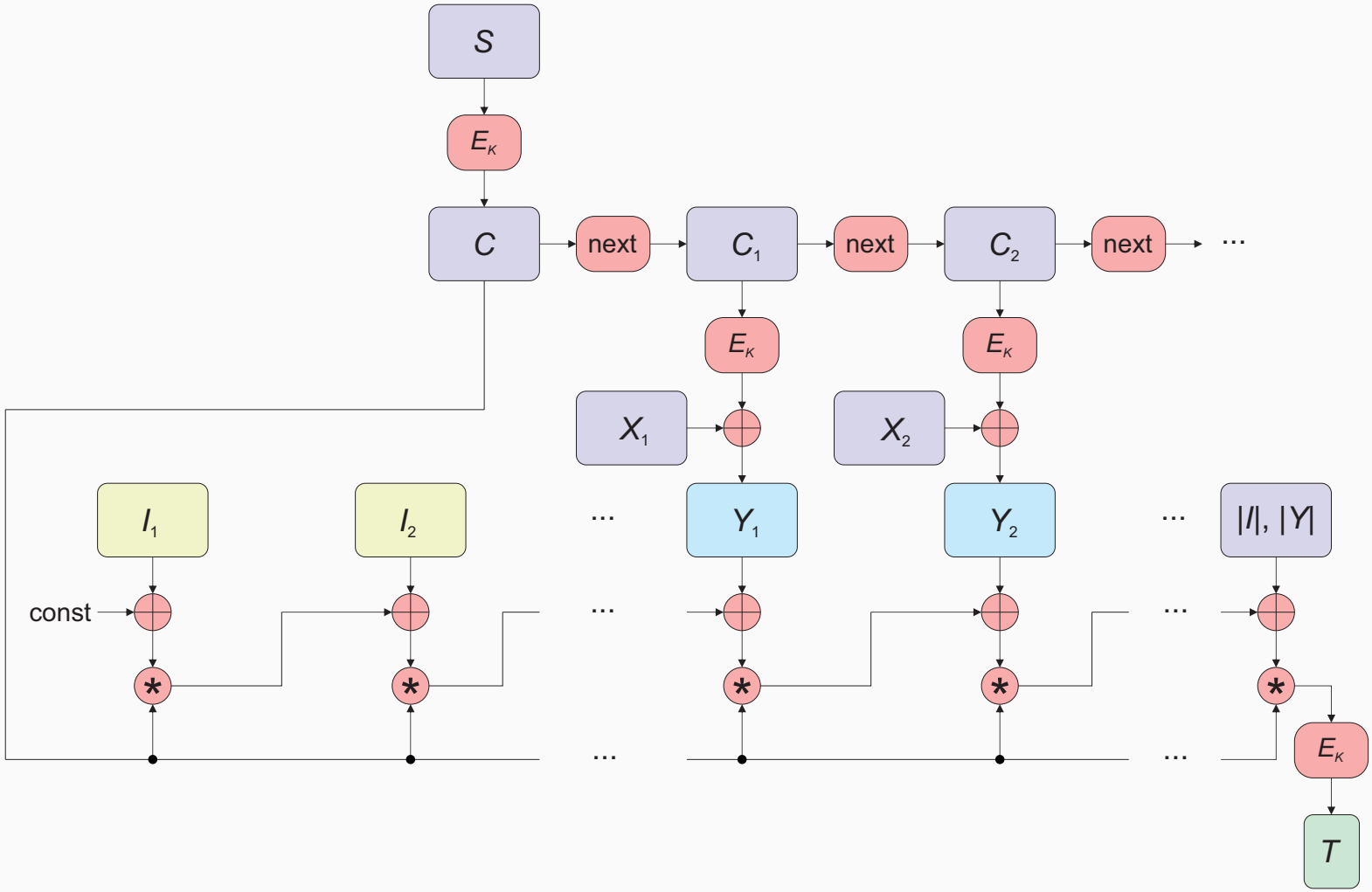
$$\begin{aligned}\textbf{CHE} = &\ \textbf{C}\text{ounter (шифрование в режиме CTR*)}\\ &+ \textbf{H}\text{ash (полиномиальное хэширование)}\\ &+ \textbf{E}\text{ncrypt (зашифрование хэш-значения)}\end{aligned}$$

* точнее CTR2, ГОСТ 28147-89!

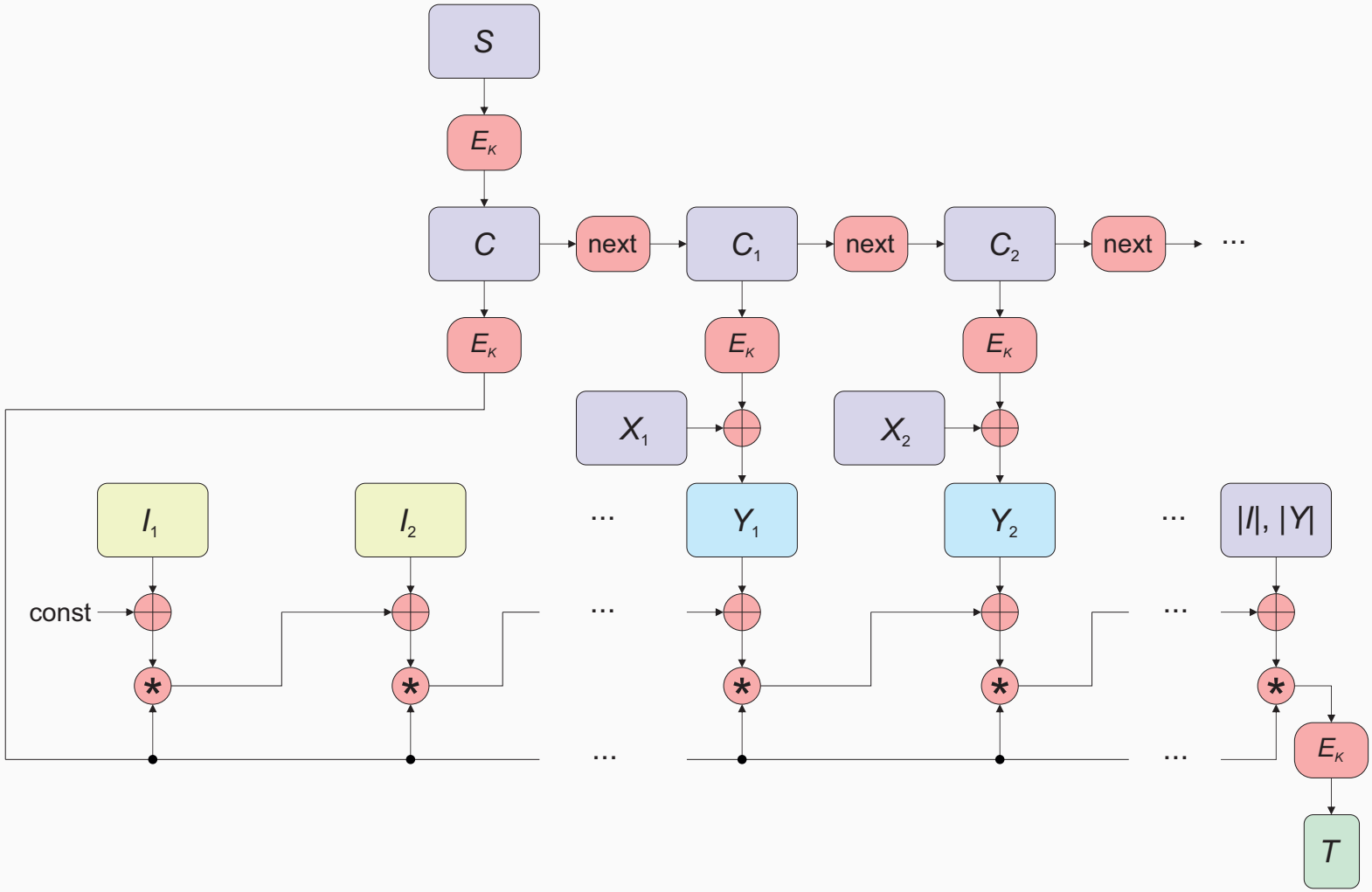
Компоненты

- $E = \{E_K : K \in \mathcal{K}\} \subset \mathrm{Perm}(n)$ — блочный шифр на $\{0,1\}^n$;
- $\mathtt{next}$ — почти-полноцикловая подстановка на $\{0,1\}^n \sim \mathbb{F}_{2^n}$:
  $\mathtt{next}(x) = a * x + b$, a — примитивный элемент, b — ненулевой.

Режим CHE



Режим DWP



Режим DWP

Отличия от CHE

- дополнительный вызов E_K;
- `next` — полноцикловая подстановка на $\{0,1\}^n \sim \mathbb{Z}_{2^n}$:
  $\texttt{next}(x) = (x+1) \bmod 2^n$ (совместимость с обычным CTR).

Модель противника

Доступ: оракул $O\colon (X, I, S) \mapsto (Y, T)$

Контракт: либо случайные синхропосылки, либо неповторяющиеся

Реализации оракула:

- $\mathrm{Mode}[E_K]$, $\mathrm{Mode} \in \{\mathsf{CHE}, \mathsf{DWP}\}$, $K \in_R \mathcal{K}$ (штатная реализация);
- случайная функция ρ (идеальная реализация)

Задача: отличить штатную реализацию (1) от идеальной (0)

Преобладание (A^O — ответ A при доступе к O):

$$\mathbf{Adv}^{\mathtt{priv}}_{\mathrm{Mode}[E]}(A) = \left|\mathbf{P}\left\{A^{\mathrm{Mode}[E_K]} = 1\right\} - \mathbf{P}\left\{A^{\rho} = 1\right\}\right|$$

Упрощение:

$$\mathbf{Adv}^{\mathtt{priv}}_{\mathrm{Mode}[\mathrm{Perm}(n)]}(A) = \left|\mathbf{P}\left\{A^{\mathrm{Mode}[\pi]} = 1\right\} - \mathbf{P}\left\{A^{\rho} = 1\right\}\right|$$

Стойкость

Ограничения для A

- разрешается выполнить q запросов к оракулу,
- общее число блоков X в этих запросах не должно превосходить r,
- суммарное число блоков в каждой отдельной паре (X, I) должно быть меньше d.

[Agi20, `https://eprint.iacr.org/2020/331`](Теоремы 2, 4):

$$\mathbf{Adv}^{\mathtt{priv}}_{\mathsf{CHE}[\mathsf{Perm}(n)]}(A) \leq\approx \frac{1}{2^{n+1}}\left((2d+4)qr + (3d+3)q^2\right),$$

$$\mathbf{Adv}^{\mathtt{priv}}_{\mathsf{DWP}[\mathsf{Perm}(n)]}(A) \leq\approx \frac{1}{2^{n+1}}\left((2d+4)qr + (5d+3)q^2\right).$$

Стойкость при выпуске промежуточных имитовставок

Ослабление контракта: противник может делать запрос (X', I, S), вложенный в (X, I, S): X' является префиксом X.

Уточнение ограничений: вложенные запросы учитываются в q, однако суммарное число блоков r открытых текстов не меняется.

Штатная реализация: не меняется.

Идеальная реализация: ответ $(Y', T') = \rho(X', I, S)$ вложен в $(Y, T) = \rho(X, I, S)$: Y' является префиксом Y.

Теорема

Оценки теорем 2 и 4 из [Agi20] для $\mathbf{Adv}^{\mathtt{priv}}_{Mode[\mathsf{Perm}(n)]}(A)$ *остаются справедливыми, если противник кроме регулярных запросов* (X, I, S) *может делать вложенные запросы* (X', I, S) *с выпуском промежуточных имитовставок* T'.

Реализация в BELT

Новая редакция СТБ 34.101.31 (`github.com/bcrypto/belt`):

Примечание 3 — При вычислении $(Y, T) = \texttt{belt-dwp}(X, I, K, S)$ разрешается выдавать один или несколько промежуточных результатов $(Y', T') = \texttt{belt-dwp}(X', I, K, S)$. Здесь X' — префикс X, а Y' будет префиксом Y. Выдача промежуточных результатов позволяет дискретизировать процесс защиты, что оказывается полезным при передаче сообщений X большой длины. При снятии защиты промежуточная пара (Y', T') обрабатывается с помощью алгоритма $\texttt{belt-dwp}^{-1}$ обычным образом. Если $\texttt{belt-dwp}^{-1}(Y', I, T', K, S) = \perp$, то снятие защиты должно быть прервано. Сказанное относится также к алгоритмам `belt-che` и $\texttt{belt-che}^{-1}$.

Реализация в BELT

Квоты ключей (ограничение на r)

Уровень гарантий	`belt-dwp`	`belt-che`
Средний ($\mathbf{Adv} \leq 2^{-32}$)	$2^{48}\sqrt{\frac{2}{7d+7}}$	$2^{48}\sqrt{\frac{2}{5d+7}}$
Высокий ($\mathbf{Adv} \leq 2^{-48}$)	$2^{40}\sqrt{\frac{2}{7d+7}}$	$2^{40}\sqrt{\frac{2}{5d+7}}$
Максимальный ($\mathbf{Adv} \leq 2^{-64}$)	$2^{32}\sqrt{\frac{2}{7d+7}}$	$2^{32}\sqrt{\frac{2}{5d+7}}$