Обзор алгоритмов аутентифицированного шифрования – финалистов конкурса CAESAR

Виктория Власова

Лаборатория Касперского

22 марта 2018

Competition for
Authenticated
Encryption:
Security,
Applicability, and
Robustness

ГГ.	Конкурс	Орг.	Описание
1997-2000	AES		блочные шифры
2000-2003	CRYPTREC		несколько категорий алгоритмов
2000-2003	NESSIE		несколько категорий алгоритмов
2004-2008	eStream		поточные шифры
2007-2012	SHA-3		функции хеширования
2013-2015	PHC		алгоритм хеширования паролей
2013-2018	**CAESAR**		схемы аутентифицированного шифрования
2016-?	PQC		алгоритмы с открытым ключом, устойчивые к квантовым атакам

Table 1: Криптографические конкурсы.

Система аутентифицированного шифрования со связанными данными (AEAD)

$$\Pi = (\mathcal{K}, Enc, Dec),$$

$Enc_K(H, N, M)$ – алгоритм зашифрования,
$Dec_K(H, N, C, T)$ – алгоритм расшифрования,
$K \in \mathcal{K} \subseteq \{0,1\}^k$ – секретный ключ,
$N \in \mathcal{N} \subseteq \{0,1\}^n$ – одноразовый вектор (nonce),
$T \in \mathcal{T} \subseteq \{0,1\}^t$ – имитовставка,
$H \in \mathcal{H} \subseteq \{0,1\}^*$ – связанные данные (associated data),
$M \in \mathcal{M} \subseteq \{0,1\}^*$ – открытый текст,
$C \in \mathcal{C} \subseteq \{0,1\}^*$ – шифртекст.

$$Enc : \mathcal{K} \times \mathcal{N} \times \mathcal{H} \times \mathcal{M} \to \mathcal{C} \times \mathcal{T},$$

$$Dec : \mathcal{K} \times \mathcal{N} \times \mathcal{H} \times \mathcal{C} \times \mathcal{T} \to \mathcal{M} \cup \{\perp\}.$$

Система аутентифицированного шифрования со связанными данными (AEAD)

$$Enc_K(H, N, M) = (C, T),$$

$$Dec_K(H, N, C, T) = \begin{cases} M, & \text{если пара } (C, T) \text{ аутентифицирована,} \\ \perp, & \text{в противном случае.} \end{cases}$$

$Dec_K(H, N, Enc_K(H, N, M)) = M$ для любых (K, H, N, M).

Рассматриваеваемые свойства алгоритмов

- Возможность распараллеливания зашифрования/расшифрования.
- «Online» (результат обработки блока данных не зависит от последующих блоков).
- Инволютивность.
- Возможность вычисления промежуточных кодов аутентификации.
- «Provable security» (прямая зависимость между стойкостью алгоритма и лежащего в его основе базового примитива).
- Стойкость при повторном использовании одноразового вектора.
- Отсутствие возможности получить информацию о результате расшифрования, если шифртекст не прошел аутентификацию алгоритмом.

Варианты использования

1. среды с ограниченными ресурсами
   - для реализации на небольшой аппаратной области и/или при помощи небольшого количества кода для 8-разрядных процессоров
2. высокопроизводительные приложения
   - для эффективной реализации на 64-битных ЦП серверов и/или выделенном оборудовании
3. допустимо стойкие при нарушении рекомендаций к использованию ("Defense in depth")
   - обеспечение целостности при повторном использовании одноразового вектора

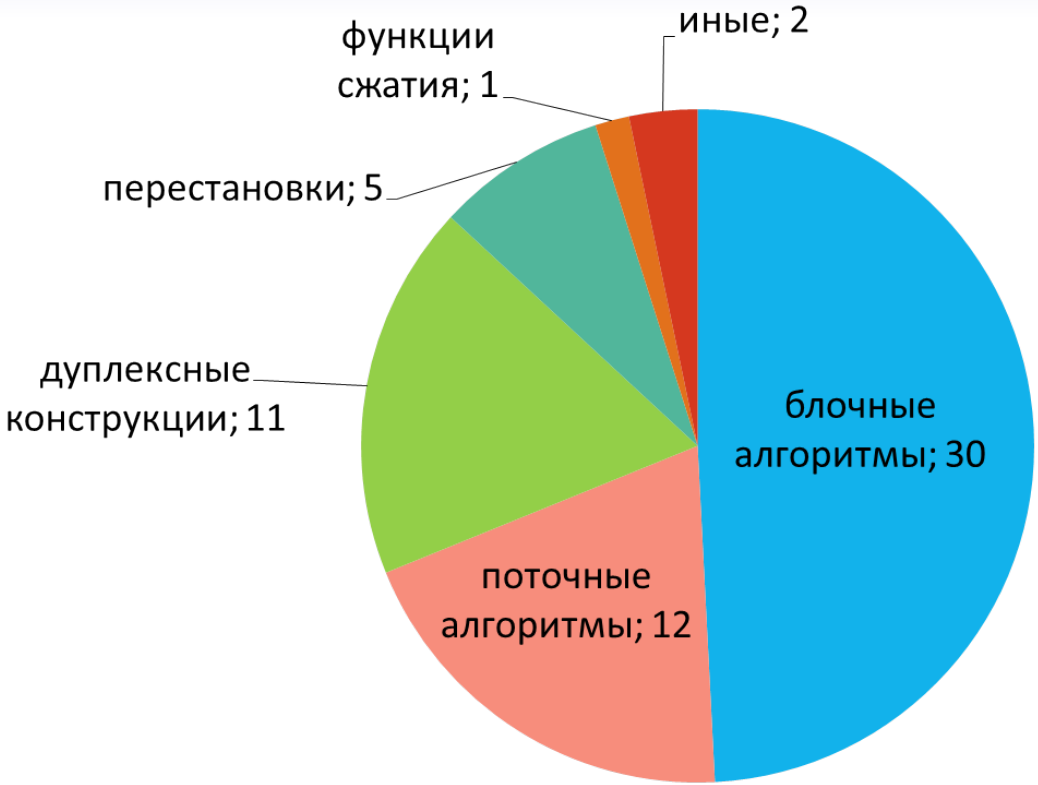
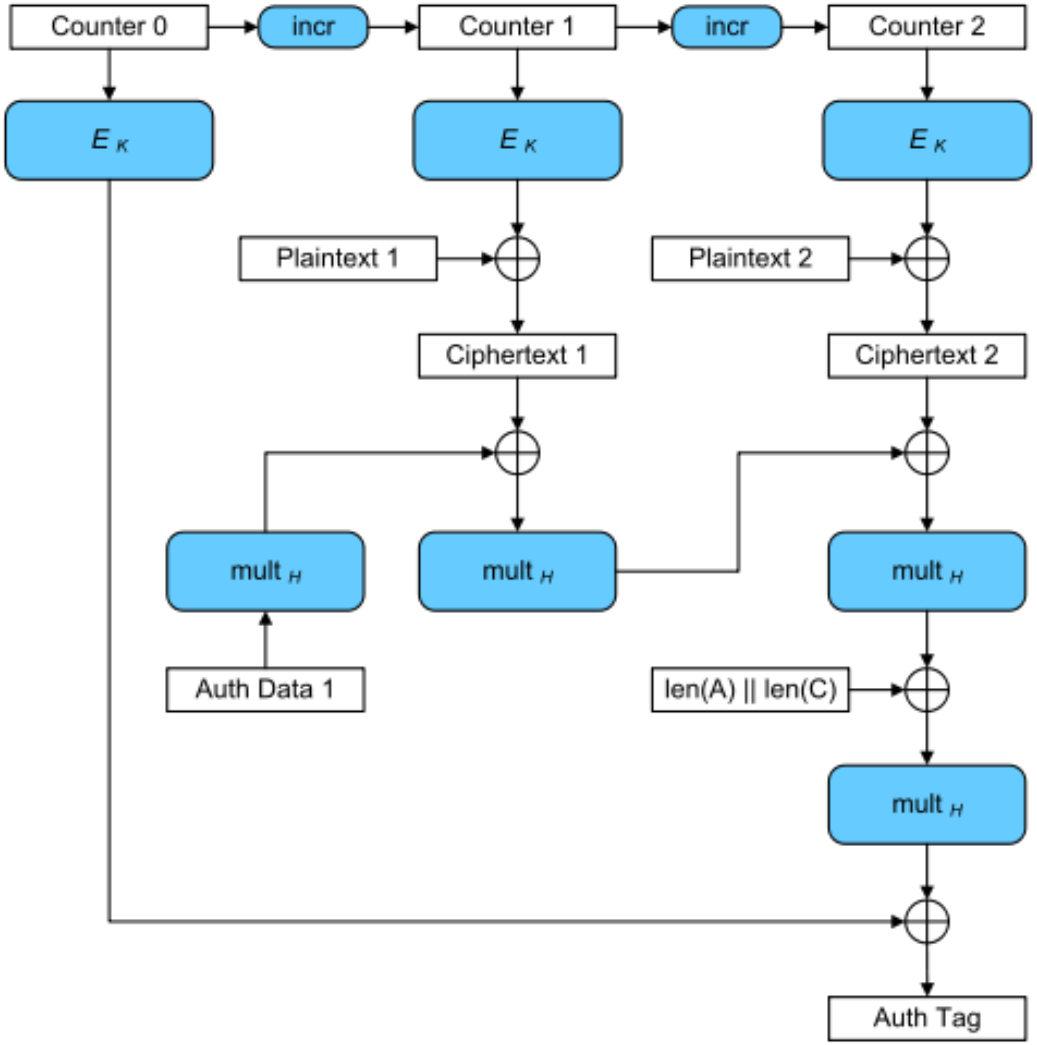


Figure 1: Базовые примитивы [AFL16]

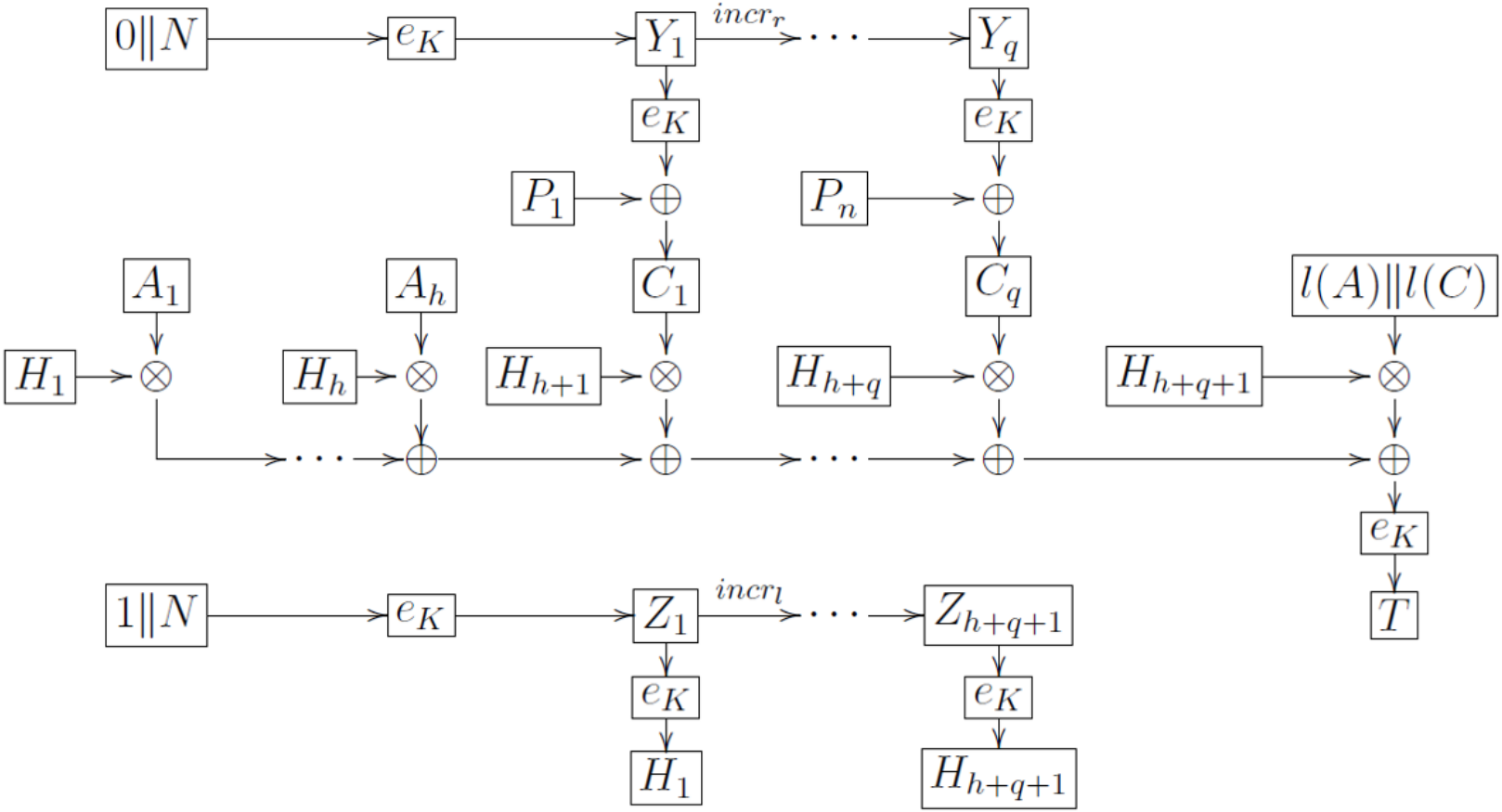
[AFL16] Abed, F., Forler, C., Lucks, S.: General classification of the authenticated encryption schemes for the CAESAR competition. Computer Science Review (2016)

Figure 2: Участники 3 раунда

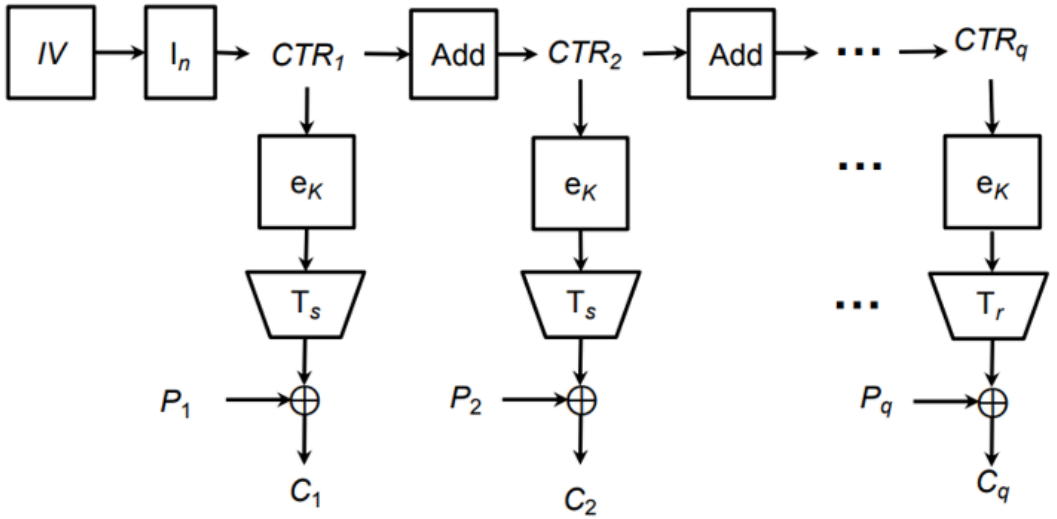
Вне конкурса: GCM

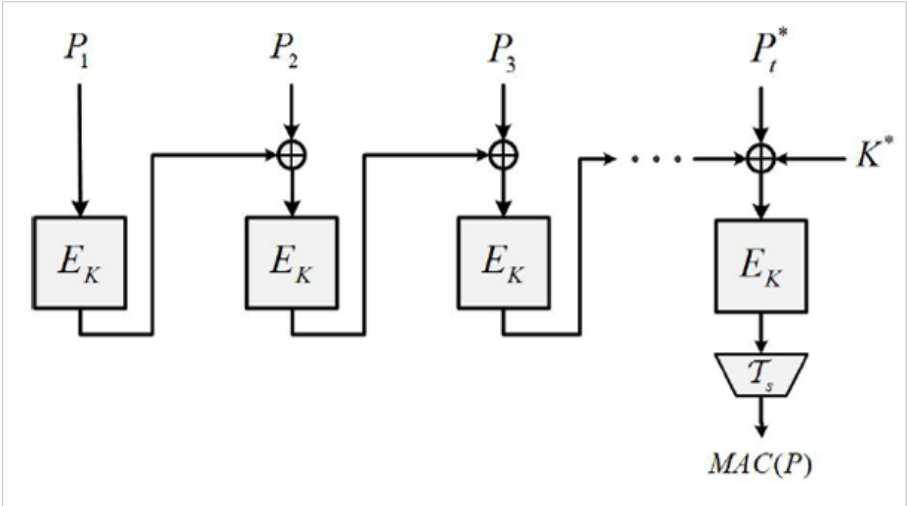


Вне конкурса: MGM

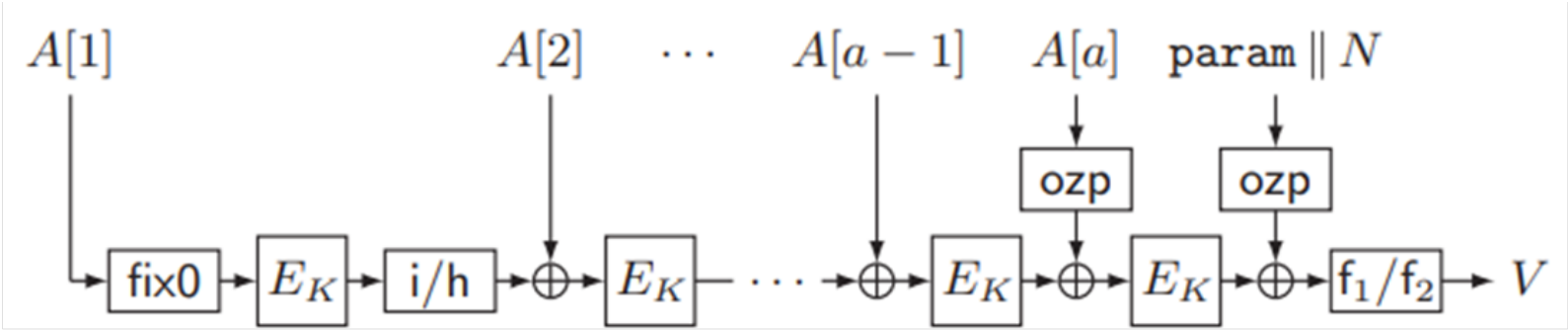


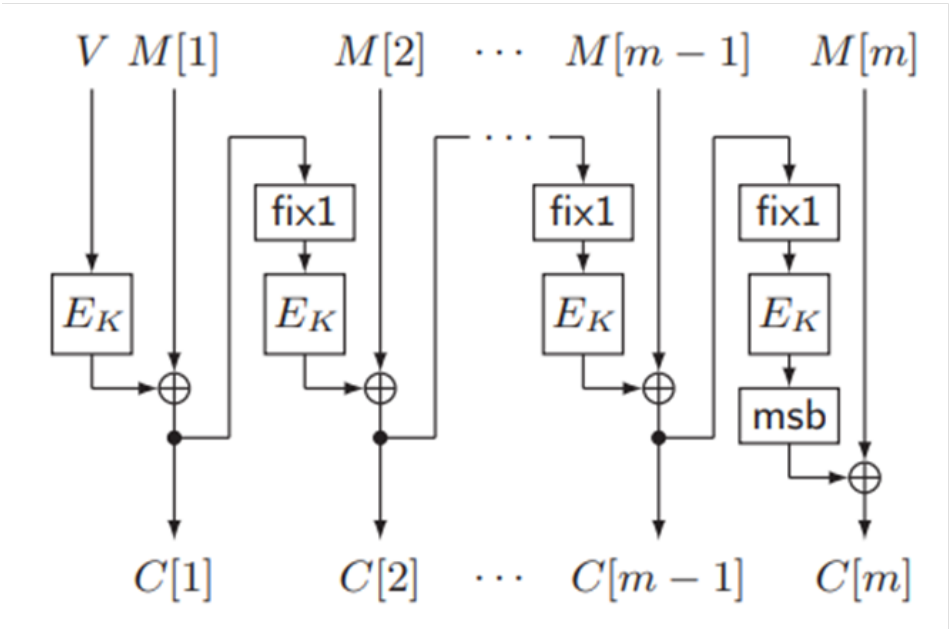
Вне конкурса: 8 бит

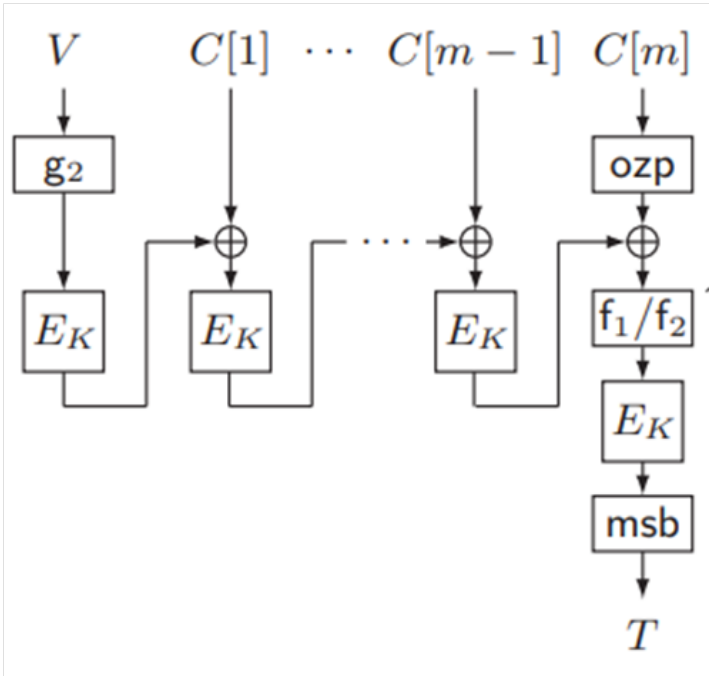




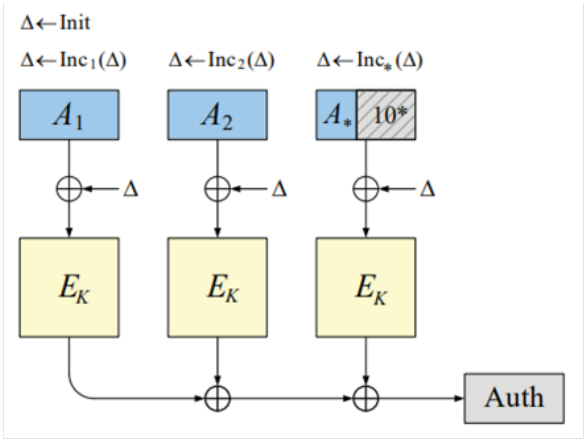
CLOC&SILC

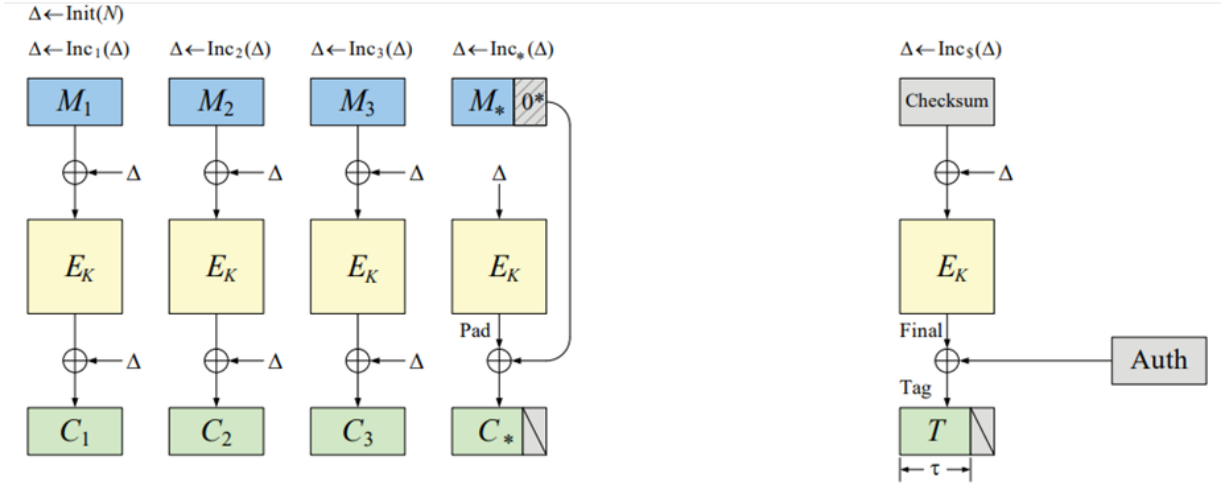

A[1]
A[2]
· · ·
A[a − 1]
A[a]
param ‖ N
ozp
ozp
fix0
E_K
i/h
E_K
· · ·
E_K
E_K
E_K
f1/f2
V


V
M[1]
M[2]
· · ·
M[m − 1]
M[m]
fix1
fix1
fix1
E_K
E_K
E_K
E_K
E_K
msb
C[1]
C[2]
· · ·
C[m − 1]
C[m]


V
C[1]
· · ·
C[m − 1]
C[m]
g2
ozp
E_K
E_K
E_K
f1/f2
E_K
msb
T

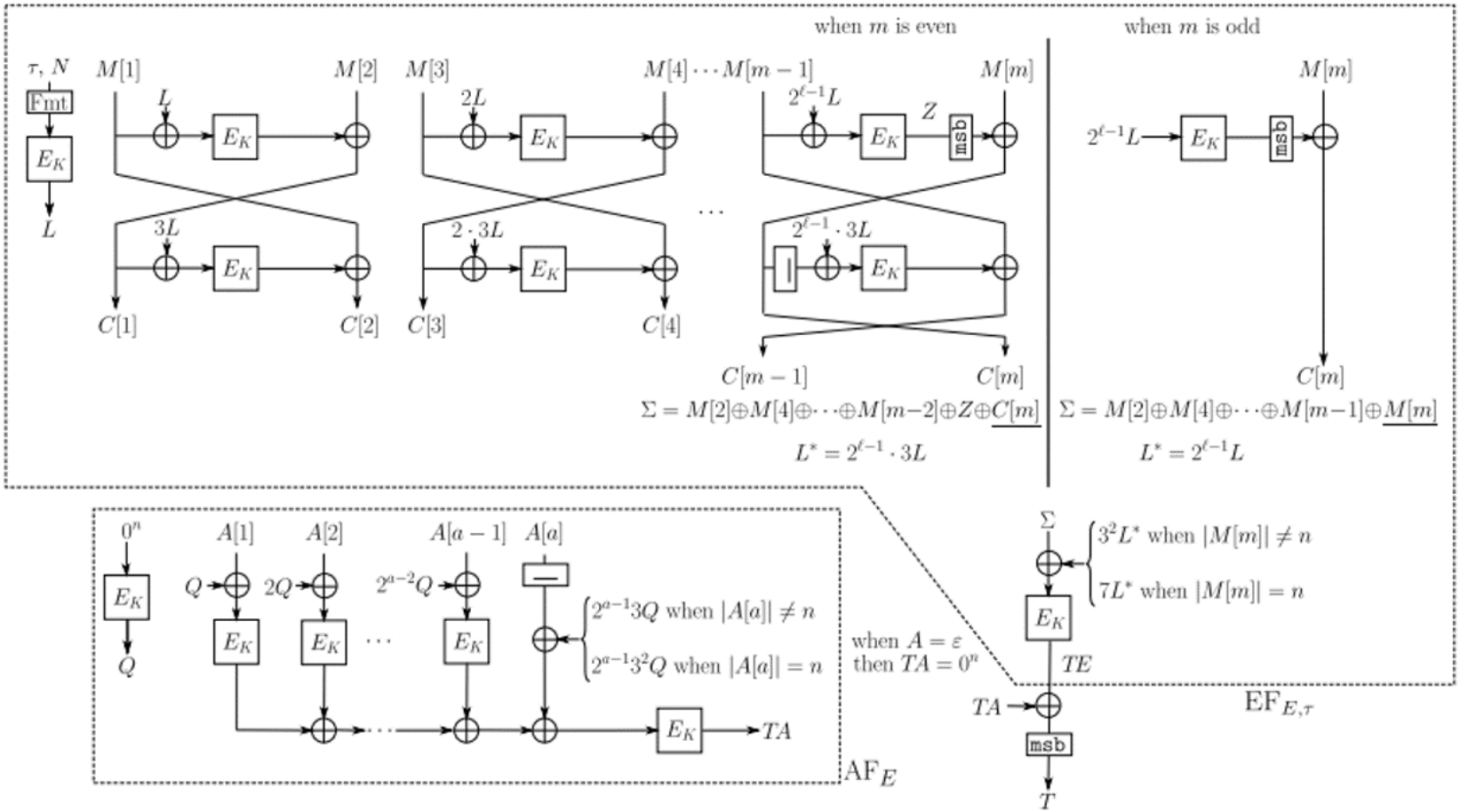
OCB



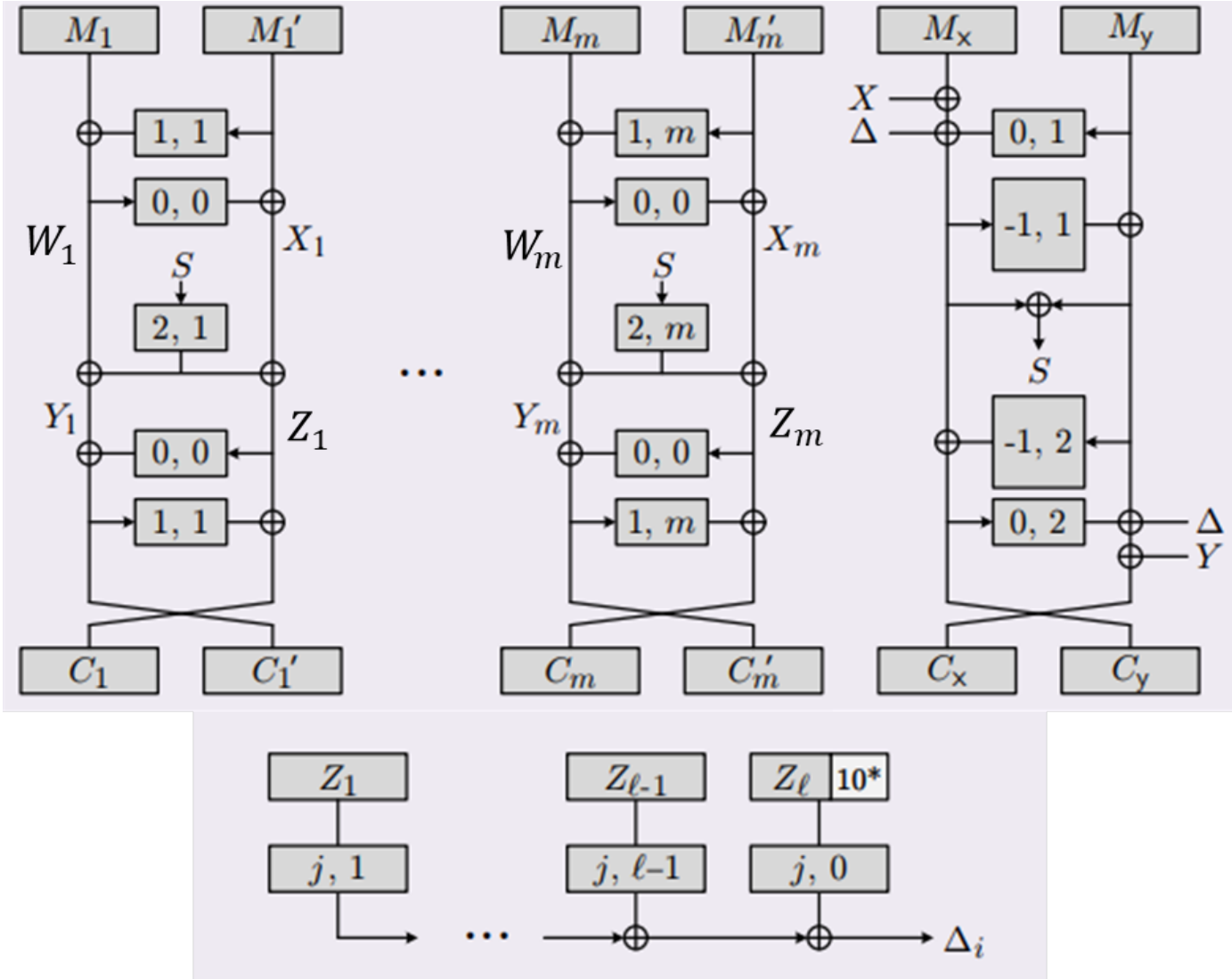


* Идея настраеваемого блочного шифра (tweakable block cipher)

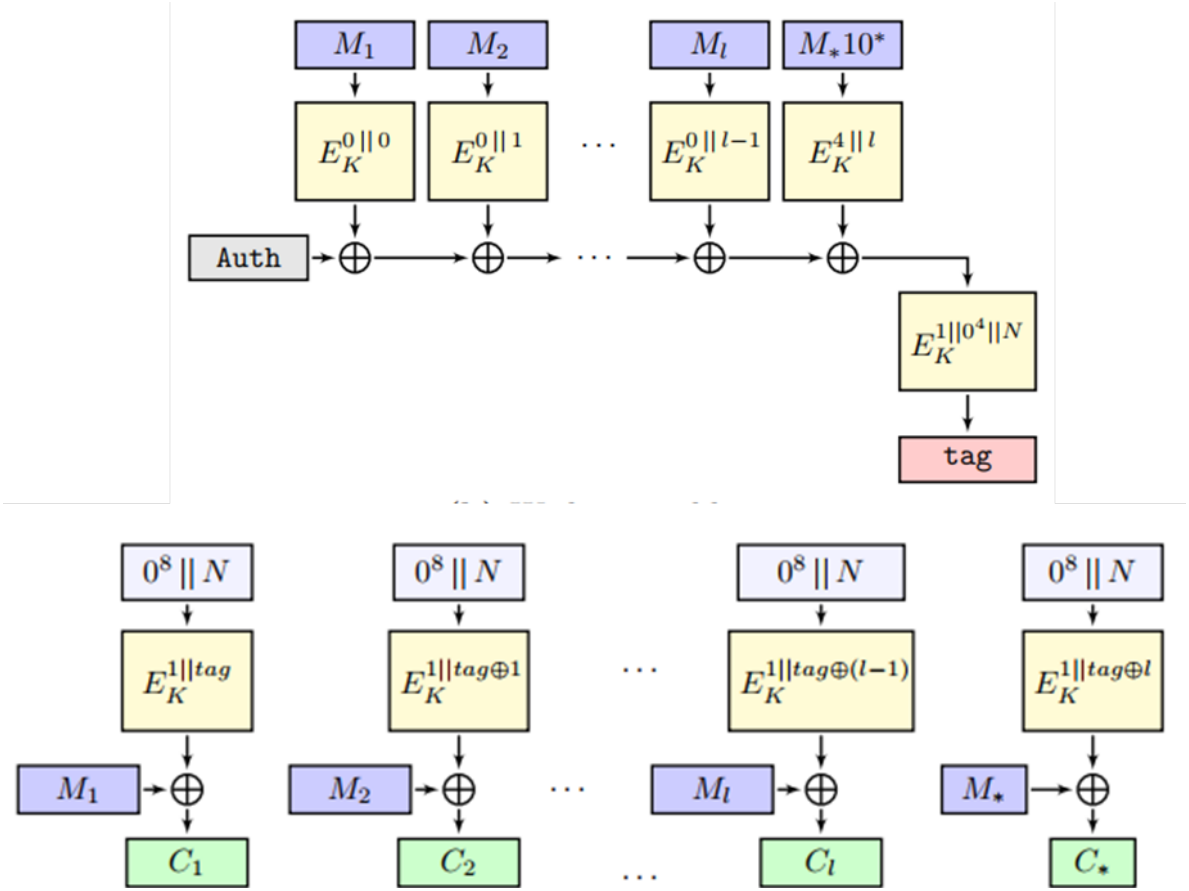
OTR


when m is even
when m is odd
τ, N
Fmt
E_K
L
$M[1]$
$M[2]$
$M[3]$
$M[4] \cdots M[m-1]$
$M[m]$
$2L$
$3L$
$2 \cdot 3L$
$2^{\ell-1}L$
$2^{\ell-1} \cdot 3L$
Z
msb
$C[1]$
$C[2]$
$C[3]$
$C[4]$
$C[m-1]$
$C[m]$
$\Sigma = M[2] \oplus M[4] \oplus \cdots \oplus M[m-2] \oplus Z \oplus C[m]$
$L^* = 2^{\ell-1} \cdot 3L$
$\Sigma = M[2] \oplus M[4] \oplus \cdots \oplus M[m-1] \oplus M[m]$
$L^* = 2^{\ell-1}L$
0^n
$A[1]$
$A[2]$
$A[a-1]$
$A[a]$
Q
$2Q$
$2^{a-2}Q$
$2^{a-1}3Q$ when $|A[a]| \neq n$
$2^{a-1}3^2Q$ when $|A[a]| = n$
TA
AF_E
when $A = \varepsilon$ then $TA = 0^n$
Σ
3^2L^* when $|M[m]| \neq n$
$7L^*$ when $|M[m]| = n$
TE
T
$\mathrm{EF}_{E,\tau}$

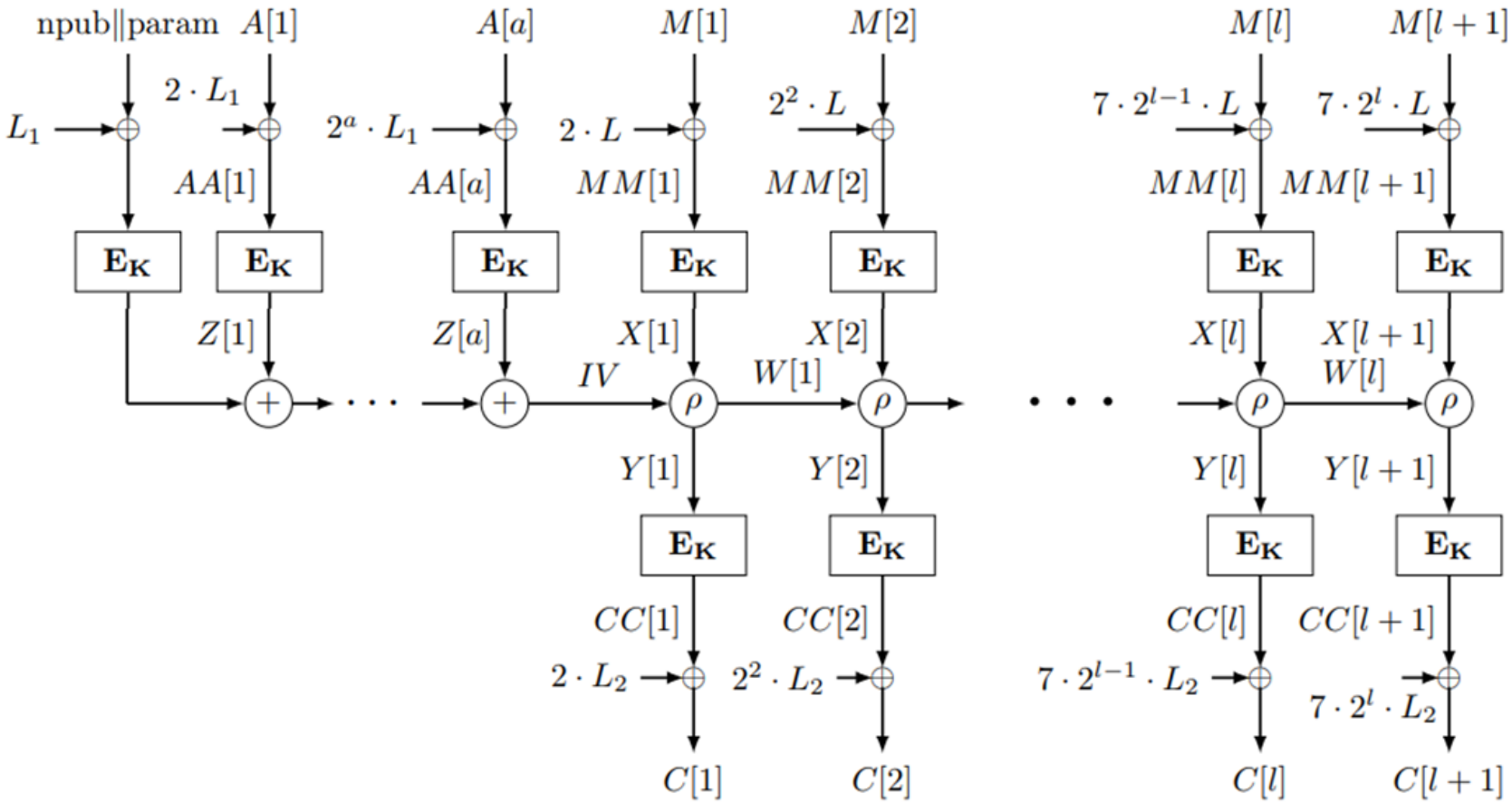
AEZ


M_1
M_1'
M_m
M_m'
M_x
M_y
1, 1
0, 0
2, 1
0, 0
1, 1
1, m
0, 0
2, m
0, 0
1, m
0, 1
-1, 1
-1, 2
0, 2
W_1
X_1
Y_1
Z_1
W_m
X_m
Y_m
Z_m
X
Δ
S
Δ
Y
C_1
C_1'
C_m
C_m'
C_x
C_y
Z_1
$Z_{\ell-1}$
Z_ℓ
10*
j, 1
j, ℓ–1
j, 0
Δ_i

Deoxys


M_1
M_2
M_l
M_*10^*
$E_K^{0||0}$
$E_K^{0||1}$
$E_K^{0||l-1}$
$E_K^{4||l}$
Auth
$E_K^{1||0^4||N}$
tag
$0^8 || N$
$E_K^{1||tag}$
$E_K^{1||tag\oplus 1}$
$E_K^{1||tag\oplus(l-1)}$
$E_K^{1||tag\oplus l}$
M_1
M_2
M_l
M_*
C_1
C_2
C_l
C_*

COLM


npub‖param
A[1]
A[a]
M[1]
M[2]
M[l]
M[l + 1]
L1
2 · L1
2^a · L1
2 · L
2^2 · L
7 · 2^{l−1} · L
7 · 2^l · L
AA[1]
AA[a]
MM[1]
MM[2]
MM[l]
MM[l + 1]
EK
Z[1]
Z[a]
X[1]
X[2]
X[l]
X[l + 1]
IV
W[1]
W[l]
ρ
Y[1]
Y[2]
Y[l]
Y[l + 1]
CC[1]
CC[2]
CC[l]
CC[l + 1]
2 · L2
2^2 · L2
7 · 2^{l−1} · L2
7 · 2^l · L2
C[1]
C[2]
C[l]
C[l + 1]

Ketje, Keyak

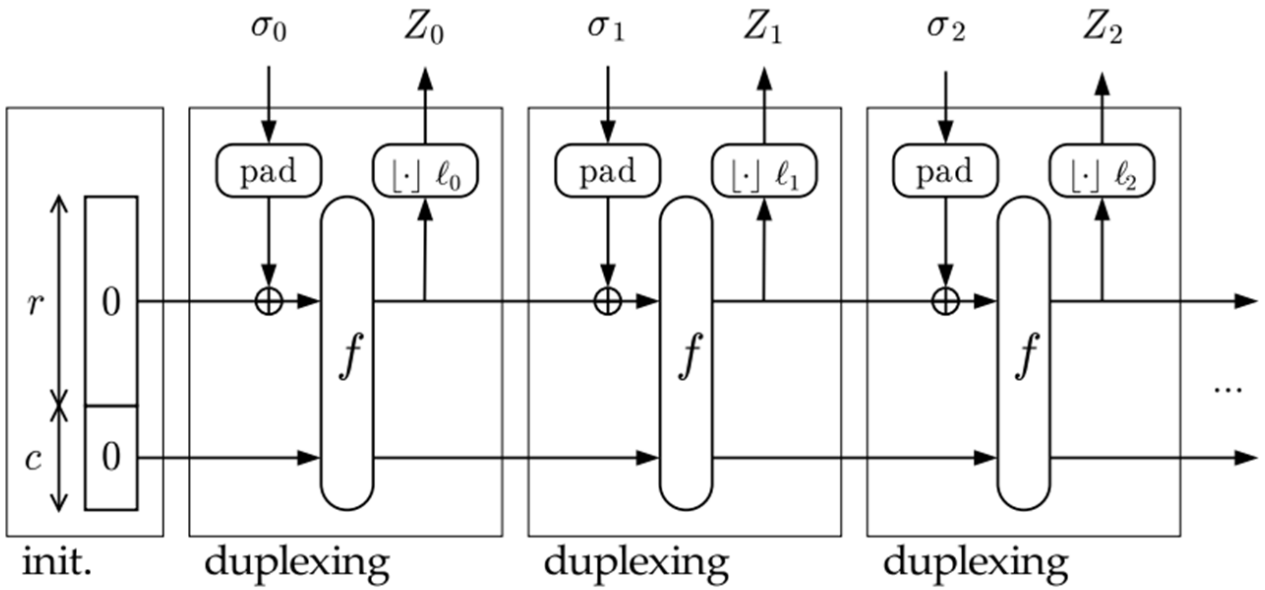


Figure 3: Дуплексная конструкция

NORX, Ascon

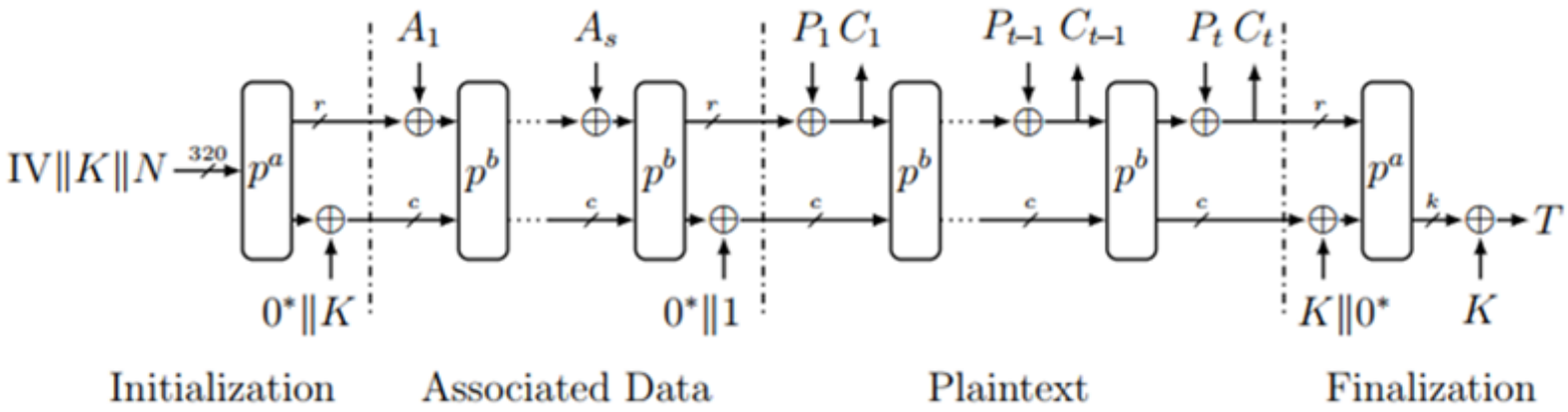
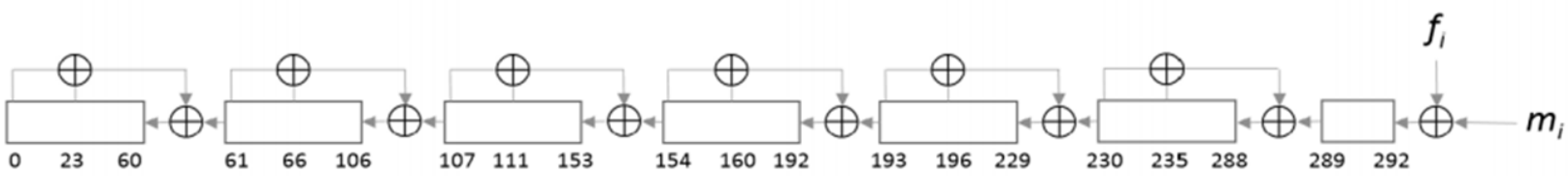


Figure 4: Схема алгоритма Ascon

ACORN


f_i
m_i
0 23 60
61 66 106
107 111 153
154 160 192
193 196 229
230 235 288
289 292

Другие системы на основе поточных алгоритмов

$S_i = (S_i[1], \ldots, S_i[q])$ – внутреннее состояние из q слов

1. Инициализация

$$(S[1], \ldots, S[q]) = Init(K, N, parameretrs)$$
$$S_{i+1} = StateUpdate(S_i, f(K, N)), \quad i = 1, \ldots, c_{Init}$$

2. Обработка связанных данных

$$S_{i+1} = StateUpdate(S_i, AD_i), \quad i = 1, \ldots, c_{AD}$$

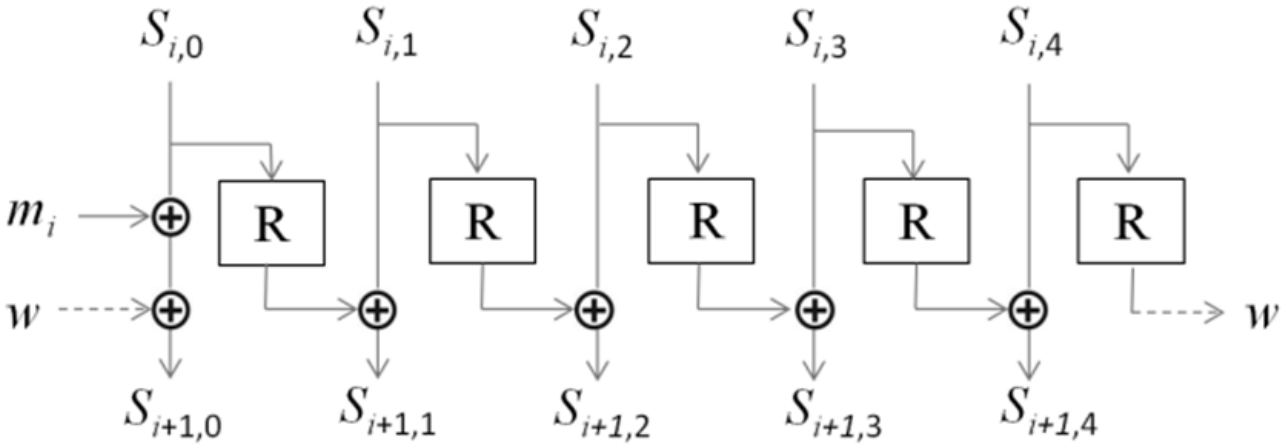
3. Зашифрование

$$\left.\begin{aligned} C_i &= M_i \oplus (S_i[a] \oplus S_i[b] \oplus (S_i[c] \& S_i[d])) \\ S_{i+1} &= StateUpdate(S_i, M_i) \end{aligned}\right\} i = 1, \ldots, c_M$$

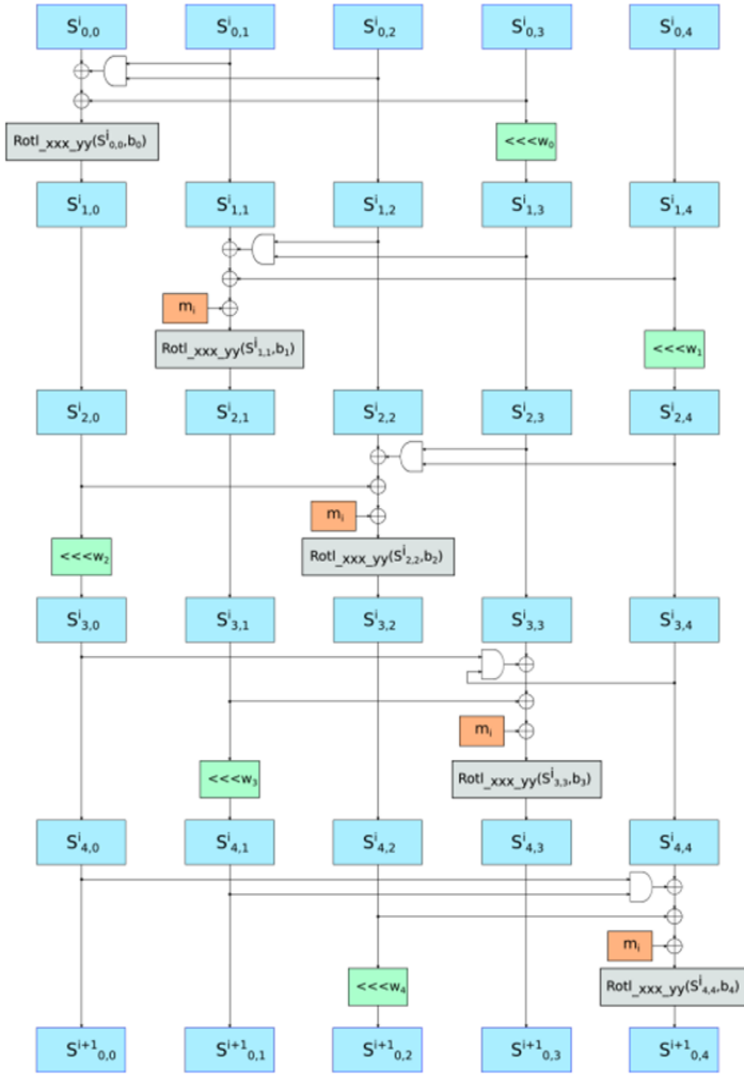
4. Вычисление имитовставки

$$S_{i+1} = StateUpdate(S_i, M_i), \quad i = 1, \ldots, c_{Final};$$
$$T = TagGen(S[1], \ldots, S[q])$$

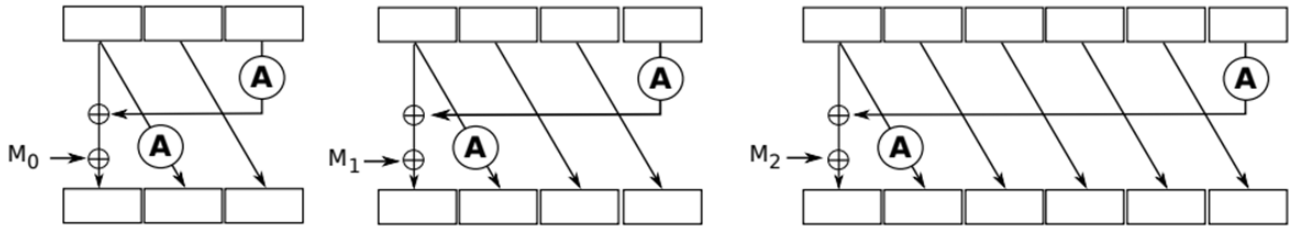
AEGIS



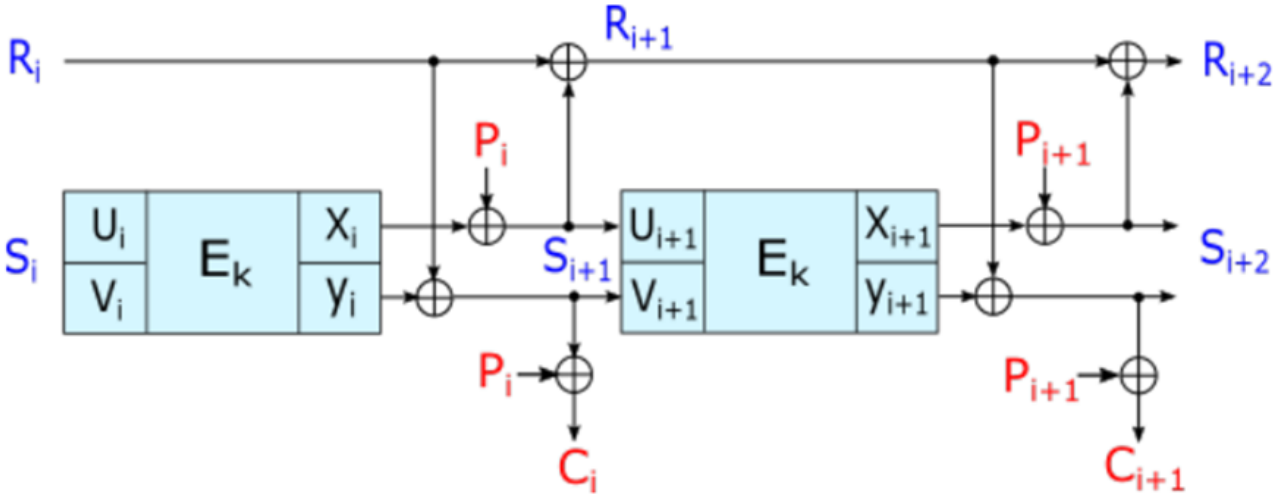
MORUS

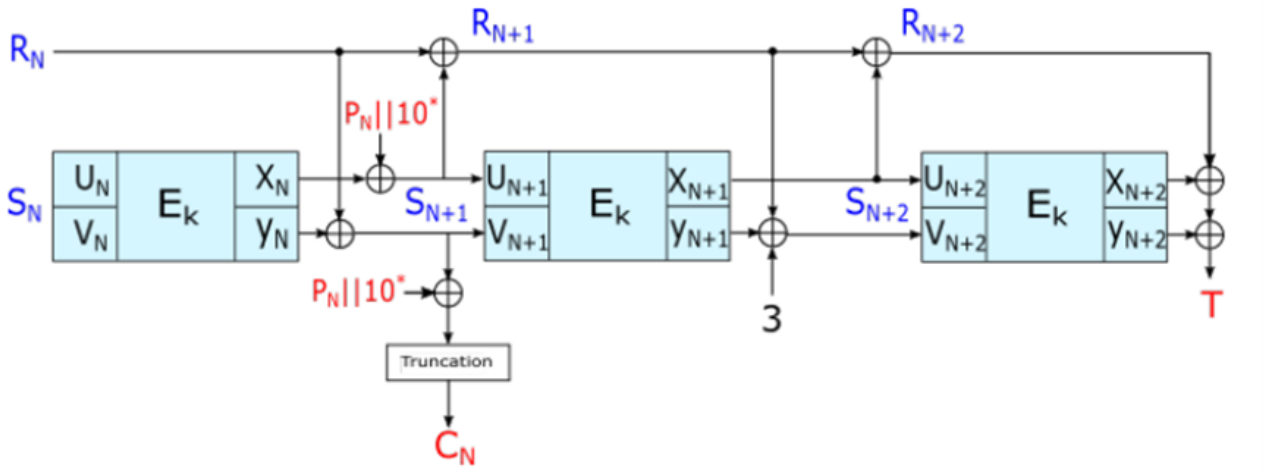

$S^i_{0,0}$
$S^i_{0,1}$
$S^i_{0,2}$
$S^i_{0,3}$
$S^i_{0,4}$
Rotl_xxx_yy($S^i_{0,0}$,b_0)
<<<w_0
$S^i_{1,0}$
$S^i_{1,1}$
$S^i_{1,2}$
$S^i_{1,3}$
$S^i_{1,4}$
m_i
Rotl_xxx_yy($S^i_{1,1}$,b_1)
<<<w_1
$S^i_{2,0}$
$S^i_{2,1}$
$S^i_{2,2}$
$S^i_{2,3}$
$S^i_{2,4}$
m_i
<<<w_2
Rotl_xxx_yy($S^i_{2,2}$,b_2)
$S^i_{3,0}$
$S^i_{3,1}$
$S^i_{3,2}$
$S^i_{3,3}$
$S^i_{3,4}$
m_i
<<<w_3
Rotl_xxx_yy($S^i_{3,3}$,b_3)
$S^i_{4,0}$
$S^i_{4,1}$
$S^i_{4,2}$
$S^i_{4,3}$
$S^i_{4,4}$
m_i
<<<w_4
Rotl_xxx_yy($S^i_{4,4}$,b_4)
$S^{i+1}_{0,0}$
$S^{i+1}_{0,1}$
$S^{i+1}_{0,2}$
$S^{i+1}_{0,3}$
$S^{i+1}_{0,4}$

Tiaoxin



JAMBU


R_i
R_{i+1}
R_{i+2}
P_i
P_{i+1}
S_i
U_i
V_i
E_k
X_i
y_i
S_{i+1}
U_{i+1}
V_{i+1}
E_k
X_{i+1}
y_{i+1}
S_{i+2}
P_i
P_{i+1}
C_i
C_{i+1}


R_N
R_{N+1}
R_{N+2}
$P_N||10^*$
S_N
U_N
V_N
E_k
X_N
y_N
S_{N+1}
U_{N+1}
V_{N+1}
E_k
X_{N+1}
y_{N+1}
S_{N+2}
U_{N+2}
V_{N+2}
E_k
X_{N+2}
y_{N+2}
$P_N||10^*$
3
T
Truncation
C_N

Производительность

Результаты тестирования производительности на ПЛИС (Xilinx Virtex-6) [ATHENa]:

Algorithm	Throughput (Mbps)	Area (LUTs)	Throughput/Area (Mbps/LUT)
MORUS	49,556	3,397	14,5
AEGIS	70,934	3,46	9,3
ACORN	11,304	508	9,1
TIAOXIN	52,796	7,112	7,4
Ketje	24,843	1,238	5,5
NORX	24,519	2,921	5,2
Ascon	5,085	1,27	3,2
AES-OTR	7,708	3,492	1,6
SILC	4,048	3,079	1,3
Keyak	12,6	6,223	1,2
JAMBU-AES	2,008	1,84	1,1
Deoxys	2,882	3,175	0,91
JAMBU-SIMON	939	1,048	0,89
CLOC	2,979	3,143	0,74
OCB	3,109	4,254	0,73
AEZ	3,271	4,73	0,69
COLM	3,109	7,143	0,39

[ATHENa] George Mason University: ATHENa: Automated Tools for Hardware EvaluatioN. (2017)

Победители

1. среды с ограниченными ресурсами
   - ACORN (поточный, )
   - Ascon (поточный, )
2. высокопроизводительные приложения
   - AEGIS (поточный, )
   - MORUS (поточный, )
   - OCB (режим БШ, )
3. допустимо стойкие при нарушении рекомендаций к использованию ("Defense in depth")
   - COLM (режим БШ, )
   - Deoxys-II (режим БШ, )

Спасибо за внимание!

Вопросы?