CAESAR candidate PiCipher

Danilo Gligoroski, ITEM, NTNU, Norway
Hristina Mihajloska, FCSE, UKIM, Macedonia
Simona Samardjiska, ITEM, NTNU, Norway
and FCSE, UKIM, Macedonia
Håkon Jacobsen, ITEM, NTNU, Norway
Rune Erlend Jensen, IDI, NTNU, Norway
Mohamed El-Hadedy, University of Virginia, USA

NTNU
Innovation and Creativity

Design goals for PiCipher

1. To be nonce based authenticated encryption cipher with associated data with security ranges between 96 and 256 bits of security (CAESAR requested feature)
2. To be easier than AES-GCM to run it in a parallel mode (CAESAR comparison with AES-GCM)
   - To be faster than AES-GCM on the hardware that has AES-NI (but using other parallel potentials of the same hardware like many cores and SIMD)
   - To be faster than AES-GCM on hardware that does not have AES-NI
   - To be faster than AES-GCM on any parallel architecture
   - To be able to offer incremental encryptions and tag productions (Extra feature)
3. To offer better than AES-GCM security features in a case when nonce is reused (CAESAR comparison with AES-GCM and Extra feature)
4. To offer better than AES-GCM resistance for producing second tag preimages (CAESAR comparison with AES-GCM and Extra feature)
   - To be resistant to insider attacks that know the secret key
5. To offer better than AES-GCM properties for preventing DoS attacks (CAESAR comparison with AES-GCM and Extra feature)
6. For certain parameters to offer the flexibility of tweakable (wide-block) encryption (that gives authentication too) (Extra feature)
7. For certain parameters to be lightweight in HW, for other parameters to be fast in SW

NTNU
Innovation and Creativity

Design principles in PiCipher

- It is based on several solid cryptographic concepts
  - Encrypt-then-MAC principle,
  - XOR MAC scheme,
  - Two-pass sponge construction
- Its permutation is based on 16-bit or 32-bit or 64-bit ARX operations
- Possibility to Plug&Play other permutation in PiCipher

NTNU
Innovation and Creativity

The main component in PiCipher is “Triplex”

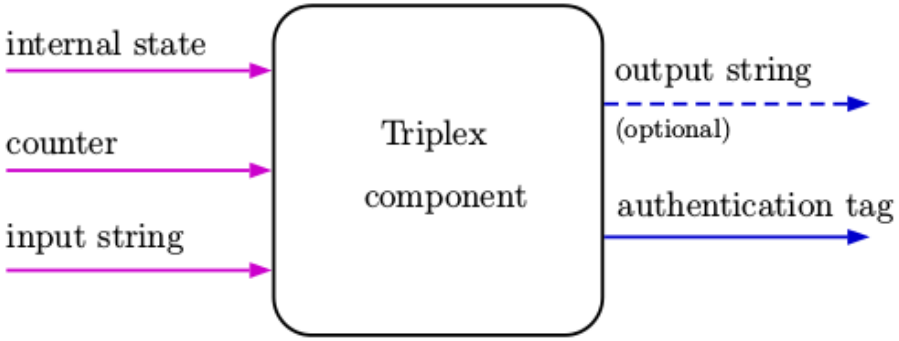
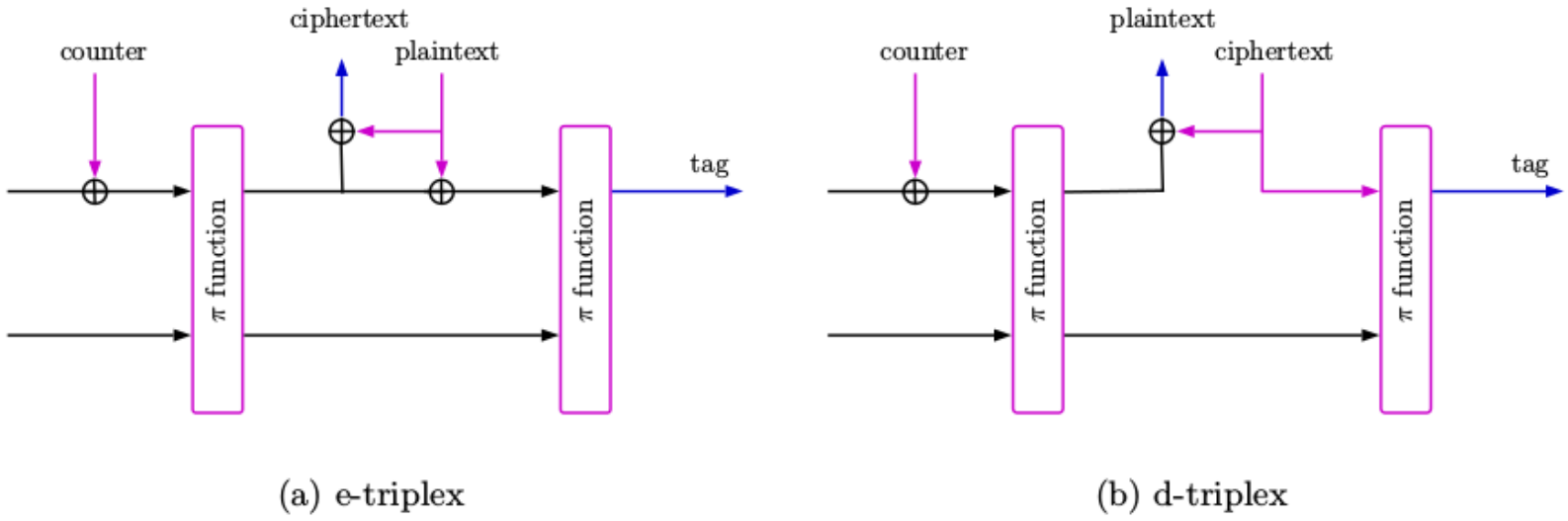


Fig. 1: A general scheme of the triplex component

Inside the Triplex



(a) e-triplex (b) d-triplex

Fig. 2: The Triplex component

Why “Triplex”, why not Sponge Duplex?

NTNU
Innovation and Creativity

Why “Triplex”, why not Sponge Duplex?

We did not want to violate the rights of the US Patent US2842789 A: “Combined sponge and squeegee with duplex control means”

NTNU
Innovation and Creativity

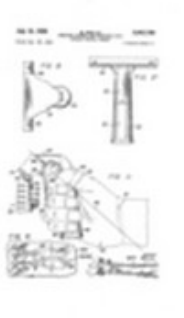
Why “Triplex”, why not Sponge Duplex?

Patents

Combined sponge and squeegee with duplex control means

US 2842789 A

IMAGES (2)



of the sponge eans”

NTNU
Innovation and Creativity

Why “Triplex”, why not Sponge Duplex?

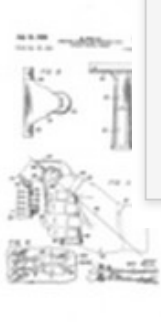
Patents

of the

Combined spong control means

US 2842789 A

IMAGES (2)



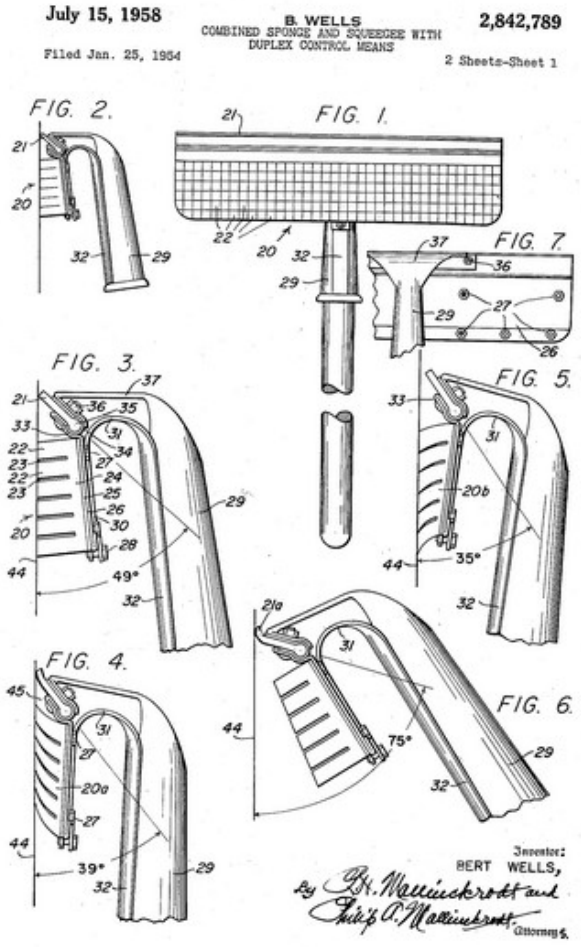
Publication number	US2842789 A
Publication type	Grant
Publication date	15 Jul 1958
Filing date	25 Jan 1954
Priority date ⓘ	25 Jan 1954
Inventors	Bert Wells
Original Assignee	Bert Wells
Export Citation	BiBTeX, EndNote, RefMan

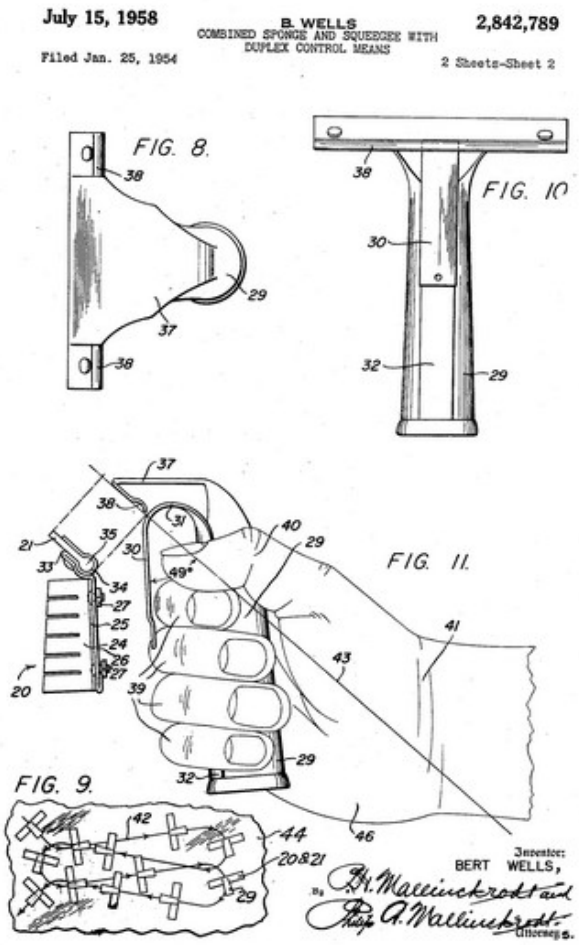
Patent Citations (10), Referenced by (23), Classifications (10)

External Links: USPTO, USPTO Assignment, Espacenet

NTNU
Innovation and Creativity

Why “Triplex”, why not Sponge Duplex?





Inside PiCipher

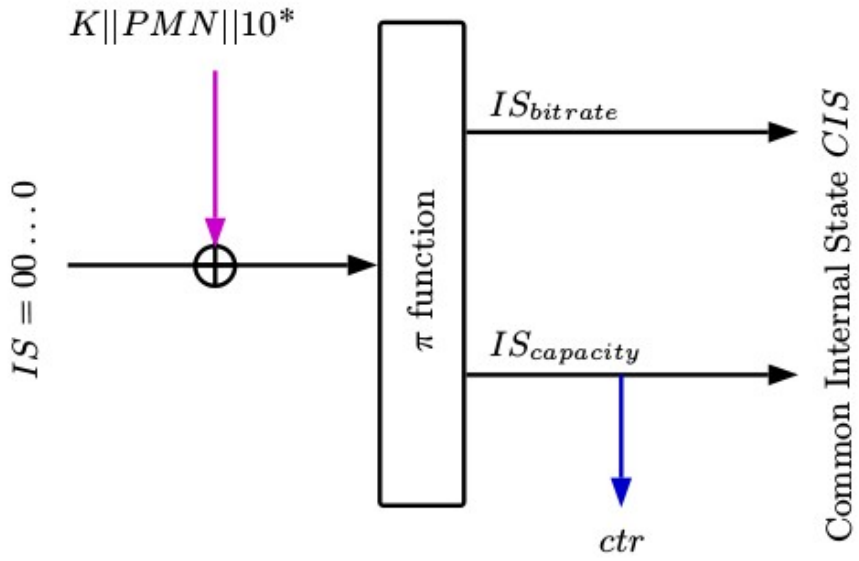


Fig. 3: Initialization step

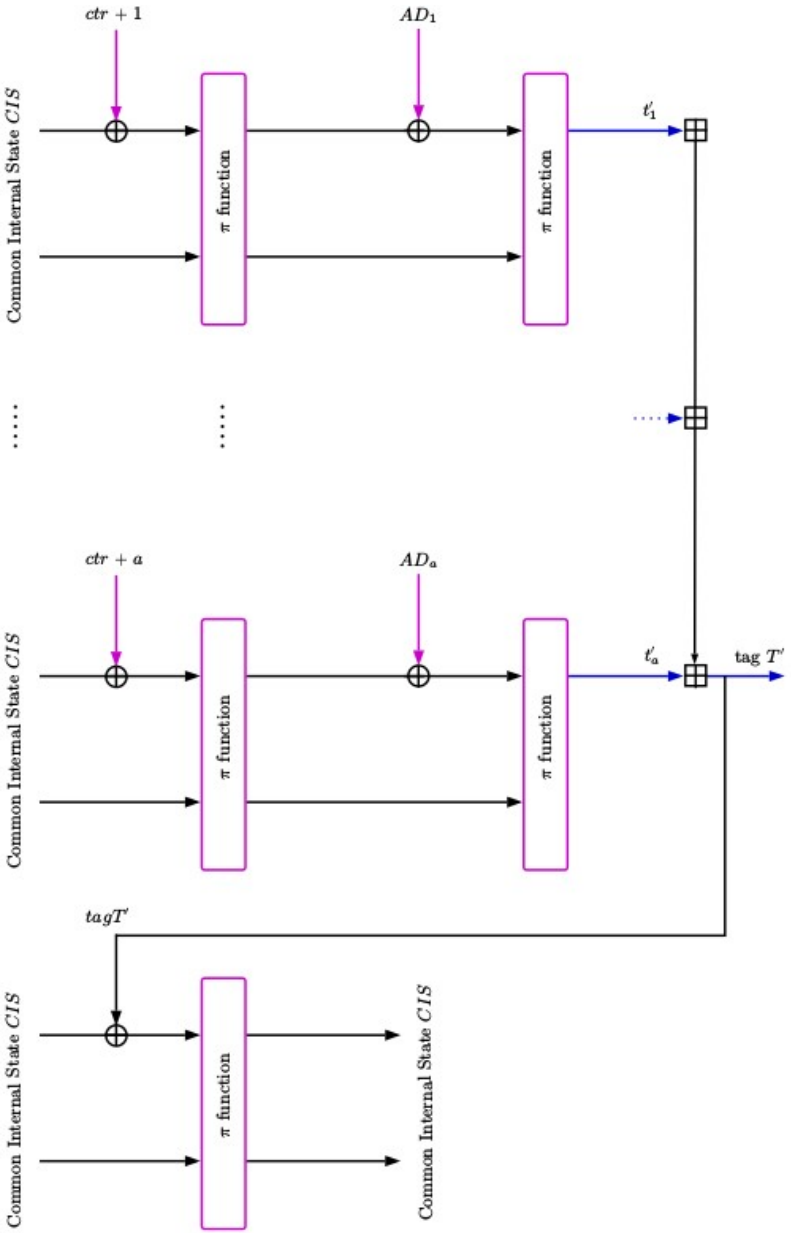


Fig. 4: Processing the associated data AD with a blocks in parallel

Inside PiCipher

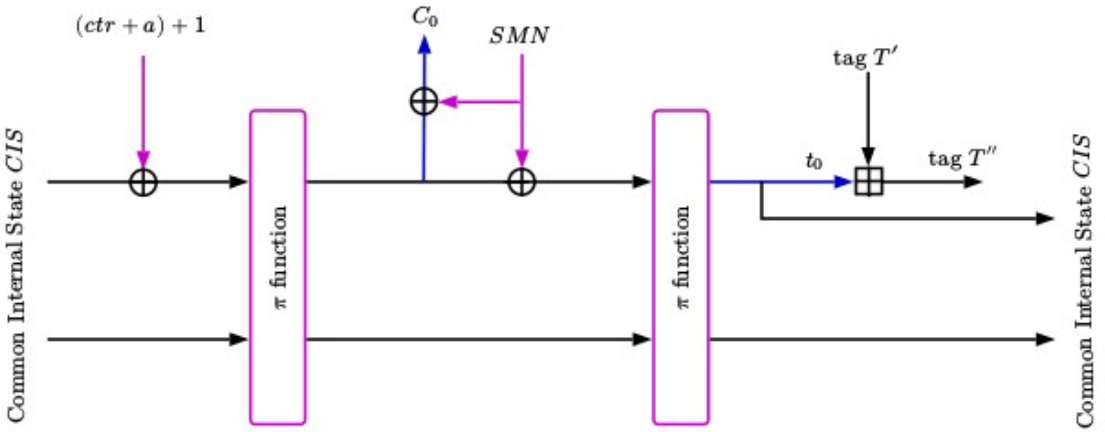


Fig. 5: Processing the secret message number SMN

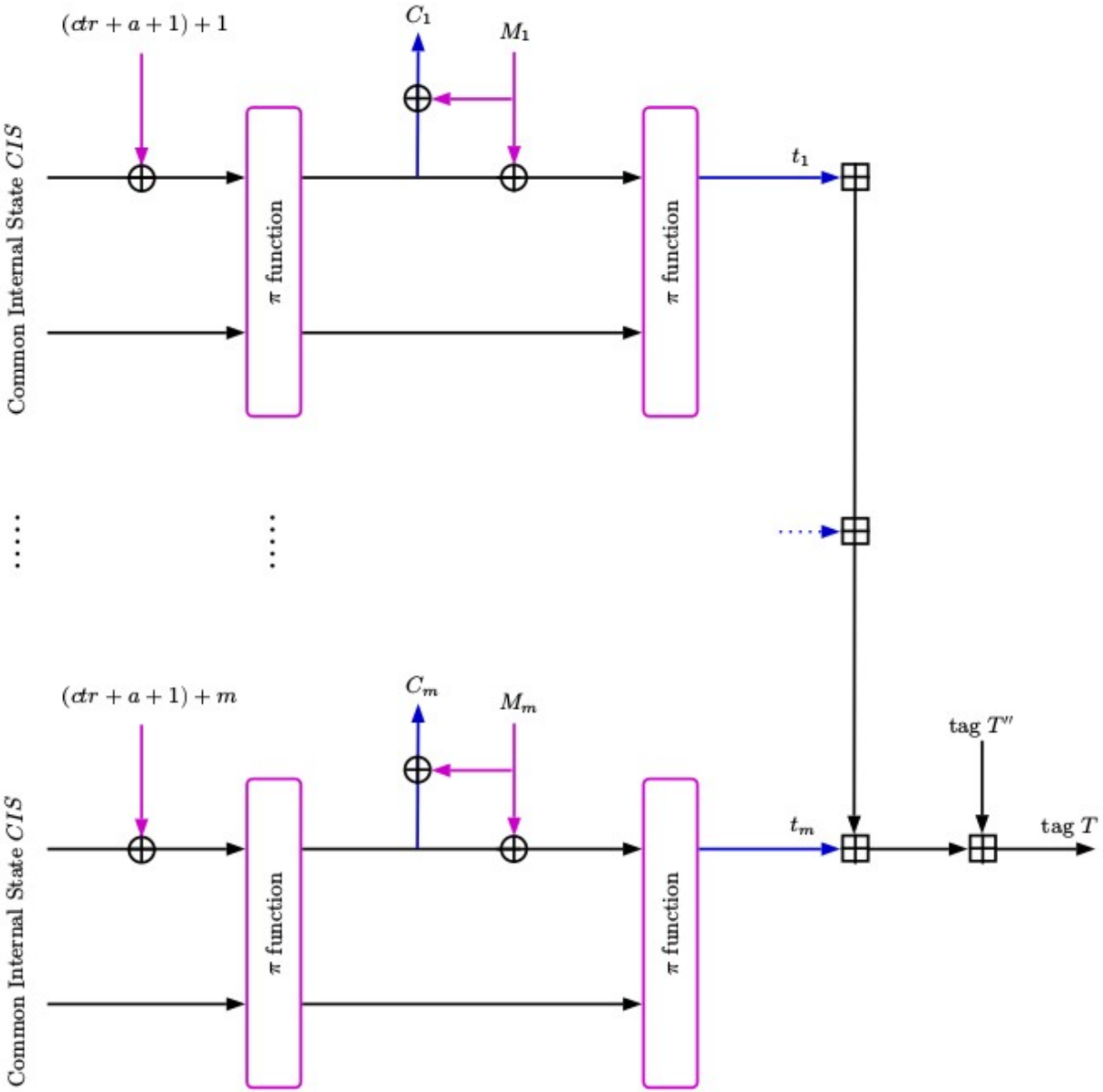


Fig. 6: Processing the message M with m blocks in parallel

General overview how each of the design goals are achieved

1. To be nonce based authenticated encryption cipher with associated data with security ranges between 96 and 256 bits of security (CAESAR requested feature)

	Word size ω (in bits)	$klen$ (in bits)	PMN (in bits)	SMN (in bits)	b (in bits)	N	$bitrate$ (in bits)	Tag t (in bits)	R
π16-Cipher096	16	96	32	0 or 128	256	4	128	128	4
π16-Cipher128	16	128	32	0 or 128	256	4	128	128	4
π32-Cipher128	32	128	128	0 or 256	512	4	256	256	4
π32-Cipher256	32	256	128	0 or 256	512	4	256	256	4
π64-Cipher128	64	128	128	0 or 512	1024	4	512	512	4
π64-Cipher256	64	256	128	0 or 512	1024	4	512	512	4

NTNU
Innovation and Creativity

General overview how each of the design goals are achieved

2. To be easier than AES-GCM to run it in a parallel mode (CAESAR comparison with AES-GCM)
   - To be faster than AES-GCM on the hardware that has AES-NI (but using other parallel potentials of the same hardware like many cores and SIMD)
   - To be faster than AES-GCM on hardware that does not have AES-NI
   - To be faster than AES-GCM on any parallel architecture
   - To be able to offer incremental encryptions and tag productions (Extra feature)

General overview how each of the design goals are achieved

2. To be easier than AES-GCM to run it in a parallel mode (CAESAR comparison with AES-GCM)

General overview how each of the design goals are achieved

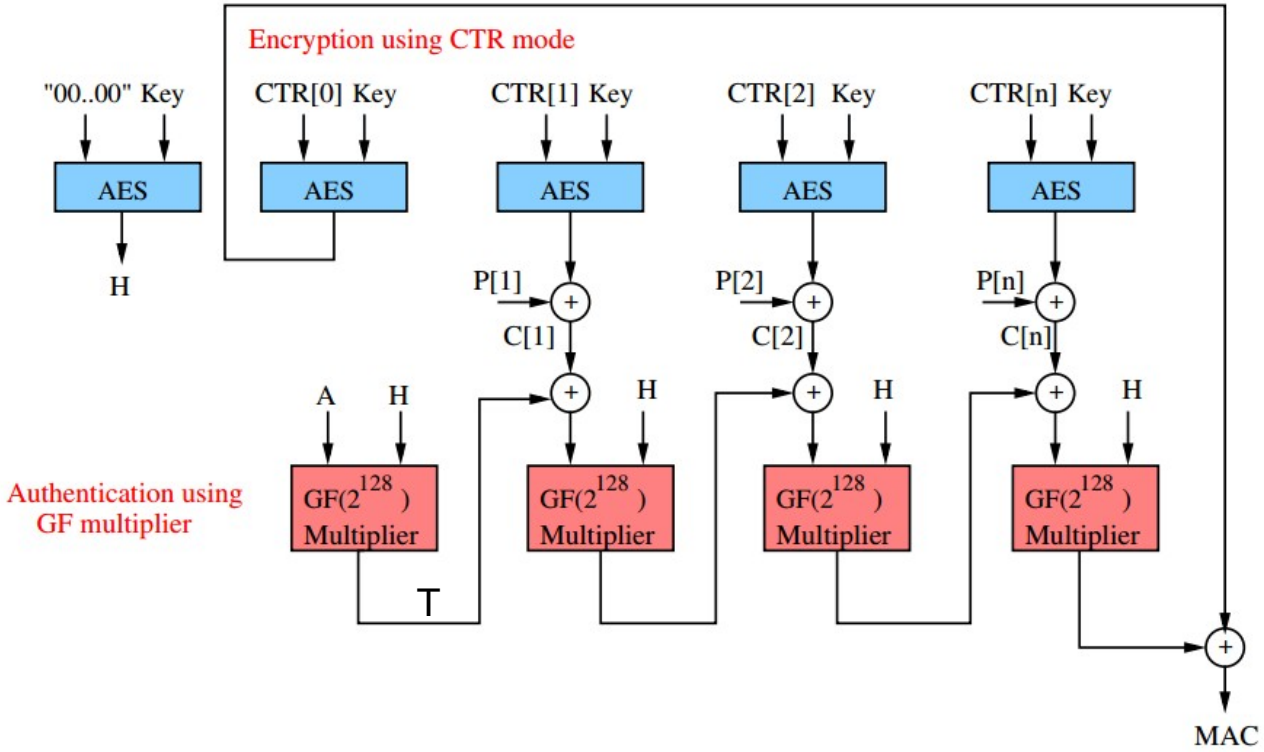
How AES-GCM can run in fully parallel mode?

2. To be easier than A … nparison with AES-GCM)

General overview how each of the design goals are achieved

How AES-GCM can run in fully parallel mode?

2. To be easier than A arison with AES-GCM)
   - To be faster than A ng other parallel



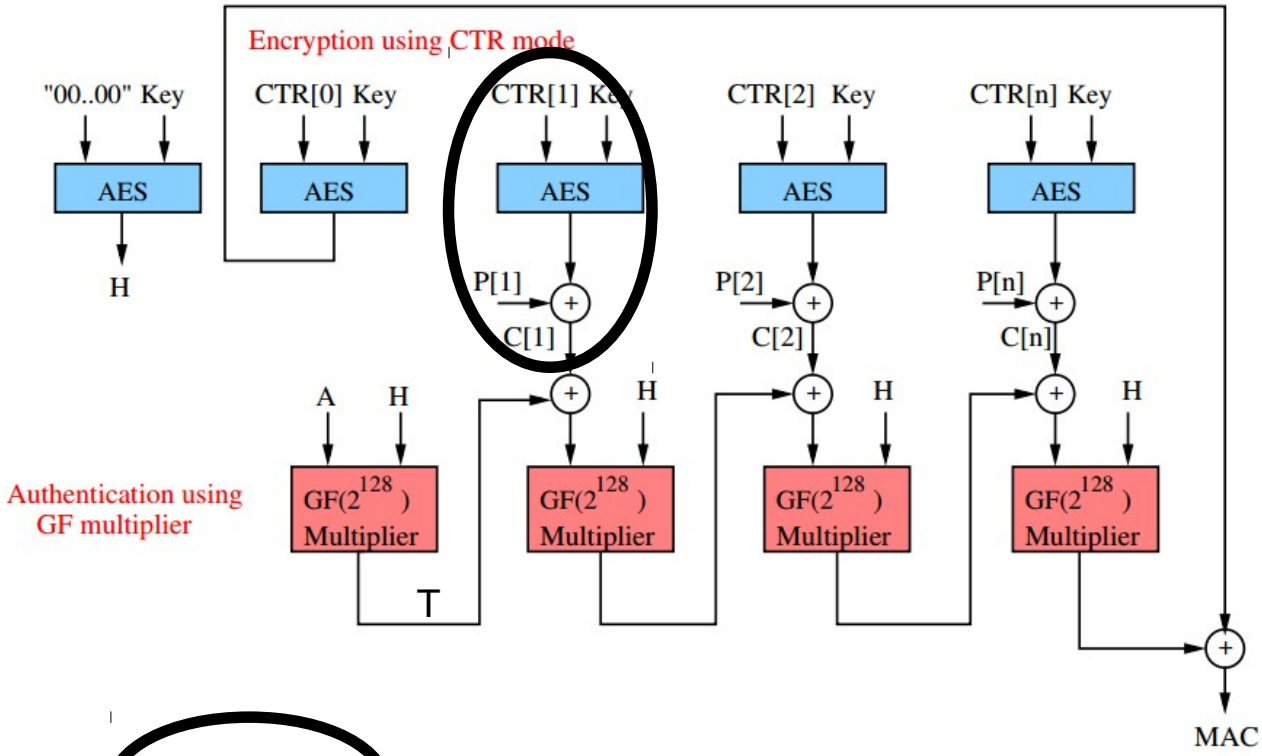
$$MAC = (T+C[1]).H^{N} + (C[2]).H^{N-1} + \ldots + (C[n-1]).H^{2} + (C[n]).H$$

NTNU
Innovation and Creativity

General overview how each of the design goals are achieved

2. To be easier than A … mparison with AES-GCM)

How AES-GCM can run in fully parallel mode?

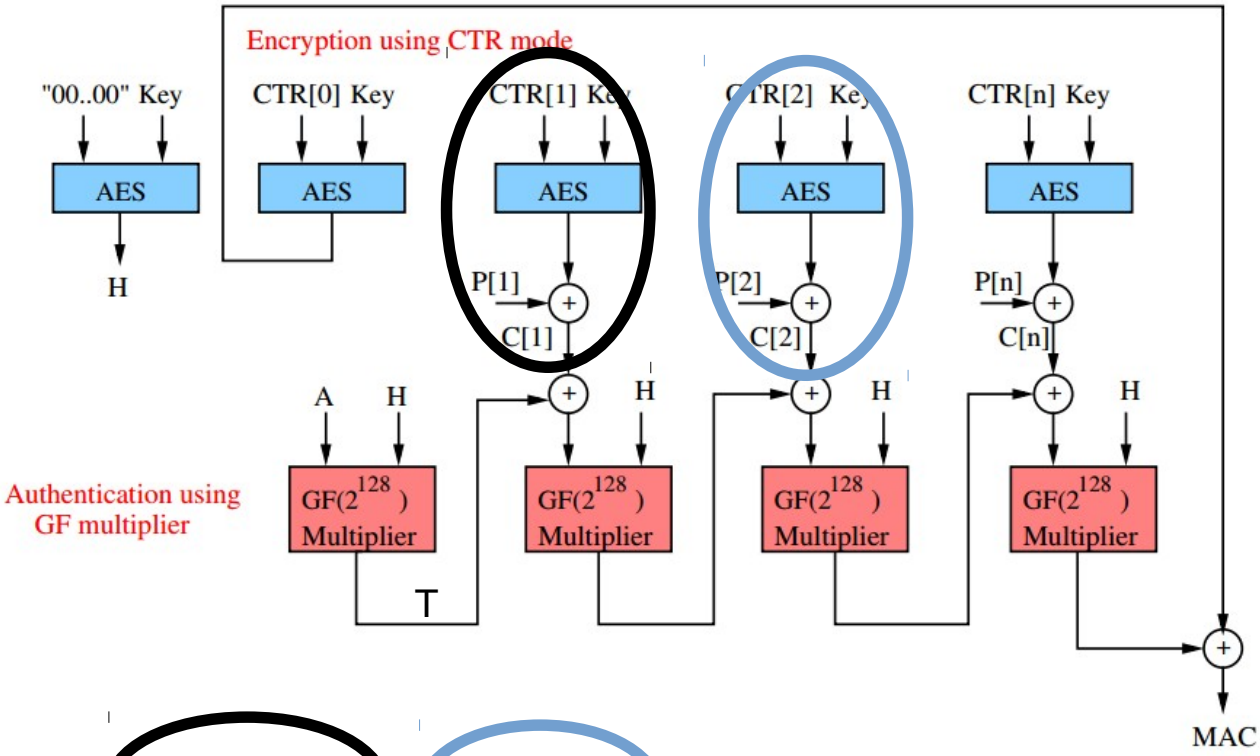


$$MAC = (T+C[1]).H^{N} + (C[2]).H^{N-1} + \ldots + (C[n-1]).H^{2} + (C[n]).H$$

General overview how each of the design goals are achieved

How AES-GCM can run in fully parallel mode?

2. To be easier than A … arison with AES-GCM)
   - To be faster than A … ng other parallel



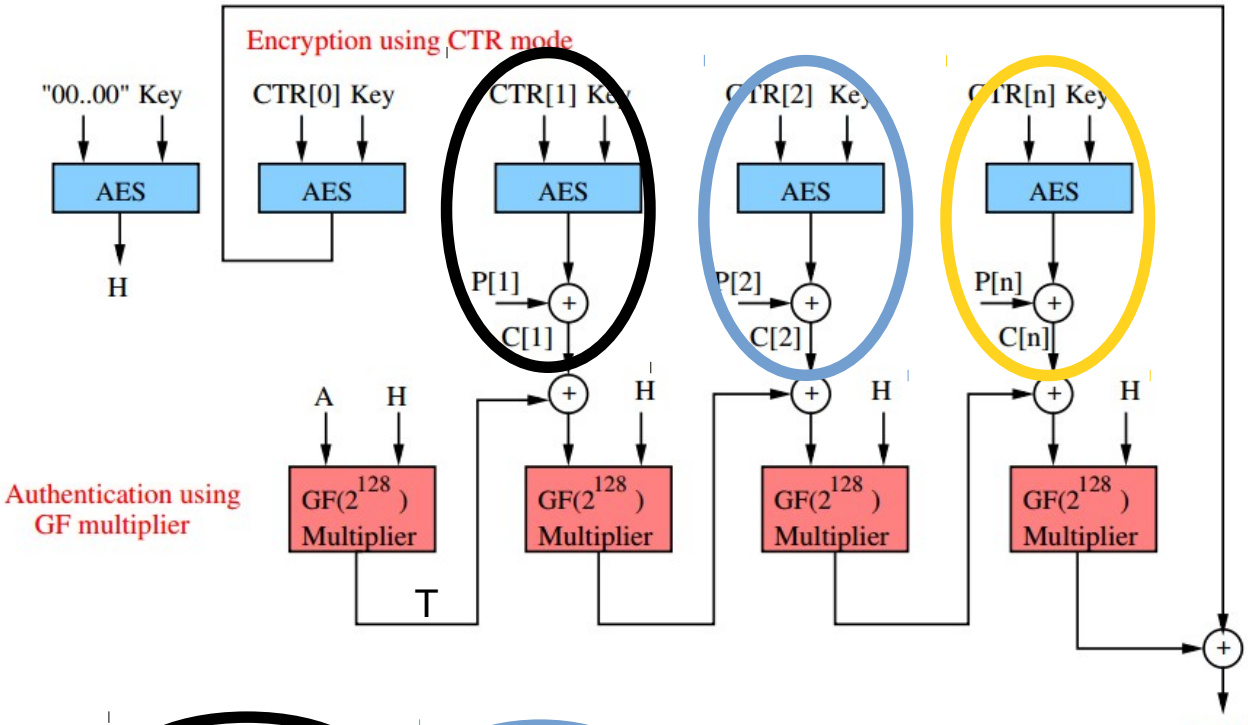
$$MAC = (T+C[1]).H^{N} + (C[2]).H^{N-1} + \ldots + (C[n-1]).H^{2} + (C[n]).H$$

NTNU Innovation and Creativity

General overview how each of the design goals are achieved

How AES-GCM can run in fully parallel mode?

2. To be easier than A … arison with AES-GCM)
   - To be faster than A … ng other parallel

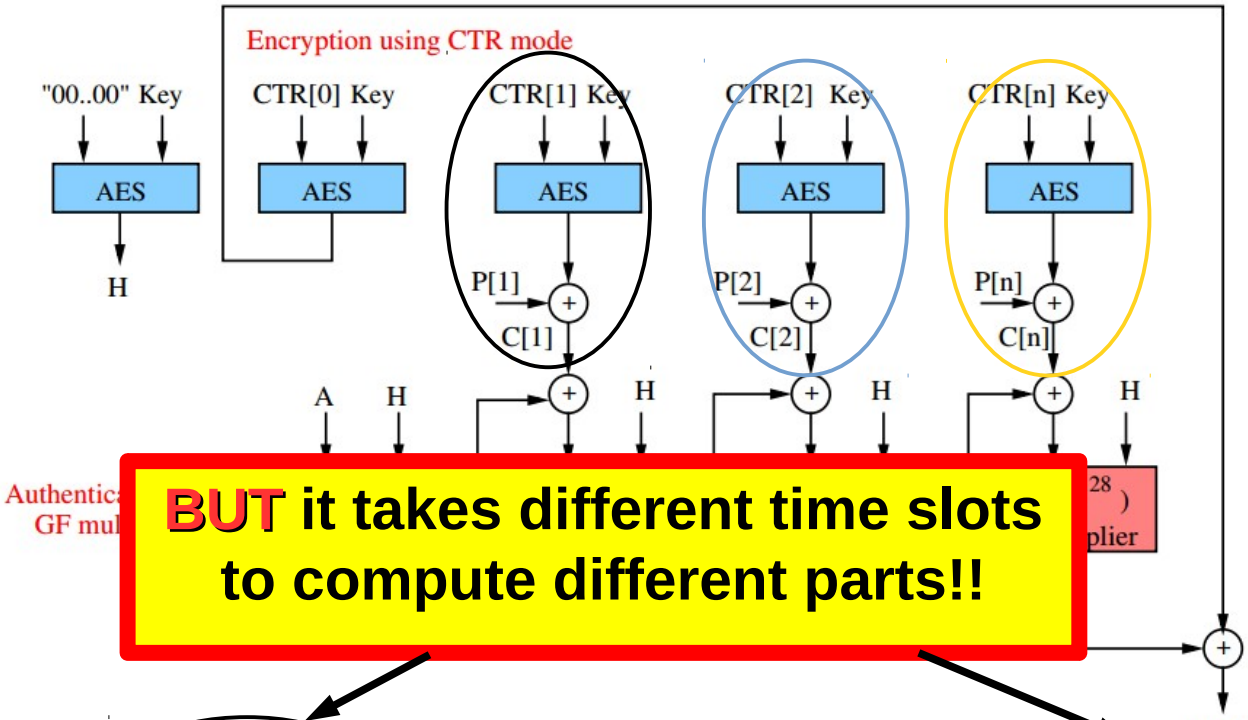


$$MAC = (T+C[1]).H^{N} + (C[2]).H^{N-1} + \ldots + (C[n-1]).H^{2} + (C[n]).H$$

General overview how each of the design goals are achieved

How AES-GCM can run in fully parallel mode?

2. To be easier than A arison with AES-GCM)
   - To be faster than A ng other parallel



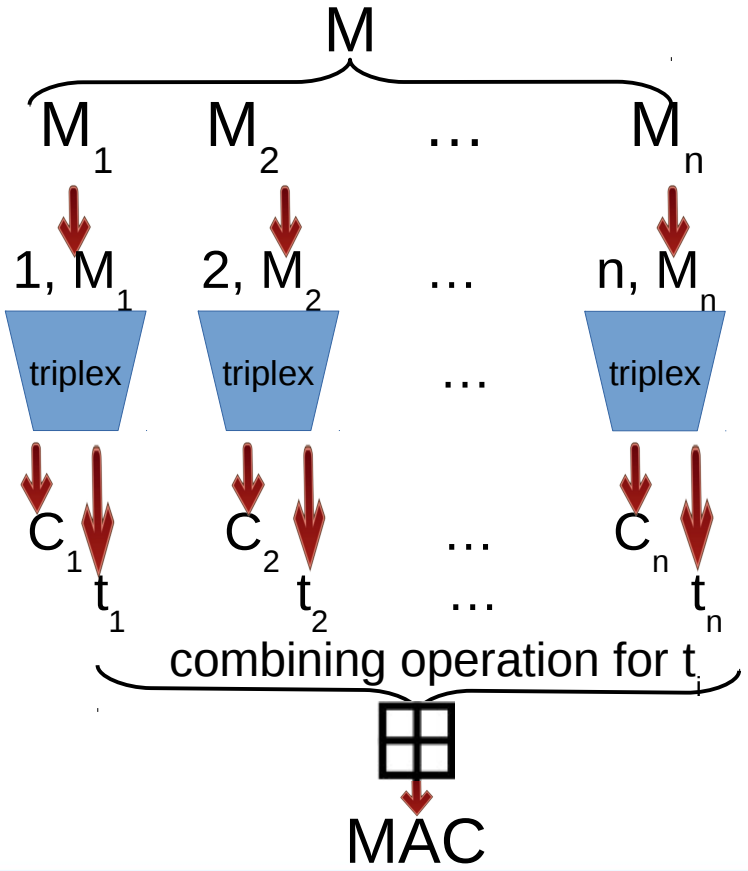
BUT it takes different time slots to compute different parts!!

$$MAC = (T+C[1]).H^{N} + (C[2]).H^{N-1} + \ldots + (C[n-1]).H^{2} + (C[n]).H$$

General overview how each of the design goals are achieved

2. To be easier than A … arison with AES-GCM)
   - To be faster than A … ng other parallel

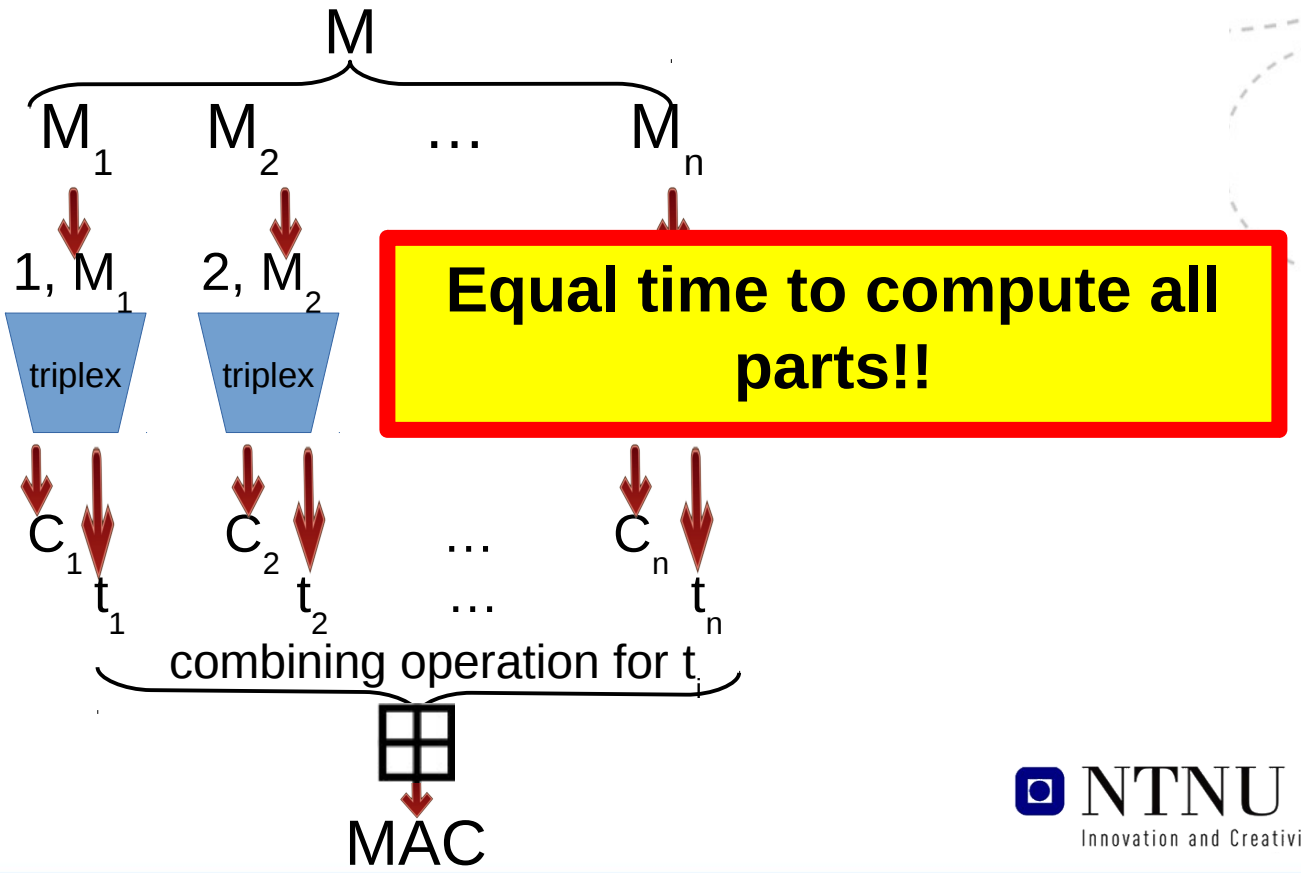
How parallel operations are performed in PiCipher?



General overview how each of the design goals are achieved

2. To be easier than A … arison with AES-GCM)
   - To be faster than A … ng other parallel

How parallel operations are performed in PiCipher?

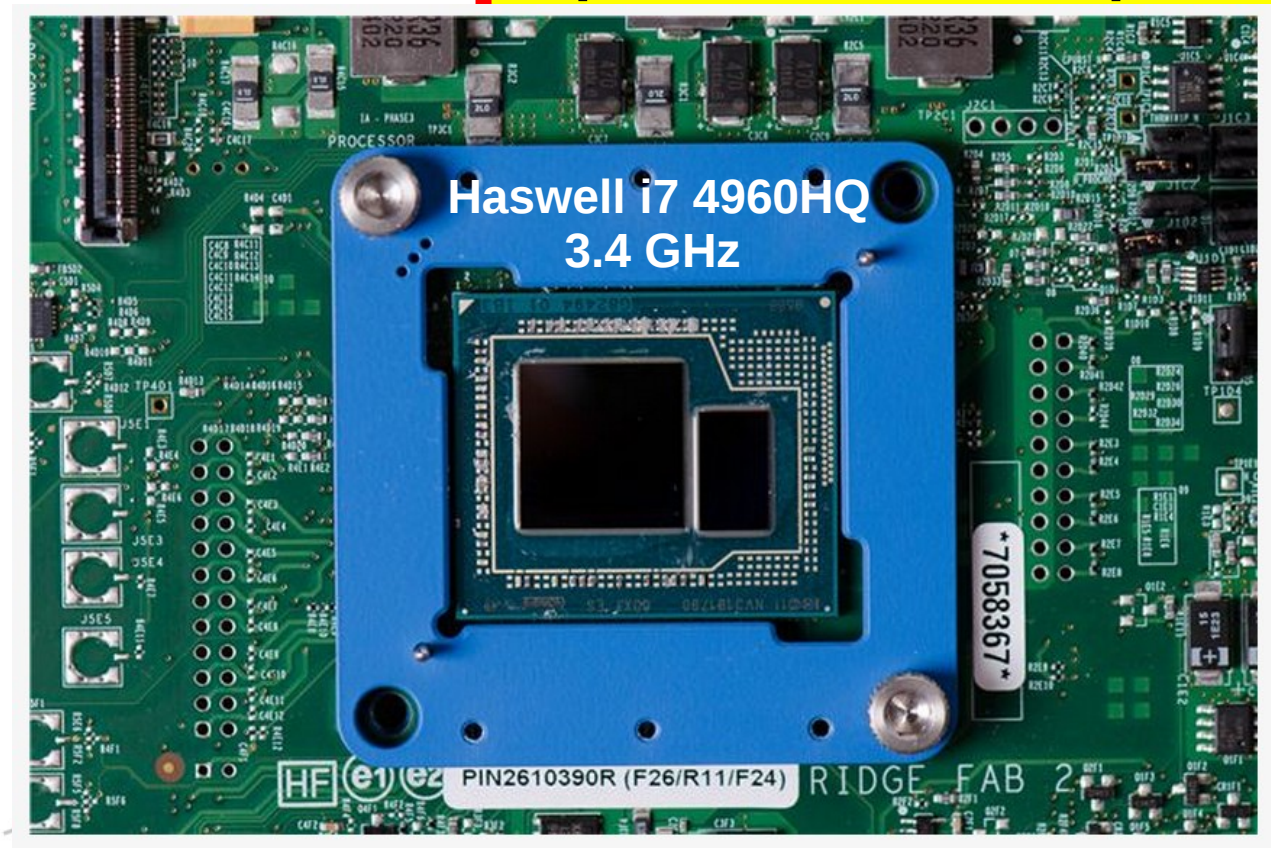


Equal time to compute all parts!!

General overview how each of the design goals are achieved

2. To be easier than A… …arison with AES-GCM)
   - To be faster than A… …ng other parallel

How parallel operations are performed in PiCipher?



…ne to compute all parts!!

MAC

General overview how each of the design goals are achieved

2. To be easier than A… …arison with AES-GCM)
   - To be faster than A… …ng other parallel

How parallel operations are performed in PiCipher?

AES-GCM ~ 1cpb ~ up to 26 Gbps?

…ne to compute all parts!!

…n

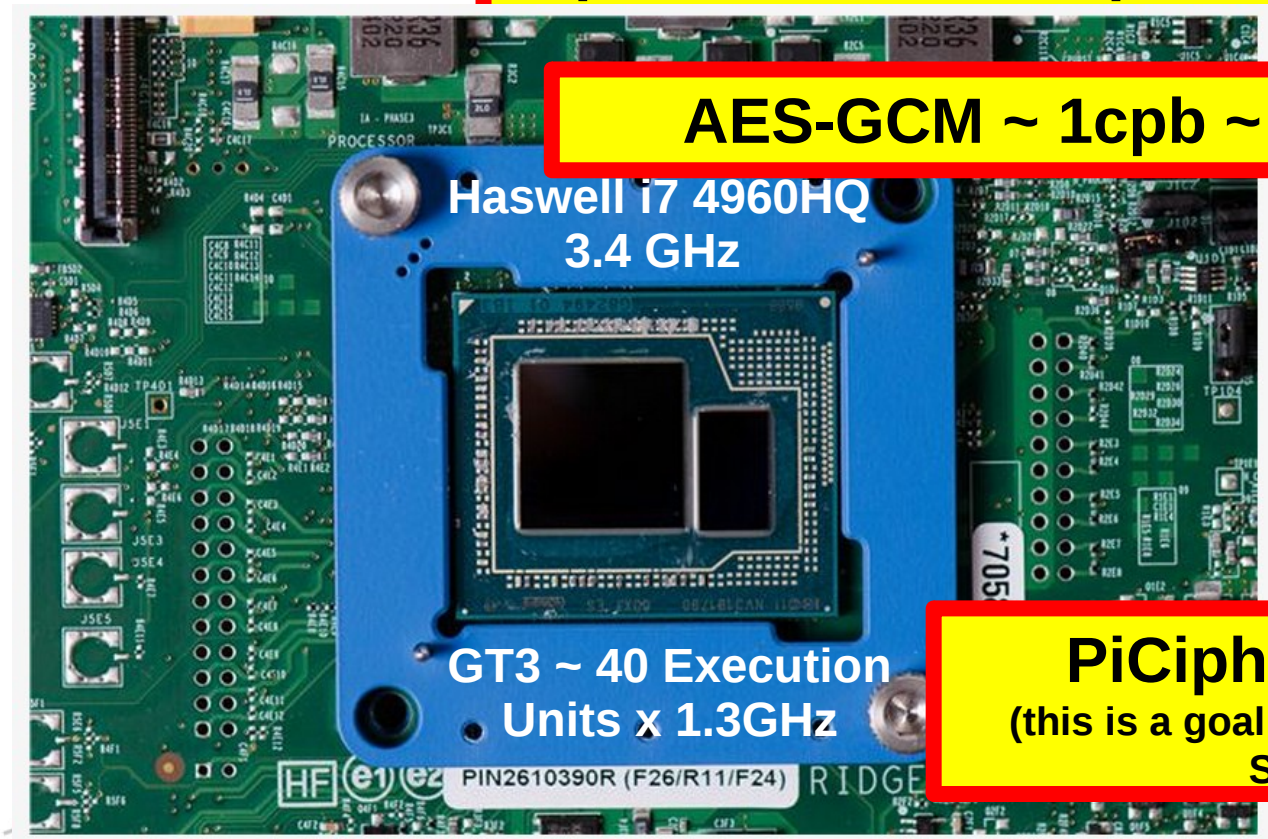
MAC

General overview how each of the design goals are achieved

2. To be easier than A… …arison with AES-GCM)
   - To be faster than A… …ng other parallel

How parallel operations are performed in PiCipher?

AES-GCM ~ 1cpb ~ up to 26 Gbps?



…ne to compute all parts!!

PiCipher ~ 26 Gbps?
(this is a goal – will it be measurable in SUPERCOP?)

MAC

NTNU
Innovation and Creativity

General overview how each of the design goals are achieved

- **PiCipher uses NONCE=(PMN, SMN)**
- **In case M1 is encrypted with (K, AD, (PMN,SMN1)) and M2 is encrypted with (K, AD, (PMN,SMN2)) then maximal (as the number of key bits) confidentiality and integrity are preserved**
  - **+ something EXTRA: No information if M1= M2**

3. To offer better than AES-GCM security features in a case when nonce is reused (CAESAR comparison with AES-GCM and Extra feature)

General overview how each of the design goals are achieved

- **PiCipher uses NONCE=(PMN, SMN)**
- **In case M1 is encrypted with (K, AD, (PMN,SMN1)) and M2 is encrypted with (K, AD, (PMN,SMN2)) then maximal (as the number of key bits) confidentiality and integrity are preserved**
  - **+ something EXTRA: No information if M1= M2**

3. To offer better than AES-GCM security features in a case when nonce is reused (CAESAR comparison with AES-GCM and Extra feature)

This intermediate level of robustness against repeated (K, AD, PMN) have only two CAESAR candidates: ICEPOLE and PiCipher.

General overview how each of the design goals are achieved

4. To offer better than AES-GCM resistance for producing second tag preimages (CAESAR comparison with AES-GCM and Extra feature)
   - To be resistant to insider attacks that know the secret key

General overview how each of the design goals are achieved

In last DIAC 2013 we advocated that tag second preimage resistance is in the line of ROBUSTNESS that is mentioned in the CAESAR call.

4. To offer better than AES-GCM resistance for producing second tag preimages (CAESAR comparison with AES-GCM and Extra feature)
   - To be resistant to insider attacks that know the secret key

NTNU
Innovation and Creativity

General overview how each of the design goals are achieved

In last DIAC 2013 we advocated that tag second preimage resistance is in the line of ROBUSTNESS that is mentioned in the CAESAR call.

This CRYPTO 2014 we got extra argument in the paper "Security of Symmetric Encryption against Mass Surveillance", Bellare, Paterson, Rogaway

Using AEAD where the attacker (performing mass surveillance) can easily produce second tag preimages is scary.

NTNU
Innovation and Creativity

General overview how each of the design goals are achieved

Majority of sponge-based AE ciphers offer that extra feature of being second tag preimage resistant.

But in that case they are not parallel and incremental.

4. To offer better than AES-GCM resistance for producing second tag preimages (CAESAR comparison with AES-GCM and Extra feature)
   - To be resistant to insider attacks that know the secret key

General overview how each of the design goals are achieved

In our initial submission we gave security values for the hardness of finding second tag preimages that were in the range between 2^{52}, 2^{104} and 2^{208} for keys of 96, 128 and 256 bits.

4. To offer better than AES-GCM resistance for producing second tag preimages (CAESAR comparison with AES-GCM and Extra feature)
   - To be resistant to insider attacks that know the secret key

NTNU
Innovation and Creativity

General overview how each of the design goals are achieved

In our initial submission we gave security values for the hardness of finding second tag preimages that were in the range between 2^{52}, 2^{104} and 2^{208} for keys of 96, 128 and 256 bits.

HOWEVER

Gaetan in "Tag Second-preimage Attack against π-cipher" applied Wagner's generalized birthday attack and found second tag preimages with complexities: 2^{22} using messages long 2^{11} blocks, 2^{31} using messages long 2^{16} blocks, and 2^{45} using messages long 2^{22} blocks

NTNU
Innovation and Creativity

General overview how each of the design goals are achieved

We responded that:
1. Either we will abandon the claims about that Extra feature
OR
2. We will tweak the cipher

4.To offer better than AES-GCM resistance for producing second tag preimages (CAESAR comparison with AES-GCM and Extra feature)

- To be resistant to insider attacks that know the secret key

General overview how each of the design goals are achieved

We responded that:
1. Either we will abandon the claims about that Extra feature
OR
2. We will tweak the cipher

4.To offer better than AES-GCM resistance for producing second tag preimages (CAESAR comparison with AES-GCM and Extra feature)

And on DIAC 2014 workshop we officially claim this:

We are not tweaking the cipher, but we still claim the extra feature of being second tag preimage resistant.

NTNU
Innovation and Creativity

General overview how each of the design goals are achieved

How is that possible?

4. To offer better than AES-GCM resistance for producing second tag preimages (CAESAR comparison with AES-GCM and Extra feature)
   - To be resistant to insider attacks that know the secret key

NTNU
Innovation and Creativity

General overview how each of the design goals are achieved

How is that possible?

$$\min_{m \leqslant N_{max}} O\left(m \cdot 2^{\frac{tlen}{1+\lg\lfloor m \rfloor}}\right)$$

Complexity for finding second tag preimages if the size of the tag is tlen, and the size of the message is m blocks.

General overview how each of the design goals are achieved

How is that possible?

$$\min_{m \leqslant N_{max}} O\left(m \cdot 2^{\frac{tlen}{1+\lg\lfloor m \rfloor}}\right)$$

Complexity for finding second tag preimages if the size of the tag is tlen, and the size of the message is m blocks.

For short messages such as (1500 bytes messages as the most common IP packet size) m=24 and the second preimage attack has complexity 2^{106}.

NTNU
Innovation and Creativity

General overview how each of the design goals are achieved

How is that possible?

We will clarify the tag second preimage resistance of PiCipher in the coming updated documentation.

Comple… if the size of t… age is m blocks.

For short messages such as (1500 bytes messages as the most common IP packet size) m=24 and the second preimage attack has complexity 2^{106}.

NTNU
Innovation and Creativity

General overview how each of the design goals are achieved

5. To offer better than AES-GCM properties for preventing DoS attacks (CAESAR comparison with AES-GCM and Extra feature)

General overview how each of the design goals are achieved

- **This is achieved with the use of SMN.**
- **SMN is the first value that is decrypted.**
- **If there is a protocol that tells the receiver what is the next SMN value that it expects, then there is no need to continue with the decryption if decrypted SMN is not the same as the expected SMN.**

- **Much faster reaction by receiver**

5. To offer better than AES-GCM properties for preventing DoS attacks (CAESAR comparison with AES-GCM and Extra feature)

NTNU
Innovation and Creativity

General overview how each of the design goals are achieved

6. For certain parameters to offer the flexibility of tweakable (wide-block) encryption (that gives authentication too) (Extra feature)

General overview how each of the design goals are achieved

- **The default parameters for PiCipher are:**
  1. Word size 16, N=4 (internal state b=256 bits)
  2. Word size 32, N=4 (internal state b=512 bits)
  3. Word size 64, N=4 (internal state b=1024 bits)

6. For certain parameters to offer the flexibility of tweakable (wide-block) encryption (that gives authentication too) (Extra feature)

NTNU
Innovation and Creativity

General overview how each of the design goals are achieved

1.We can stretch the N parameter as it suits us:
For example for encrypting each physical sector of the Advanced HDD Format with size of 4 Kbytes:

Word size 64, N=256 (internal state b=8 KBytes)

6. For certain parameters to offe lock) encryption (that gives authentication too) (Extra featı

NTNU
Innovation and Creativity

General overview how each of the design goals are achieved

7. For certain parameters to be lightweight in HW, for other parameters to be fast in SW

NTNU
Innovation and Creativity

General overview how each of the design goals are achieved

Lightweight version: Word size 16, N=4 (internal state b=256 bits) ~ 5.5K GE (not that light, but we hope we will improve it)

Fast in SW version: Word size 64, N=4 (internal state b=1024 bits) (Non-SSE version 11 cpb)

7. For certain parameters to be lightweight in HW, for other parameters to be fast in SW

NTNU
Innovation and Creativity

Inside the permutation

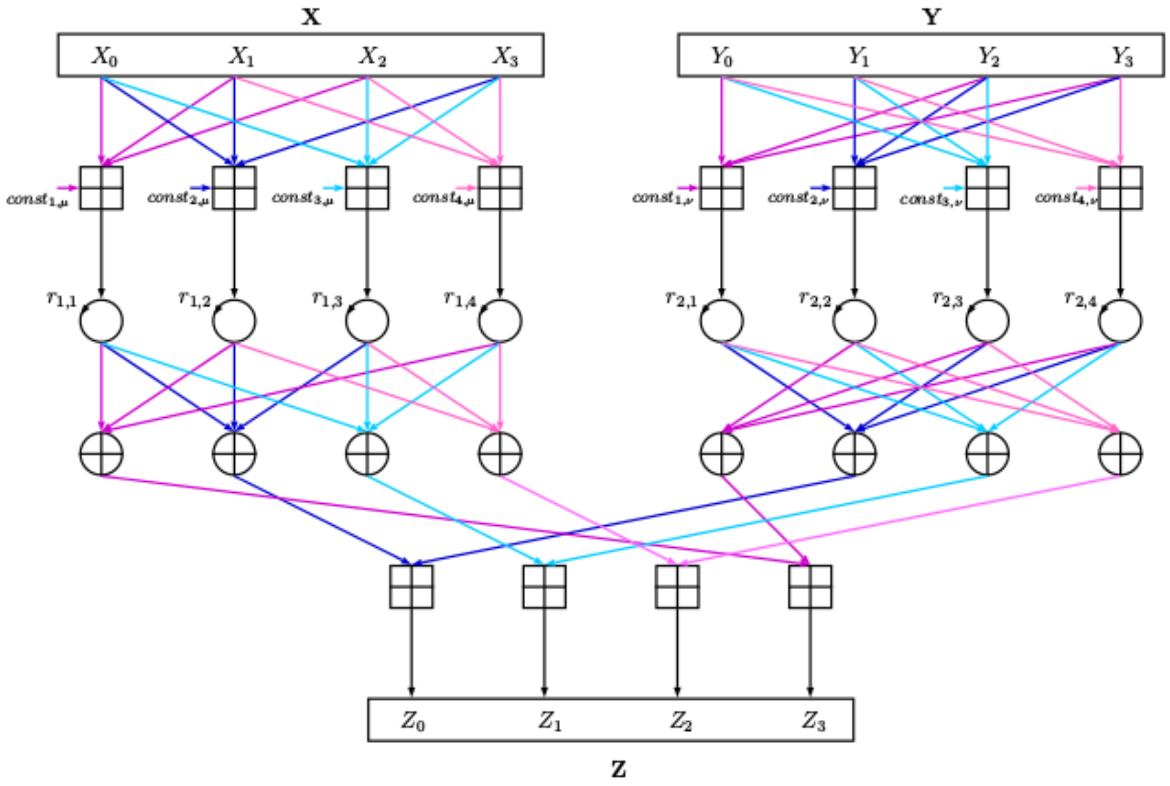


Fig. 7: Graphical representation of the ARX operation $*$.

Inside the permutation

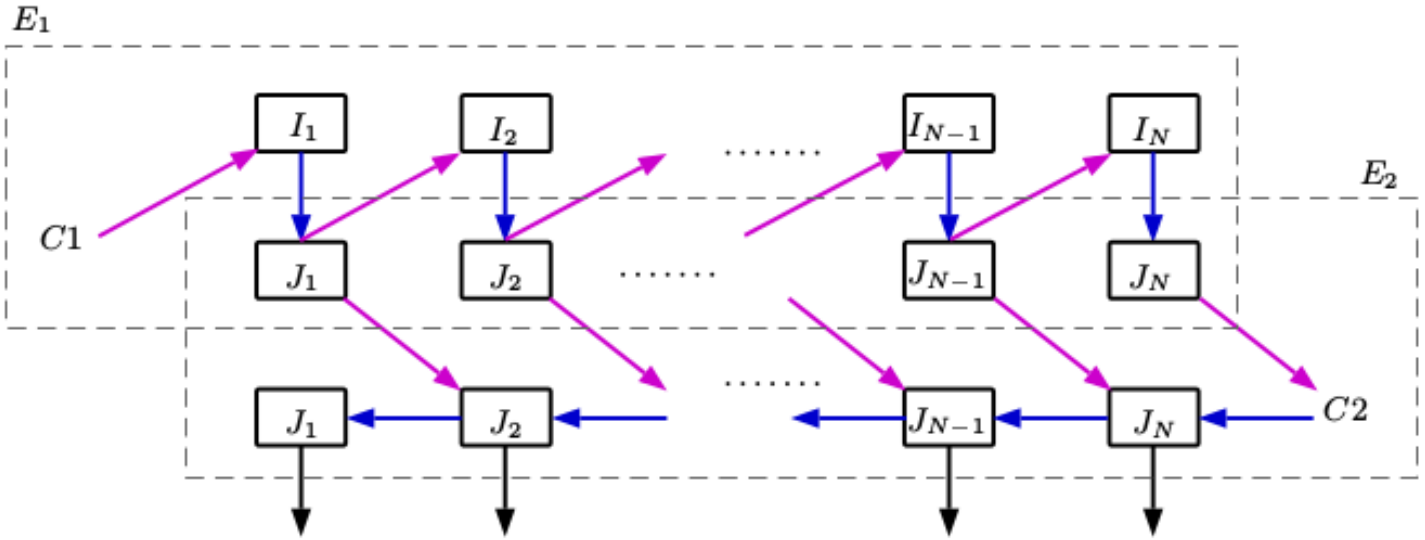


Fig. 8: One round of π-Cipher

Inside the permutation

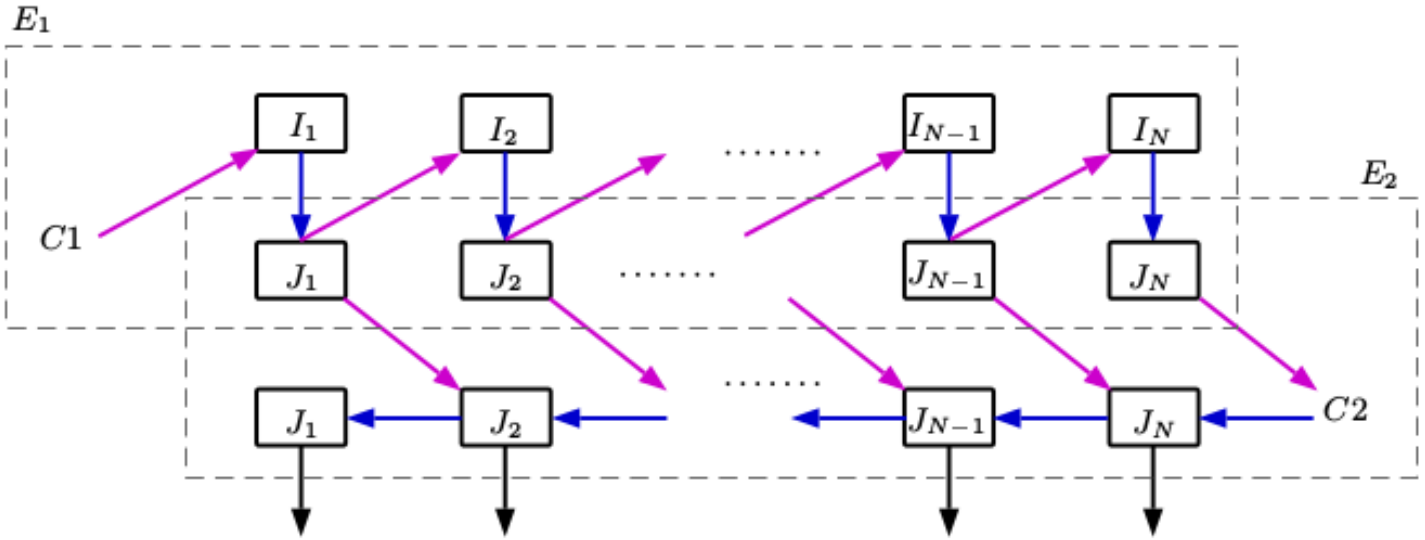


Fig. 8: One round of π-Cipher

Initial recommendation: 4 Rounds
Too conservative?
Soon we will submit for testing on SUPERCOP variants with 2 and 1 rounds.

NTNU
Innovation and Creativity

Security of PiCipher

- Since it is based on several solid cryptographic concepts
  - Encrypt-then-MAC principle,
  - XOR MAC scheme,
  - Two-pass sponge construction
- We hope that soon will have a security proof similar as the other sponge constructions (we are working on that)

NTNU
Innovation and Creativity

Security of PiCipher

- We have extensively tested the quality of used ARX permutation
- Even after one round, one bit difference introduced in the counter variable propagates in b/2 bits where b is the size of the internal state
- The number of variables that are collectively and bijectively transformed in the operation * is 4. This is making the operation * not so suitable for automatic ARX Tools that search for high probability differential characteristics (ARXTool, Gaetan Leurent)

NTNU
Innovation and Creativity

Conclusions

- In PiCipher we tried to bring novel ideas combined with solid concepts that have been confirmed and accepted by cryptographic community
- PiCipher has unique features such as massive and easy parallel capability, incrementality, a certain level of second tag preimage resistance, and a certain level of resistance if key, associated data and the public message number are repeatedly used (misused).

NTNU
Innovation and Creativity

Thank you for your attention!

NTNU
Innovation and Creativity