Multilinear Galois Mode. Об особенностях построения, функциональных возможностях и доказуемой стойкости

Владислав Ноздрунов

ТК 26

22 марта 2018 г.

В начале было слово

Июнь 2017 г.

В начале было слово

Июнь 2017 г.

- Parallel and double block cipher mode of operation (PD–mode) for authenticated encryption (CTCrypt'2017).

В начале было слово

Июнь 2017 г.

- Parallel and double block cipher mode of operation (PD–mode) for authenticated encryption (CTCrypt'2017).
  - Основывается на ~~режиме GCM~~ режиме гаммирования и мультилинейной функции.

В начале было слово

Июнь 2017 г.

- Parallel and double block cipher mode of operation (PD–mode) for authenticated encryption (CTCrypt'2017).
  - Основывается на ~~режиме GCM~~ режиме гаммирования и мультилинейной функции.

Июль 2017 г.

В начале было слово

Июнь 2017 г.

- Parallel and double block cipher mode of operation (PD–mode) for authenticated encryption (CTCrypt'2017).
  - Основывается на ~~режиме GCM~~ режиме гаммирования и мультилинейной функции.

Июль 2017 г.

- Представление в рабочую группы ТК 26.

Multilinear Galois Mode (MGM)

Multilinear Galois Mode (MGM)

- Длина блока n – произвольная, четная.

Multilinear Galois Mode (MGM)

- Длина блока n – произвольная, четная.
- Одноразовый вектор N длины $n - 1$ с требованием *уникальности*.

Multilinear Galois Mode (MGM)

- Длина блока n – произвольная, четная.
- Одноразовый вектор N длины $n - 1$ с требованием *уникальности*.
- Конструктивное ограничение длин ОТ и АД
  - $0 \leq |P| < 2^{n/2}$;
  - $0 \leq |A| < 2^{n/2}$;
  - $0 < |P| + |A| < 2^{n/2}$.

Multilinear Galois Mode (MGM)

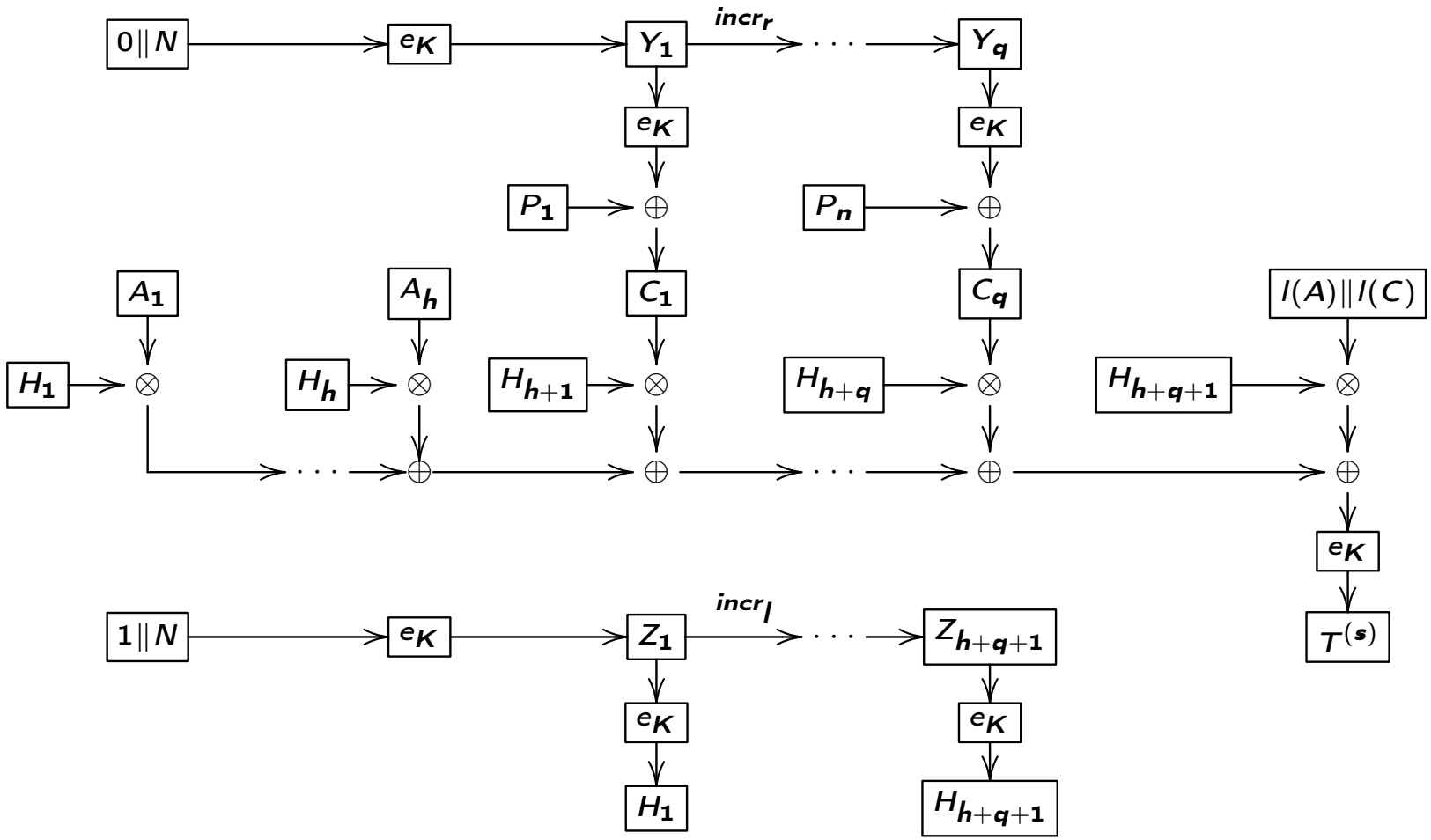
- Длина блока n – произвольная, четная.
- Одноразовый вектор N длины $n - 1$ с требованием *уникальности*.
- Конструктивное ограничение длин OT и АД
  - $0 \leq |P| < 2^{n/2}$;
  - $0 \leq |A| < 2^{n/2}$;
  - $0 < |P| + |A| < 2^{n/2}$.
- Длина имитовставки s: $0 < s \leq n$.

Multilinear Galois Mode (MGM)

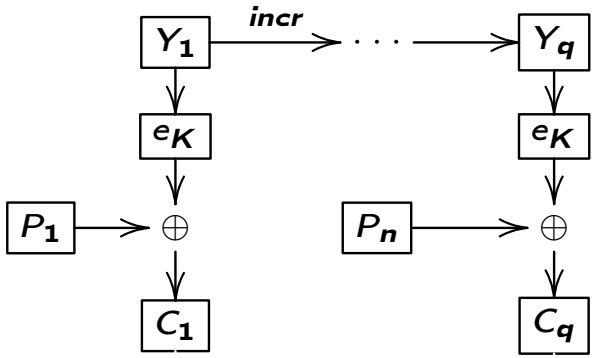
- Длина блока n – произвольная, четная.
- Одноразовый вектор N длины $n - 1$ с требованием *уникальности*.
- Конструктивное ограничение длин ОТ и АД
  - $0 \leq |P| < 2^{n/2}$;
  - $0 \leq |A| < 2^{n/2}$;
  - $0 < |P| + |A| < 2^{n/2}$.
- Длина имитовставки s: $0 < s \leq n$.

значение s единожды выбирается для каждой конкретной шифрсистемы и никогда не меняется в процессе ее эксплуатации, также значение s считается известным любому пользователю шифрсистемы.

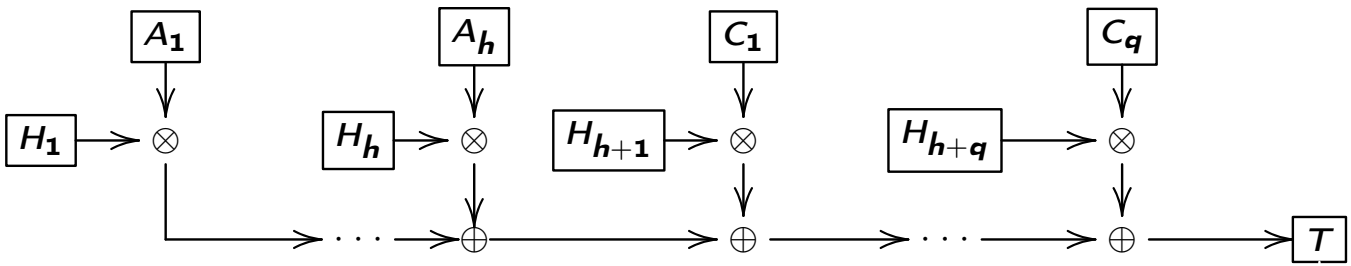
Multilinear Galois Mode (MGM)



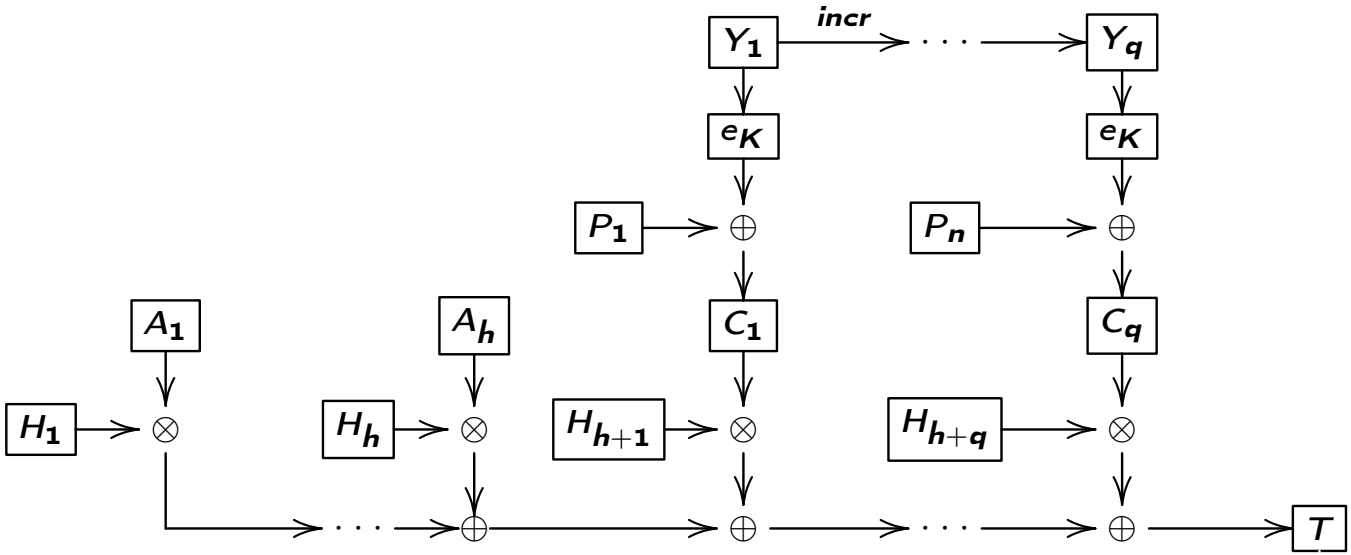
Быстрое параллельное шифрование? $\longrightarrow$ гаммирование



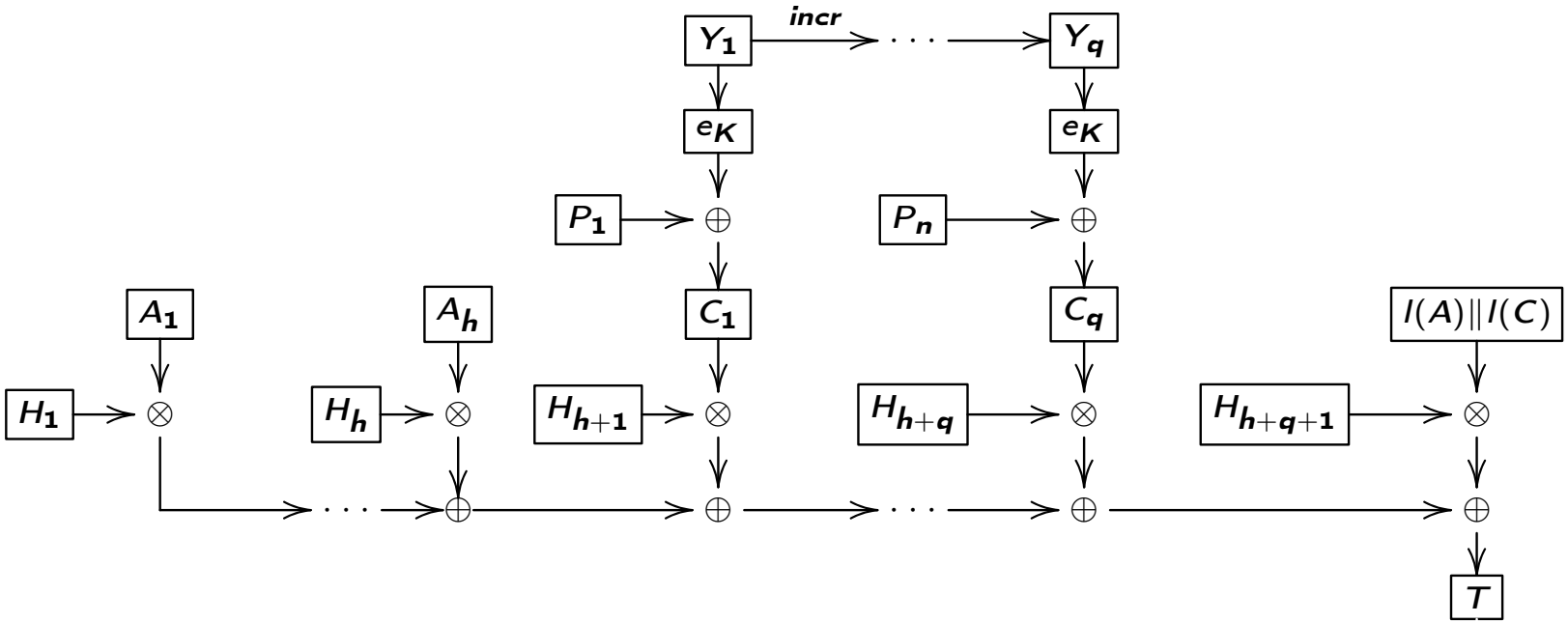
Параллелизуемость MAC? → случайность на каждый блок



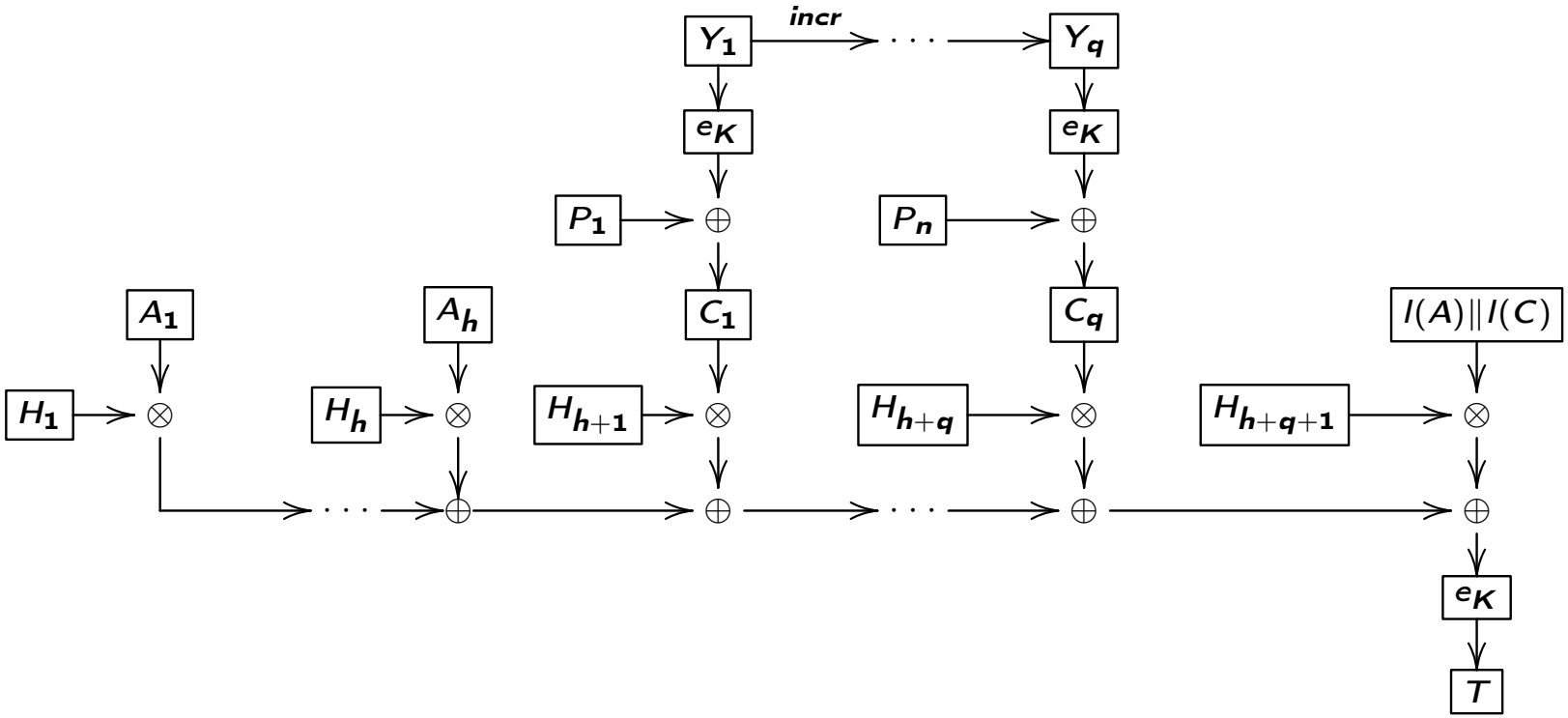
Все параллельно



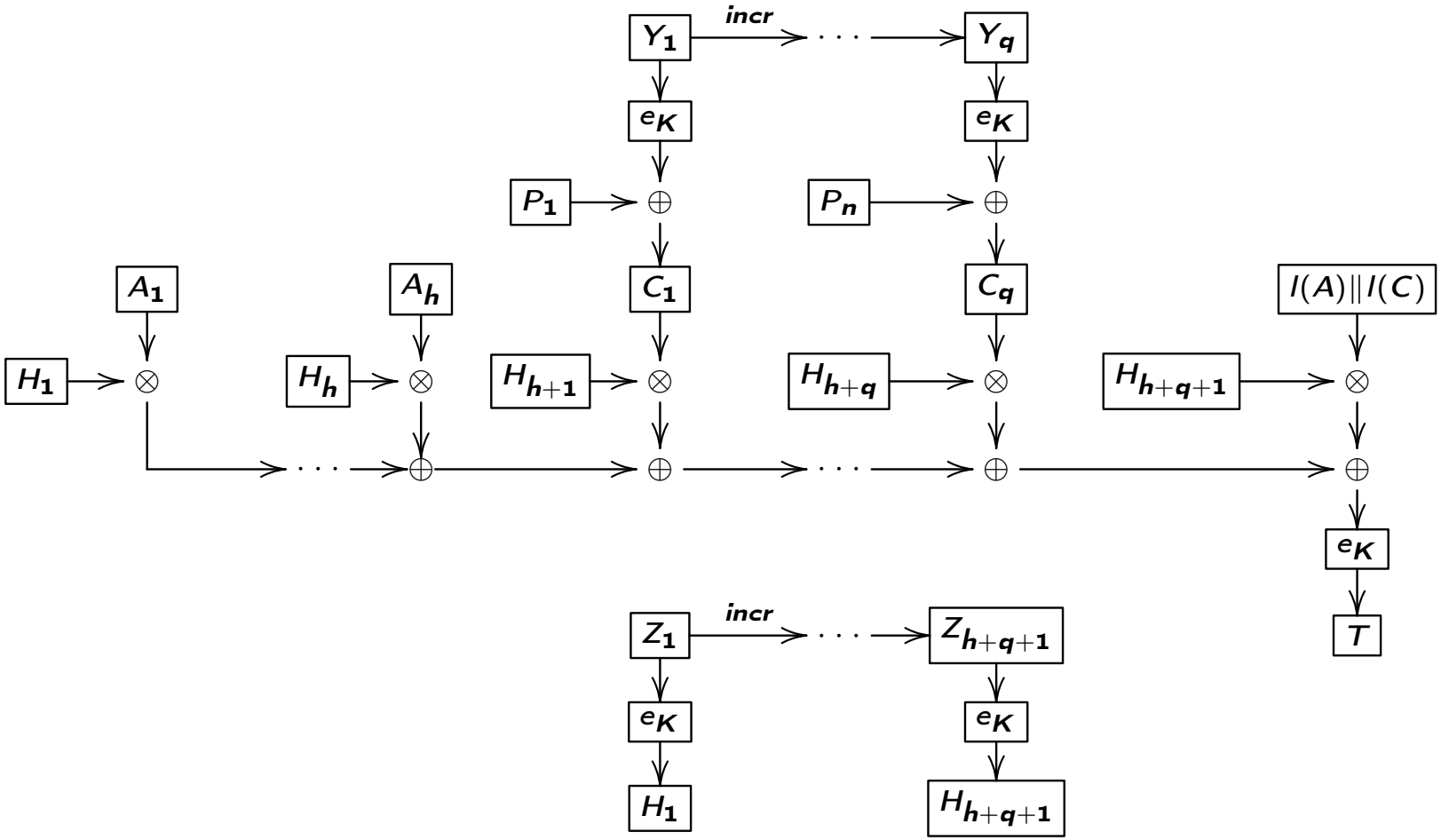
Защита от атак, использующих дополнение блока



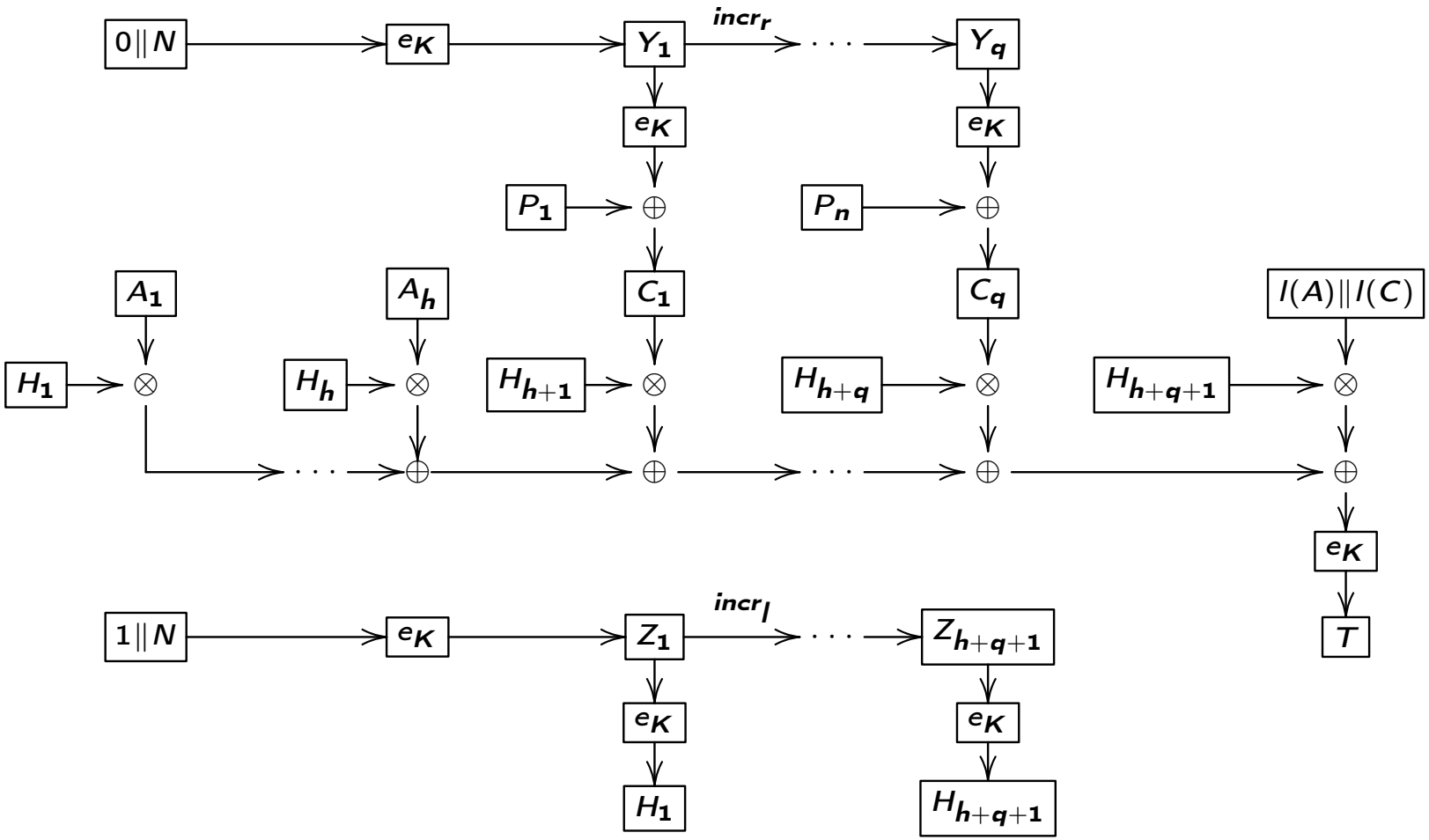
Защита от атак, использующих свойства линейности



Выработка вспомогательных секретных параметров



Защита от атак, использующих значения счетчиков



Функциональные возможности

Функциональные возможности

1. **Распараллеливание** – возможность обработки последующих блоков до конца обработки предыдущих.

Функциональные возможности

1. **Распараллеливание** – возможность обработки последующих блоков до конца обработки предыдущих.
2. **Онлайн** – возможность шифрования без знания заранее длины данных.

Функциональные возможности

1. **Распараллеливание** – возможность обработки последующих блоков до конца обработки предыдущих.
2. **Онлайн** – возможность шифрования без знания заранее длины данных.
3. **Отсутствие инверсий** – использование только одной функции для зашифрования и расшифрования.

Функциональные возможности

1. **Распараллеливание** – возможность обработки последующих блоков до конца обработки предыдущих.
2. **Онлайн** – возможность шифрования без знания заранее длины данных.
3. **Отсутствие инверсий** – использование только одной функции для зашифрования и расшифрования.
4. Возможность работы только для выработки имитовставки.

Функциональные возможности

1. **Распараллеливание** – возможность обработки последующих блоков до конца обработки предыдущих.
2. **Онлайн** – возможность шифрования без знания заранее длины данных.
3. **Отсутствие инверсий** – использование только одной функции для зашифрования и расшифрования.
4. Возможность работы только для выработки имитовставки.
5. Использование одного ключа как для шифрования, так и для выработки имитовставки.

Функциональные возможности

1. **Распараллеливание** – возможность обработки последующих блоков до конца обработки предыдущих.
2. **Онлайн** – возможность шифрования без знания заранее длины данных.
3. **Отсутствие инверсий** – использование только одной функции для зашифрования и расшифрования.
4. Возможность работы только для выработки имитовставки.
5. Использование одного ключа как для шифрования, так и для выработки имитовставки.
6. Использование одноразового вектора снижает требования к программно-аппаратной базе, по сравнению с использованием случайного вектора инициализации.

Функциональные возможности

1. **Распараллеливание** – возможность обработки последующих блоков до конца обработки предыдущих.
2. **Онлайн** – возможность шифрования без знания заранее длины данных.
3. **Отсутствие инверсий** – использование только одной функции для зашифрования и расшифрования.
4. Возможность работы только для выработки имитовставки.
5. Использование одного ключа как для шифрования, так и для выработки имитовставки.
6. Использование одноразового вектора снижает требования к программно-аппаратной базе, по сравнению с использованием случайного вектора инициализации.
7. **Предвычисления** – возможность проведения вспомогательных вычислений, направленных на ускорение работы, до получения открытого текста и ассоциированных данных (необходимо знание одноразового вектора).

Безопасность шифрования

Теорема

Пусть E_K – блочный шифр, $K \in \mathcal{K}$, тогда для любых t, q, μ и q', которое определяется из равенства $\mu = q' \cdot n$, верно

$$Adv^{lor-cpa}_{CTR}(t, q, \mu) \leq 2 \cdot Adv^{prp}_{E_K}(t, q') + \frac{(q-1)\mu}{n \cdot (2^n - \mu/n + q - 1)} - \frac{q(q-1)}{2^n - \mu/n + q - 1}.$$

Безопасность аутентификации

Теорема

Для любых натуральных чисел $q_e, q_v, \mu_e, \mu_v, t$ верно неравенство

$$Adv^{auth}_{MGM}(q_e, q_v, \mu_e, \mu_v, t) \leq \frac{(\mu')^2}{n^2 \cdot 2^n} + \frac{q_v}{2^{s-1}} + \frac{q'(q'-1)}{2^{n+1}} + \\ + Adv^{prp}_{E_K}(q', t'),$$

где $q' = (2\lceil \mu_e/n \rceil + 3q_e + \lceil \mu_v/n \rceil + 2q_v)$, $\mu' = \mu_e + \mu_v$, $t' = t + O(q')$.

Сравнение с GCM

	Шифрование	Аутентификация
MGM	$\frac{(q-1)\mu}{n\cdot(2^n-\mu/n+q-1)}$	$\frac{(\mu')^2}{n^2\cdot 2^n}+\frac{q_v}{2^{s-1}}+\frac{q'(q'-1)}{2^{n+1}}$
GCM	$\frac{0.5(\mu+q+1)^2}{2^n}$	$\frac{0.5(\mu+q_e+q_v+1)^2}{2^n}+\frac{q_v(\mu'+1)}{2^s}$

Таблица: Сравнение MGM и GCM. В таблице использованы следующие обозначения: $q'=(2\lceil\mu_e/n\rceil+3q_e+\lceil\mu_v/n\rceil+2q_v)$, $\mu'=\mu_e+\mu_v$.

Сравнение финалистов конкурса CAESAR и режима MGM

Алгоритм	MGM	COLM	OCB	Deoxys-II	ACORN	AEGIS	Ascon	MORUS
Примитив	BC	BC	BC	BC	SC	Dedic	Sponge	Dedic
Распараллеливание Enc/Dec	+/+	+/+	+/+	+/+	+/+	+/-	-/-	-/-
Онлайн	+	+	+	+	+	+	+	+
Отсутствие инверсий	+	-	-	-	+	+	+	+
Инкрементация AD/AE	-/-	+/-	-/-	-/-	-/-	-/-	-/-	-/-
Доказуем. стойкость	+	-	+	+	-	-	+	-
Предвычисл.	+	-	-	-	+	-	+	+
Кол-во вызовов БШ	$2m+4$	$2m+4$	$m+2$	$2m+1$				

Благодарю за внимание.

Вопросы?