О шифровании данных в устройствах с блочной внутренней структурой

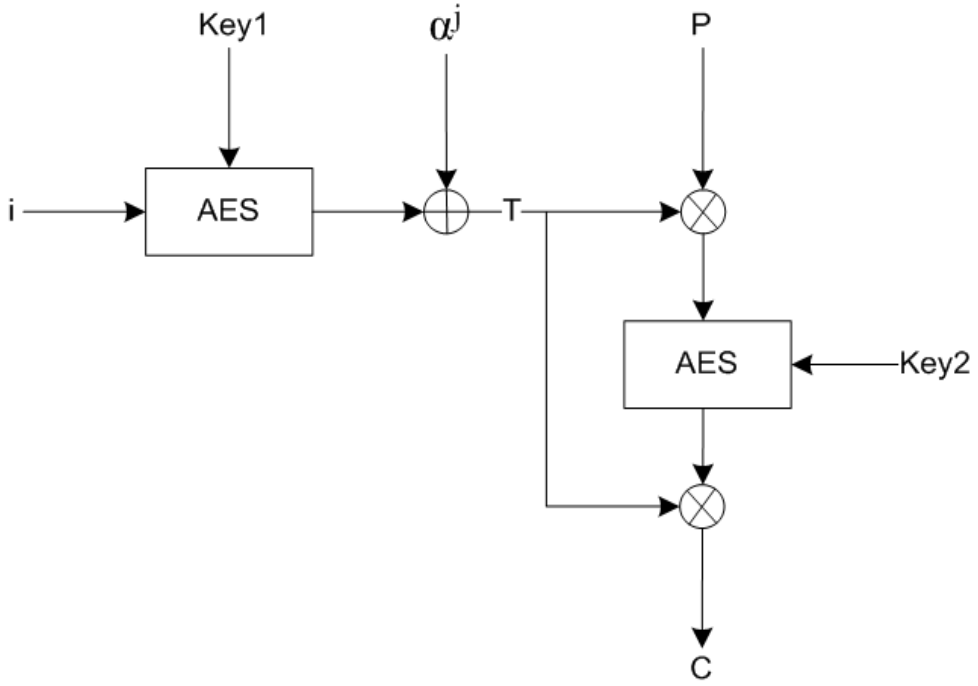
Коробов В.В.

РусКрипто’2014

Стандарты IEEE P1619

- ✓ IEEE P1619-2007 - IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices
- ✓ IEEE P1619.1-2007 - IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices
- ✓ IEEE P1619.2-2010 - IEEE Standard for Wide-Block Encryption for Shared Storage Media

IEEE P1619-2007



i – номер сектора;

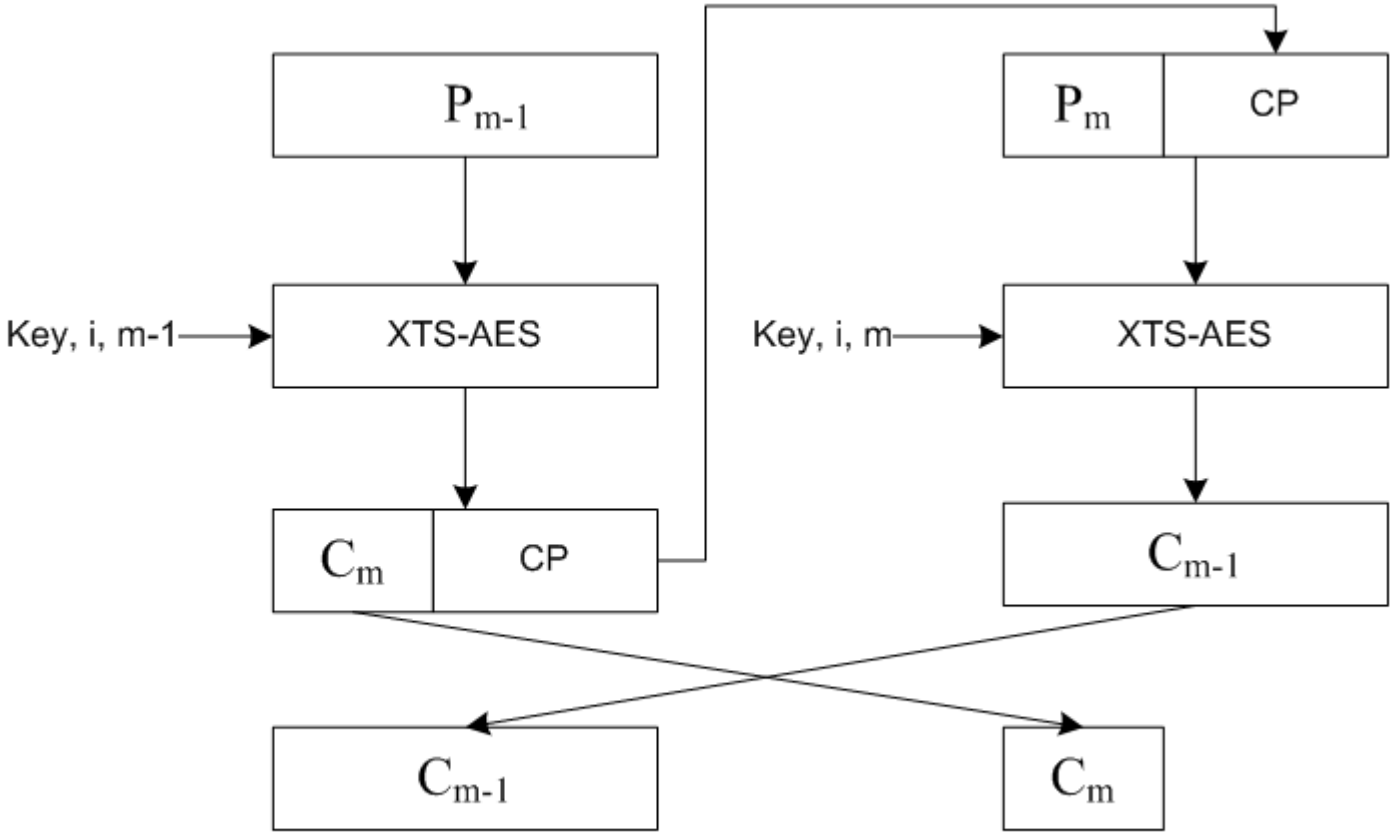
j – номер 128-битного блока внутри сектора (не больше 2^{20});

α – примитивный элемент поля GF(2^{128});

Key_1, Key_2 – части ключа;

T –« tweak value».

IEEE P1619-2007



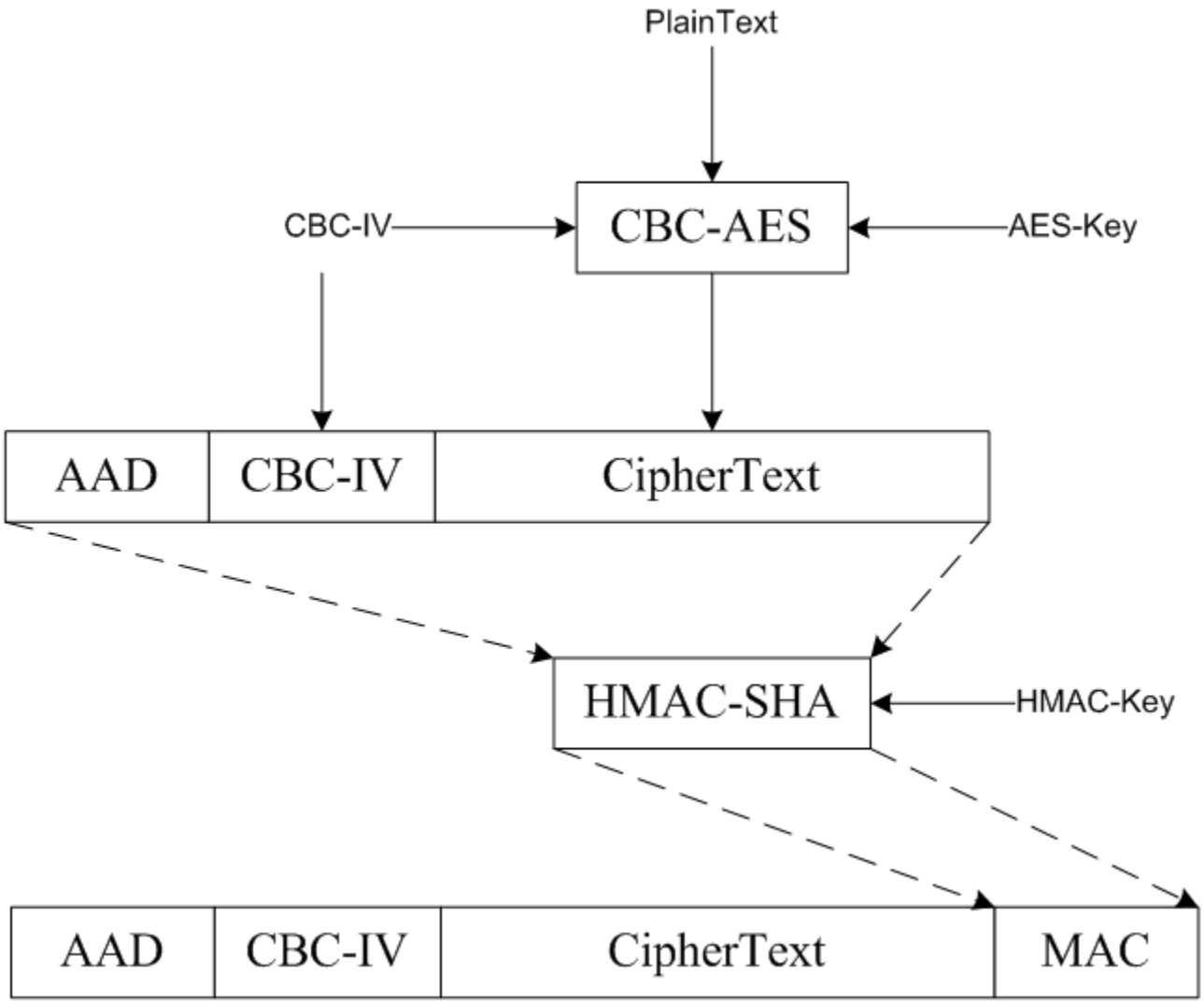
m – последний блок, размер которого не кратен 128 битам.

IEEE P1619.1-2007

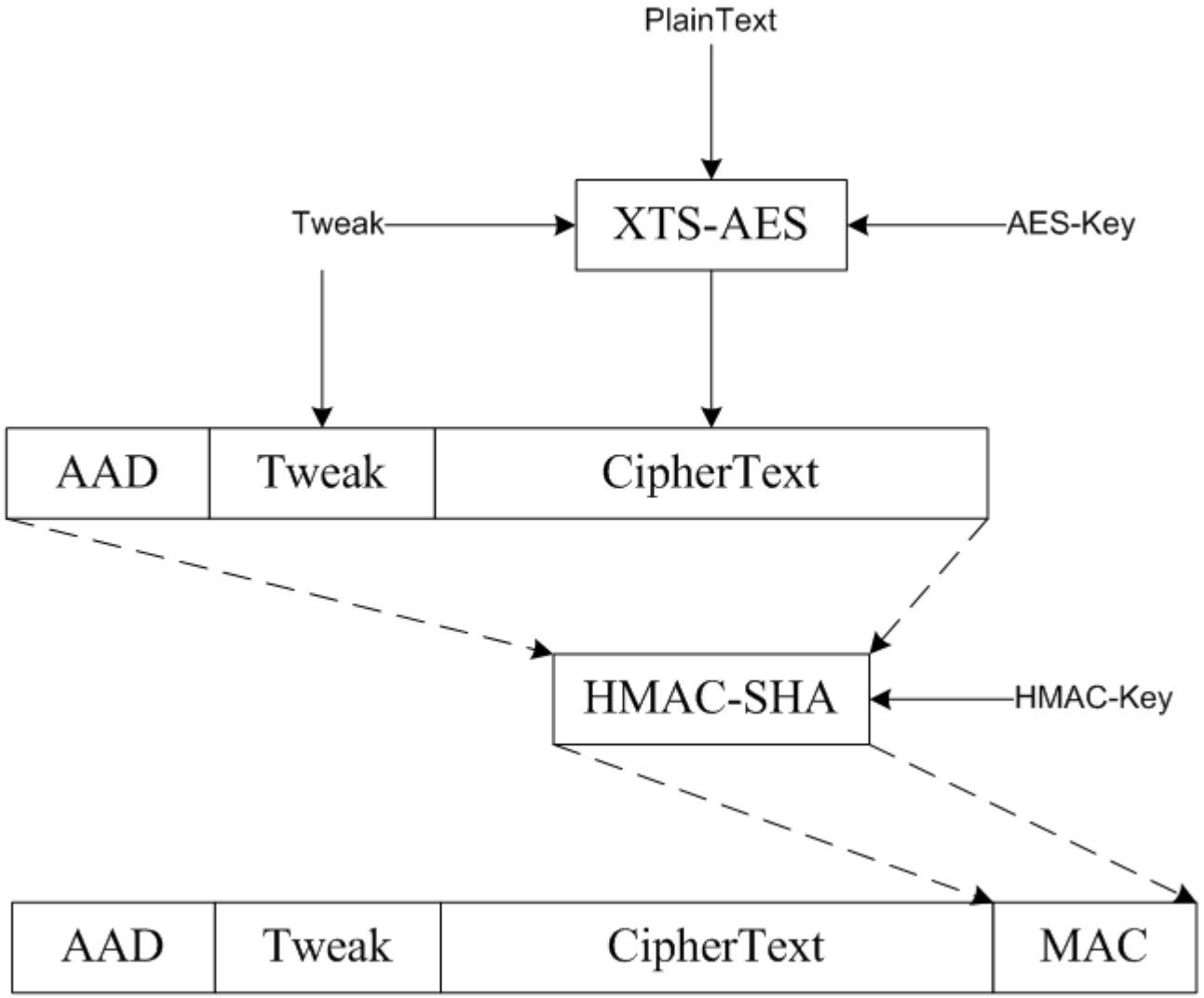
Описаны режимы аутентифицированного шифрования:

- ✓ CBC-MAC (CCM);
- ✓ Galois/counter mode (GCM);
- ✓ Cipher Block Chaining with HMAC-SHA (CBC-HMAC-SHA);
- ✓ Tweakable block-cipher with HMAC (XTS-AES-256-HMAC-SHA-512)

CBC-HMAC-SHA


PlainText
CBC-IV
CBC-AES
AES-Key
AAD
CBC-IV
CipherText
HMAC-SHA
HMAC-Key
AAD
CBC-IV
CipherText
MAC

XTS-AES-256-HMAC-SHA-512



IEEE P1619.2-2010

- ✓ Описаны режимы шифрования:
  - EME2-AES;
  - XCB-AES.
- ✓ Режимы применяются в решениях, модель угроз которых предполагает непосредственный доступ нарушителя к шифротексту.

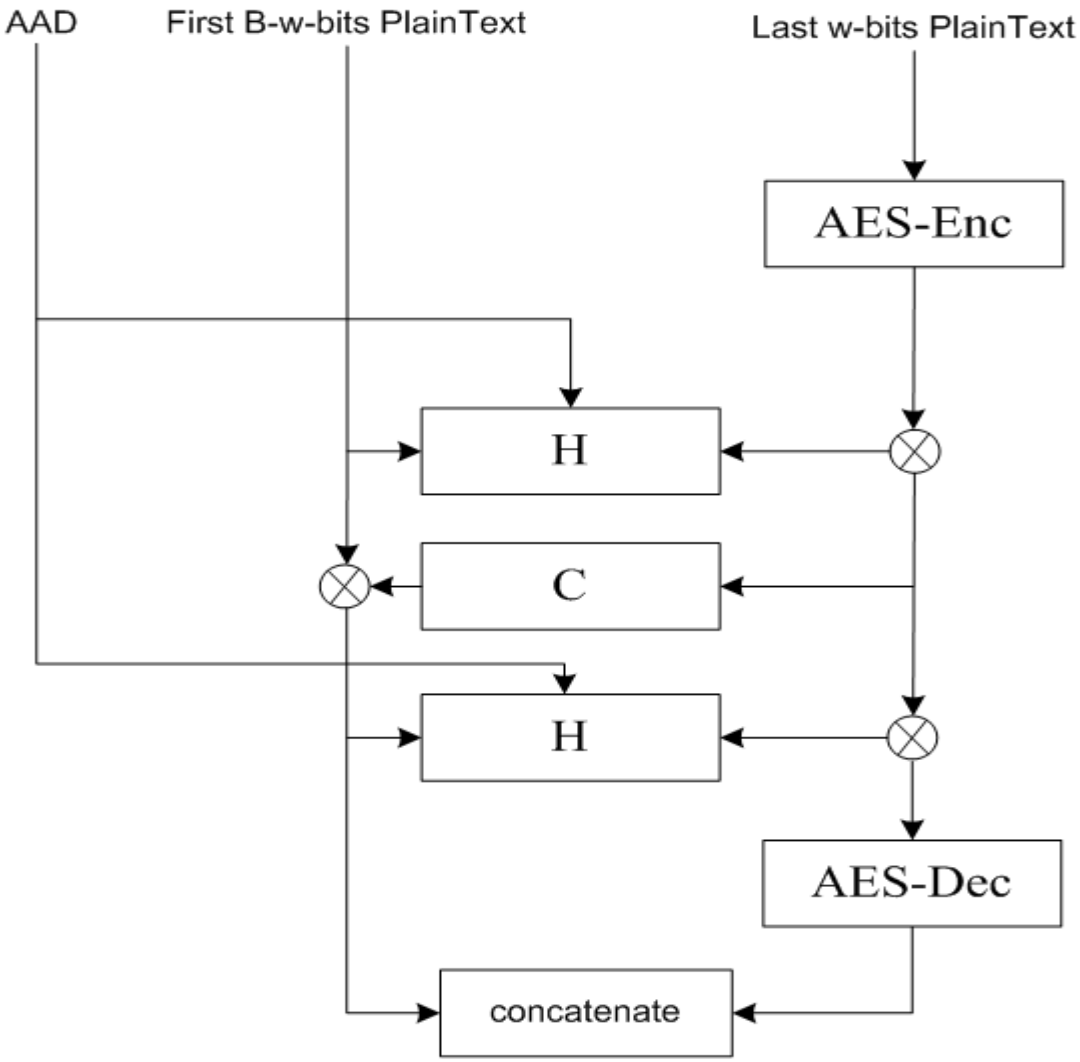
- ✓ Выбор режима зависит от требований к размеру аппаратной реализации, производительности.

	EME2-AES	**XCB-AES**
Шифрование AES	2n+1	n+1
Сдвиг и сложение по модулю 2	3n	–
Умножение в поле $GF(2^{128})$	–	2n

EME2-AES

- ✓ encrypt-mix-encrypt;
- ✓ возможность обработки ассоциированных данных;
- ✓ шифрование данных в режиме простой замены;
- ✓ перемешивание с использованием вычислений в поле Галуа;
- ✓ используются произвольные ключи.

XCB-AES

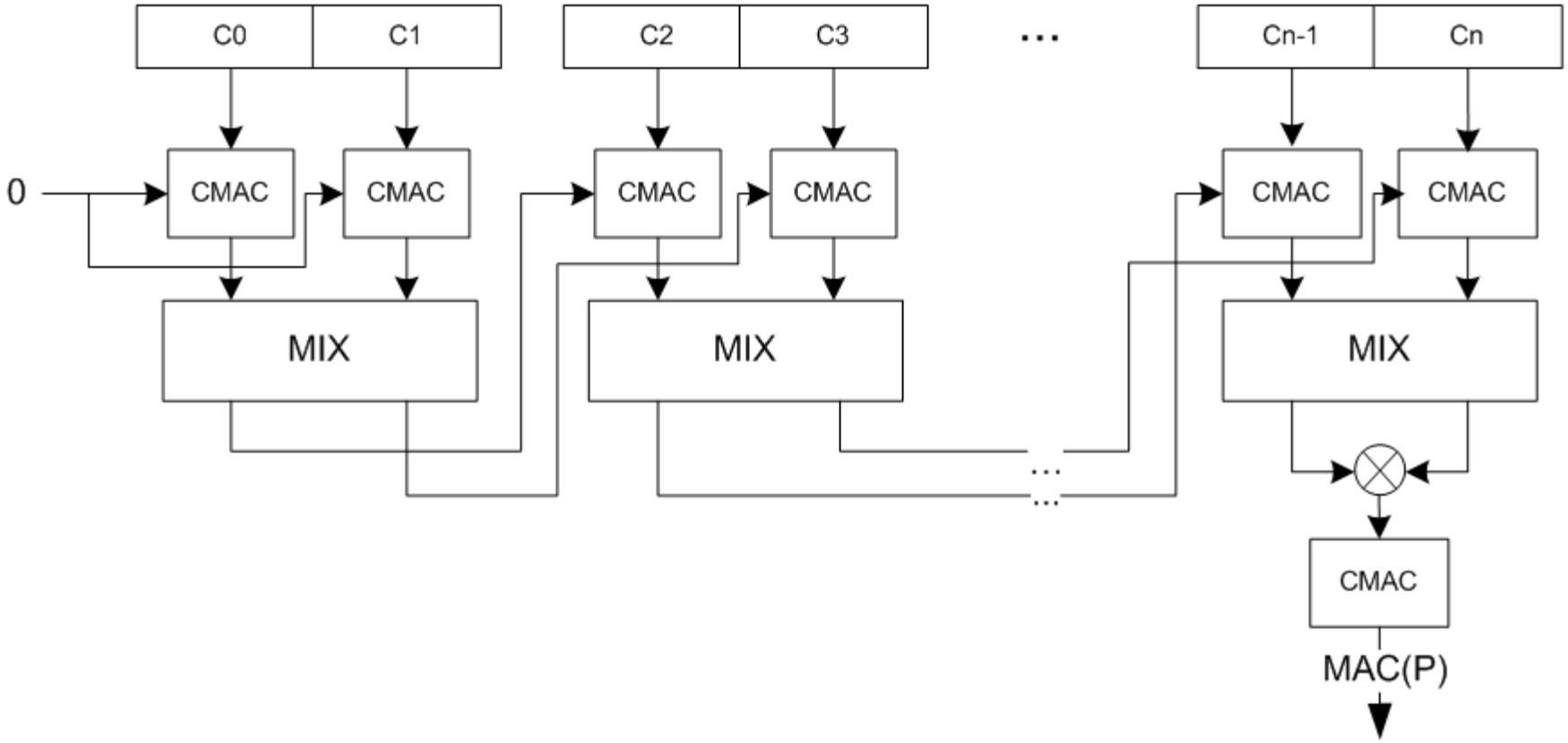

AAD
First B-w-bits PlainText
Last w-bits PlainText
AES-Enc
H
C
H
AES-Dec
concatenate

Особенности применения рекомендуемых режимов совместно с российскими ГОСТ

- ✓ при использовании со «старыми» версиями ГОСТ необходимо:
  - корректировать разрядность поля Галуа;
  - учитывать размер входных данных блочного шифра.

- ✓ при использовании с последними версиями ГОСТ дополнительных действий не требуется.

Распараллеливание шифрования и выработки имитозащитной вставки



Спасибо за внимание!

Вопросы?