Режимы блочных шифров: вопросы синтеза, анализа и эксплуатационные качества

Василий Шишкин

«РусКрипто'2014»

26 марта, 2014

Содержание доклада

Перейдем к разделу:

Блочные шифры

- блочные шифры получили широчайшее распространение и используются для решения множества различных задач обеспечения безопасности информации
- реализация различных криптографических функций с использованием блочных шифров достигается за счет специальных конструкций (схем, механизмов) – режимы (работы)
- универсальность: любой блочный шифр может использоваться с любым режимом

Планы стандартизации: блочные шифры

Блочный шифр с длиной блока 64 бита

- алгоритм ГОСТ 28147-89 с одним фиксированным (открытым) набором узлов замены
- эффективен для платформ с ограниченными ресурсами

Блочный шифр с длиной блока 128 битов

- перспективный алгоритм блочного шифрования (РусКрипто'2013)
- эффективная программная реализация
- позволяет обрабатывать на одном ключе большой объем информации

Планы стандартизации: блочные шифры

Блочный шифр с длиной блока 64 бита

- алгоритм ГОСТ 28147-89 с одним фиксированным (открытым) набором узлов замены
- эффективен для платформ с ограниченными ресурсами

Блочный шифр с длиной блока 128 битов

- перспективный алгоритм блочного шифрования (РусКрипто'2013)
- эффективная программная реализация
- позволяет обрабатывать на одном ключе большой объем информации

Разработка отдельного стандарта по режимам работы

- устоявшаяся международная практика (например, стандарты ISO)
- различные длины блока
- обеспечение взаимозаменяемости

Группы режимов работы блочных шифров

- режимы шифрования
- режимы выработки имитовставки
- режимы аутентифицированного шифрования
- специализированные режимы

Разработка отдельного стандарта по режимам работы

- устоявшаяся международная практика (например, стандарты ISO)
- различные длины блока
- обеспечение взаимозаменяемости

Группы режимов работы блочных шифров

- режимы шифрования
- режимы выработки имитовставки
- режимы аутентифицированного шифрования
- специализированные режимы

Проекты стандартов

Алгоритмы блочного шифрования

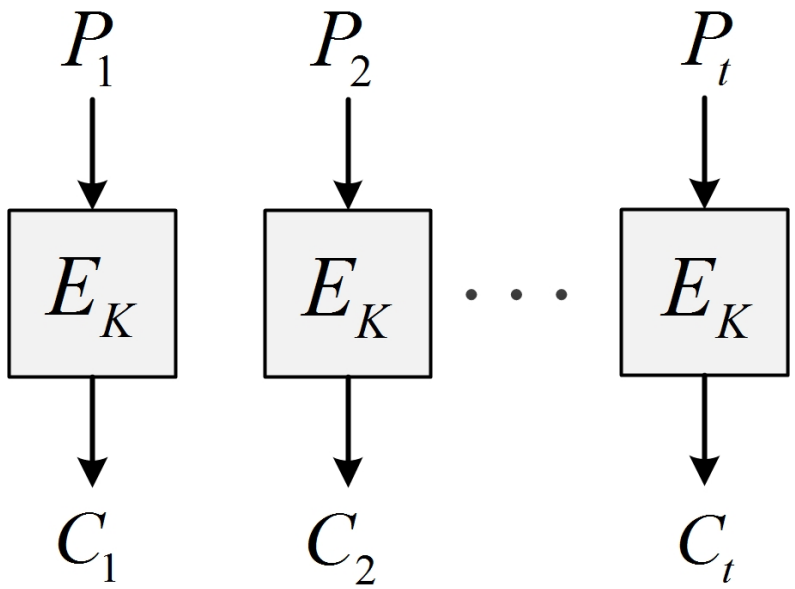
«Информационная технология. Криптографическая защита информации. Блочные шифры»

Режимы работы

«Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров»

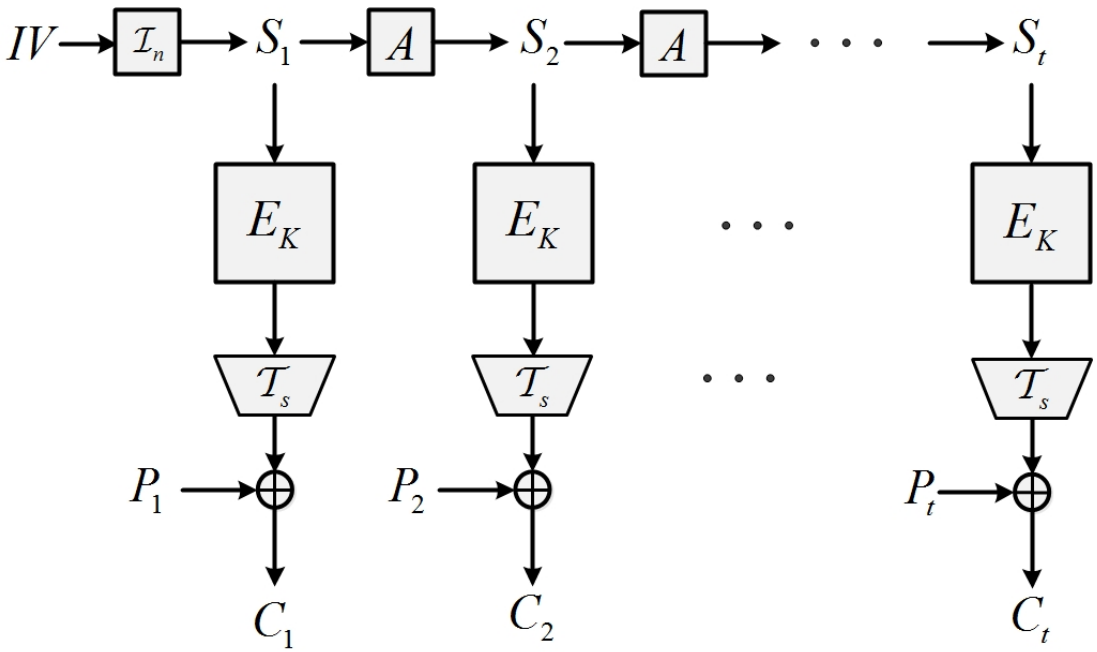
Перейдем к разделу:

Режим простой замены / ECB



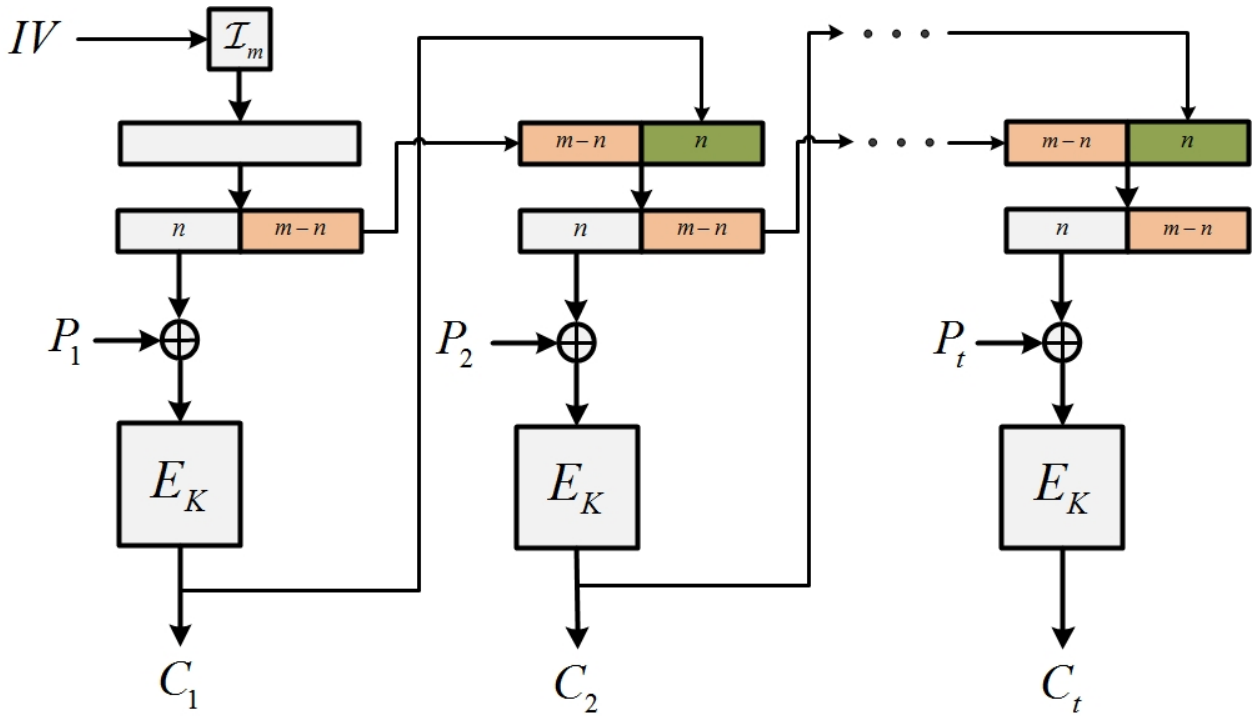
- не рекомендуется на одном ключе шифровать более одного блока данных

Режим гаммирования / CTR



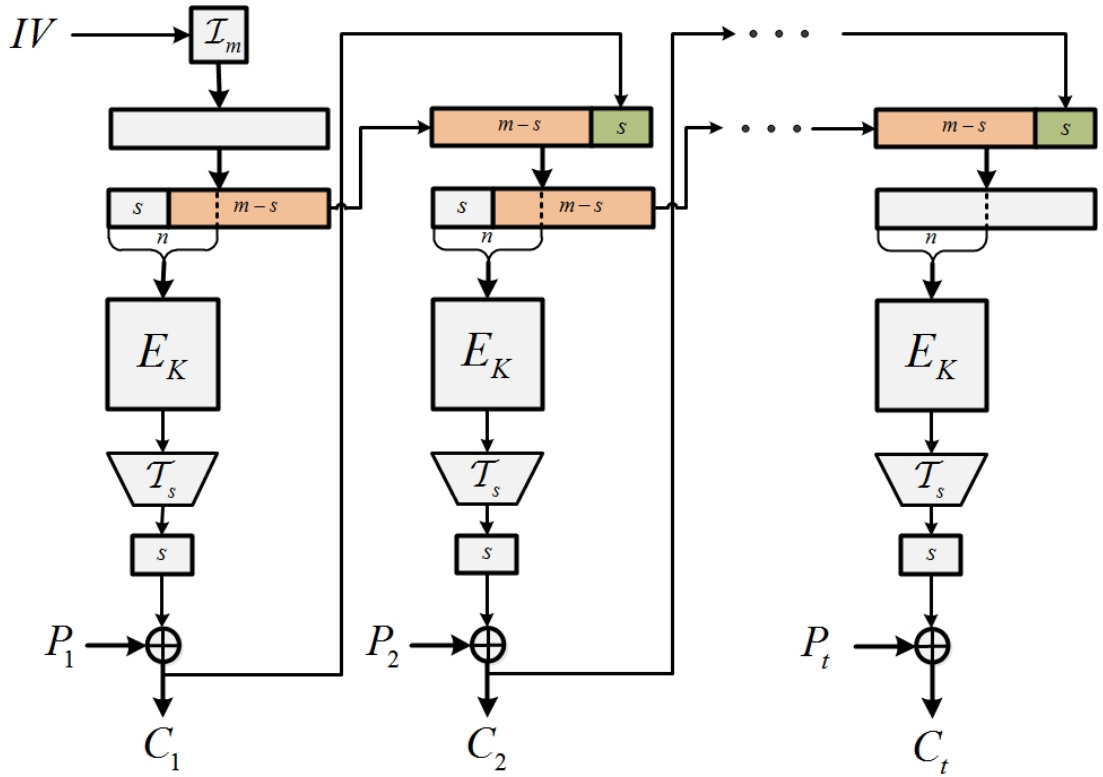
- инициализационный вектор: уникальный
- $\boldsymbol{S_i \in V_n}$, $\boldsymbol{IV \in V_{\frac{n}{2}}}$, $\boldsymbol{S_1 = IV||0^{\frac{n}{2}}}$, $\boldsymbol{S_{i+1} = A(S_i) = S_i \boxplus 1}$
- гарантированность периода, возможность распараллеливания

Режим простой замены с зацеплением / CBC



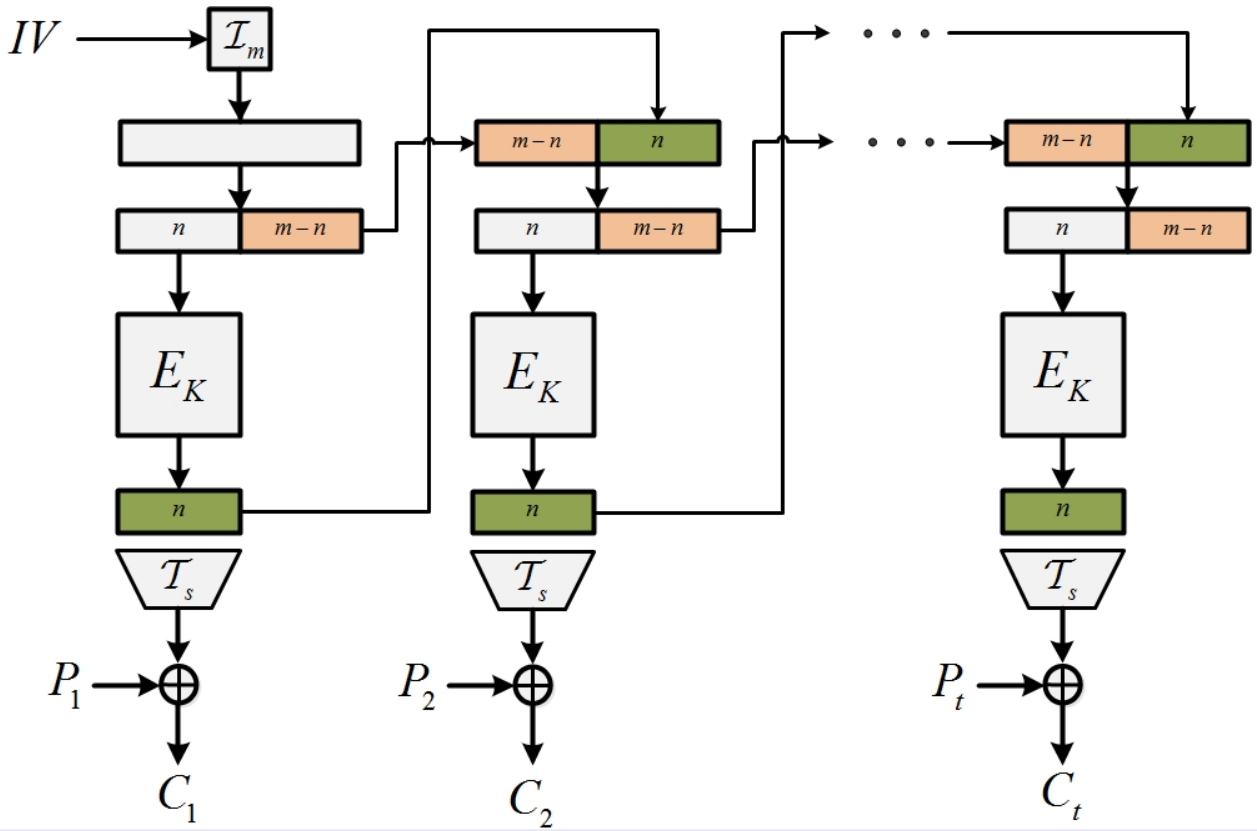
- инициализационный вектор: псевдослучайный
- при $\boldsymbol{m = kn}$ – распараллеливание на $\boldsymbol{k}$ процессоров

Гаммирование с обр. связью по шифртексту / CFB



- инициализационный вектор: псевдослучайный
- при $\boldsymbol{m = kn}$ – распараллеливание на $\boldsymbol{k}$ процессоров
- самосинхронизация

Гаммирование с обратной связью по выходу / OFB



- инициализационный вектор: уникальный/псевдослучайный
- при $\boldsymbol{m = kn}$ – распараллеливание на $\boldsymbol{k}$ процессоров

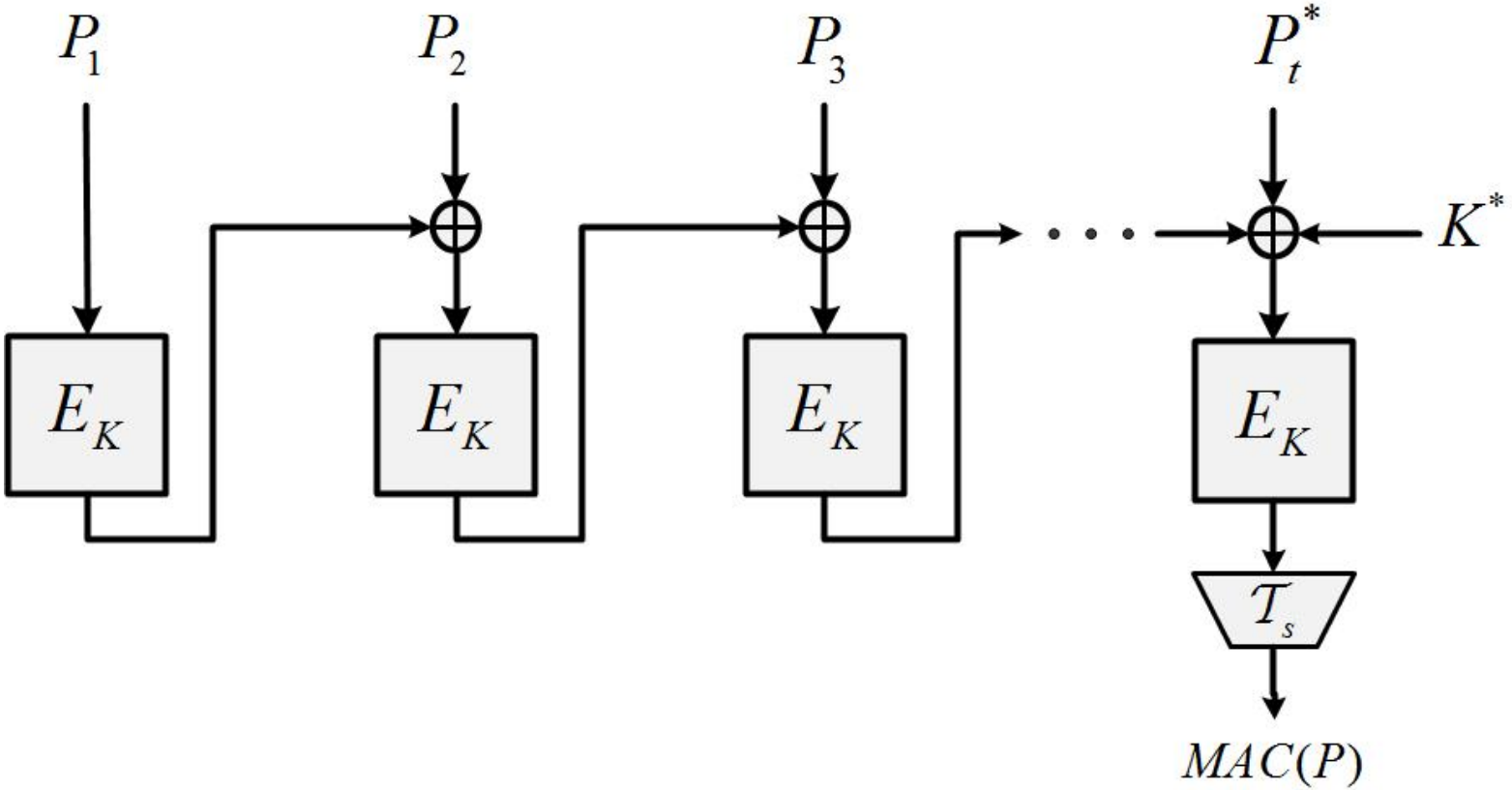
Перейдем к разделу:

Подходы к синтезу

- наиболее распространенными ключевыми функциями хэширования на основе блочных шифров являются различные варианты и модификации конструкции CBC-MAC, такие как ANSI X9.9, ANSI X9.19, FIPS 113, ISO 8731, ISO/IEC 9797, RIPEMAC, TMAC, XCBC и др.
- OMAC1 (CMAC)
  - оптимальный среди существующих (по совокупности своих криптографических и эксплуатационных качеств)
  - стандартизированный ISO
  - наиболее изученная, проверенная временем конструкция

Подходы к синтезу

- наиболее распространенными ключевыми функциями хэширования на основе блочных шифров являются различные варианты и модификации конструкции CBC-MAC, такие как ANSI X9.9, ANSI X9.19, FIPS 113, ISO 8731, ISO/IEC 9797, RIPEMAC, TMAC, XCBC и др.
- OMAC1 (CMAC)
  - оптимальный среди существующих (по совокупности своих криптографических и эксплуатационных качеств)
  - стандартизированный ISO
  - наиболее изученная, проверенная временем конструкция



- наличие результатов о доказуемой стойкости
- возможность обработки на одном ключе до порядка $\mathbf{2^{n/2}}$ блоков

Перейдем к разделу:

Подходы к синтезу

- Общая композиция
- Двухпроходные режимы
- На основе универсальной хэш-функции
- На основе смещений

на основе универсальной хэш-функции

- многообещающие, но спорные эксплуатационные свойства
- стойкость ниже ожидаемой

на основе смещений

- возможно, наилучшие эксплуатационные свойства
- патентные ограничения, недостаточный анализ

двухпроходной

- приемлемые эксплуатационные свойства
- наибольшая уверенность в стойкости

на основе универсальной хэш-функции

- многообещающие, но спорные эксплуатационные свойства
- стойкость ниже ожидаемой

на основе смещений

- возможно, наилучшие эксплуатационные свойства
- патентные ограничения, недостаточный анализ

двухпроходной

- приемлемые эксплуатационные свойства
- наибольшая уверенность в стойкости

на основе универсальной хэш-функции

- многообещающие, но спорные эксплуатационные свойства
- стойкость ниже ожидаемой

на основе смещений

- возможно, наилучшие эксплуатационные свойства
- патентные ограничения, недостаточный анализ

двухпроходной: режим гаммирования и вариант CBC-MAC

- приемлемые эксплуатационные свойства
- наибольшая уверенность в стойкости

Спасибо за внимание

Вопросы?