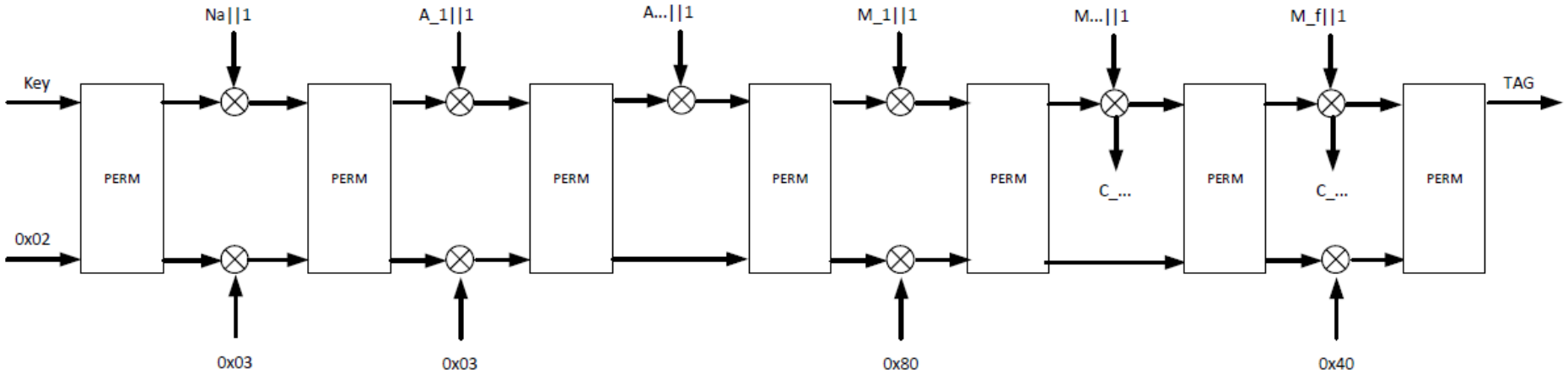
Examples of GMU Designs

Xoodyak
(AEAD+Hash)

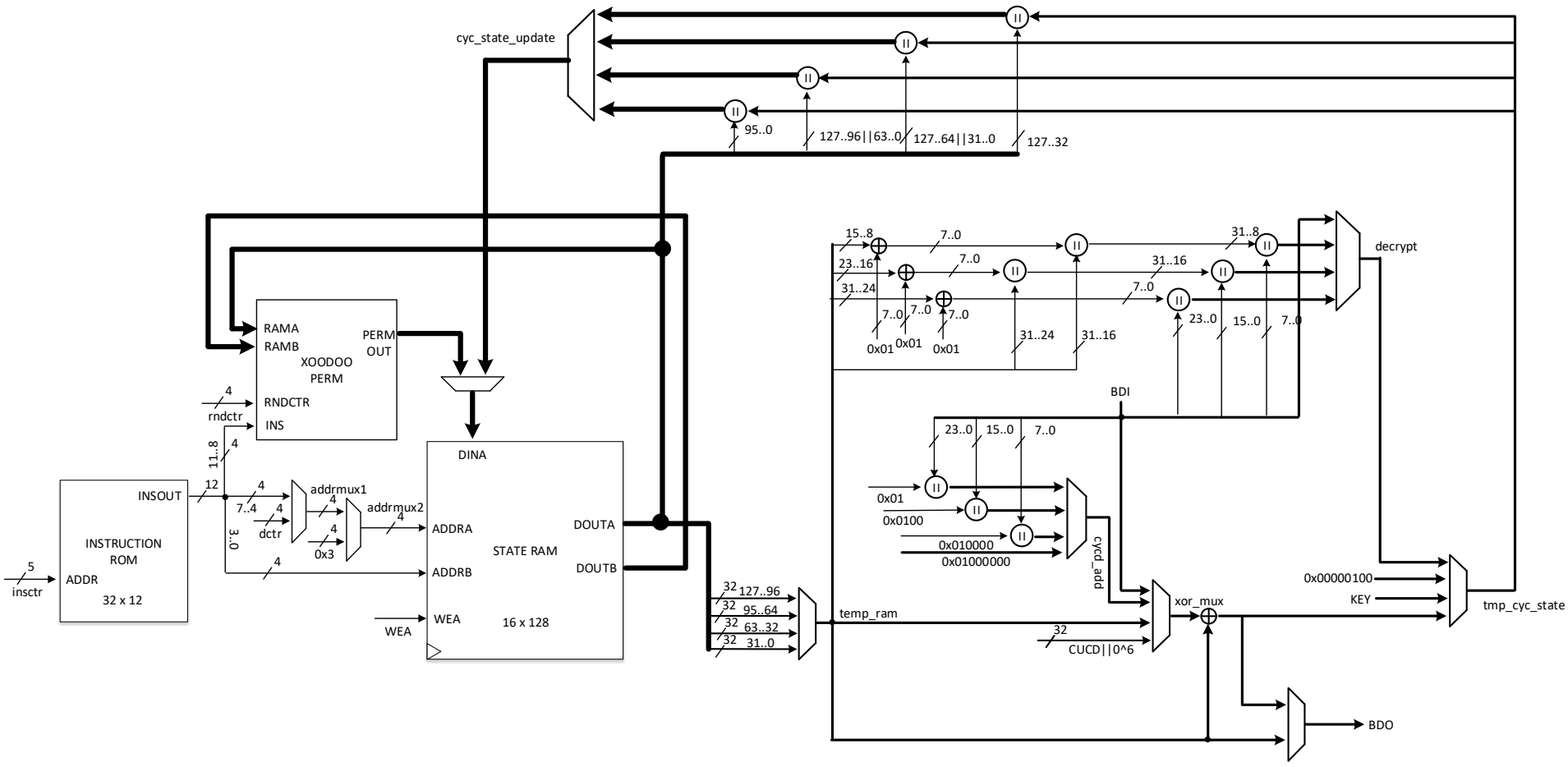
Xoodyak – Basic Features

- Sponge Construction : Cyclist

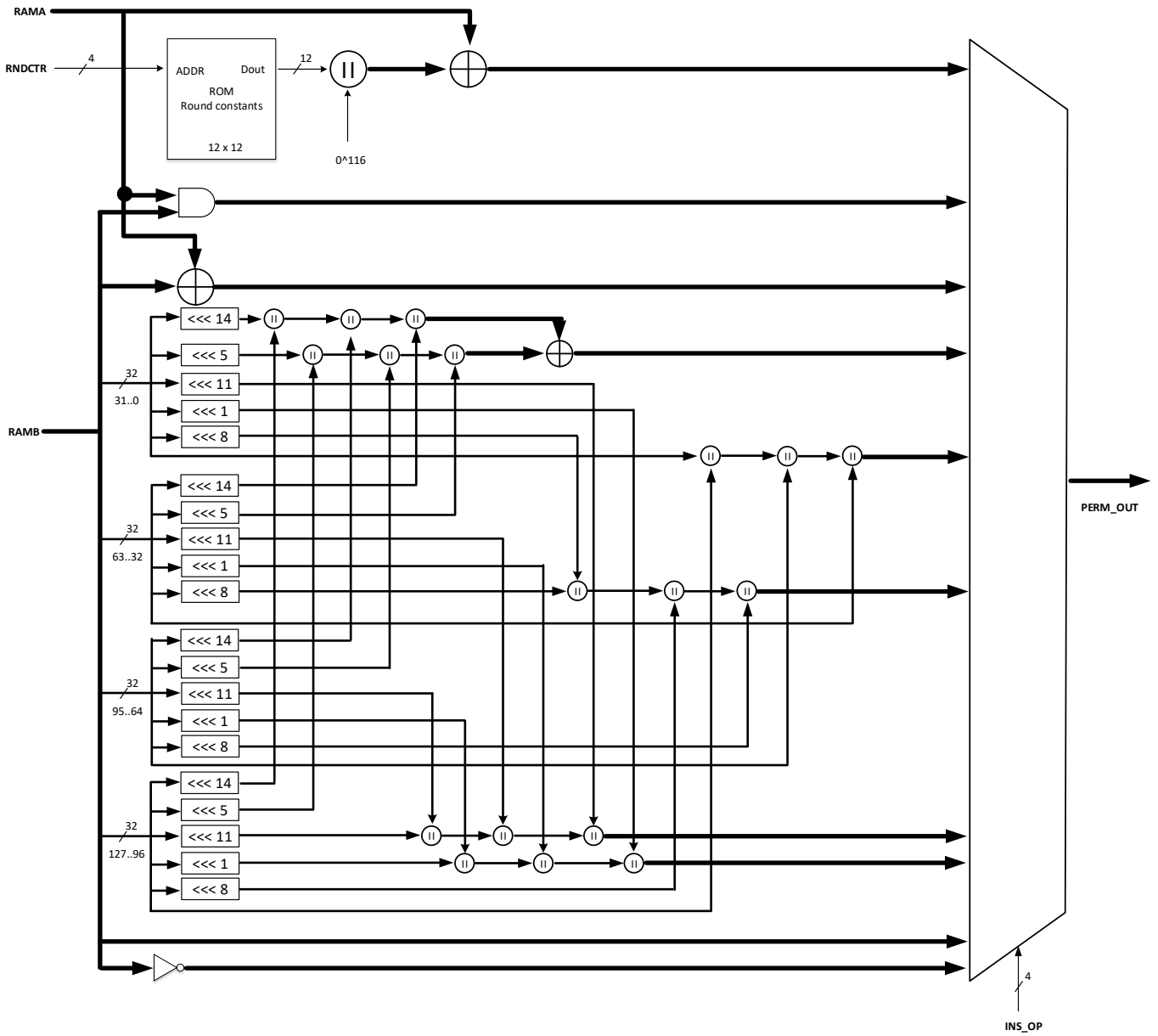


- Permutation Xoodoo
  - State 384 bits
    - Broken into 3 planes
      - Each plane consists of 4 lanes
  - 12 Rounds
  - Operations: cyclist shift, complement, product, and bitwise xor

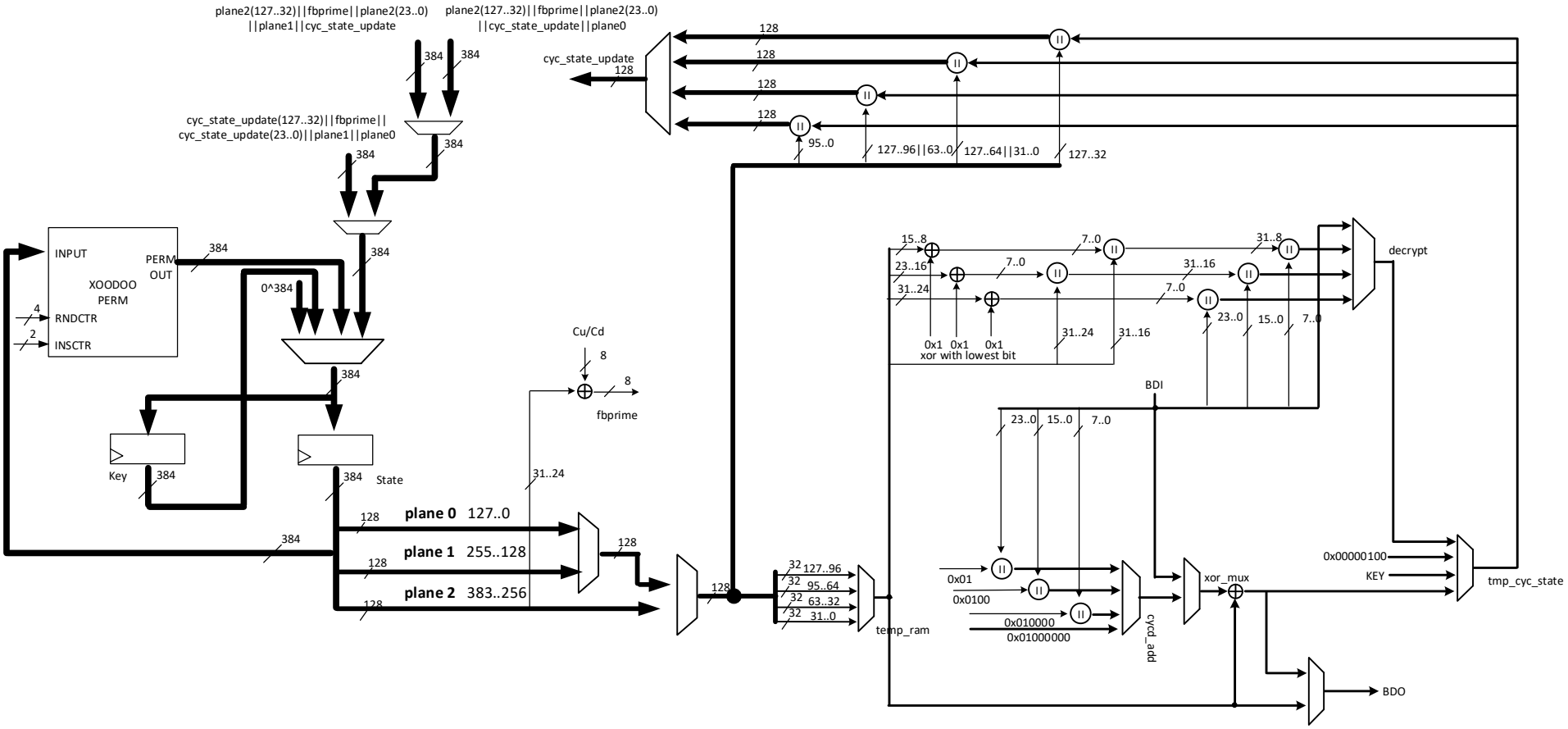
Xoodyak-128 – Block Diagram : Top Level



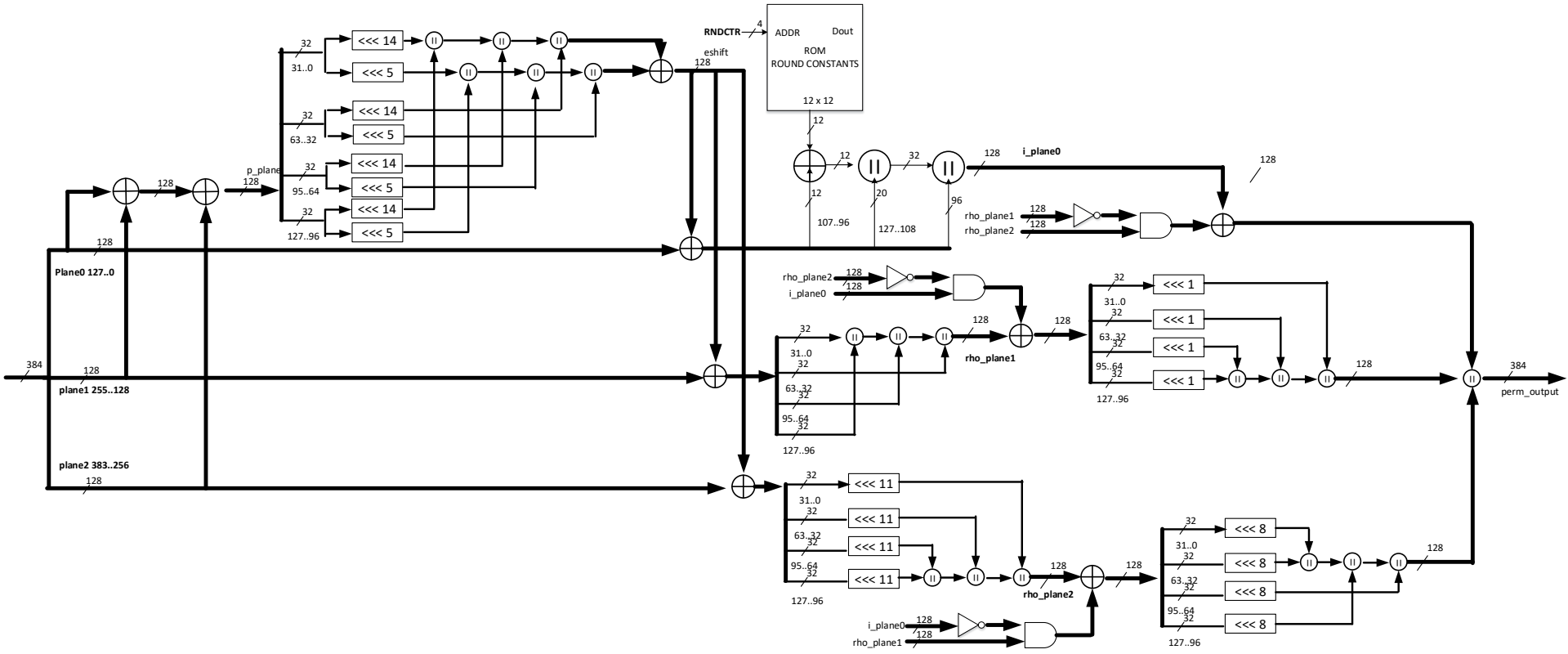
Xoodyak-128 – Block Diagram : Xoodoo Permutation



Xoodyak-384 – Block Diagram : Top Level



Xoodyak-384 – Block Diagram : Xoodoo Permutation



Xoodyak-128 – Timing Analysis

	AD	Plaintext & Ciphertext	Hash Message	Tag
#Bits/Block	352	192	128	128
#Words/Block	11	6	4	4
#Cycles/Block	266	261	259	

Key setup time: 269
Execution time of authenticated encryption: 262+(266·Na)+(261·Nm)+4
Execution time of authenticated decryption: 262+(266·Na)+(261·Nc)+4
Execution time for hashing: 12+(259·Nh)+4

Authentication Throughput for large Na = 352/(266·T) = 1.3233·f
Encryption Throughput for large Nm = 192/(261·T) = 0.7356·f
Decryption Throughput for large Nc = 192/(261·T) = 0.7356·f
Hashing Throughput for large Nh = 128/(259·T) = 0.4942·f

T – clock period in μs, f – clock frequency in MHz, All Throughputs in Mbits/s

Xoodyak-384 – Timing Analysis

	AD	Plaintext & Ciphertext	Hash Message	Tag
#Bits/Block	352	192	128	128
#Words/Block	11	6	4	4
#Cycles/Block	24	19	17	

Key setup time: 17
Execution time of authenticated encryption: 18+(24·Na)+(19·Nm)+4
Execution time of authenticated decryption: 18+(24·Na)+(19·Nc)+4
Execution time for hashing: 1+(17·Nh)+4

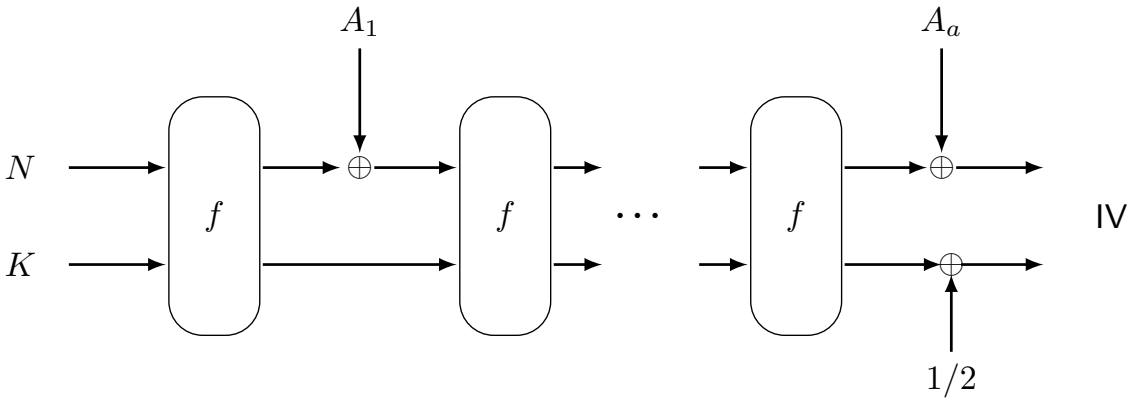
Authentication Throughput for large Na = 352/(24·T) = 14.6667·f
Encryption Throughput for large Nm = 192/(19·T) = 10.1053·f
Decryption Throughput for large Nc = 192/(19·T) = 10.1053·f
Hashing Throughput for large Nh = 128/(17·T) = 7.5294·f

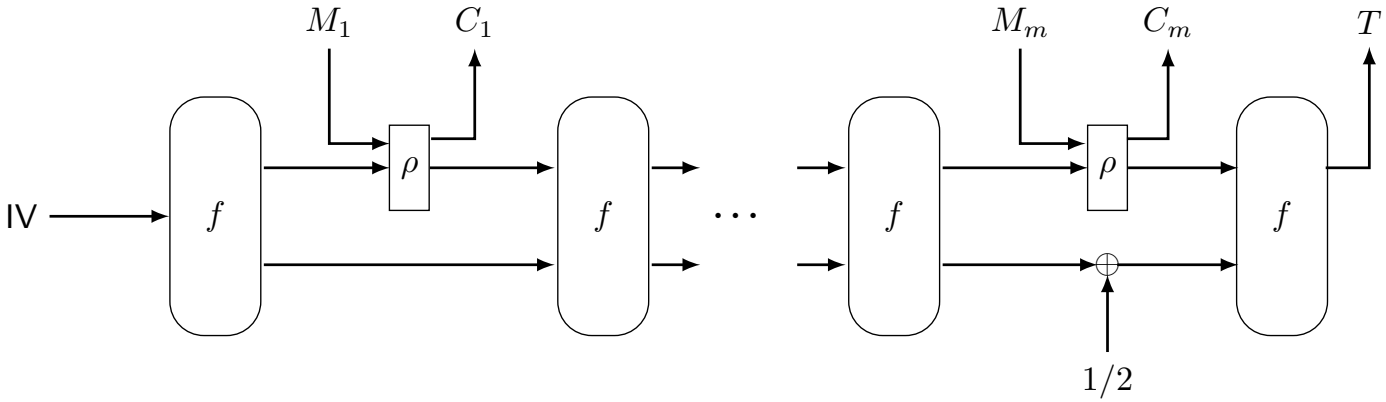
T – clock period in μs, f – clock frequency in MHz, All Throughputs in Mbits/s

PHOTON-Beetle
(AEAD+Hash)

PHOTON-Beetle – Basic Features

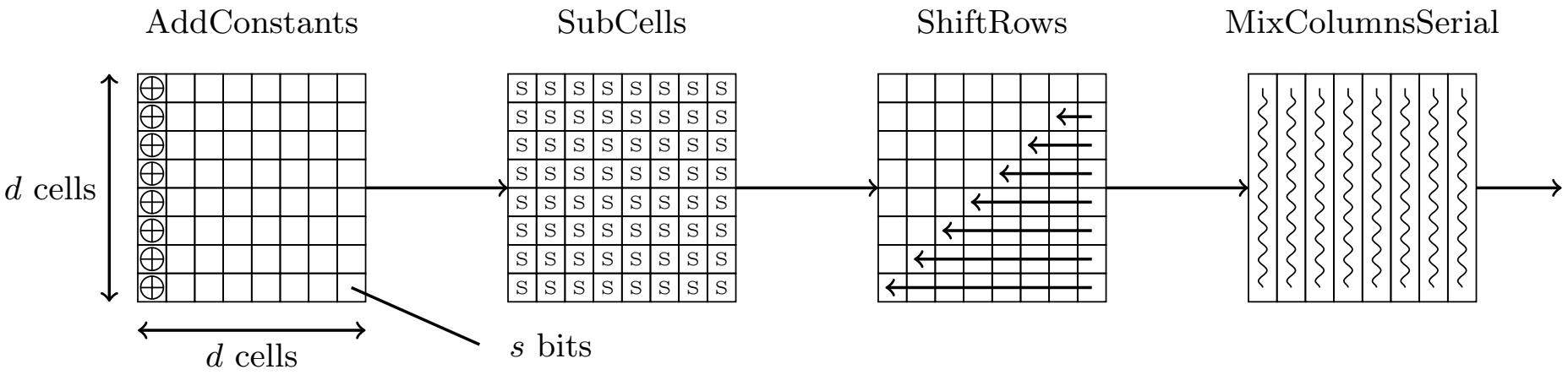
- Sponge Construction





PHOTON-Beetle – Basic Features

- One round of a PHOTON permutation



x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S-box	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

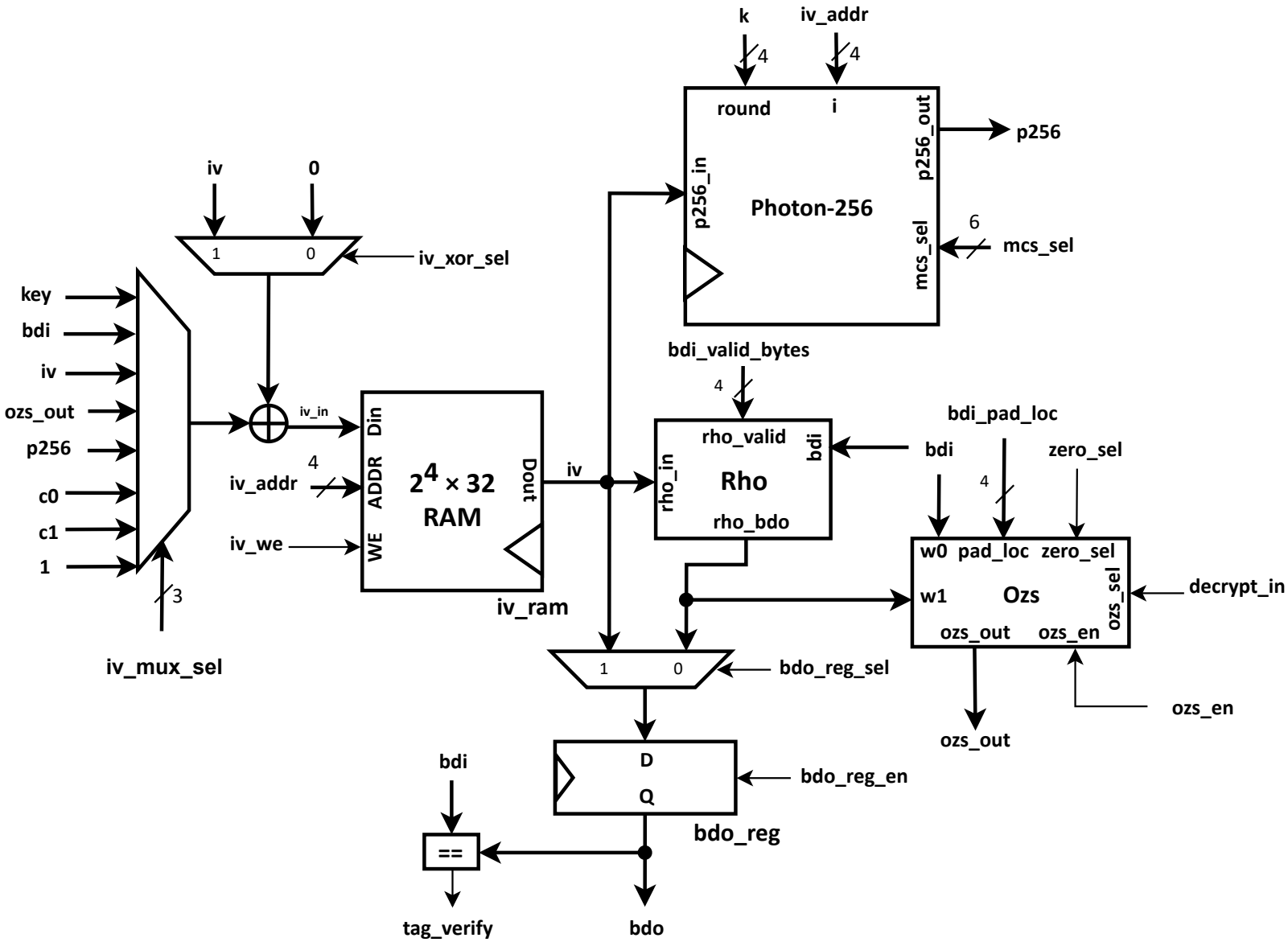
MixColumnSerial(X)

1 : $M \leftarrow \mathsf{Serial}[2, 4, 2, 11, 2, 8, 5, 6]$;

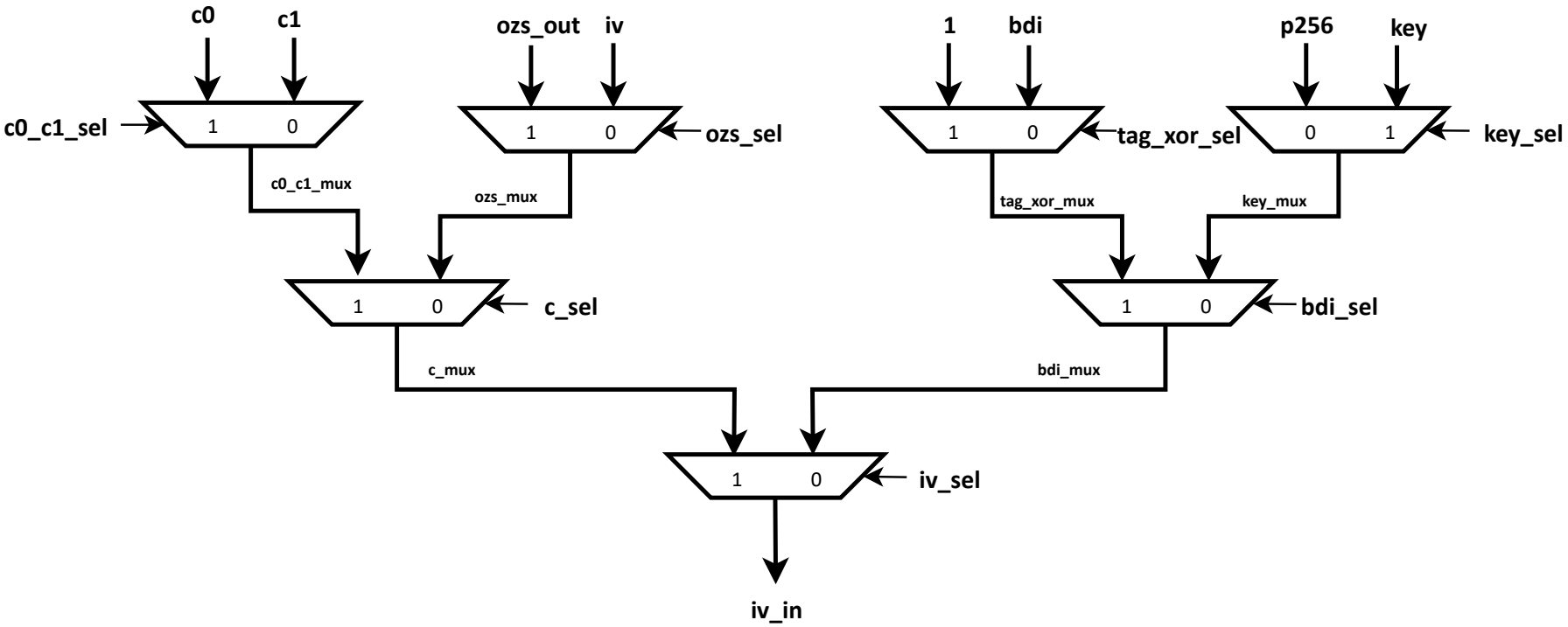
2 : $X \leftarrow M^8 \odot X$;

return X;

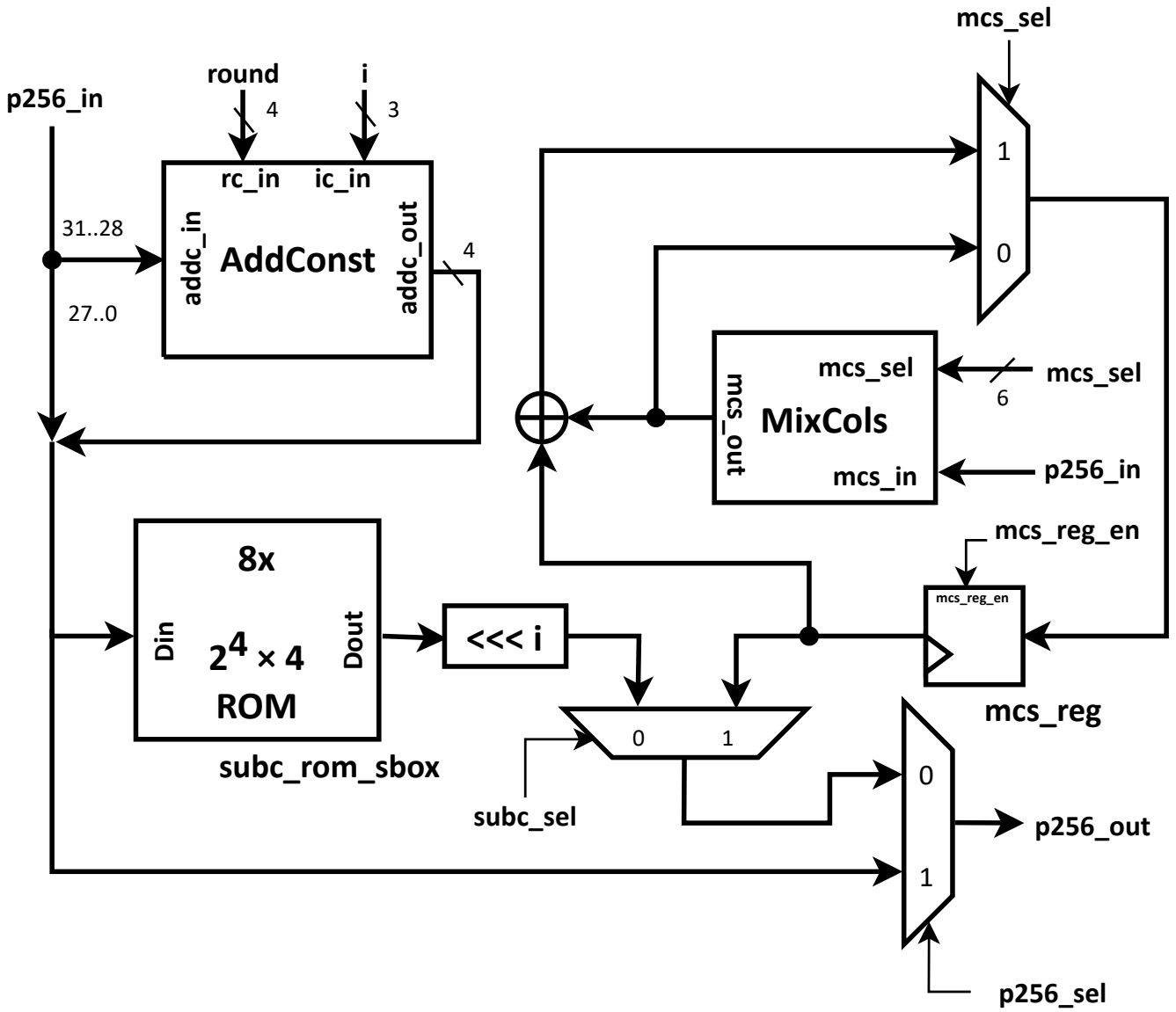
PHOTON-Beetle – Block Diagram : Top Level



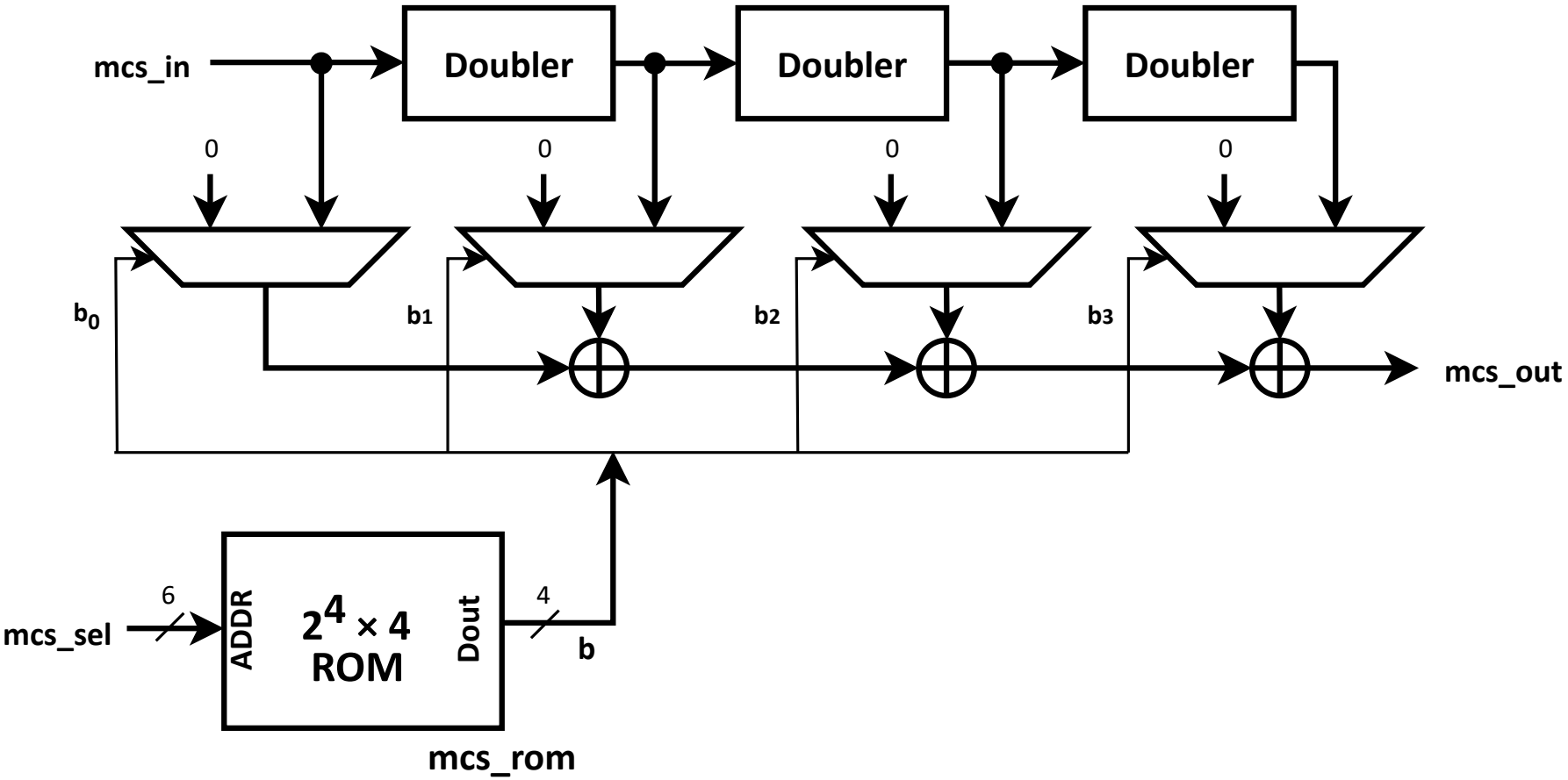
PHOTON-Beetle – Block Diagram : Datapath Mux



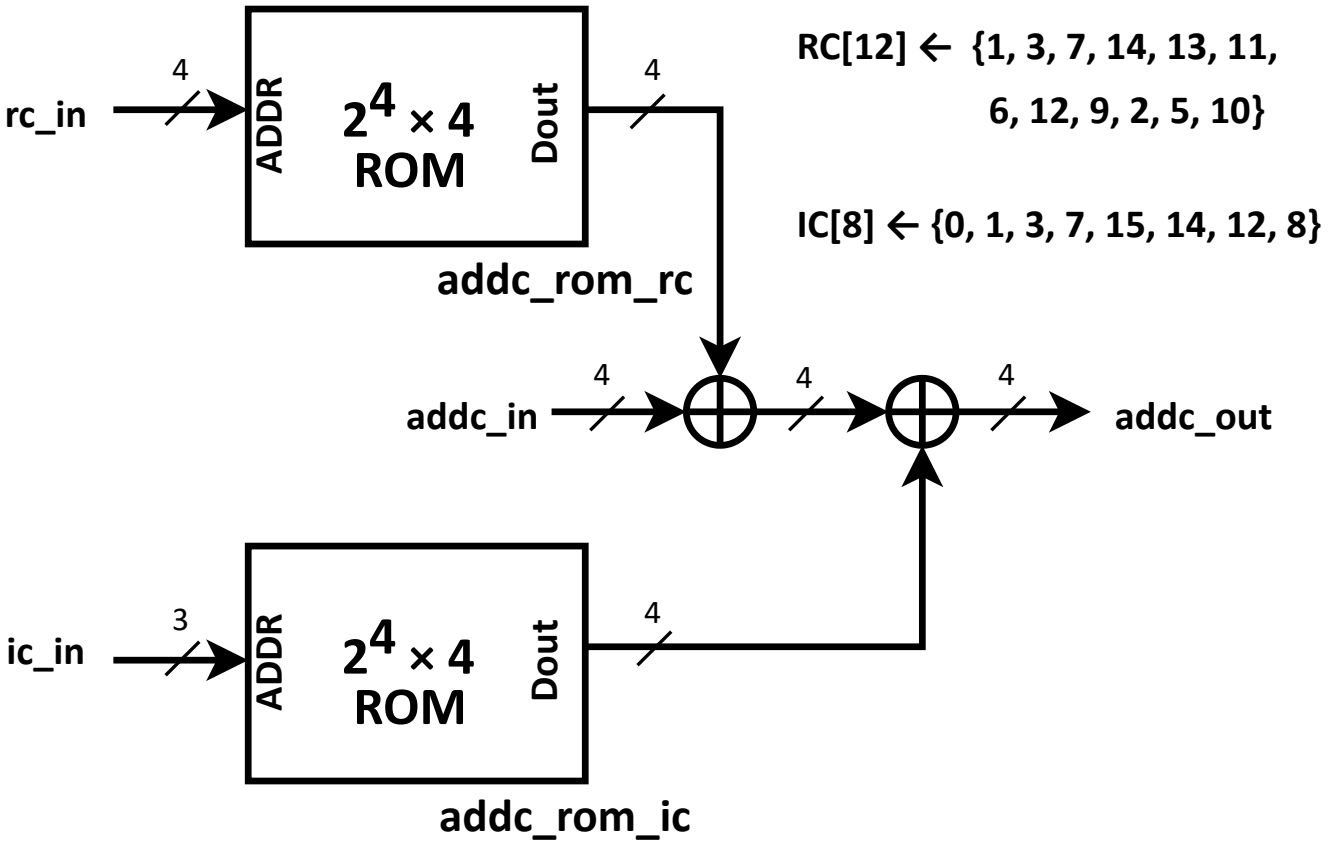
PHOTON-Beetle – Block Diagram : Photon-256



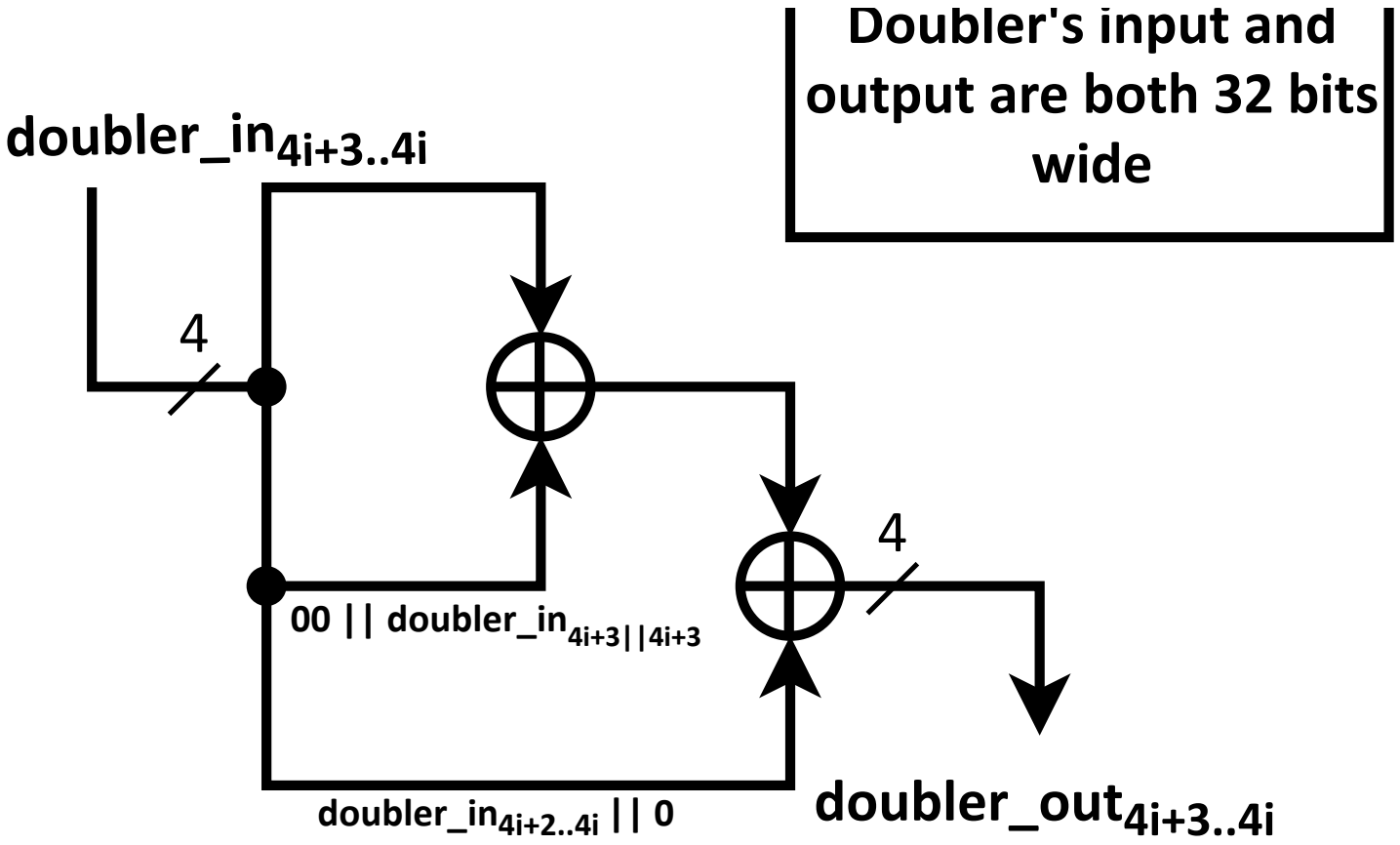
PHOTON-Beetle – Block Diagram : MixCols



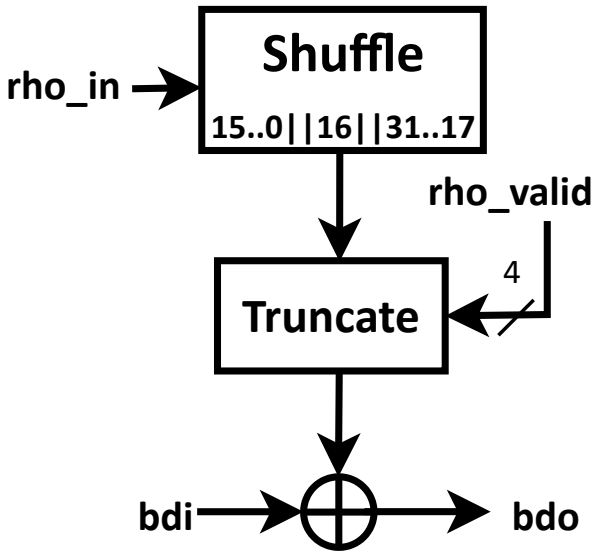
PHOTON-Beetle – Block Diagram : AddConst

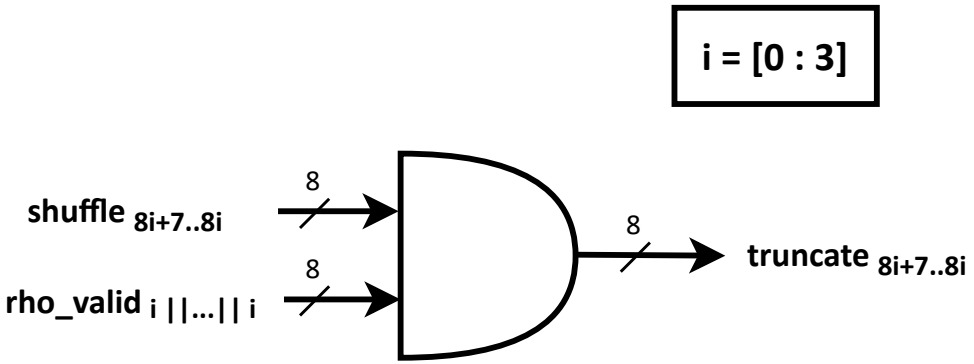


PHOTON-Beetle – Block Diagram : Doubler

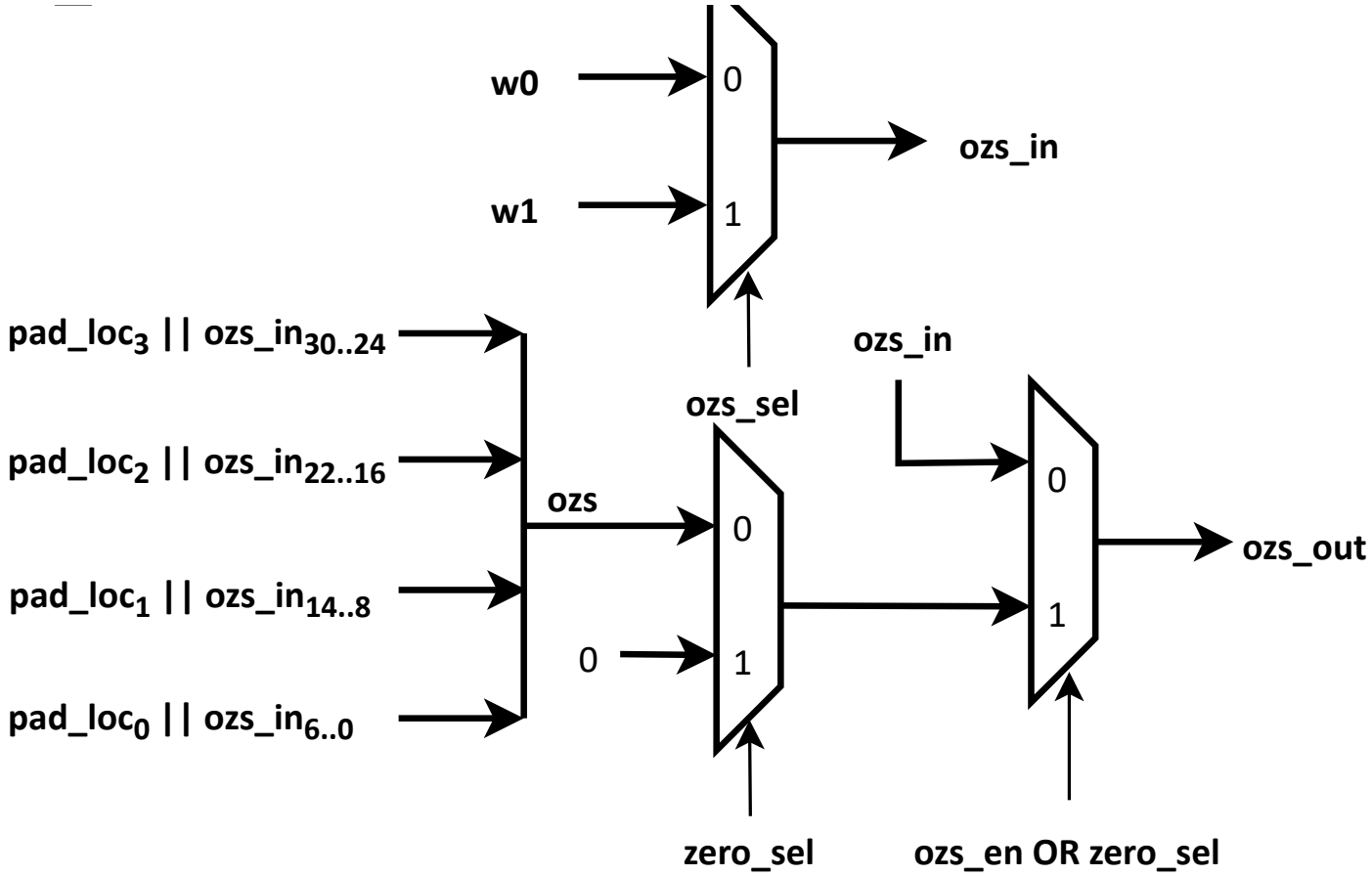


PHOTON-Beetle – Block Diagram : Rho





PHOTON-Beetle – Block Diagram : Ozs



PHOTON-Beetle – Timing Analysis

	AD	Plaintext & Ciphertext	Hash Message	Tag
#Bits/Block	32	32	32	128
#Words/Block	1	1	1	4
#Cycles/Block	28	28	28	

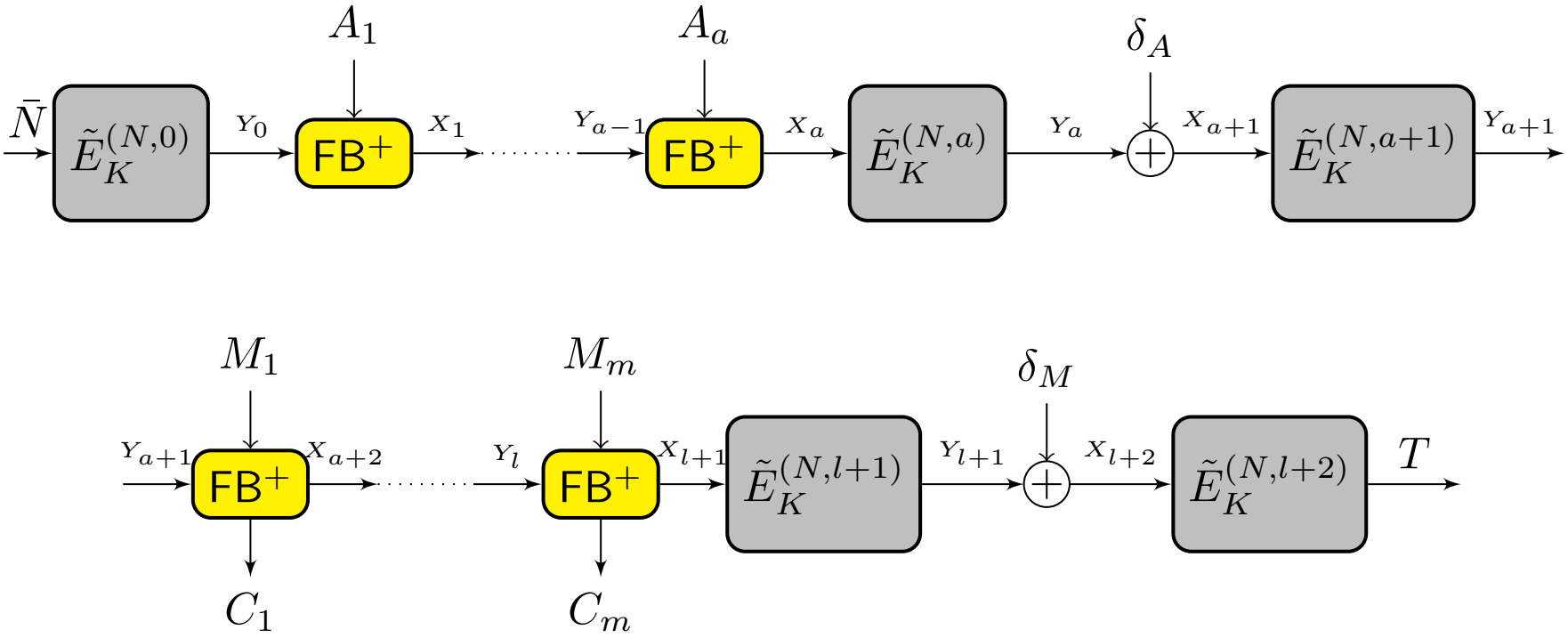
Key setup time: 12
Execution time of authenticated encryption: 12+(28·Na)+(28·Nm)+34
Execution time of authenticated decryption: 12+(28·Na)+(28·Nc)+40
Execution time for hashing: 14+(28·Nh)+57

Authentication Throughput for large Na = 32/(28·T) = 1.1429·f
Encryption Throughput for large Nm = 32/(28·T) = 1.1429·f
Decryption Throughput for large Nc = 32/(28·T) = 1.1429·f
Hashing Throughput for large Nh = 32/(28·T) = 1.1429·f

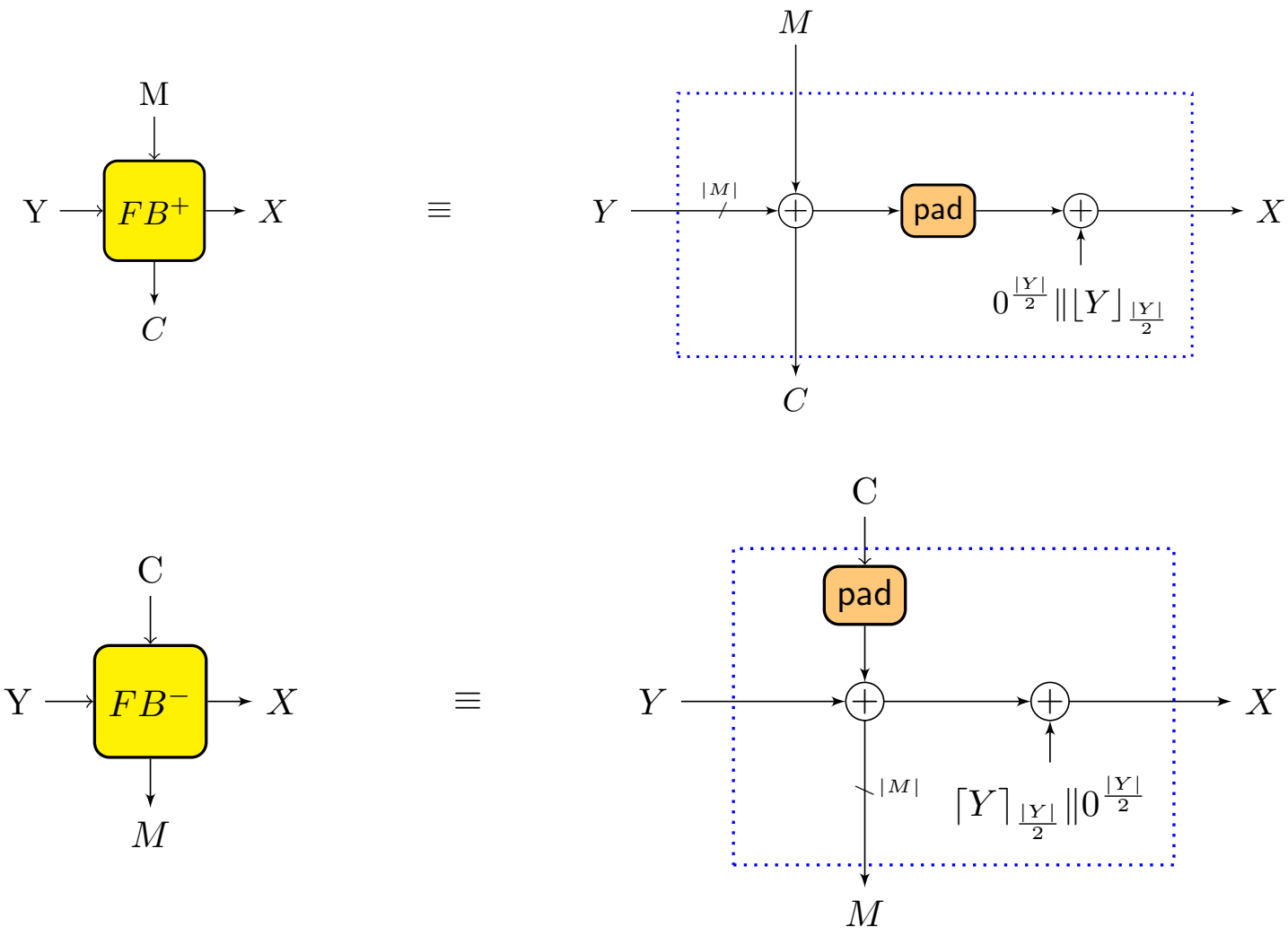
T – clock period in μs, f – clock frequency in MHz, All Throughputs in Mbits/s

mixFeed
(AEAD)

mixFeed – Basic Features



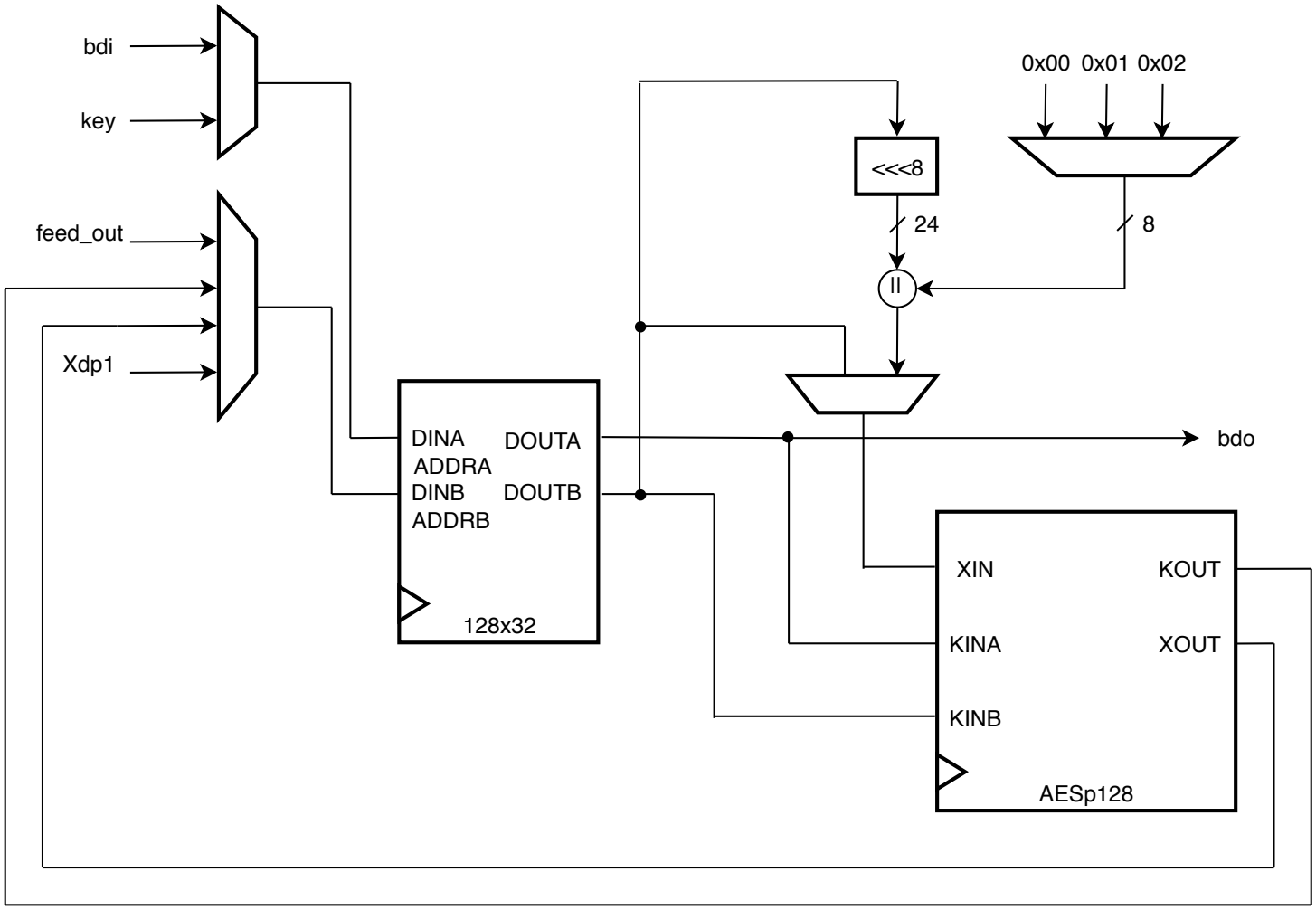
mixFeed – Basic Features



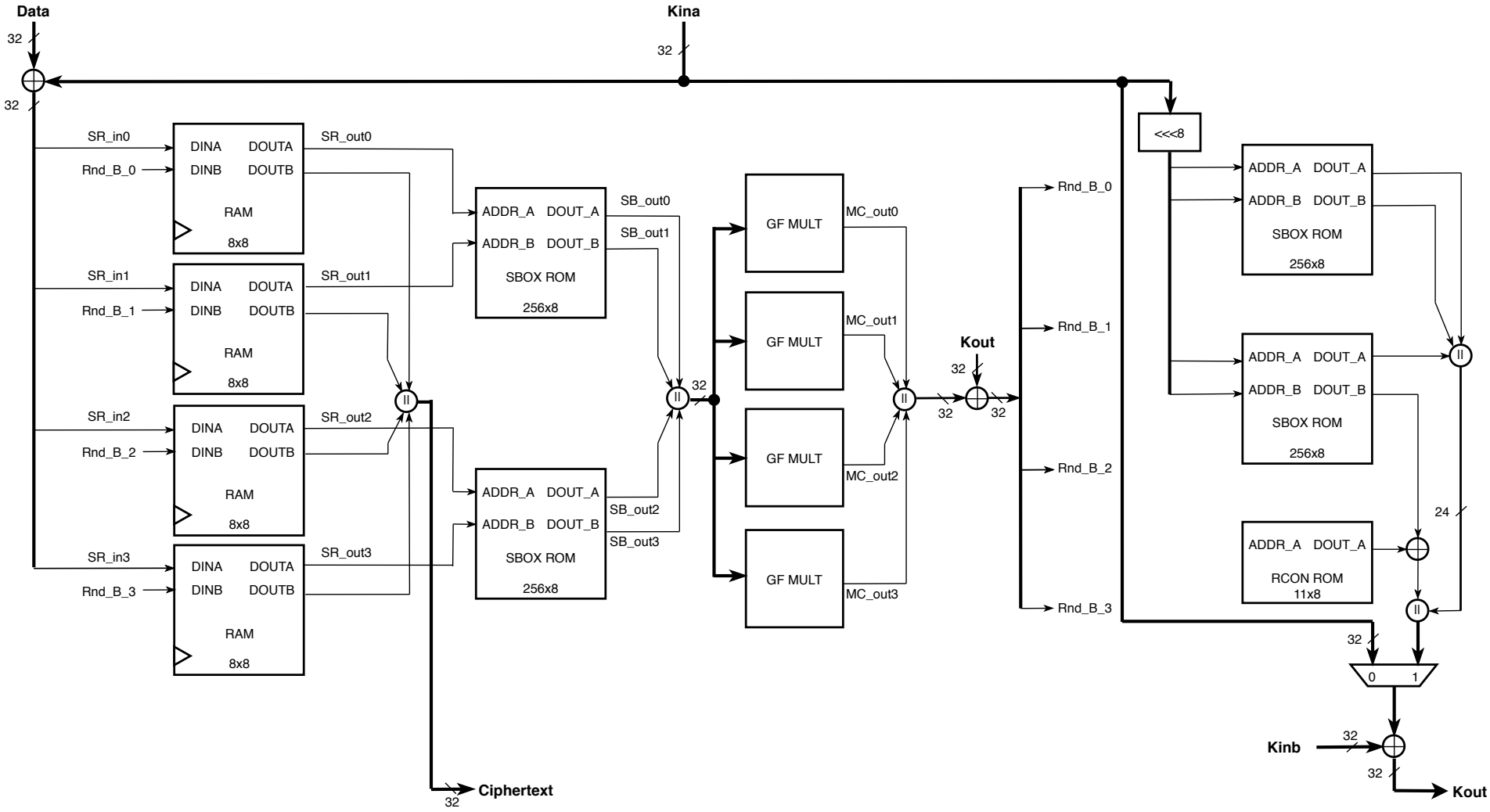
mixFeed – Basic Features

- Nonce dependent key – key is initialized using AES and Nonce
- Minimally XORED mixture feedback – use minimum XORs to process each block
- Inverse free – AES Encrypt permutation is used for mixFeed Encrypt and Decrypt operations
- AES'128 is recommended block cipher. AES'128 differs from AES128 by adding mixcolumns to the final encryption round. Design rationale is to simplify AES controller implementation
- Key updated internally AES Key Gen (11th round KeyGen is next Key)

mixFeed – Block Diagram : Top Level



mixFeed – Block Diagram : AESp128



mixFeed – Timing Analysis

	AD	Plaintext & Ciphertext	Tag
#Bits/Block	128	128	128
#Words/Block	4	4	4
#Cycles/Block	62	62	

Key setup time: 4

Execution time of authenticated encryption: $128+(62 \cdot Na)+(62 \cdot Nm)+4$

Execution time of authenticated decryption: $128+(62 \cdot Na)+(62 \cdot Nc)+8$

Authentication Throughput for large Na = $128/(62 \cdot T) = 2.6129 \cdot f$

Encryption Throughput for large Nm = $128/(62 \cdot T) = 2.6129 \cdot f$

Decryption Throughput for large Nc = $128/(62 \cdot T) = 2.6129 \cdot f$

T – clock period in μs, f – clock frequency in MHz, All Throughputs in Mbits/s

Pyjamask
(AEAD)

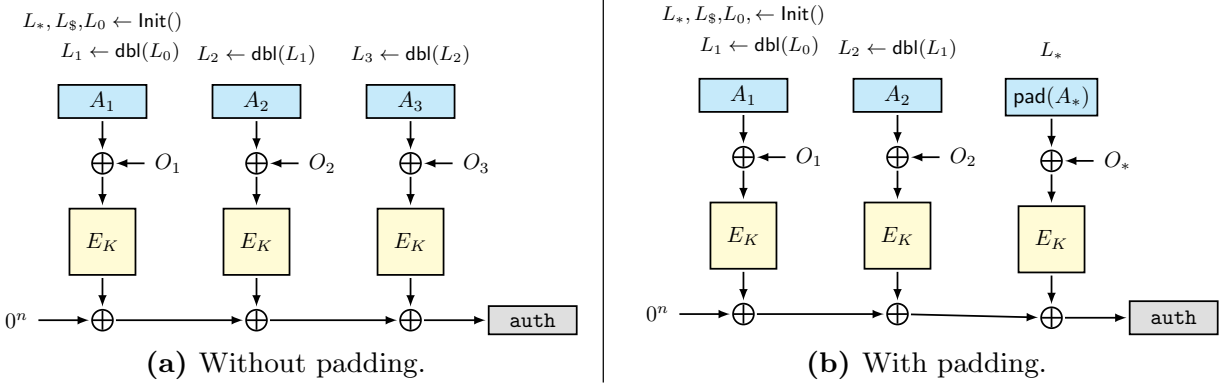
Pyjamask – Basic Features

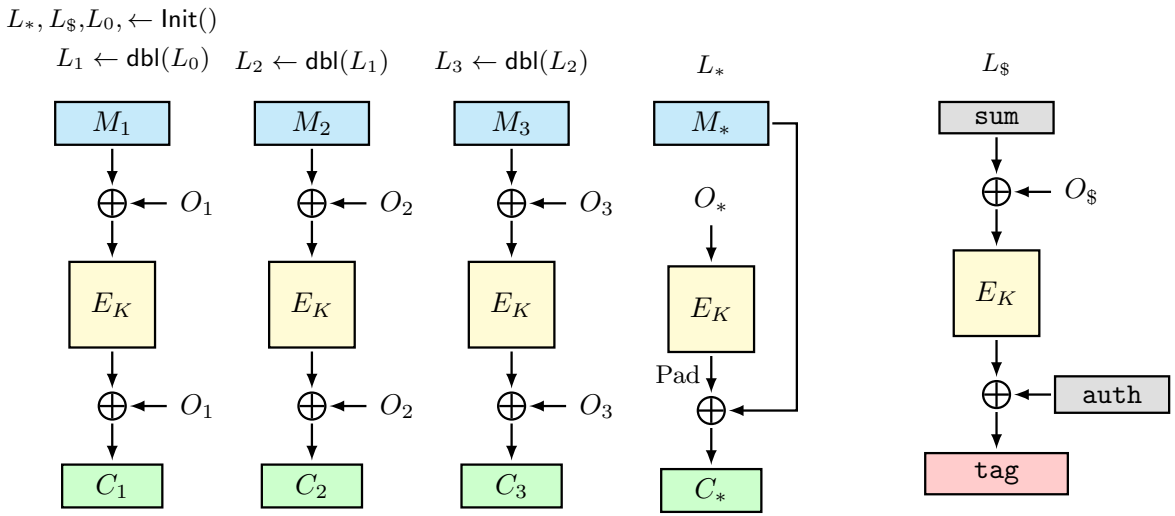
- Targets side-channel attack resistance as a main goal
- Smallest number of AND gates per bit
- Two variants – Pyjamask96 and Pyjamask128

Instance	State size n	Rows r	Columns n/r	Key size k	Rounds
`Pyjamask-96`	96	3	32	128	14
`Pyjamask-128`	128	4	32	128	14

Pyjamask – Basic Features

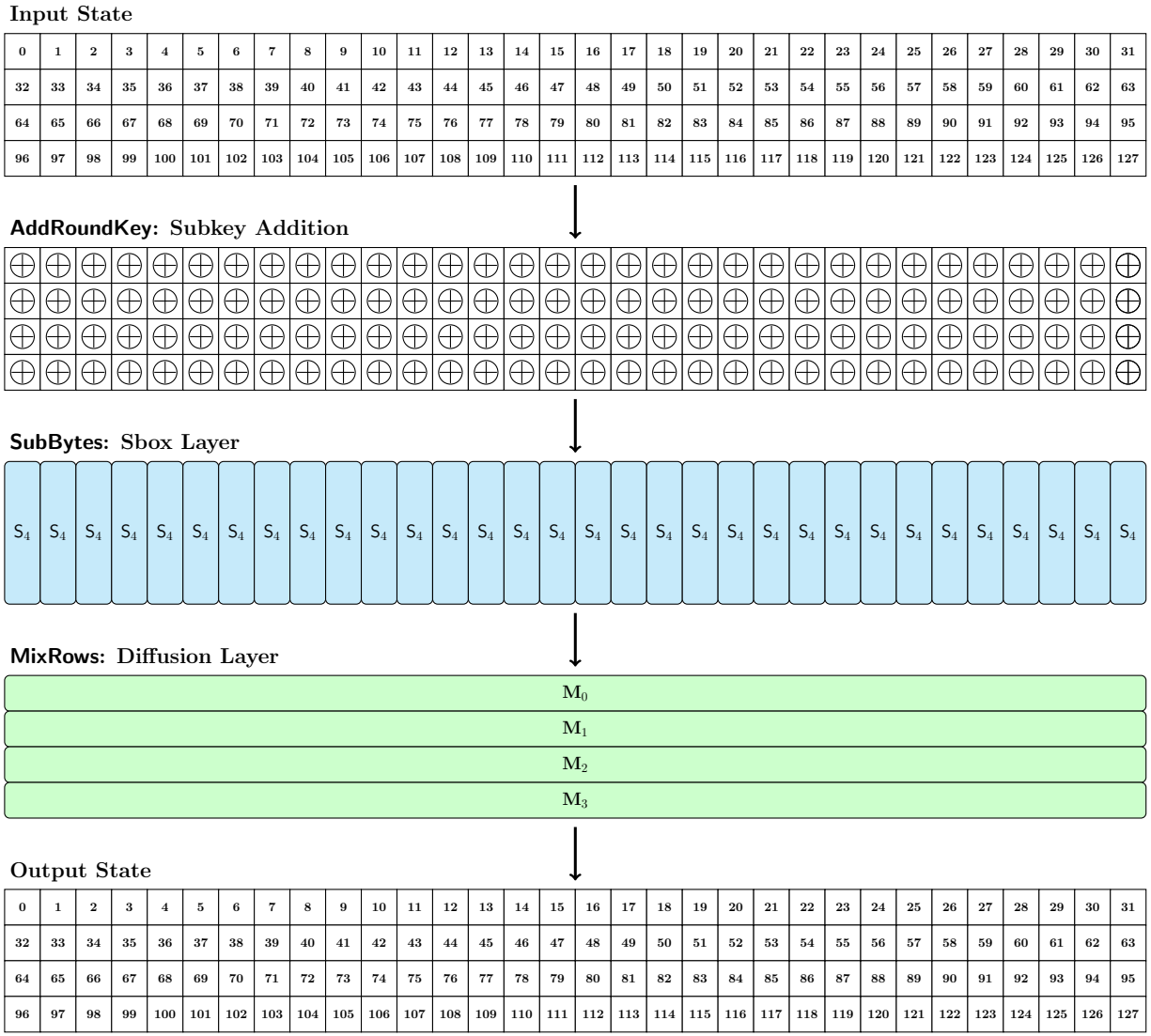
- OCB mode





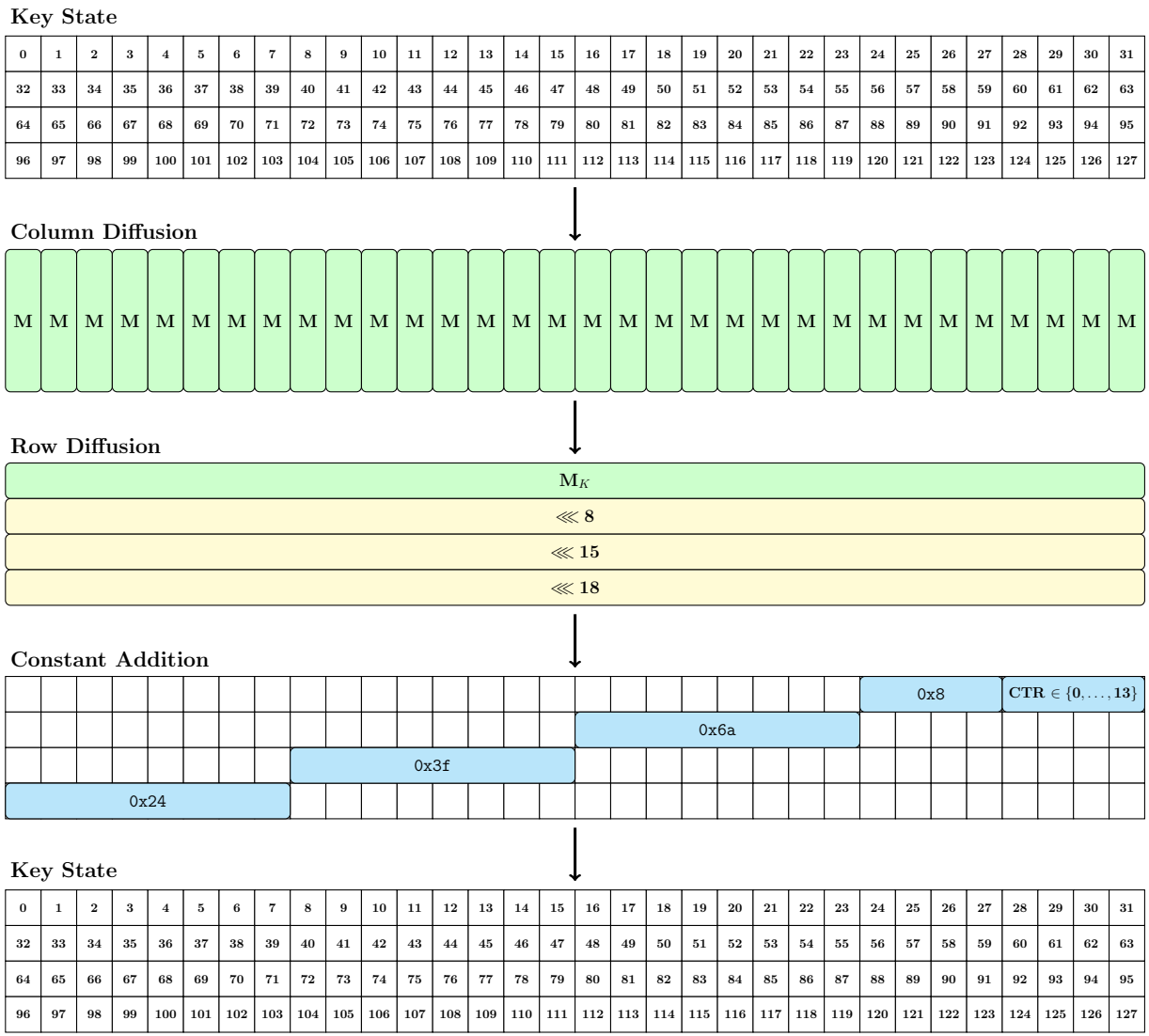
Pyjamask – Basic Features

Round function of Pyjamask-128

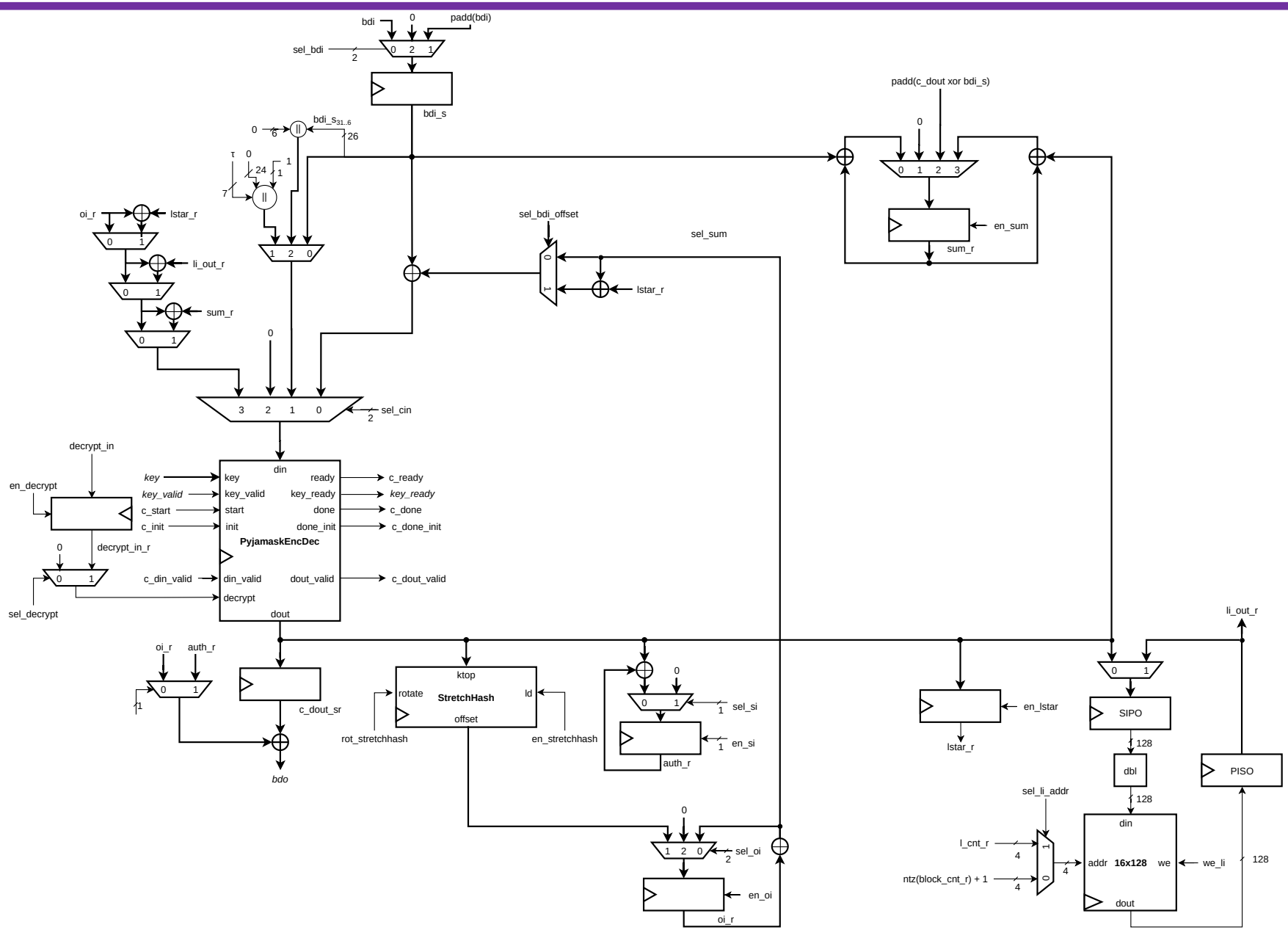


Pyjamask – Basic Features

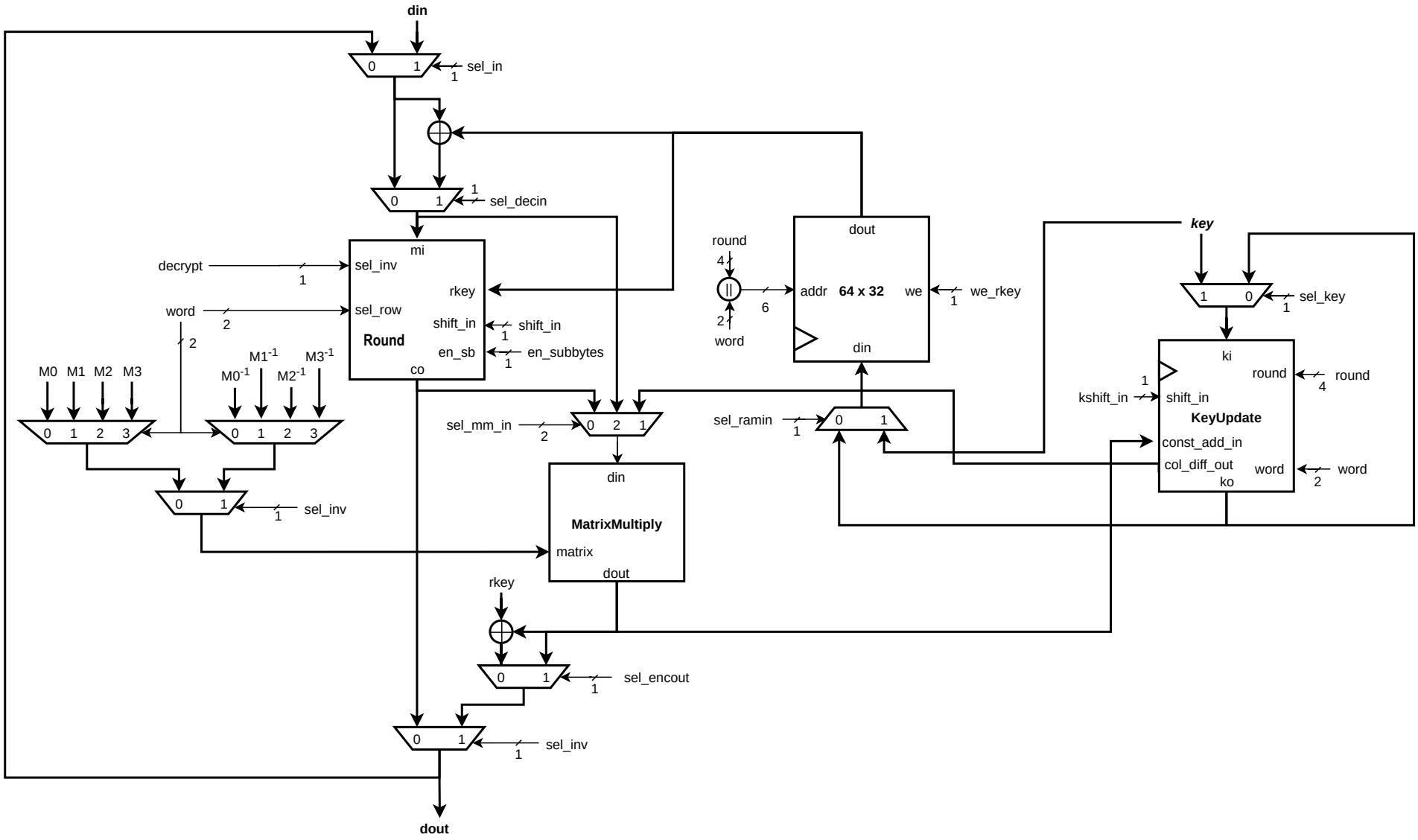
- Key schedule of Pyjamask-96 and Pyjamask-128



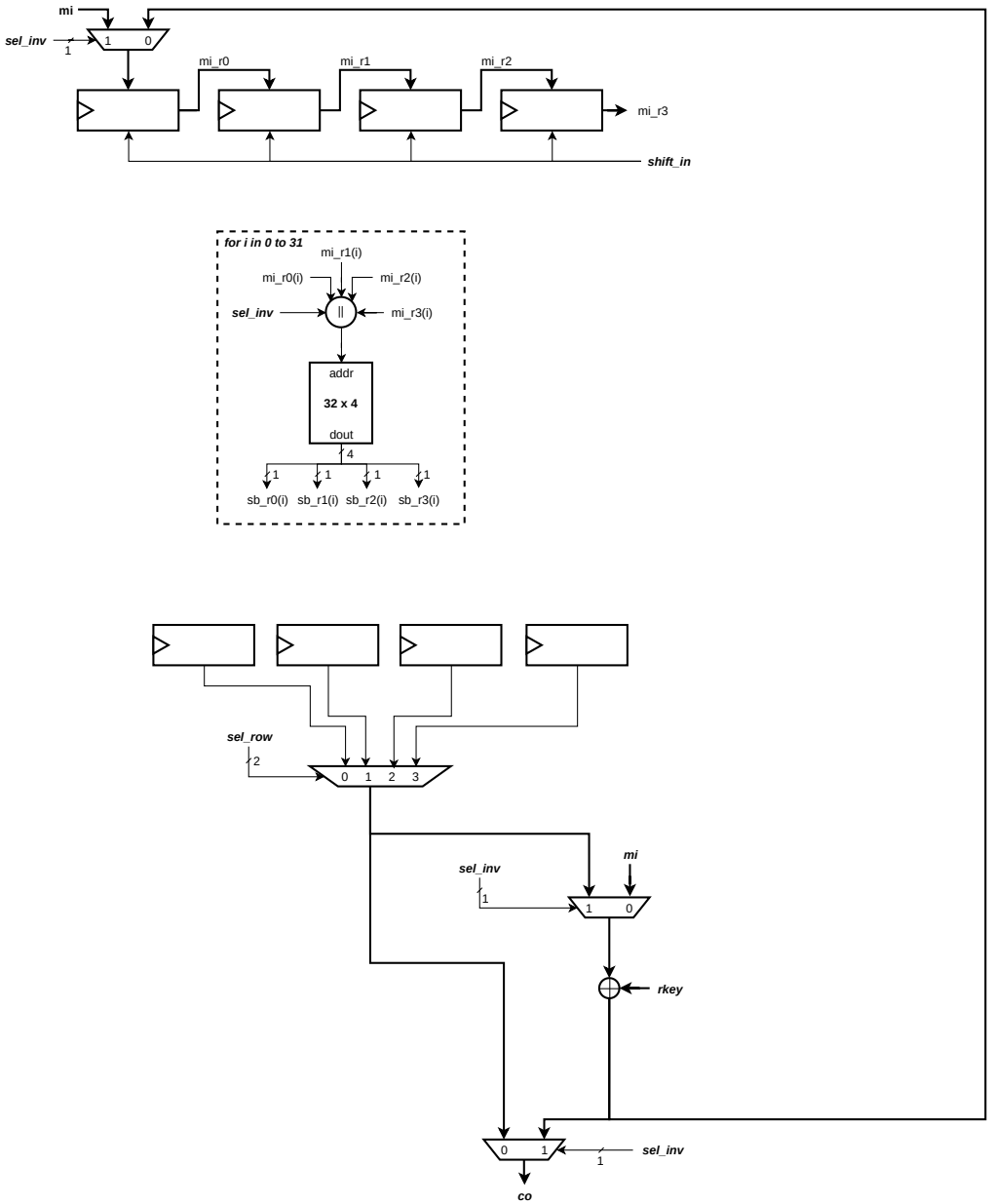
Pyjamask – Block Diagram : Top Level



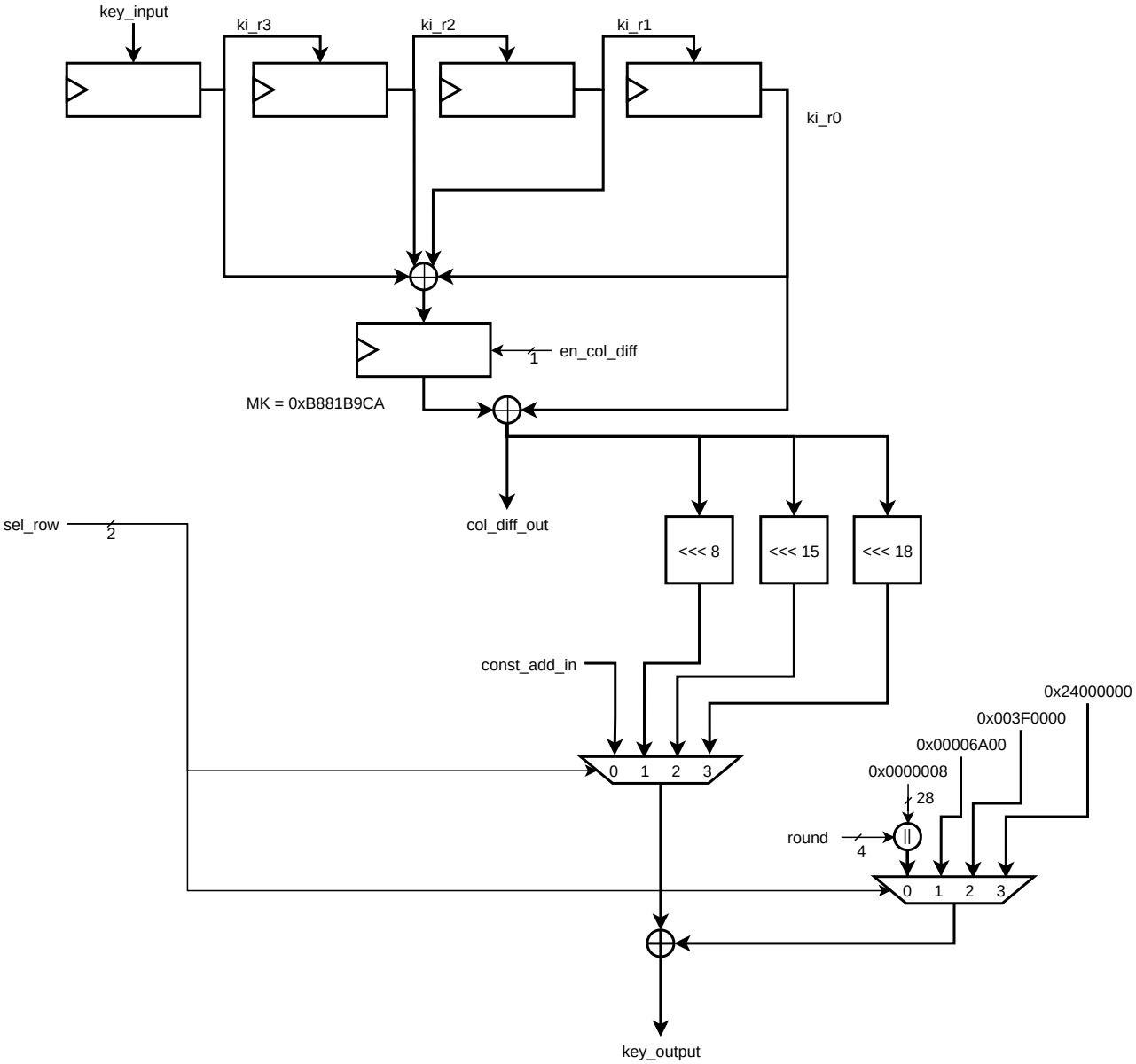
Pyjamask – Block Diagram : PyjamaskEncDec



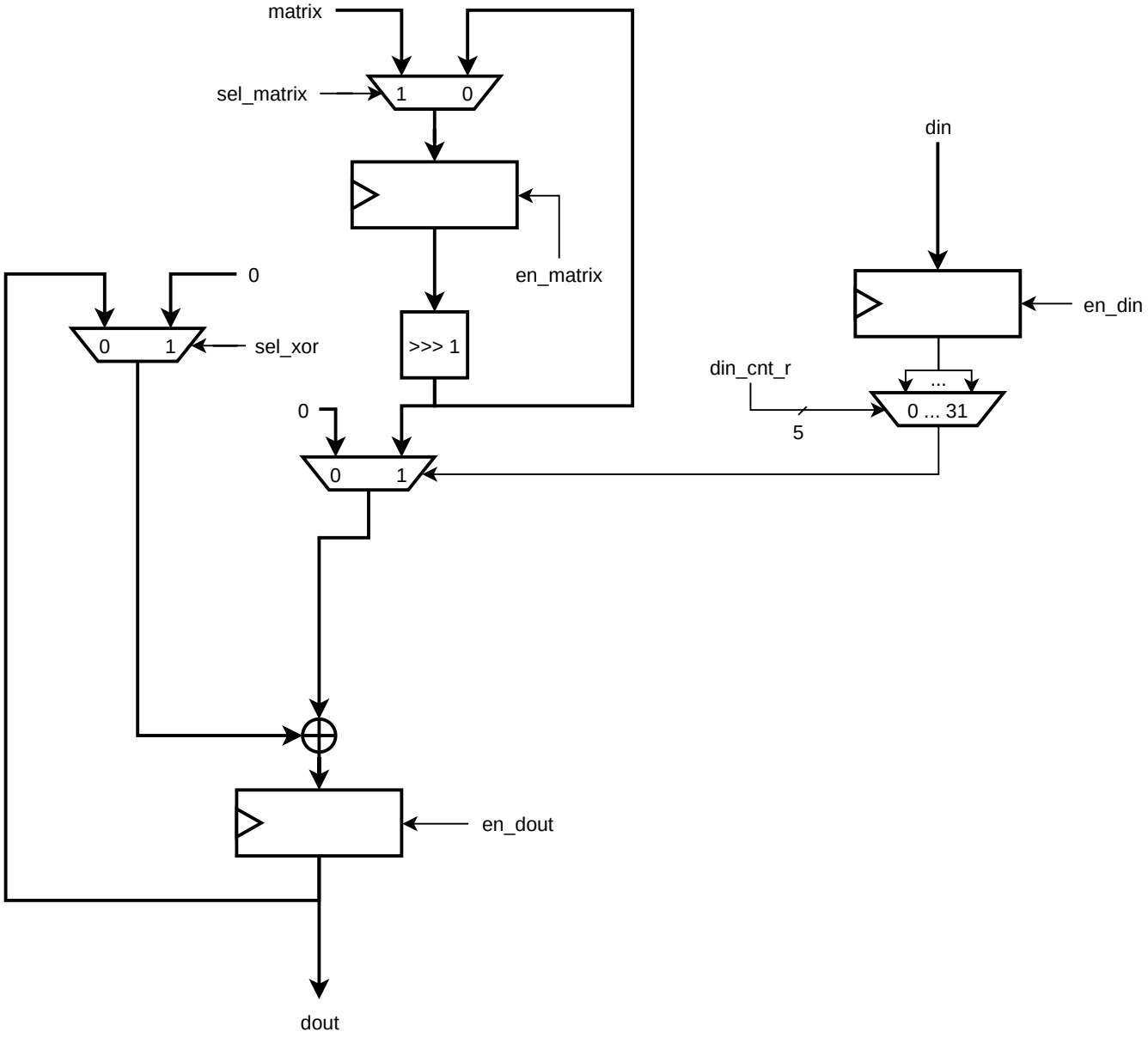
Pyjamask – Block Diagram : Round



Pyjamask – Block Diagram : KeyUpdate



Pyjamask – Block Diagram : MatrixMultiply



Pyjamask – Timing Analysis

	AD	Plaintext & Ciphertext	Tag
#Bits/Block	128	128	128
#Words/Block	4	4	4
#Cycles/Block	87	87	

Key setup time: ?
Execution time of authenticated encryption: $310+(87 \cdot Na)+(87 \cdot Nm)+79$
Execution time of authenticated decryption: $310+(87 \cdot Na)+(87 \cdot Nc)+79$

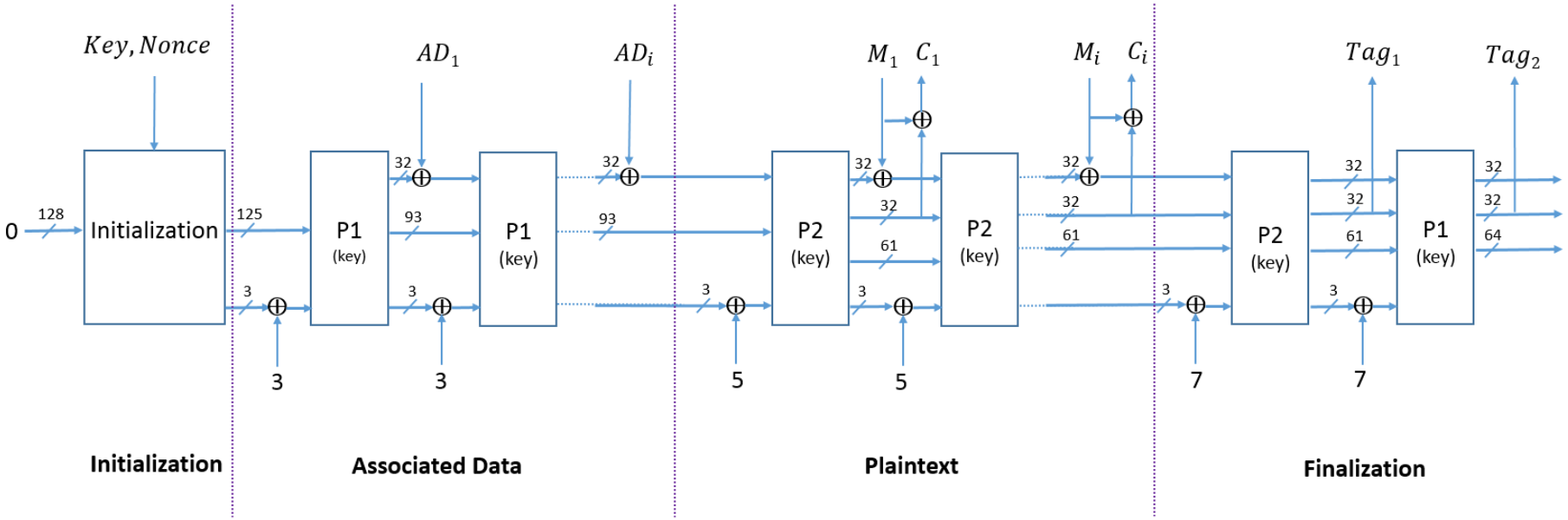
Authentication Throughput for large Na = $128/(87 \cdot T) = 1.4713 \cdot f$
Encryption Throughput for large Nm = $128/(87 \cdot T) = 1.4713 \cdot f$
Decryption Throughput for large Nc = $128/(87 \cdot T) = 1.4713 \cdot f$

T – clock period in μs, f – clock frequency in MHz, All Throughputs in Mbits/s

TinyJambu
(AEAD)

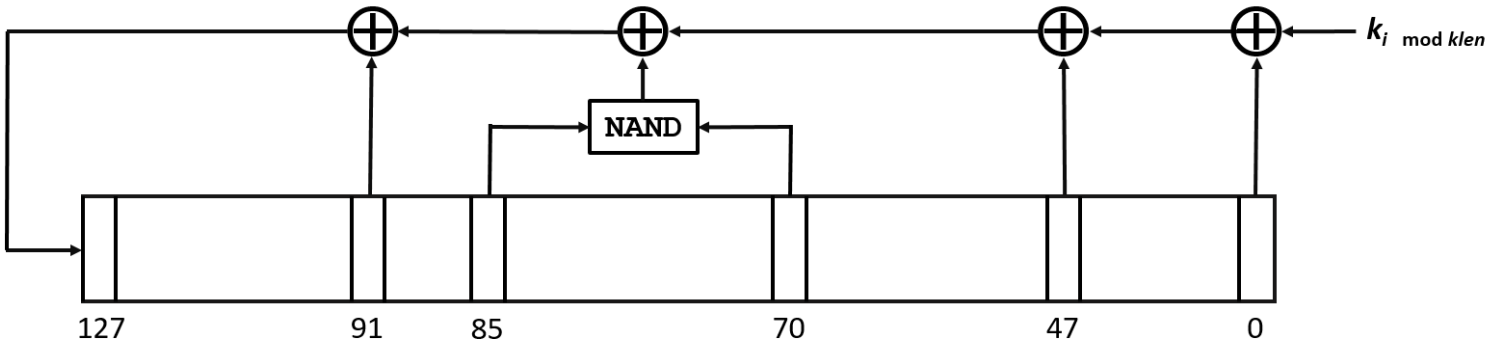
TinyJambu – Basic Features

- Sponge Construction



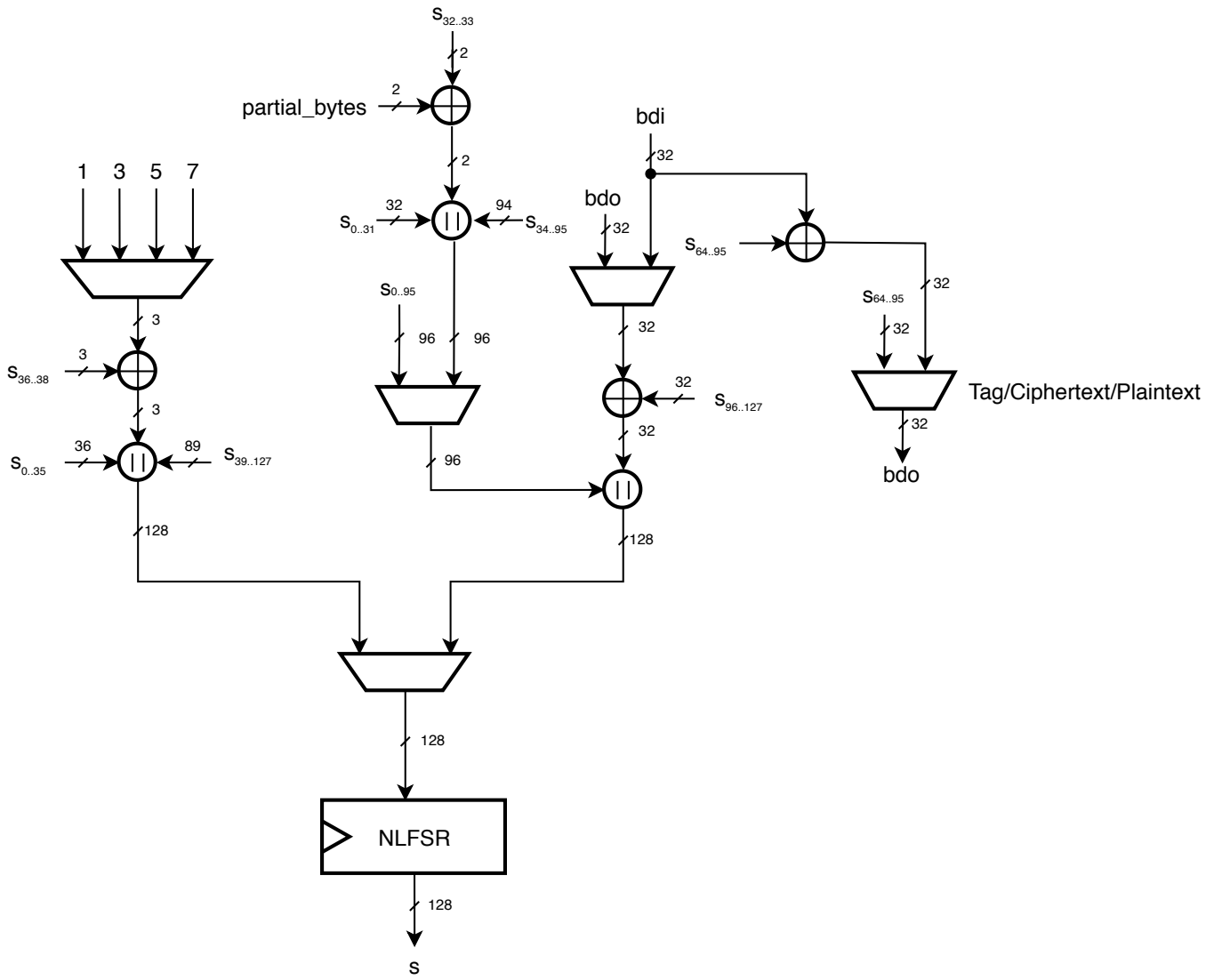
TinyJambu – Basic Features

- The Keyed Permutation

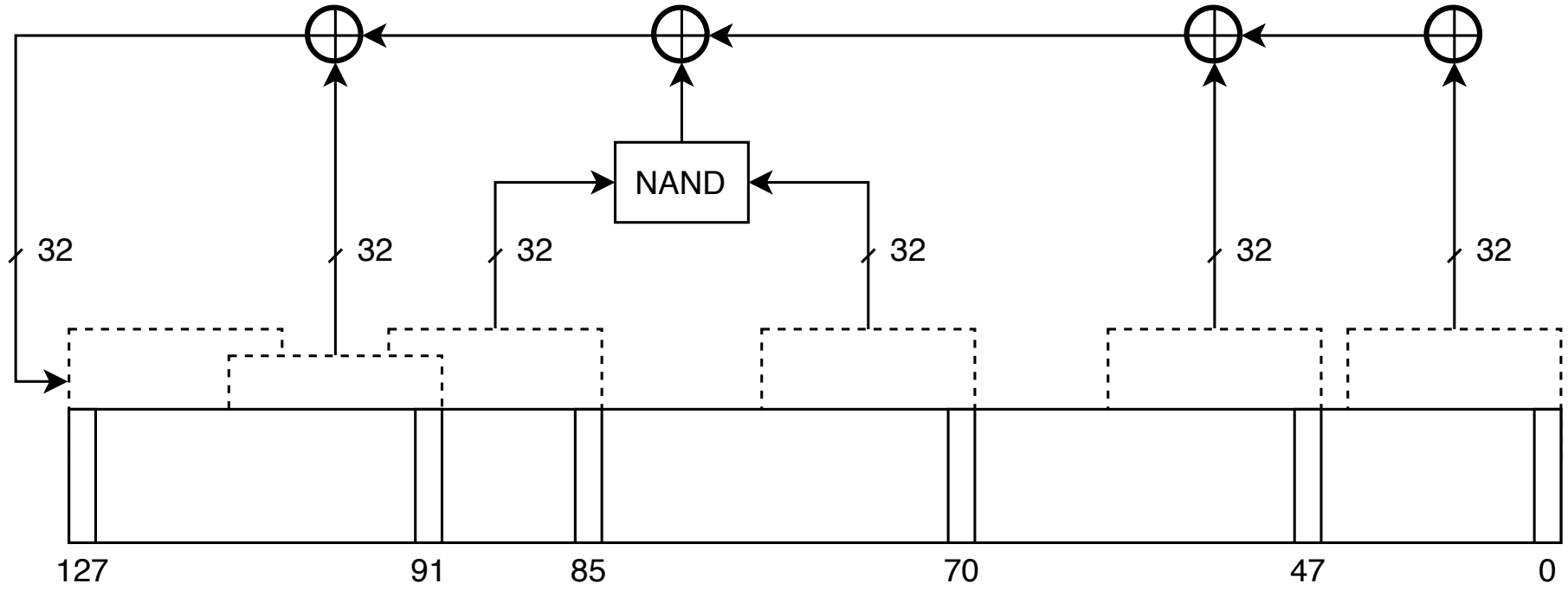


Key Setup	P_{1024}
Nonce Setup	P_{384}
Associated Data Processing	P_{384}
Encrypt	P_{1024}
Finalization	P_{1024} , P_{384}

TinyJambu – Block Diagram : Top Level



TinyJambu – Block Diagram : NLFSR



TinyJambu – Timing Analysis

	AD	Plaintext & Ciphertext	Tag
#Bits/Block	32	32	64
#Words/Block	1	1	2
#Cycles/Block	14	34	

Key setup time: 36

Execution time of authenticated encryption: 42+(14·Na)+(34·Nm)+48

Execution time of authenticated decryption: 42+(14·Na)+(34·Nc)+48

Authentication Throughput for large Na = 32/(14·T) = 2.2857·f

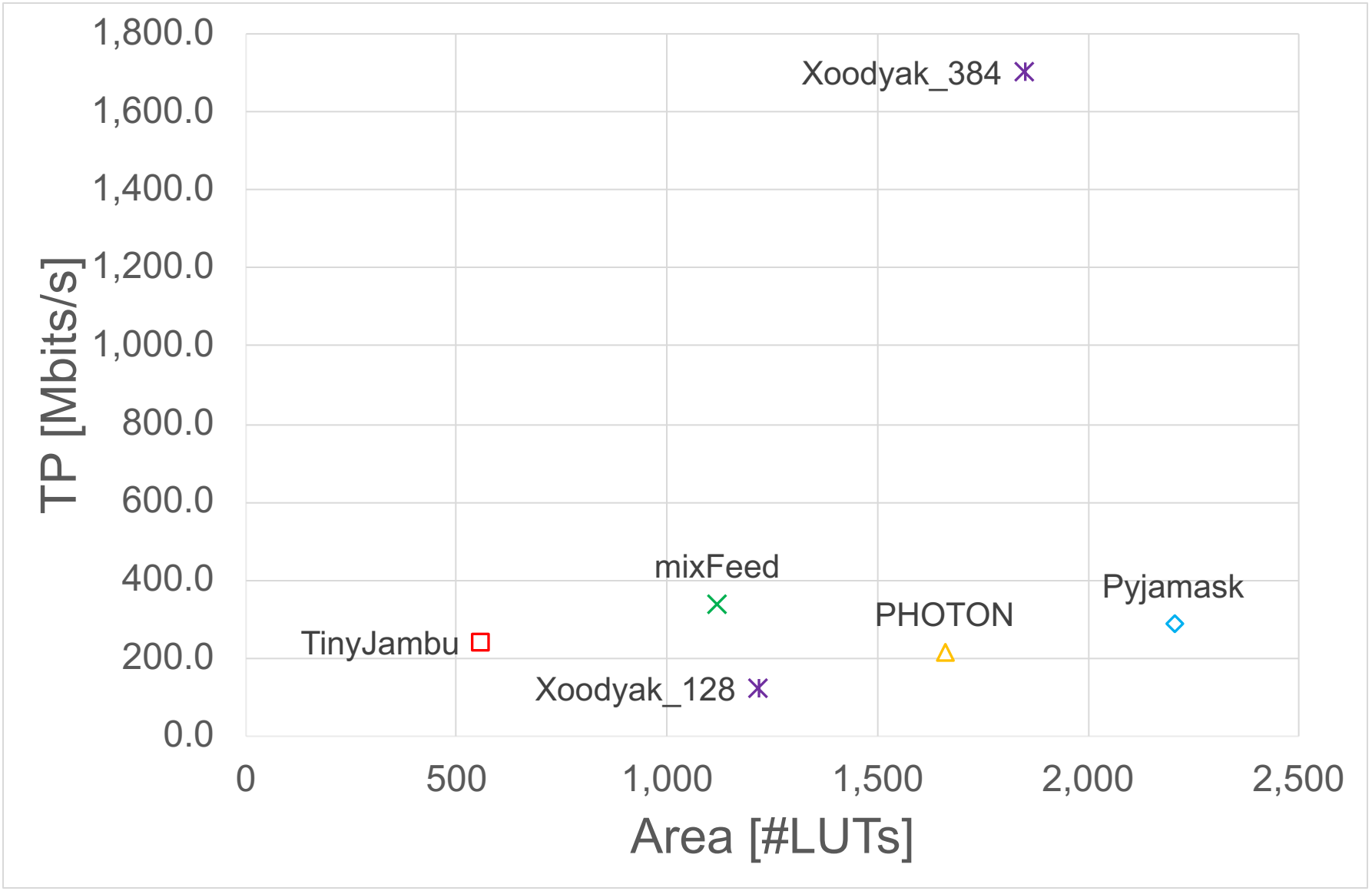
Encryption Throughput for large Nm = 32/(34·T) = 0.9412·f

Decryption Throughput for large Nc = 32/(34·T) = 0.9412·f

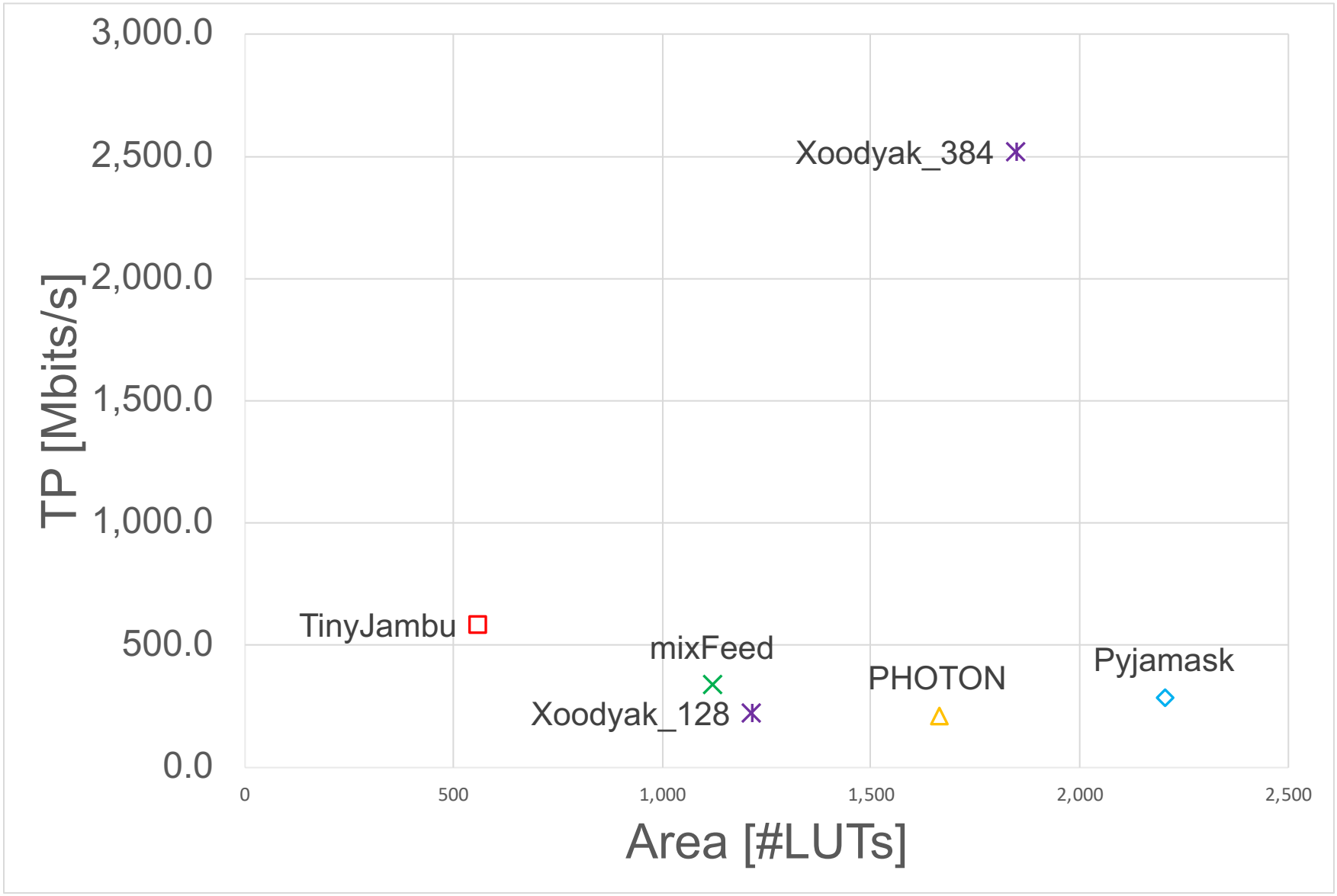
T – clock period in μs, f – clock frequency in MHz, All Throughputs in Mbits/s

Results for Unprotected Implementations

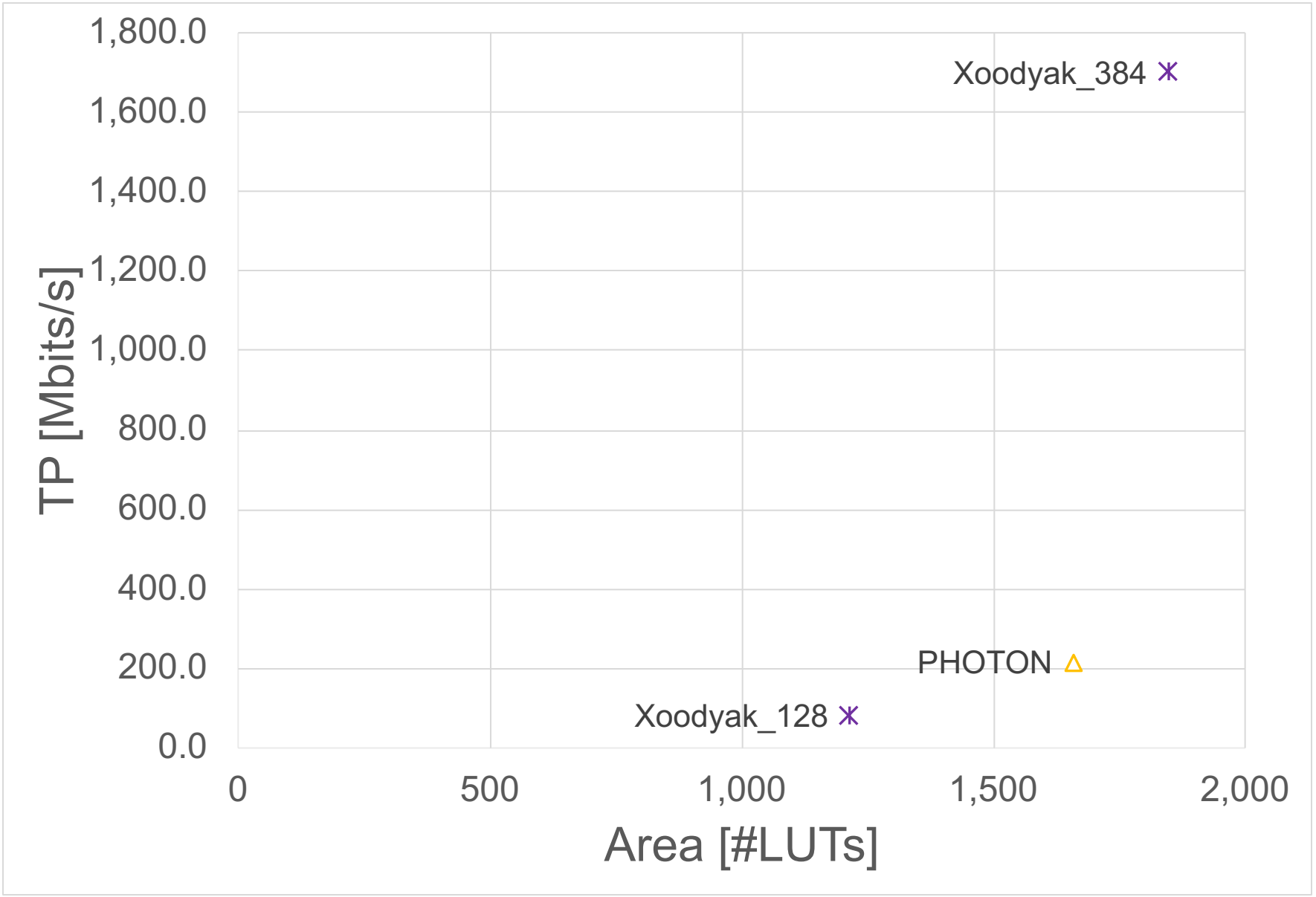
Throughput vs. Area for Encryption/Decryption of Long Messages in Artix-7



Throughput vs. Area for Authentication of Long Associated Data in Artix-7



Throughput vs. Area for Hashing of Long Messages in Artix-7



Throughput for Encryption/Decryption of Long and Short Messages in Artix-7

