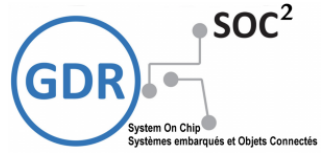
Implantation matérielle d'algorithmes de chiffrement authentifié sur FPGA

Roselyne CHOTIN

Sorbonne Université

1^{er} avril 2019



Agenda

Motivations

- Sécurité : enjeu majeur pour les objets communicants
  → Besoins en matériel pour assurer la sécurité
- Nécessité d'assurer la confidentialité, l'intégrité et l'authenticité des données : chiffrement + hachage
  → Besoin d'intégrer les deux
- Compétition CAESAR (résultats 20/02/2019)
  - Portefeuille d'algorithmes pour le chiffrement authentifié
  - Avec implantation matérielle

  → Besoin de prototyper/explorer rapidement vers FPGA et ASIC

Thèse Karim Abdellatif, CEA-DAM, 2014

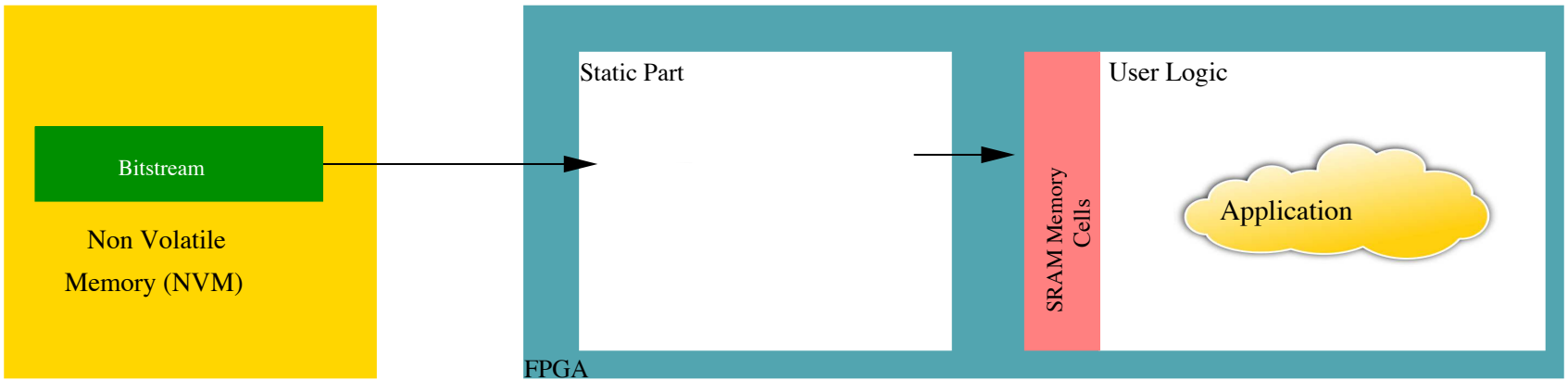
Motivations

- Sécurité : enjeu majeur pour les objets communicants
  - → Besoins en matériel pour assurer la sécurité
- Nécessité d'assurer la confidentialité, l'intégrité et l'authenticité des données : chiffrement + hachage
  - → Besoin d'intégrer les deux
- Compétition CAESAR (résultats 20/02/2019)
  - Portefeuille d'algorithmes pour le chiffrement authentifié
  - Avec implantation matérielle
  - → Besoin de prototyper/explorer rapidement vers FPGA et ASIC

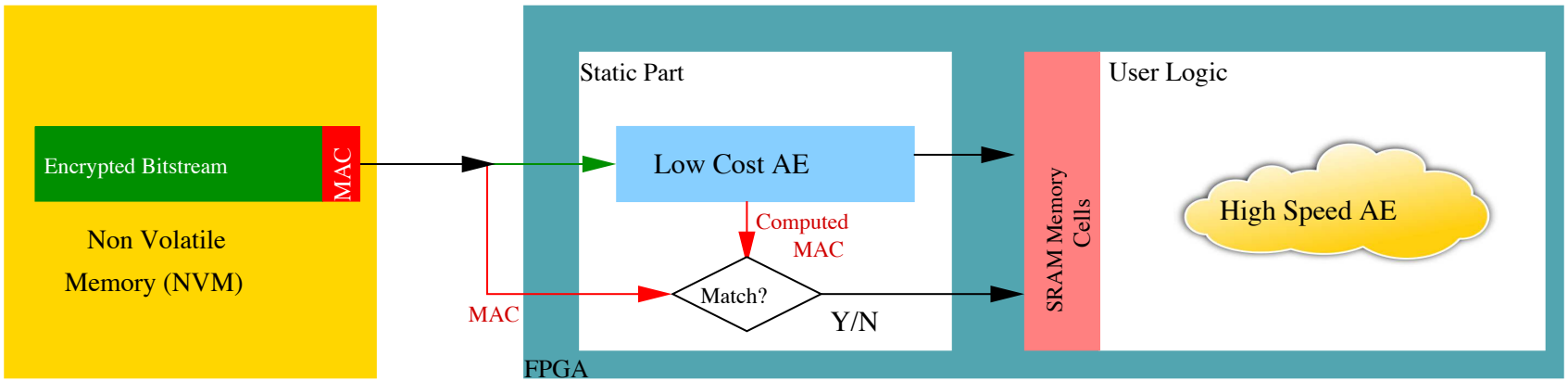
Besoin d'efficacité (taille, débit, consommation)

Thèse Karim Abdellatif, CEA-DAM, 2014

Sécurité dans les FPGAs

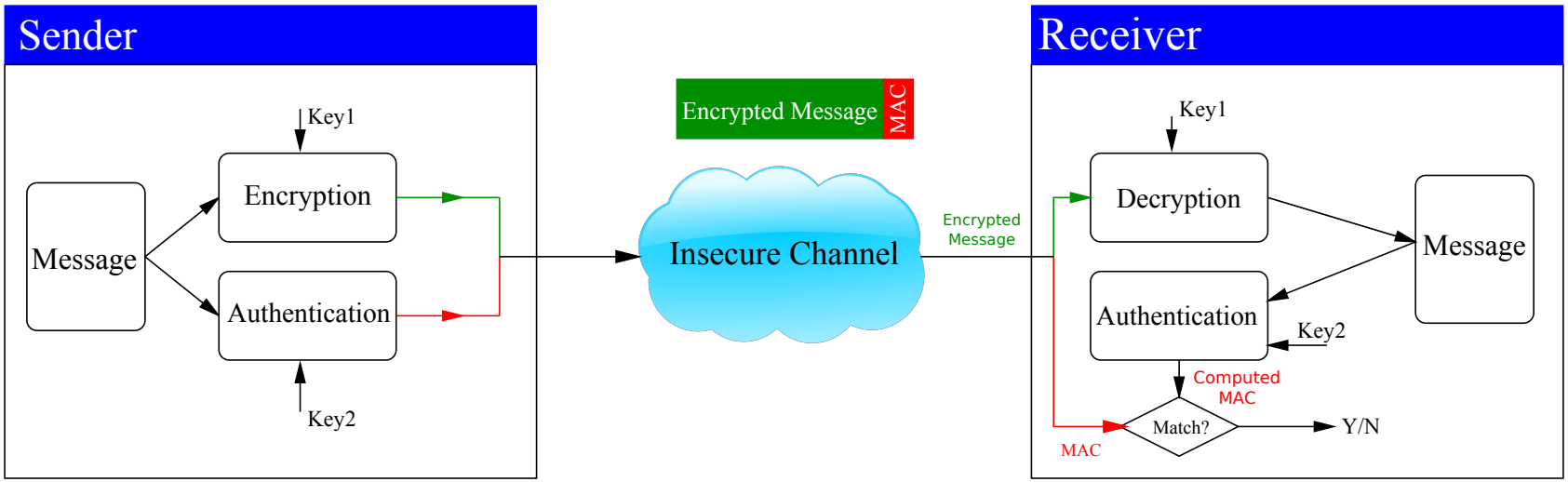


Sécurité dans les FPGAs

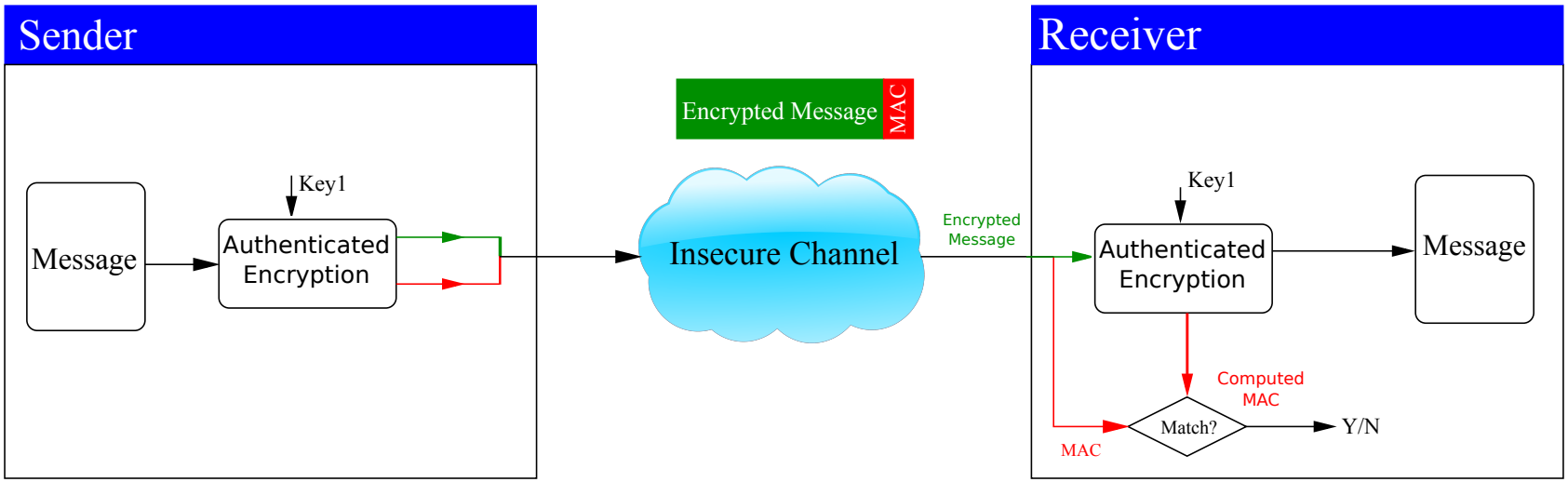


Agenda

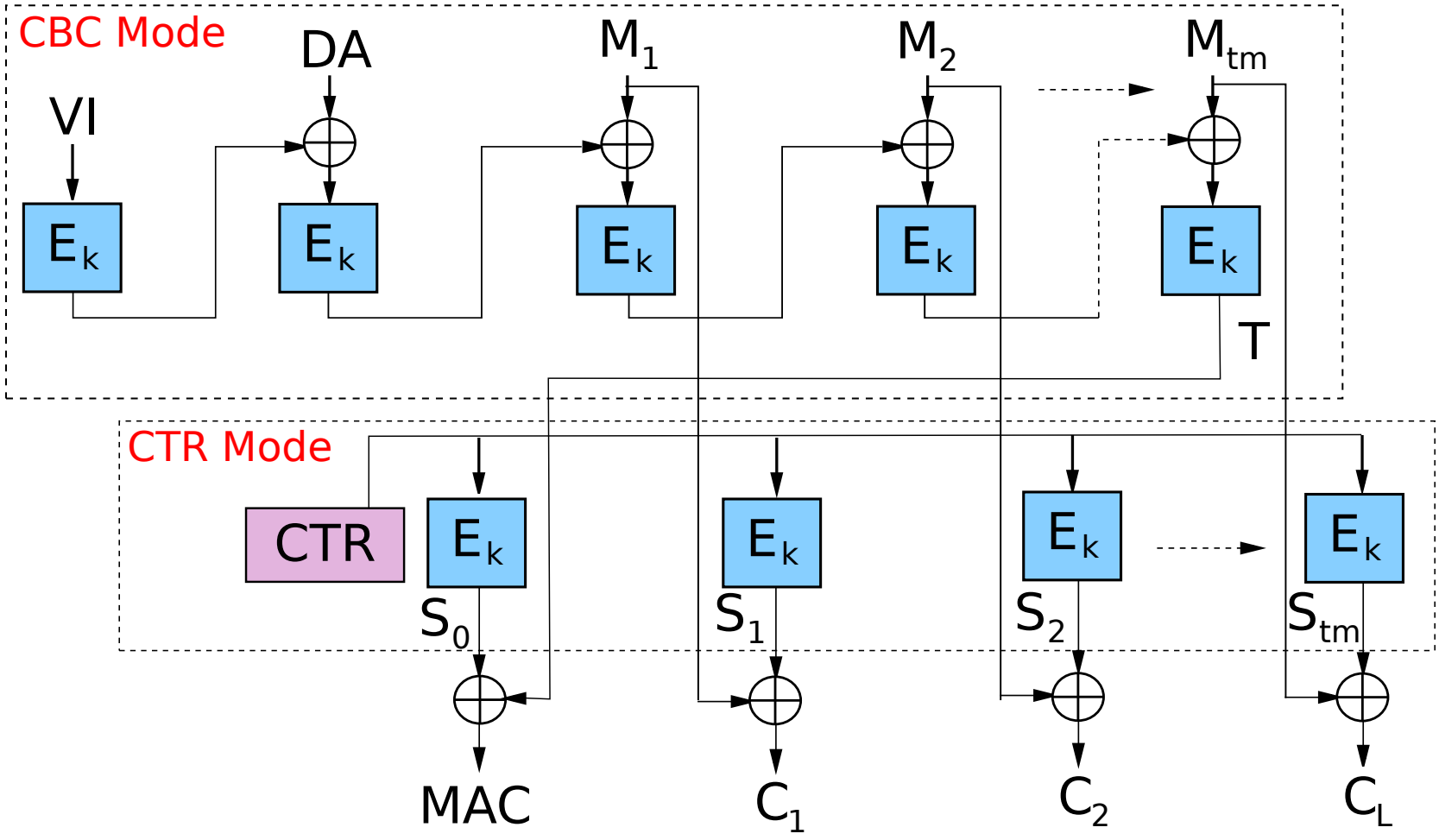
Principe du chiffrement authentifié



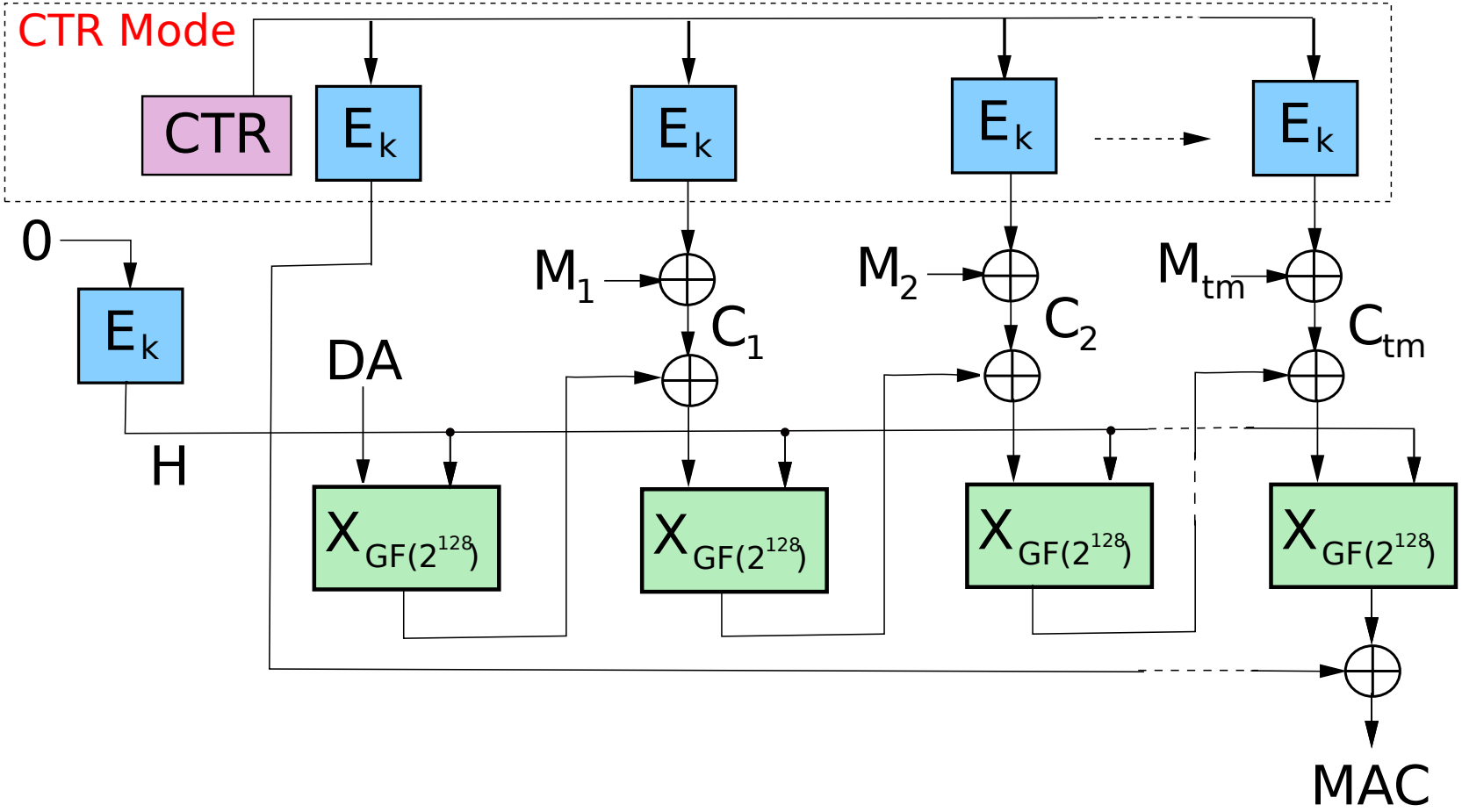
Principe du chiffrement authentifié



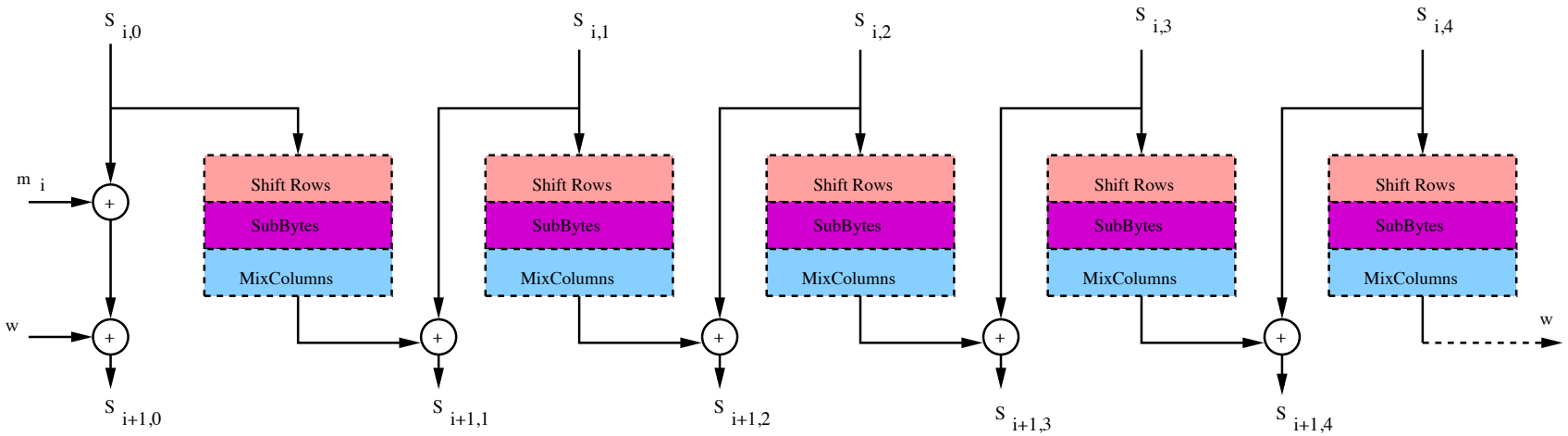
Algorithmes : Counter with Cipher block chaining Message authentication code (CCM)



Algorithmes : Galois Counter Mode (GCM)



Algorithmes : AEGIS



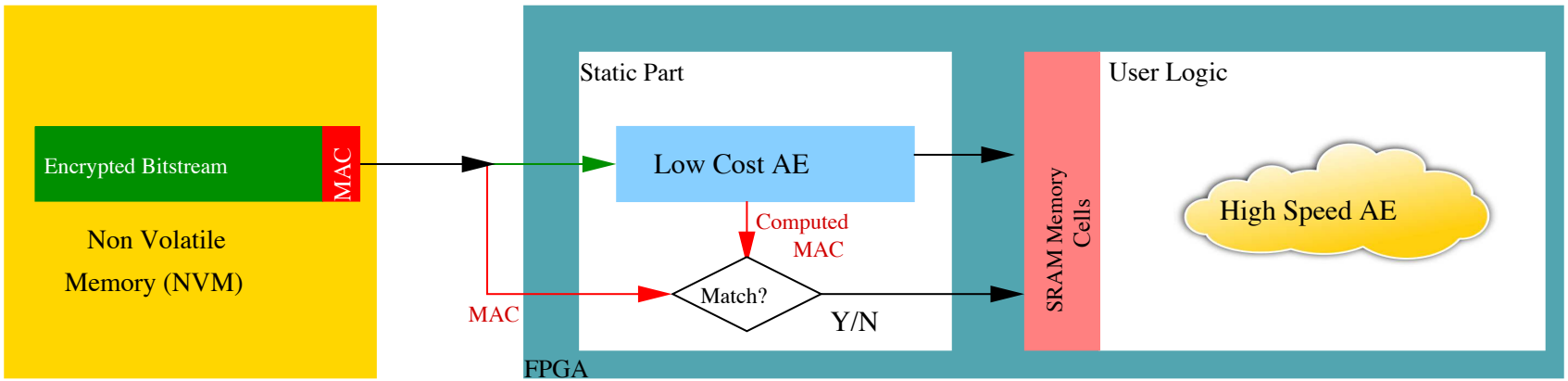
Agenda

Méthodologie suivie

- Au niveau des algorithmes
  - Amélioration de l'existant : AES-CCM, AES-GCM[1]
  - Nouvel algorithme AEGIS[2] participant à la compétition
- Environnement d'exploration
  - Utilisation des IPs de crypto
  - Evaluation des solutions
  - Raffinement
- Répondre aux contraintes d'utilisation
  - Débit important (FPGA)
  - Faible encombrement (ASIC)

[1] Algorithmes recommandés par le NIST
[2] H. Wu et B. Preneel. *AEGIS : A Fast Authenticated Encryption Algorithm* SAC 2013

Sécurité dans les FPGAs

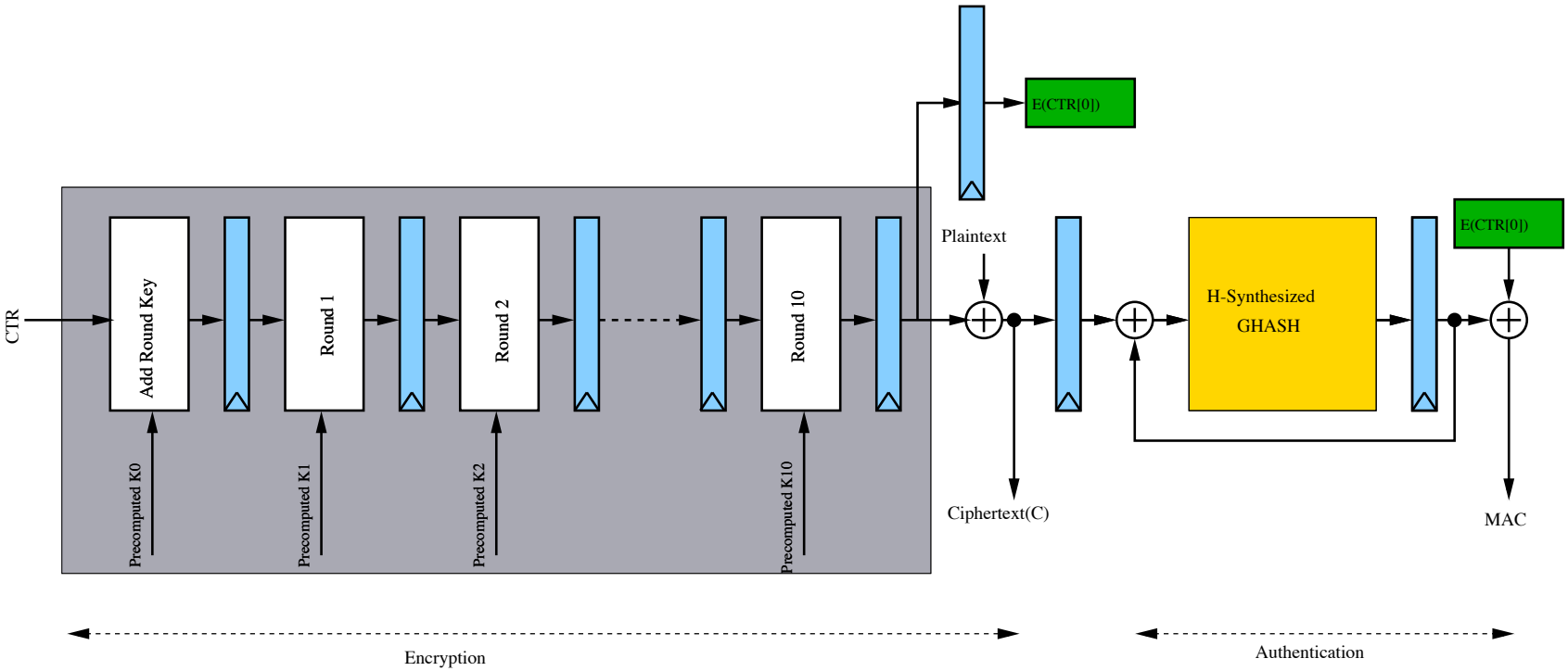


Architectures haut-débit sur FPGA

- Plusieurs réalisations de la fonction SubByte : RAM, LUT, arithmétique sur $GF(2^8)$

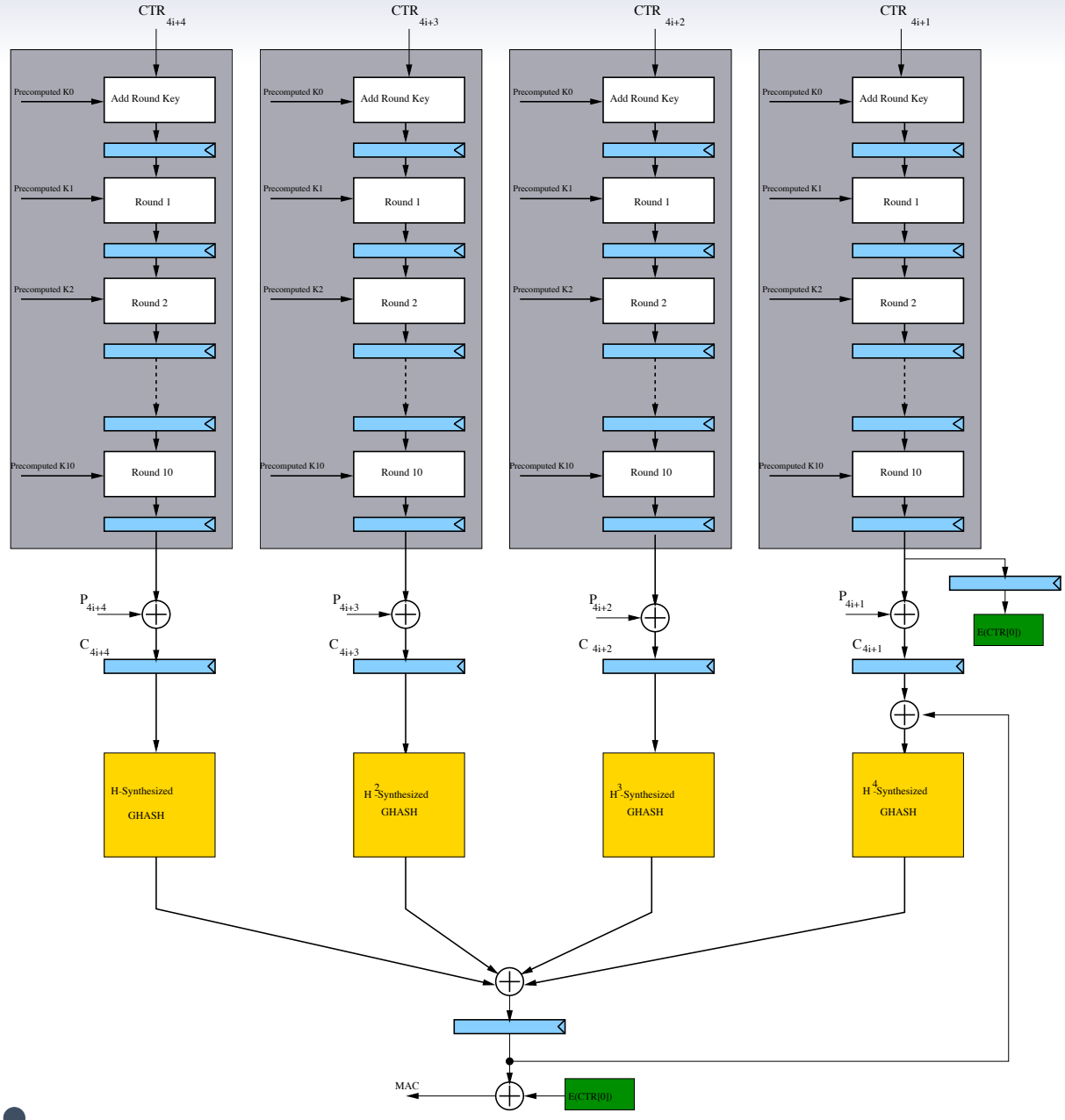
Architectures haut-débit sur FPGA

- Plusieurs réalisations de la fonction SubByte : RAM, LUT, arithmétique sur $GF(2^8)$
- La clé est synthétisée pour être embarquée dans le matériel
  - Simplification de l'AES
  - Simplification du multiplieur sur $GF(2^{128})$ (H constant)
  - Pour des applications reconfigurables avec peu de changements de clé


CTR
Add Round Key
Round 1
Round 2
Round 10
Precomputed K0
Precomputed K1
Precomputed K2
Precomputed K10
E(CTR[0])
Plaintext
Ciphertext(C)
H-Synthesized
GHASH
E(CTR[0])
MAC
Encryption
Authentication

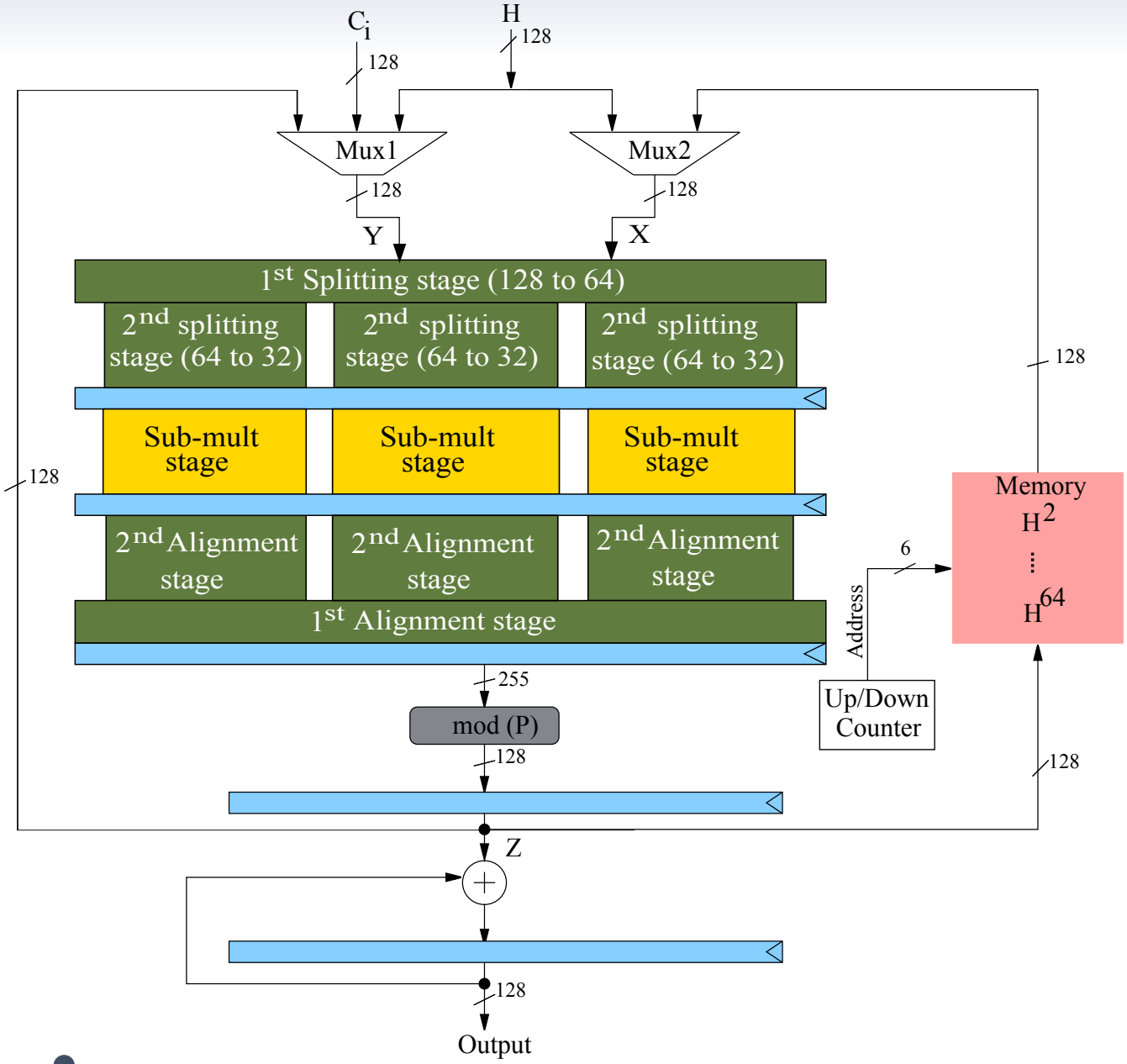
Architectures haut-débit sur FPGA

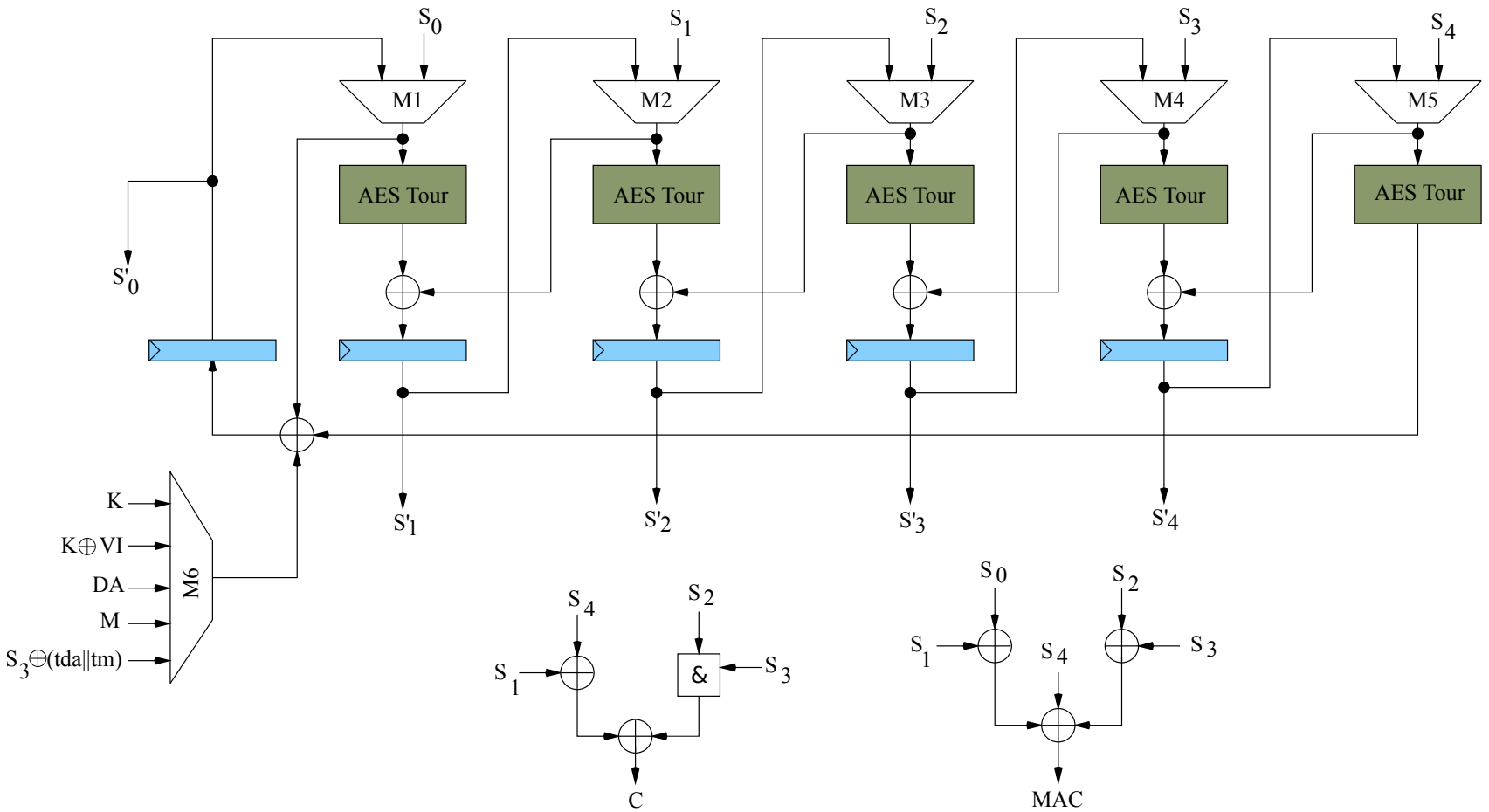
- Plusieurs réalisations de la fonction SubByte : RAM, LUT, arithmétique sur $GF(2^8)$
- La clé est synthétisée pour être embarquée dans le matériel
  - Simplification de l'AES
  - Simplification du multiplieur sur $GF(2^{128})$ (H constant)
  - Pour des applications reconfigurables avec peu de changements de clé
- Plusieurs opérateurs en parallèle


CTR 4i+4
CTR 4i+3
CTR 4i+2
CTR 4i+1
Precomputed K0
Add Round Key
Precomputed K1
Round 1
Precomputed K2
Round 2
Precomputed K10
Round 10
P 4i+4
P 4i+3
P 4i+2
P 4i+1
C 4i+4
C 4i+3
C 4i+2
C 4i+1
E(CTR[0])
H-Synthesized GHASH
H 2 -Synthesized GHASH
H 3 -Synthesized GHASH
H 4 -Synthesized GHASH
MAC
E(CTR[0])

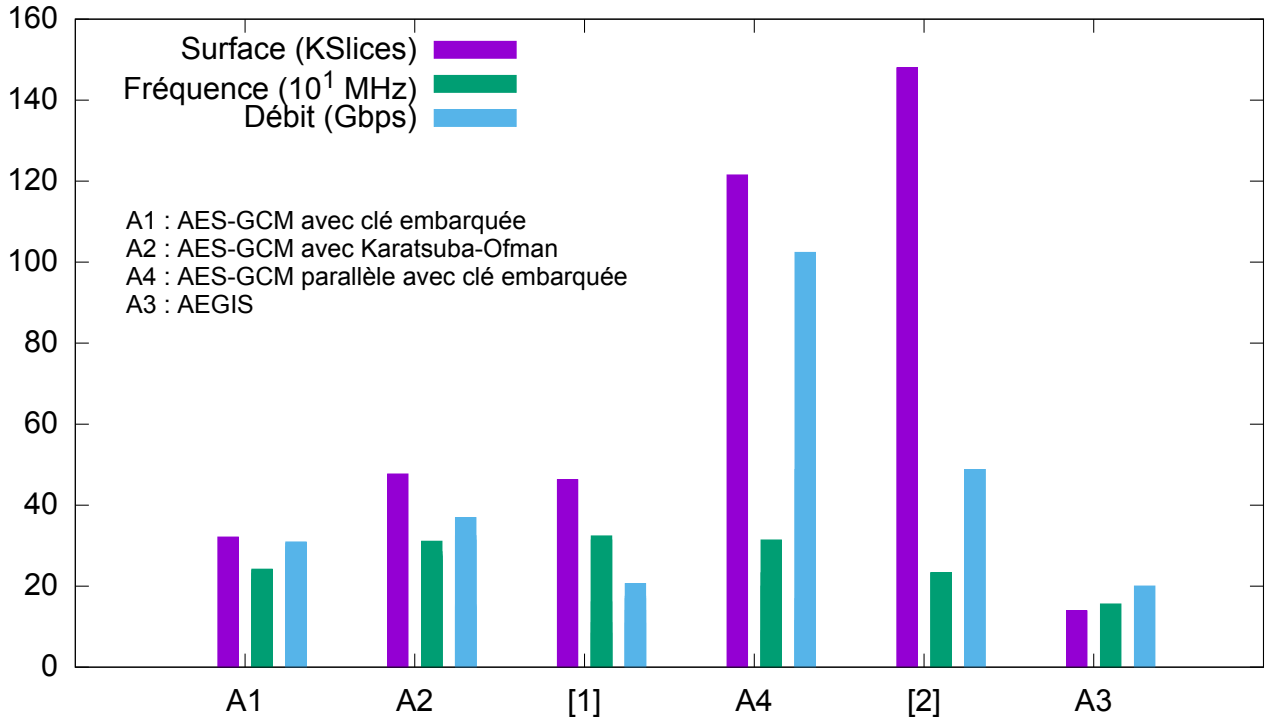
Architectures haut-débit sur FPGA

- Plusieurs réalisations de la fonction SubByte : RAM, LUT, arithmétique sur $GF(2^8)$
- La clé est synthétisée pour être embarquée dans le matériel
  - Simplification de l'AES
  - Simplification du multiplieur sur $GF(2^{128})$ (H constant)
  - Pour des applications reconfigurables avec peu de changements de clé
- Plusieurs opérateurs en parallèle
- Algorithme de Karatsuba-Ofman pour simplifier la multiplication
  - 1 multiplication sur n bits est remplacée par 3 multiplications sur $\frac{n}{2}$ bits


Ci
128
H
128
Mux1
Mux2
128
128
Y
X
1st Splitting stage (128 to 64)
2nd splitting stage (64 to 32)
2nd splitting stage (64 to 32)
2nd splitting stage (64 to 32)
Sub-mult stage
Sub-mult stage
Sub-mult stage
2nd Alignment stage
2nd Alignment stage
2nd Alignment stage
1st Alignment stage
128
128
128
6
Address
Memory
H2
H64
Up/Down Counter
255
mod (P)
128
Z
128
Output


S0
S1
S2
S3
S4
M1
M2
M3
M4
M5
AES Tour
AES Tour
AES Tour
AES Tour
AES Tour
S'0
S'1
S'2
S'3
S'4
K
K⊕VI
DA
M
S3⊕(tda||tm)
M6
S4
S2
S1
&
S3
C
S0
S2
S1
S4
S3
MAC

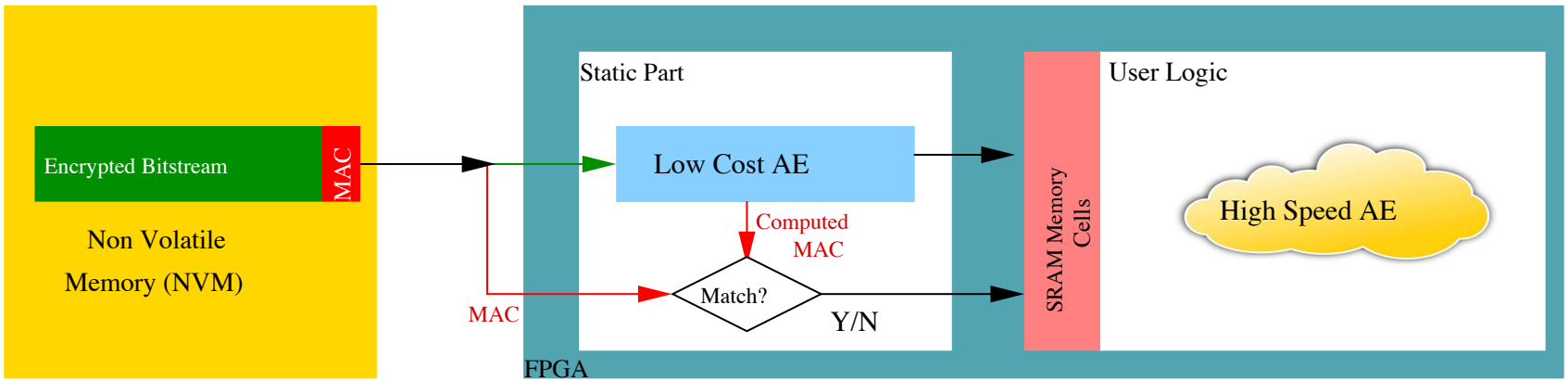
Résultats implantation LUTs



[1] Zhou et al. *Improving Throughput of AES-GCM with Pipelined Karatsuba Multipliers on FPGAs*, ARC 2009
[2] Henzen et al. *FPGA Parallel-Pipelined AES-GCM Core for 100G Ethernet Applications*, ESSCIRC 2010

Abdellatif et al., *AES-GCM and AEGIS : Efficient and High Speed Hardware Implementations*, Journal of Signal Processing Systems 2016

Sécurité dans les FPGAs



Protection du bitstream

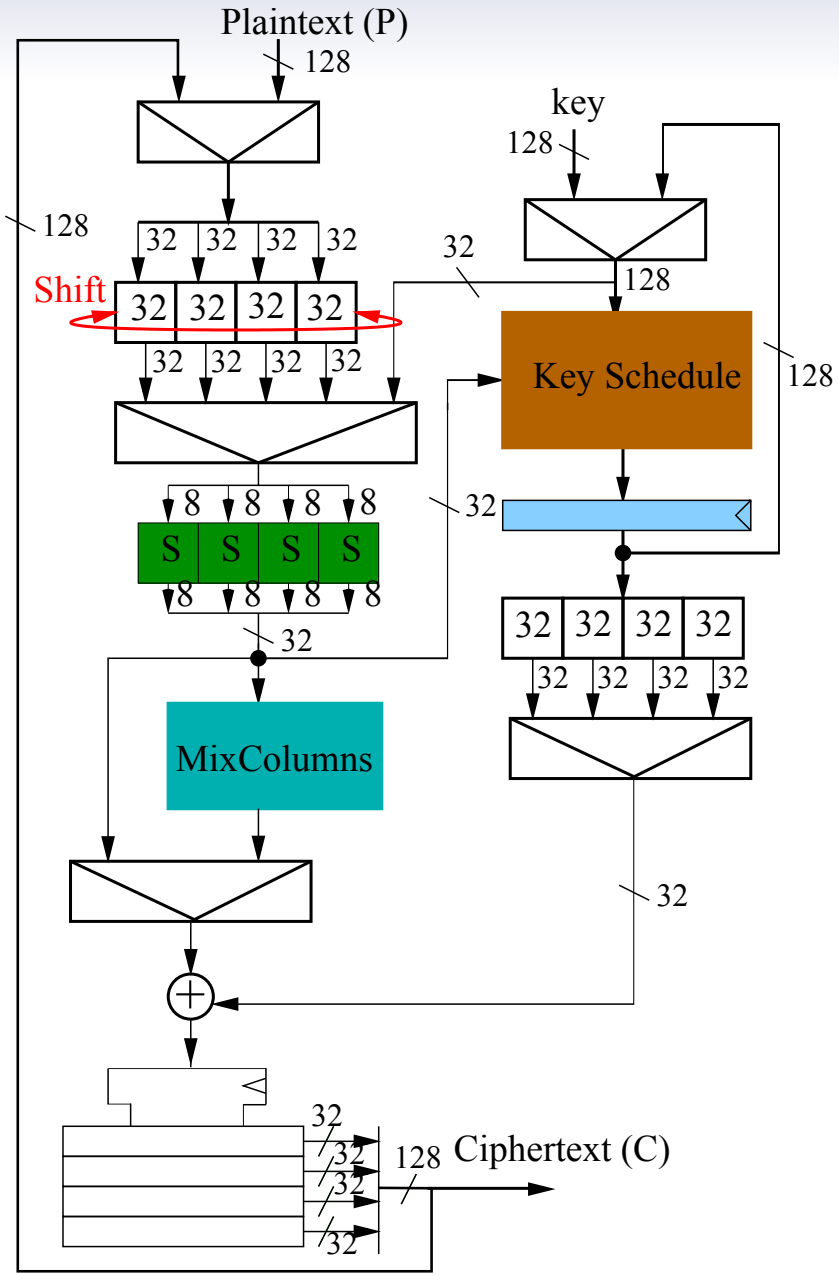
- Contre la copie, le *reverse engineering* et la falsification.
- Encombrement minimal dans la partie statique (ASIC)
- Préservation du débit de chargement et de la fréquence du FPGA

Protection du bitstream

- Contre la copie, le *reverse engineering* et la falsification.
- Encombrement minimal dans la partie statique (ASIC)
- Préservation du débit de chargement et de la fréquence du FPGA

Solution

- Réduction du chemin de données à 32 bits
- Maintient débit et fréquence du FPGA
- Séquencement adéquat des données


Plaintext (P)
128
key
128
128
32 32 32 32
32
Shift
32 32 32 32
128
32 32 32 32
Key Schedule
128
8 8 8 8
32
S S S S
8 8 8 8
32
32 32 32 32
32 32 32 32
MixColumns
32
32
128
Ciphertext (C)

Résultats d'implantation ASIC

Archi	Techno nm	Taille mm^2	Fréquence MHz	Débit Mbps
AES-CCM	90	0.045	150	192
[1] AES-CCM	90	0.057	148	434
AES-GCM	90	0.066	150	384
[1] AES+HMAC	90	0.183	101.2	1293
AEGIS	90	0.062	150	960

[1] M. M. Parelkar. *Authenticated encryption in hardware*, Thèse de doct. George Mason University, 2005.

Abdellatif et al., *Low cost Solutions for Secure Remote Reconfiguration of FPGAs*, IJES : International Journal of Embedded Systems 2014

Agenda

Conclusion

- Architectures matérielles efficaces de chiffrement authentifié
  - Pour protéger les transmissions haut-débit
  - Pour protéger la transmission du *bistream*
- Travaux en cours
  - Bibliothèque d'IPs pour la sécurité (extension clé publique)
  - Protection contre les attaques par canaux auxiliaires ou les chevaux de Troie
- A plus long terme : méthodologie de conception intégrant la sécurité
  - Evaluer la sécurité (métriques)
  - Proposer des protections
  - Intégrer cela dans le flot de conception

Questions ?