Аутентифицированное шифрование с присоединенными данными для устройств с ограниченными ресурсами

Сергей Панасенко
Компания «Актив»
panasenko@guardant.ru

Аутентифицированное шифрование с присоединенными данными

Аутентифицированное шифрование (Authenticated Encryption – AE) — шифрование данных с обеспечением контроля их целостности/ аутентичности.

Аутентифицированное шифрование с присоединенными данными (Authenticated Encryption with Associated Data – AEAD) — шифрование данных с обеспечением контроля целостности/ аутентичности зашифрованных данных, а также дополнительных (присоединенных) данных, передаваемых в открытом виде.

AEAD-шифрование реализуется (в основном) следующими способами:

- применением AEAD-режимов работы алгоритмов блочного симметричного шифрования
- применением алгоритмов аутентифицированного шифрования.

Почему AEAD-шифрование востребовано в устройствах с ограниченными ресурсами

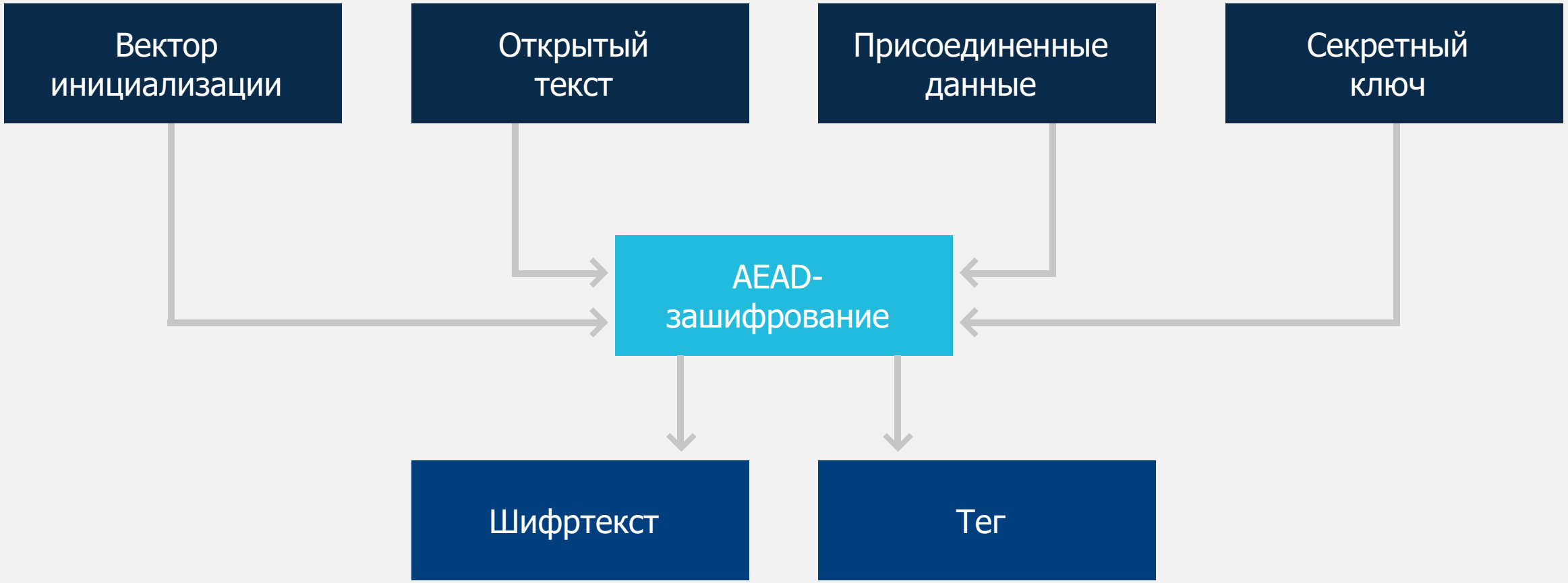
AEAD-шифрование позволяет за насколько возможно короткий промежуток времени (ограниченный однократным выполнением алгоритма) сформировать следующие данные (на примере радиочастотной (RFID) метки):

- зашифрованную полезную информацию (например, полученные от RFID-метки данные)
- аутентифицируемые присоединенные данные (например, идентификатор RFID-метки)
- тег — код аутентификации полученных данных.

RFID-метка – пример устройства, которому крайне важно иметь возможность сформировать такие данные за одно обращение, поскольку:

- RFID-метки обычно имеют ограниченные ресурсы
- RFID-метки взаимодействуют со считывателем по радиоканалу и обычно находятся в зоне действия считывателя короткий промежуток времени.

AEAD-зашифрование



Основные параметры и обеспечиваемые свойства

Параметр	Обеспечивается ли		Требуется ли однократное применение
	целостность	конфиденциальность	
Открытый текст	Да	Да	Нет
Присоединенные данные	Да	Нет	Нет
Вектор инициализации	Да	Нет	Да

AEAD-расшифрование

Режим Multilinear Galois Mode (MGM)

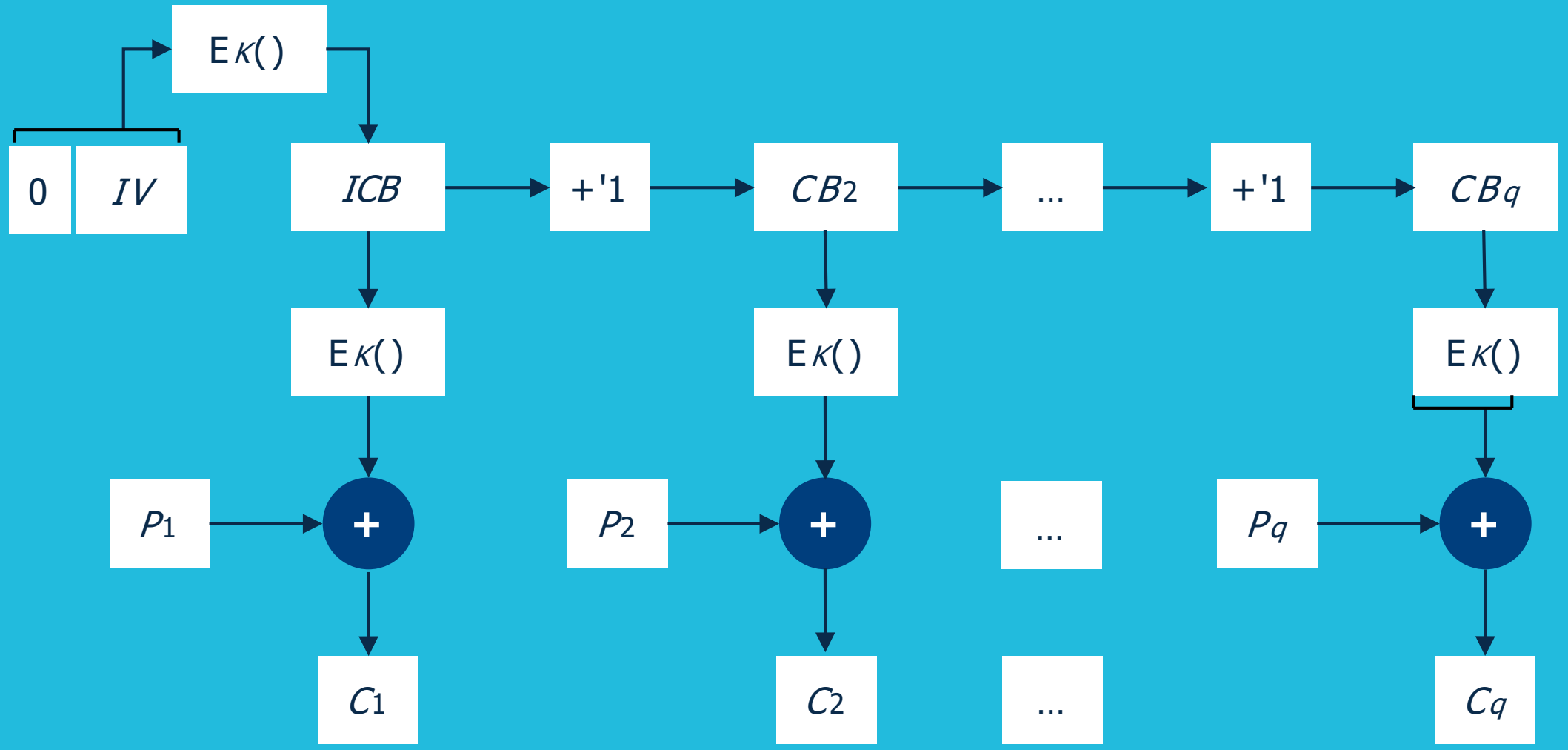
Режим MGM стандартизован:

вошел в Межгосударственный стандарт ГОСТ 34.13-2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» (внесен 25.09.2023 Изменением № 1 к ГОСТ 34.13-2018).

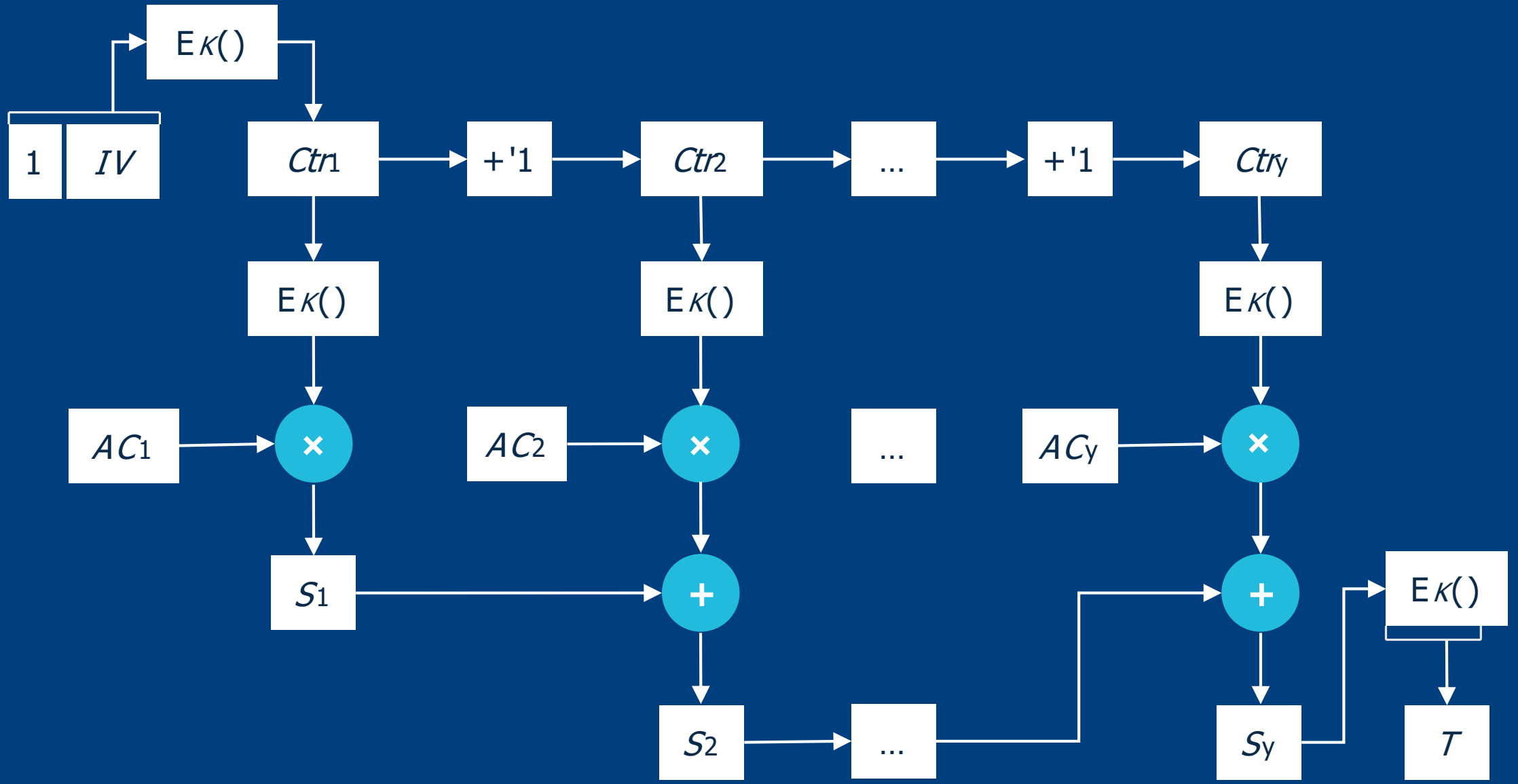
Ранее был описан в Рекомендациях по стандартизации Р 1323565.1.026-2019 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование».

Англоязычное описание: Smyshlyaev S., Nozdrunov V., Shishkin V., Griboedova E. RFC 9058. Multilinear Galois Mode (MGM).

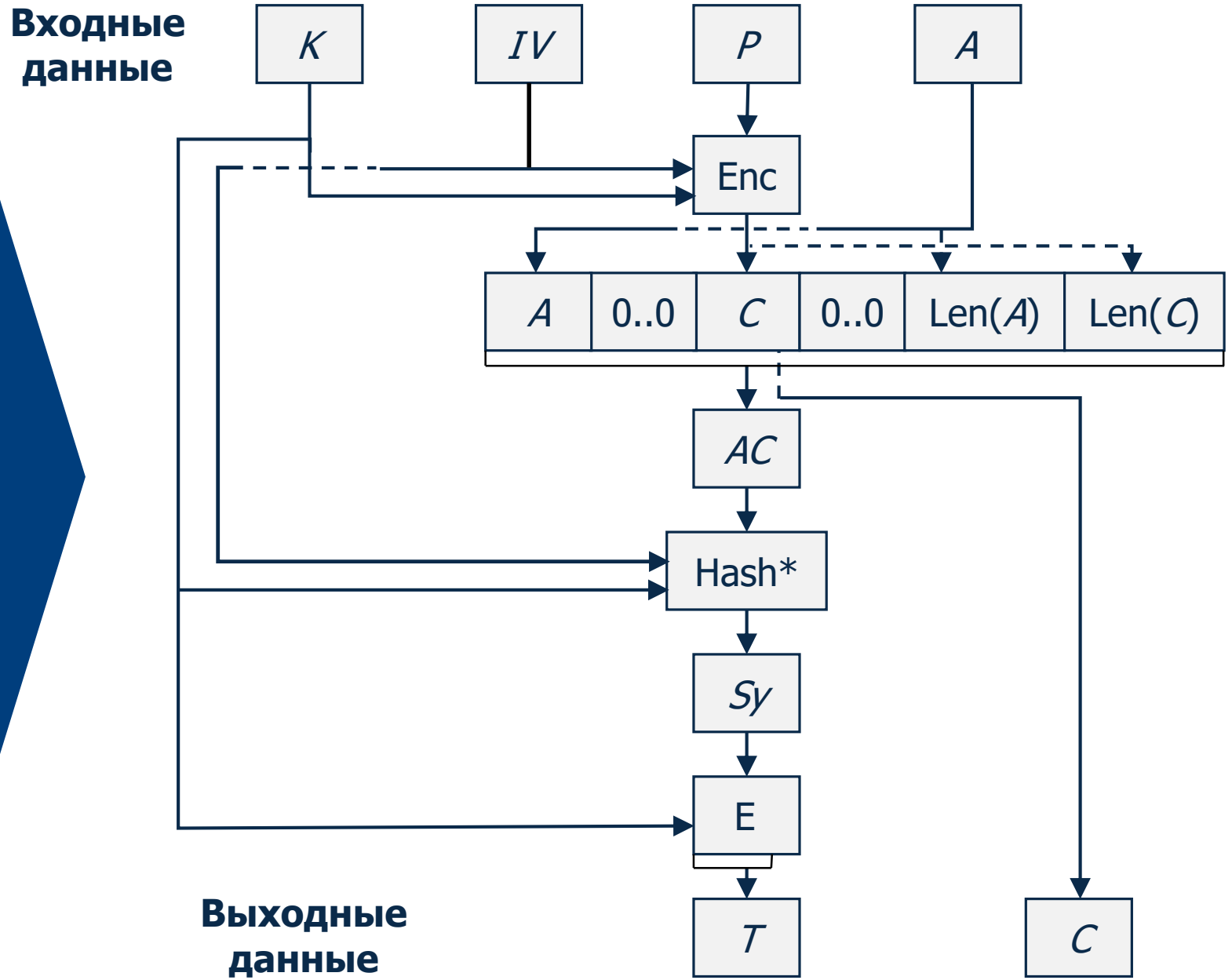
MGM: зашифрование



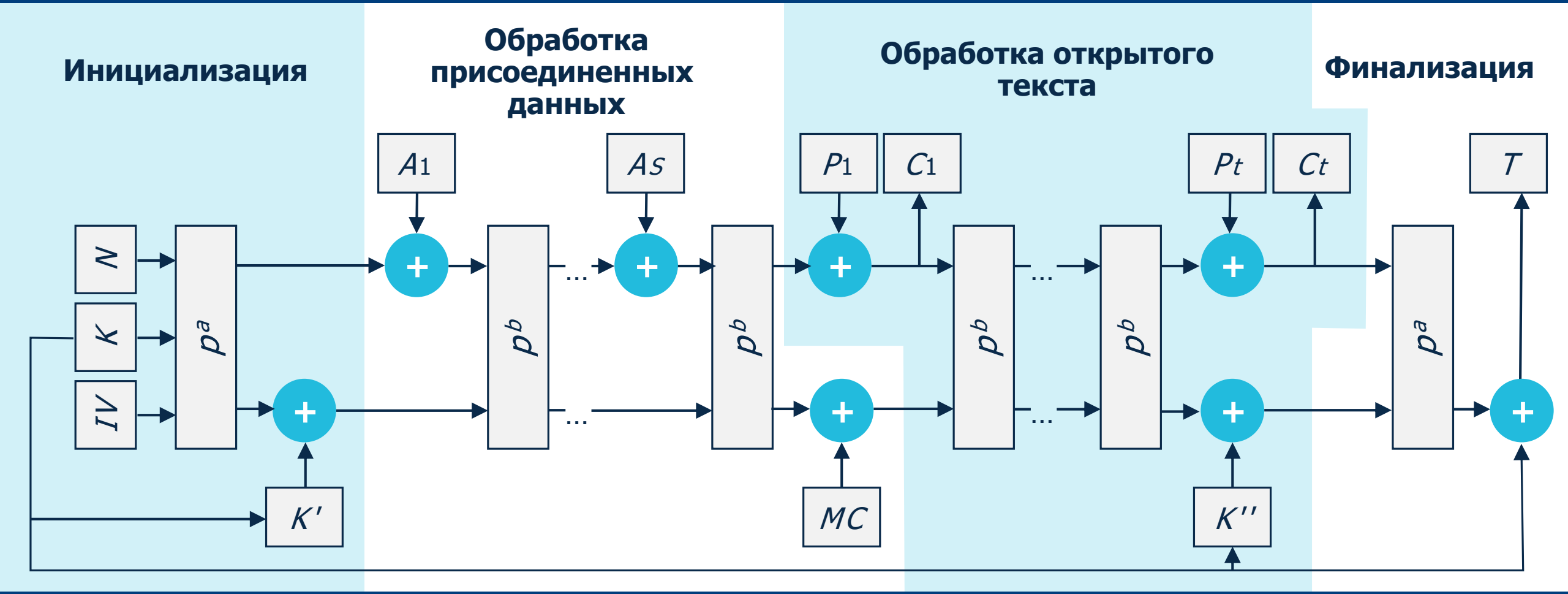
MGM: вычисление имитовставки



MGM: схема зашифрования с вычислением имитовставки



Низкоресурсный алгоритм AEAD-шифрования Ascon



Низкоресурсное стандартное AEAD-шифрование

Стандартизованное AEAD-шифрование с относительно небольшими требованиями к ресурсам можно получить сочетанием двух криптопреобразований:

- AEAD-режима MGM
- низкоресурсного алгоритма блочного симметричного шифрования с 64-битным блоком — алгоритма «Магма».

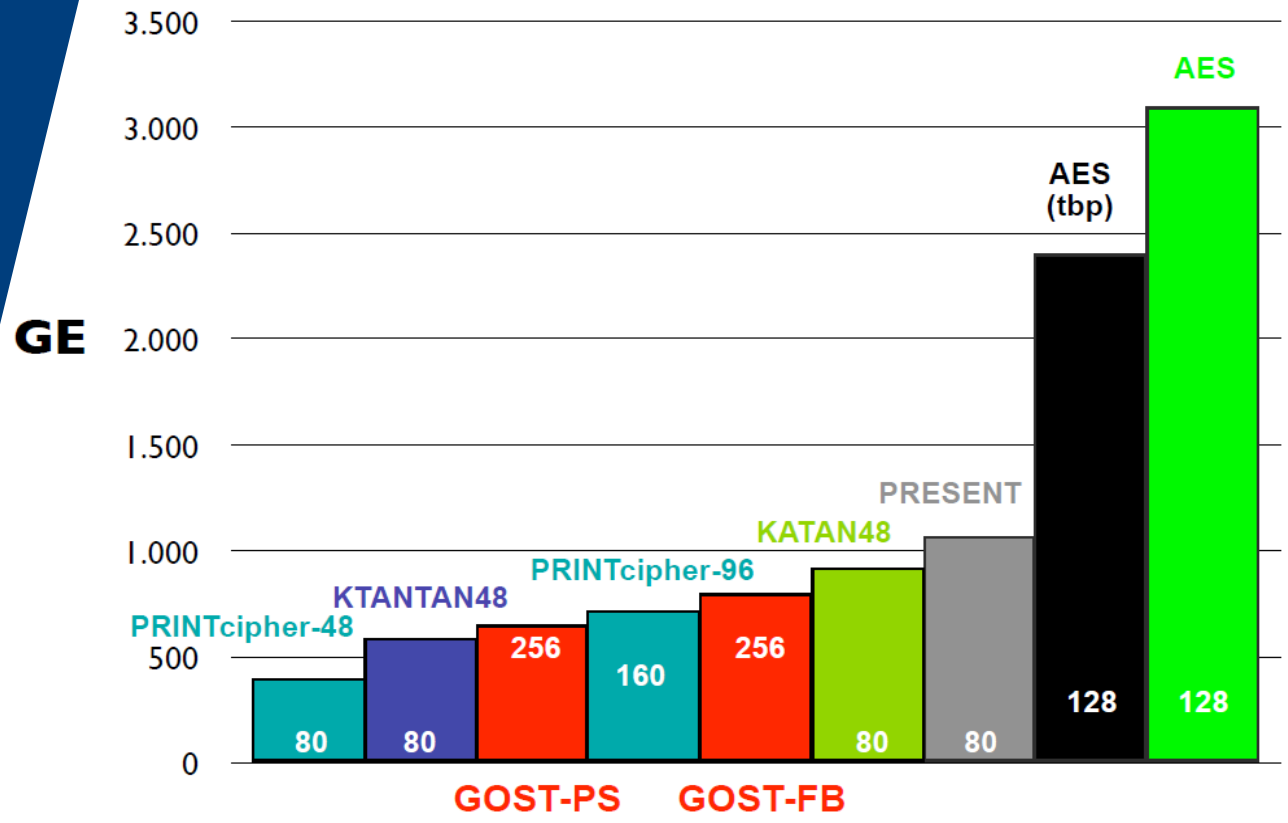


Рис. из Poschmann A., Ling S., Wang H. 256 Bit Standardized Crypto for 650 GE – GOST Revisited. 2010.

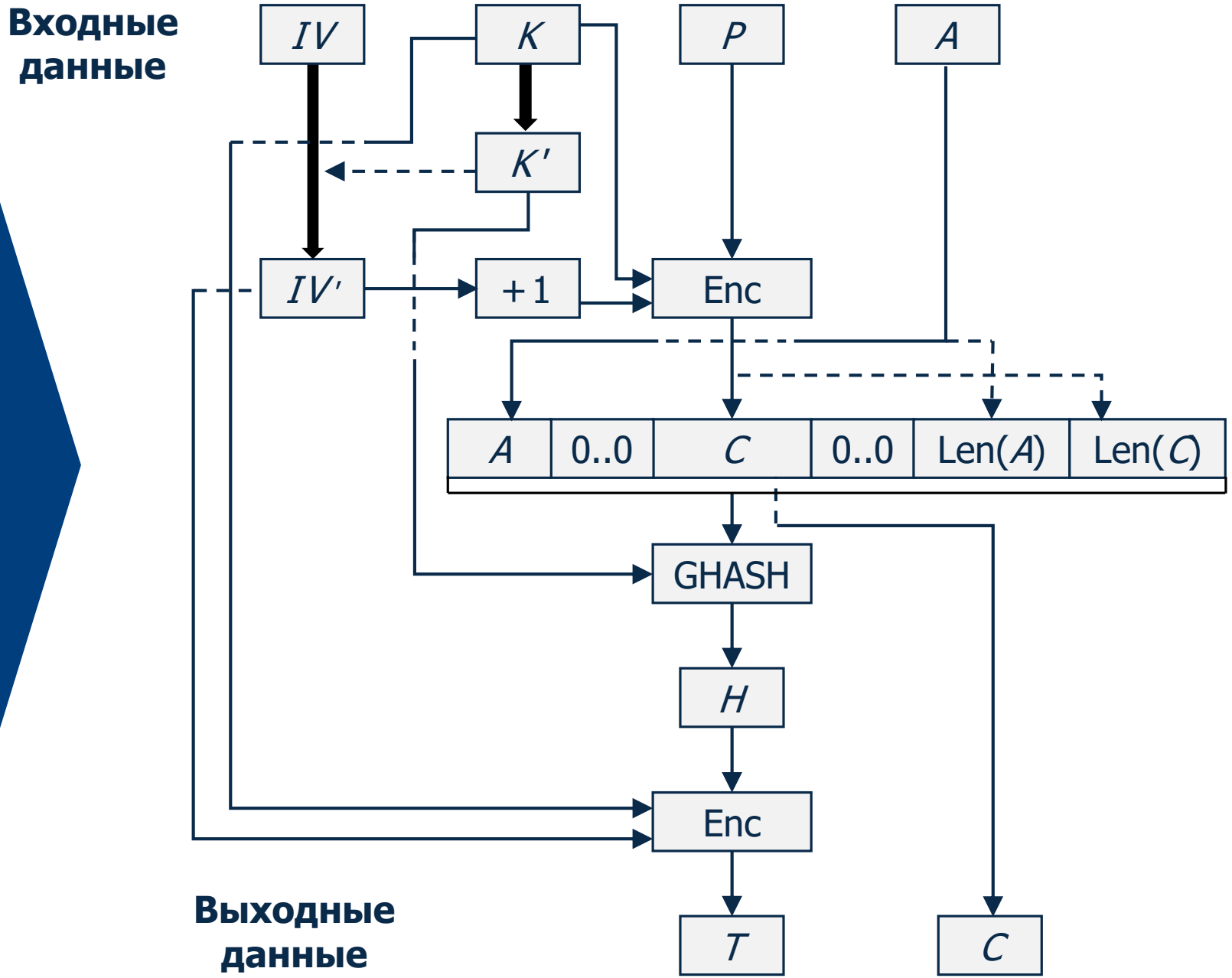
За рубежом

Очень высокий интерес к аутентифицированному шифрованию в последние десятилетия.

Основные события:

Год	Событие	Результат
2007	Выход рекомендаций NIST Special Publication 800-38D: «Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC»	Стандартизован AEAD-режим GCM
2013 – 2019	Европейский проект CAESAR (Competition for Authenticated Encryption: Security, Applicability and Robustness – «Конкурс по аутентифицированному шифрованию: безопасность, применимость и устойчивость»)	Портфолио из 6 AE-алгоритмов, включая 2 низкоресурсных: Ascon и Acorn
2017 – 2023	Конкурс NIST по отбору низкоресурсных алгоритмов AEAD-шифрования и хеширования	Выбран для стандартизации алгоритм Ascon

Режим AEAD-шифрования GCM



Ограничения MGM, GCM и Ascon

Параметр	MGM	GCM	Ascon
Максимальный размер открытого текста, бит	2^{32} или 2^{64} (суммарно)	$2^{39}-256$	*
Максимальный размер присоединенных данных, бит		$2^{64}-1$	*
Размеры вектора инициализации, бит	63 или 127	$1…2^{64}-1$	128
Длина ключа шифрования, бит	256	≥128	≤160 **
Размеры тега, бит	32…128	128, 120, 112, 104, 96, 64, 32	128
Требование уникальности вектора инициализации	Есть	Есть	Частично

* Без ограничений.

** Рекомендуемый размер ключа — 128 бит.

Заключение

1

AEAD-шифрование является востребованным в устройствах, обладающих незначительными вычислительными ресурсами, поскольку оно позволяет за однократное выполнение получить шифртекст и аутентифицирующий тег для контроля целостности шифртекста и открытых присоединенных данных.

2

Существует стандартный режим работы алгоритмов блочного симметричного шифрования, выполняющий AEAD-шифрование, – режим MGM. Данный режим вкупе с низкоресурсным алгоритмом блочного шифрования позволяет обеспечить AEAD-шифрование с относительно небольшими требованиями к ресурсам.

Спасибо за внимание!

КОМПАНИЯ АКТИВ

Вопросы?

Сергей Панасенко

Компания «Актив»

panasenko@guardant.ru

КОМПАНИЯ АКТИВ

Компания «Актив» — крупнейший в России производитель аппаратных средств электронной подписи и решений для защиты программного обеспечения. Компания на рынке уже 30 лет.

Сейчас в компании работает более 250 человек.
Из них около трети — разработчики, тестировщики и технические аналитики.

Средний возраст IT специалистов в компании — менее 30 лет.
Компания активно нанимает в том числе студентов старших курсов.
Многие руководители и лиды групп приходили работать в «Актив» студентами на позиции младших разработчиков, тестировщиков.

Компания «Актив» славится своим коллективом: здесь всегда готовы помочь разобраться в трудной проблеме, дать совет, подставить плечо.
Каждый участник команды имеет право голоса, будет выслушан и может влиять на процессы. Именно за счёт новых идей, участия молодых сотрудников компания идёт в ногу со временем и применяет современные методы и технологии в процессах разработки.

Если у Вас возник интерес к нашей компании, и Вы хотите стать ее частью, проходите по ссылке в QR-коде и присылайте резюме!