AEGIS-Based Efficient Solution for Secure Reconfiguration of FPGAs

Karim M. Abdellatif, Roselyne Chotin-Avot, Habib Mehrez

karim.abdellatif@emse.fr

Motivation

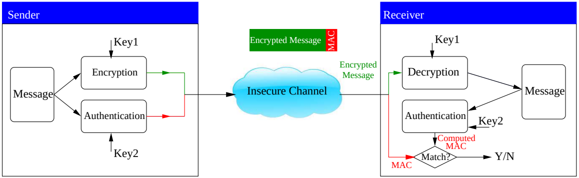
Authenticated Encryption (AE) algorithms

Low Cost Solutions for Secure FPGA Reconfiguration

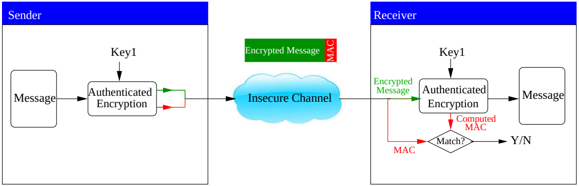
Conclusion and future work

Encryption and authentication

- First approach



- Second approach



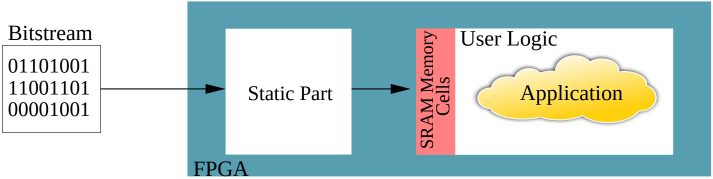
Advantages and applications of the second approach

- One can expect that this is more efficient since encryption and authentication can share a part of the computation.
- AE algorithms use only one key for encryption and authentication. Therefore, the key exchange and storage issues are better compared to using two separated algorithms.

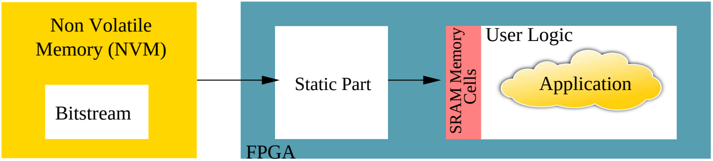
AE has been used in many widely standards such as:
Secure Sockets Layer / Transport Layer Security (SSL/TLS) [7], IPsec [7], and IEEE 802.11 (Wi-Fi) [10].

FPGAs

- They offer the capability to develop the most suitable circuit architecture of the application in a similar way to SoC systems.
- They are cost efficient, easier to manage, can immediately be put into operation and, they can continuously be reprogrammed during and after the design.



Reconfiguration FPGAs



IPs loaded on the FPGAs represent a kind of investment that requires protection.

Motivation

Authenticated Encryption (AE) algorithms

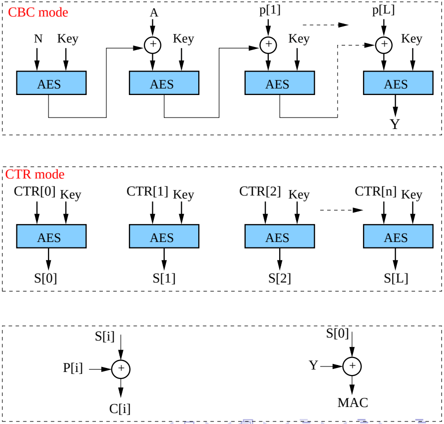
Low Cost Solutions for Secure FPGA Reconfiguration

Conclusion and future work

Counter with Cipher Block Chaining-Message Authentication Code(CCM)

CCM has been specified in:

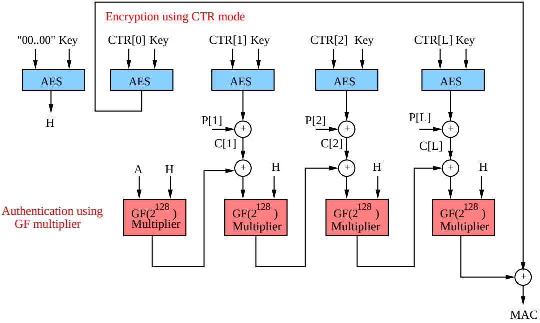
- IEEE 802.11i
- IEEE 802.15
- IEEE 802.16
- Disadvantages:
  It is not suitable for on line applications as all data must be stored in memory before CCM processing.



Galois Counter Mode (GCM)

It presets high intrinsic degree of pipelining and parallelism.

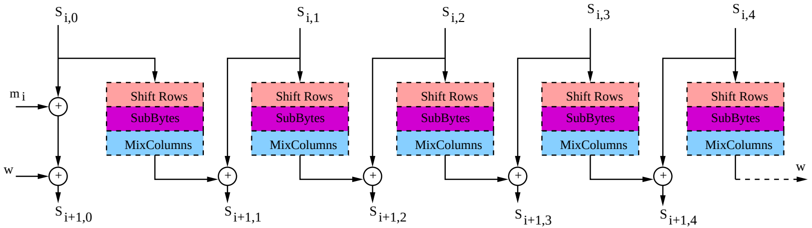
- wireless, optical, and magnetic recording systems.
- high intrinsic degree of pipelining and parallelism.
- IEEE 802.1ae and NIST 800-38D.



Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR)

- CAESAR competition is a move towards selecting a portfolio of AE schemes that should improve upon the state of the art.
- There are some AE schemes have been proposed, and more are expected to join the ranks with the ongoing CAESAR.
- we present an overview on AEGIS [36] which is considered one of the candidates to CAESAR.

AEGIS-128



$$
\begin{aligned}
S_{i+1,0} &= AESRound(S_{i,4}, S_{i,0} \oplus m_i) \\
S_{i+1,1} &= AESRound(S_{i,0}, S_{i,1}) \\
S_{i+1,2} &= AESRound(S_{i,1}, S_{i,2}) \\
S_{i+1,3} &= AESRound(S_{i,2}, S_{i,3}) \\
S_{i+1,4} &= AESRound(S_{i,3}, S_{i,4}).
\end{aligned} \tag{1}
$$

Initialization of AEGIS

1. Load the key and IV into the state as follows:

$$
\begin{aligned}
S_{-10,0} &= IV_{128} \\
S_{-10,1} &= Const1 \\
S_{-10,2} &= Const0 \\
S_{-10,3} &= K_{128} \oplus Const0 \\
S_{-10,4} &= K_{128} \oplus Const1.
\end{aligned}
$$

2. For i = -5 to -1, $m_{2i} = K_{128}$, $m_{2i+1} = K_{128} \oplus IV_{128}$.
3. For i = -10 to -1, $S_{i+1} = StateUpdate128(S_i, m_i)$.

Encryption of AEGIS

1. If the last plaintext block is not a full block, use 0 bits to pad it to 128 bits.
2. For i = 0 to $(\frac{msglen}{128} - 1)$, the state is updated to perform encryption.

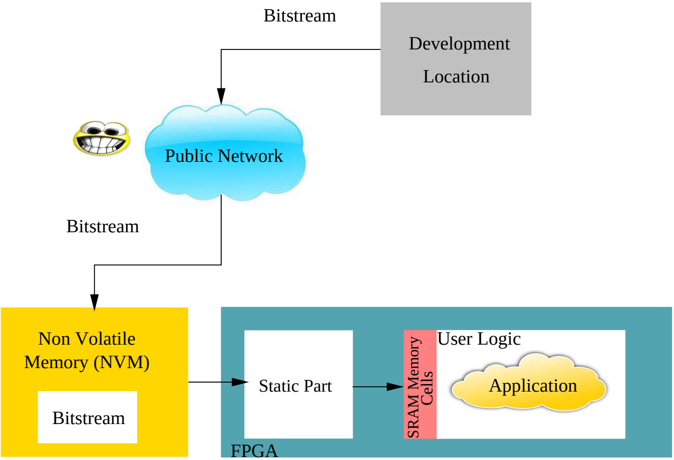
$$\begin{aligned} C_i &= P_i \oplus S_{i,1} \oplus S_{i,4} \oplus (S_{i,2} \& S_{i,3}) \\ S_{i+1} &= StateUpdate128(S_i, P_i). \end{aligned} \tag{2}$$

Authentication of AEGIS

1. Let $tmp = lenA \| msglen$, where lenA and msglen are represented as 64-bit integers
2. For i= $(\frac{msglen}{128})$ to $(\frac{msglen}{128} + 6)$, $m_i = S_{\frac{msglen}{128},3} \oplus tmp$
3. For i= $(\frac{msglen}{128})$ to $(\frac{msglen}{128} + 6)$, the state is updated: $S_{i+1} = StateUpdate128(S_i, P_i)$
4. The authentication MAC is generated from the state $\frac{msglen}{128} + 7$ as follows:

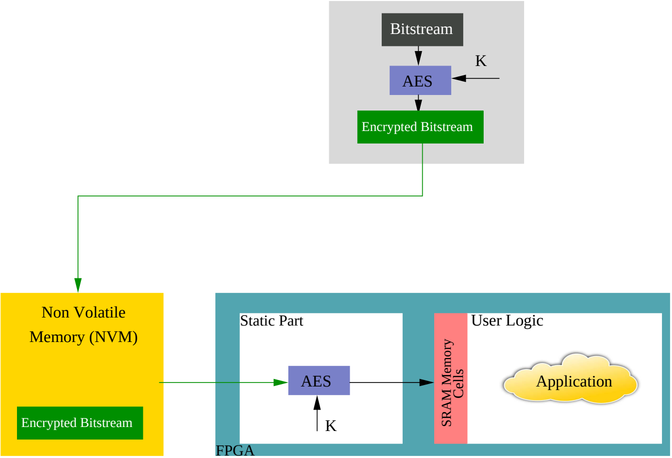
$$MAC = \oplus_{i=0}^{4}(S_{(\frac{msglen}{128}+7),i}). \quad (3)$$

Remote reconfiguration



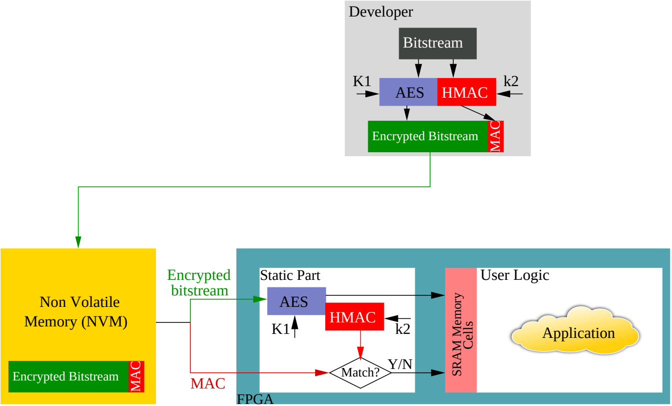
Previous Solutions

Example: Virtex-4 and Virtex-5:

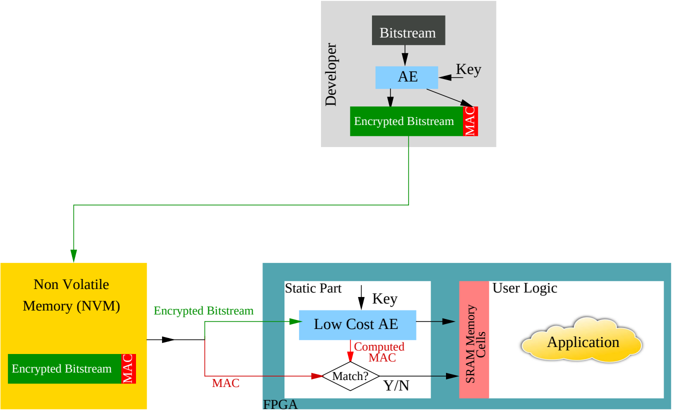


Previous Solutions

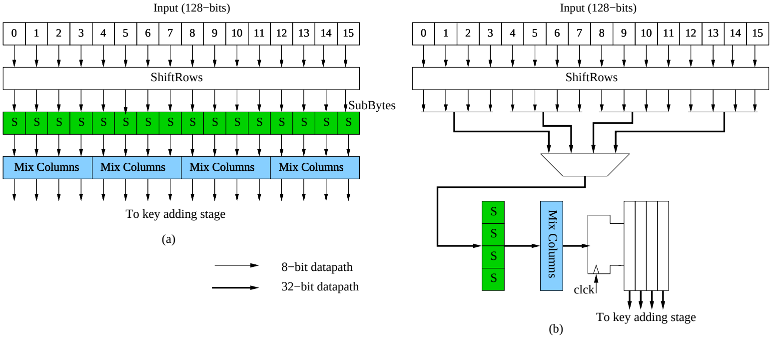
Example: Virtex-6



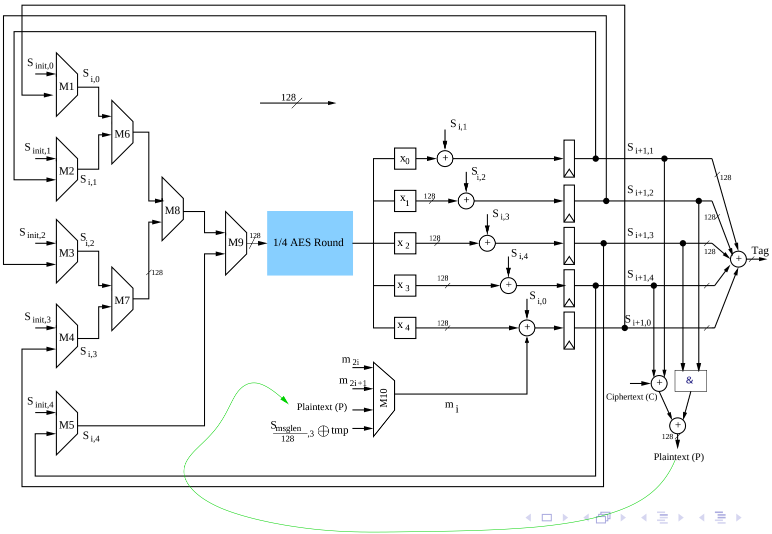
Our goal


Developer
Bitstream
AE
Key
Encrypted Bitstream
MAC
Non Volatile
Memory (NVM)
Encrypted Bitstream
MAC
Encrypted Bitstream
MAC
Static Part
Key
Low Cost AE
Computed
MAC
Match?
Y/N
SRAM Memory
Cells
User Logic
Application
FPGA

Proposed AEGIS-128



Proposed AEGIS-128



Hardware comparison

Design	Architecture	Technology	Area mm^2	Memory	Frequency MHz	Throughput Mbps	Function
This work	AES-CCM	90 nm	0.045	Yes	150	192	Decryption and authentication
This work	AES-GCM	90 nm	0.066	No	150	384	Decryption and authentication
This work	AEGIS-128	90 nm	0.062	No	150	960	Decryption and authentication
This work	AES-CCM	65 nm	0.023	Yes	150	192	Decryption and authentication
This work	AES-GCM	65 nm	0.034	No	150	384	Decryption and authentication
This work	AEGIS-128	65 nm	0.032	No	150	960	Decryption and authentication
[53]	AES	110 nm	0.099	No	222.2	526.7	Encryption/Decryption
[25]	AES-CCM	90 nm	0.057	Yes	148	434	Encryption and authentication
[25]	AES+HMAC	90 nm	0.183	No	101.2	1293	Encryption and authentication
[54]	Skein-1c	90 nm	0.064	No	286	1018	Authentication
[54]	Blake	90 nm	0.191	No	96	4475	Authentication

Conclusion

- Giving an overview of security issues used in the reconfiguration of FPGAs.
- Analyzing how well encryption and authentication are very important for trusted designs on FPGAs.
- Proposing an efficient hardware solution using AEGIS, which is added in the static part of the FPGA (silicon part) in order to decrypt and authenticate encrypted bitstream.