Confidentiality and integrity of FPGA bitstreams

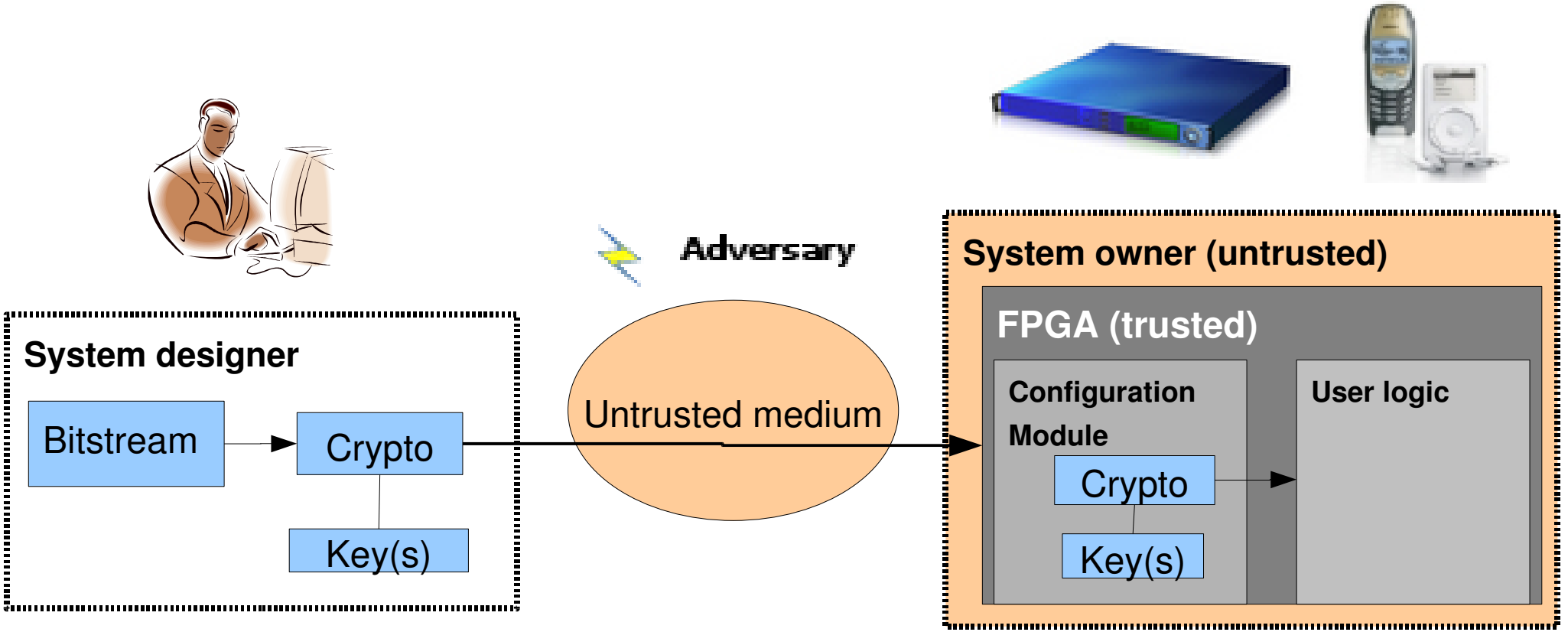
Benoît Badrignans, LIRMM / NETHEOS
Reouven Elbaz, Princeton University
David Champagne, Princeton University
Lionel Torres, LIRMM

Outline

- Security model
- State of the art
- Secure Update Mechanism (SUM)
- Conclusion / perspectives

Context

- FPGA based system for secure applications requiring remote upgrade
- Three parties : FPGA Vendor , System Designer (SD) , System owner



- Attacker can read/modify/inject bitstream (on the untrusted medium or at board level)

Threats over bitstream	Impact on FPGA design	Generic Solution	FPGA vendors solution	
			SRAM[1]	ACTEL
Unauthorized reads	Cloning / IP theft	Encryption	AES (128 / 256)	

[1]*SRAM : SRAM based FPGAs (Xilinx, Altera, Lattice)*

Threats over bitstream	Impact on FPGA design	Generic Solution	FPGA vendors solution	
			SRAM[1]	ACTEL
Unauthorized reads	Cloning / IP theft	Encryption	AES (128 / 256)	
Tampering / spoofing	Design modification	Authentication / integrity	CBC [2] + CRC [3]	AES based MAC[4]

[1]SRAM : SRAM based FPGAs (Xilinx, Altera, Lattice)

[2]CBC : Cipher Block Chaining : block cipher mode of operation

[3]CRC : Cyclic Redundancy Check

[4]MAC : Message Authentication Code

Threats over bitstream	Impact on FPGA design	Generic Solution	FPGA vendors solution	
			SRAM[1]	ACTEL
Unauthorized reads	Cloning / IP theft	Encryption	AES (128 / 256)	
Tampering / spoofing	Design modification	Authentication / integrity	CBC [2] + CRC [3]	AES based MAC [4]
Old bitstream replays	System downgrade	Unique time-stamp / Non-volatile state	X	X

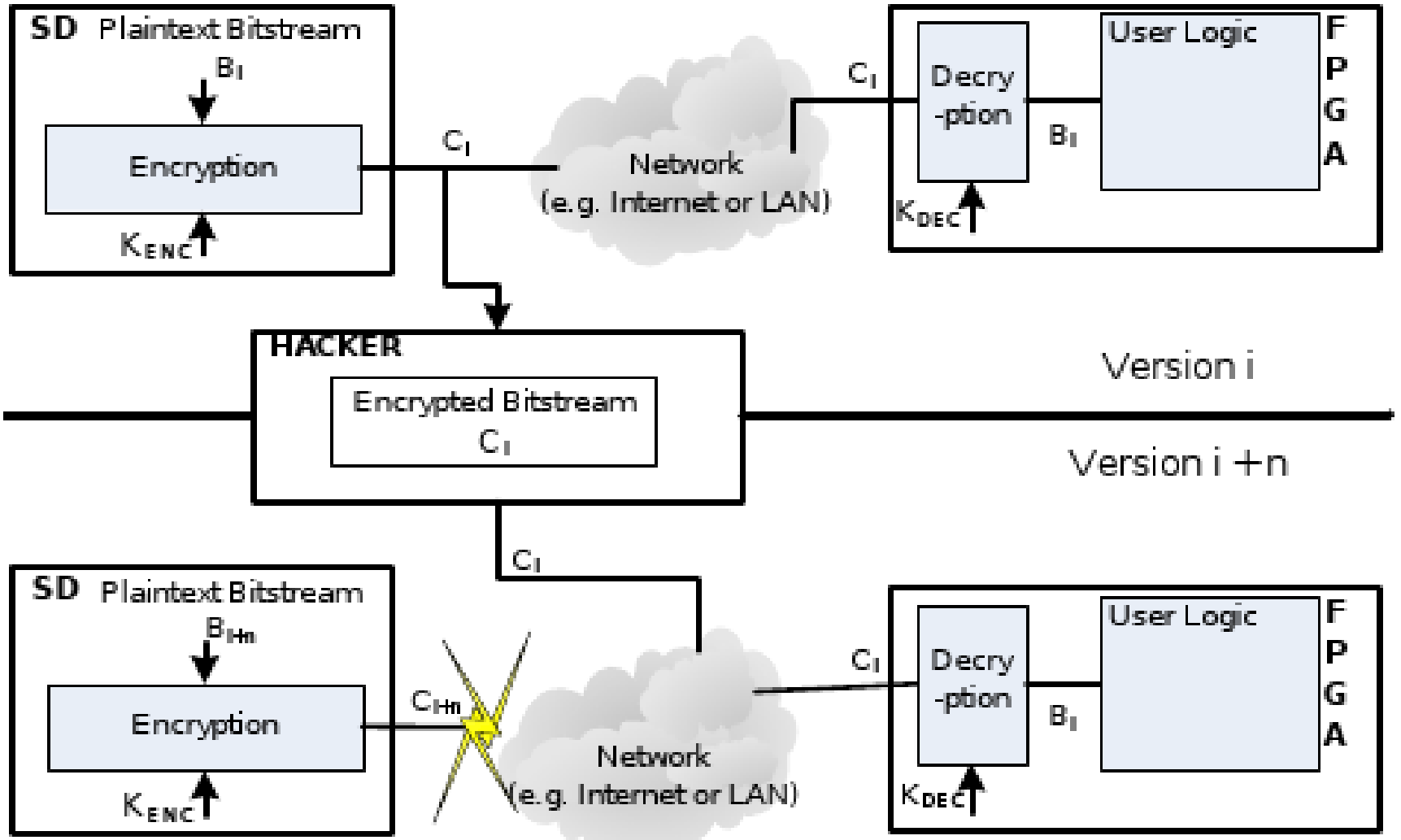
[1]SRAM : SRAM based FPGAs (Xilinx, Altera, Lattice)

[2]CBC : Cipher Block Chaining : block cipher mode of operation

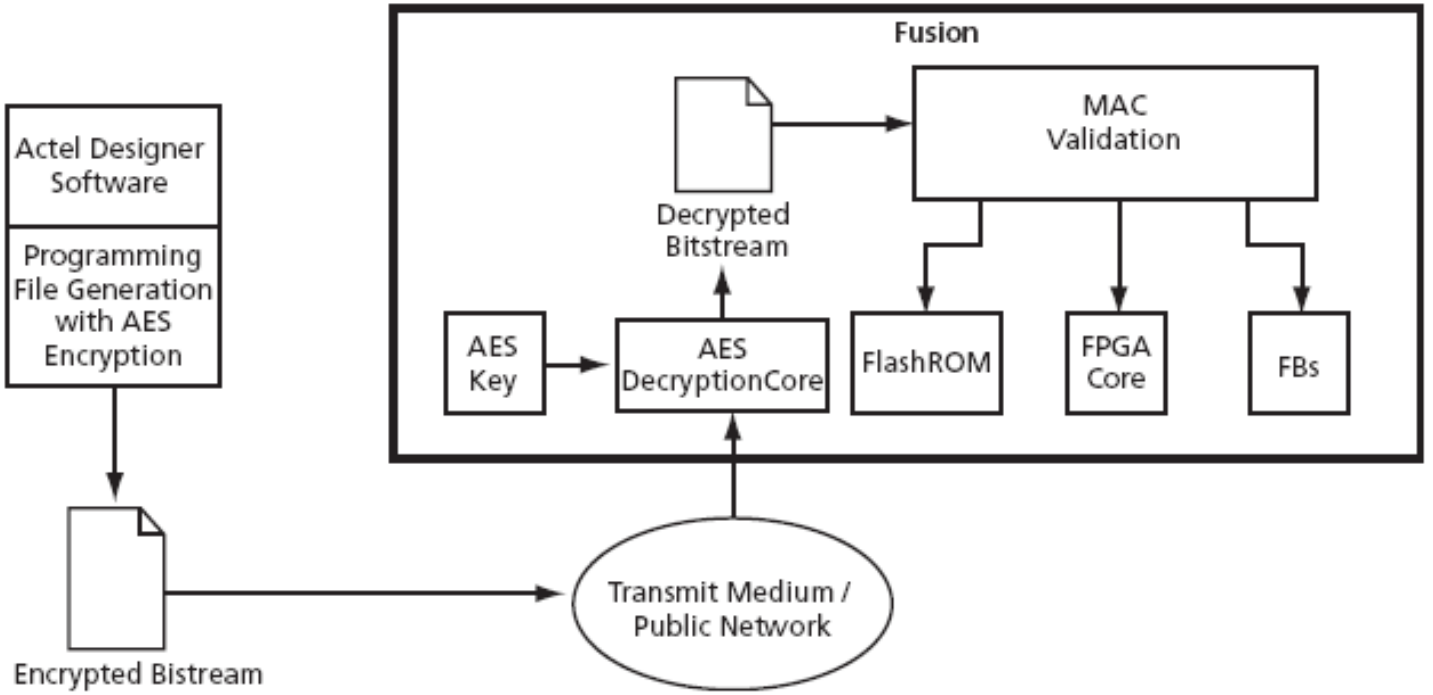
[3]CRC : Cyclic Redundancy Check

[4]MAC : Message Authentication Code

Replay attack



Actel Application Note : Fusion Security



• **Example Application Scenario Using AES in Fusion Devices**

- Confidentiality is guaranteed
- MAC prevents bitstream tampering (but no documentation)
- But bitstream version is not verified

Authentication of FPGA Bitstreams: Why and How ?

Saar Drimer, Computer Laboratory, University of Cambridge

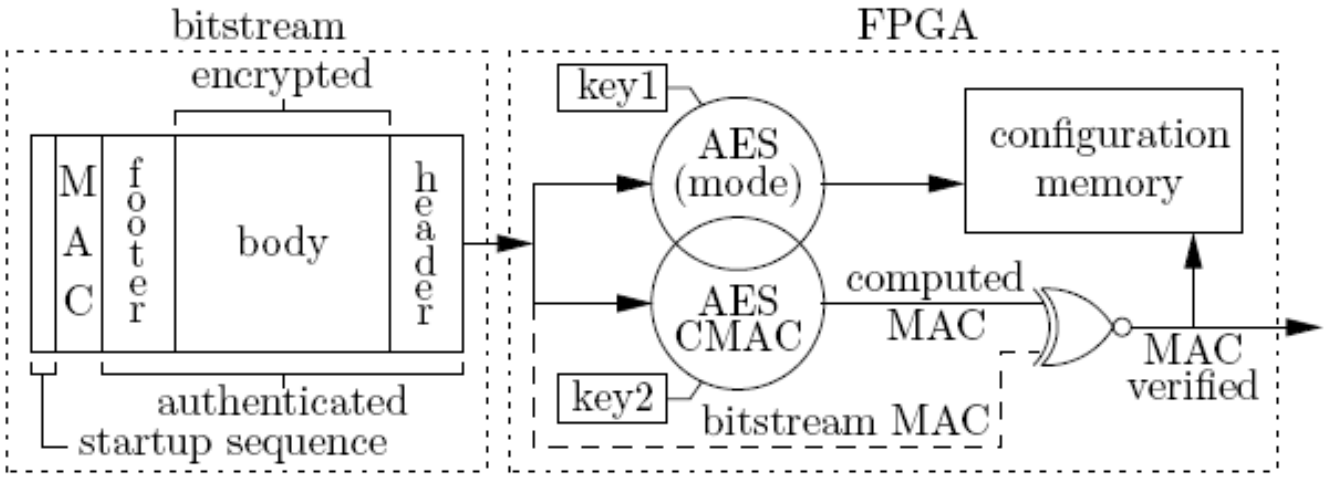


Fig. 1. Two parallel AES cores provide decryption and authenticity. The amount of shared resources depends on the modes

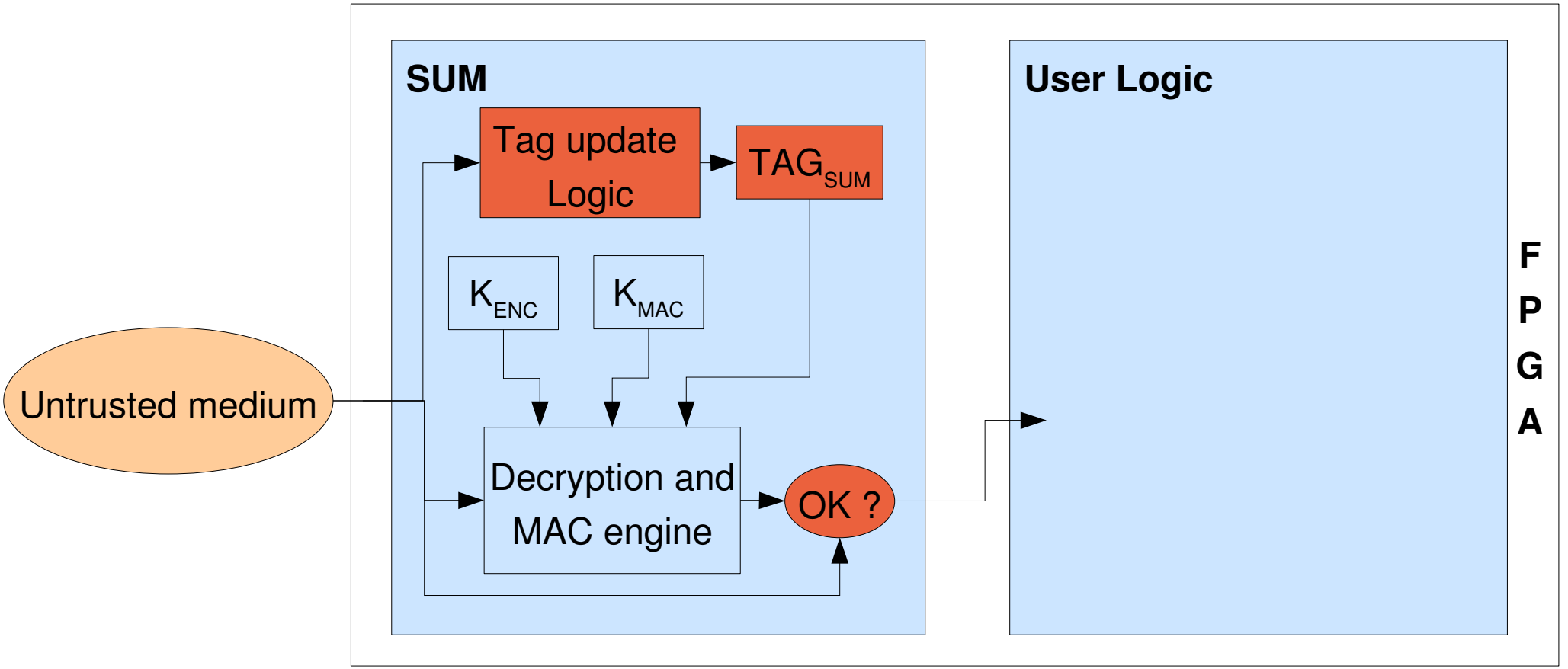
- Confidentiality is guaranteed
- MAC prevents bitstream tampering
- But bitstream version is not verified

Solutions against replay attacks

- External trusted device attesting bitstream version
  - Multi-chip solution
  - Periodic polling
  - Cost for system designer (user logic)

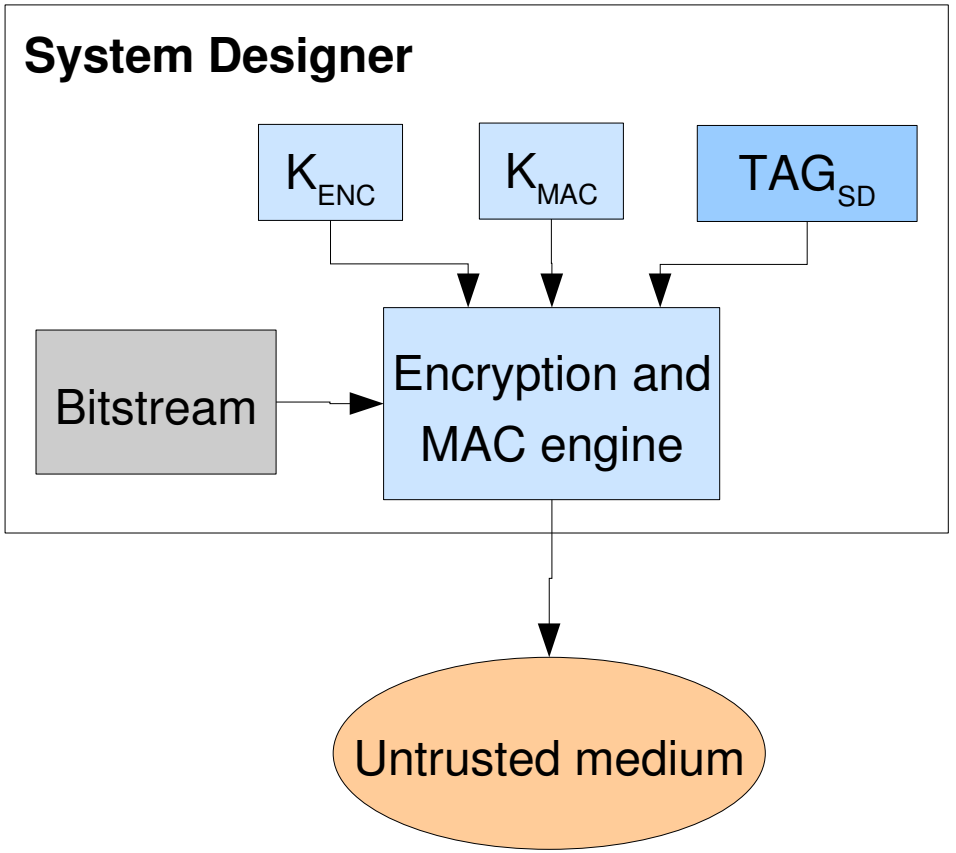
- Nonces (unique time-stamp) and Non-volatile state inside FPGA
  - No external device
  - No cost for designer if implemented by FPGA vendors

Overview



- 1 Non-Volatile Register (128 bits)
- Logic to control TAG modifications
- Comparator

TAG verification (1/2)

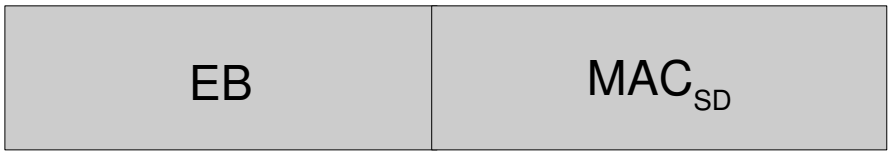


1) SD computes :

Encrypted Bitstream (EB) : $ENC_{KENC}(B)$

MAC_{SD} : MAC_{KMAC} (EB || TAG_{SD})

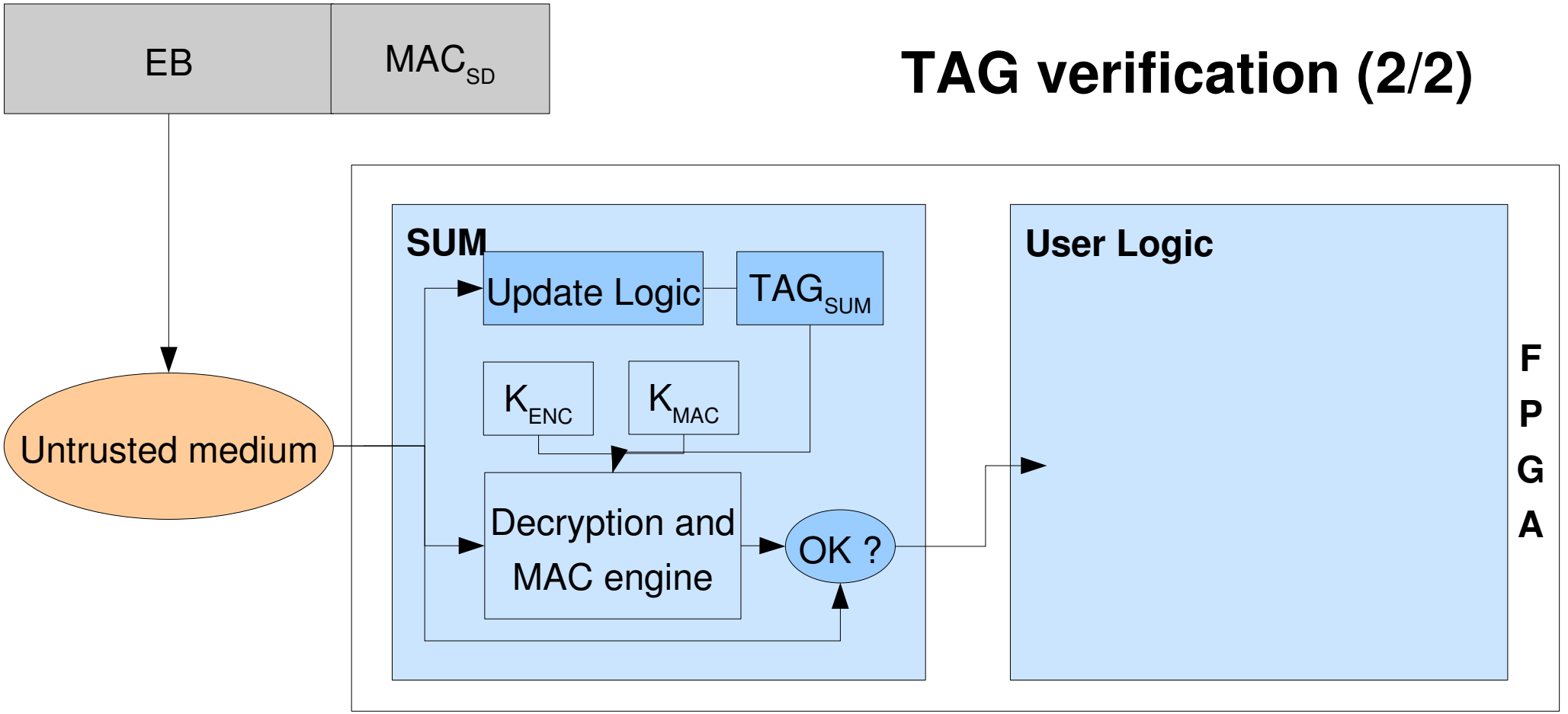
2) SD sends :



MAC : *Message Authentication Code*

|| **:** *concatenation*

TAG verification (2/2)

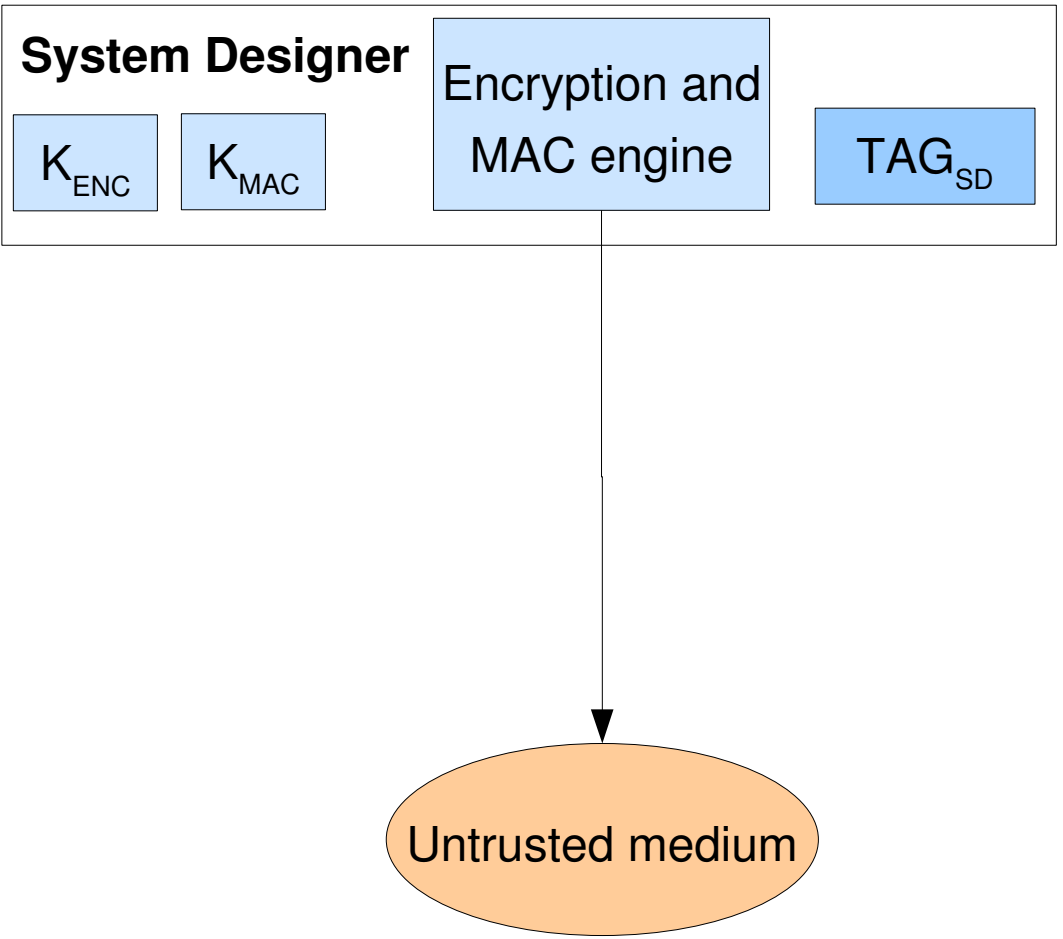


3) FPGA SUM computes MAC_{SUM} : MAC_{KMAC} (EB || TAG_{SUM}) and decrypt EB in //

4) FPGA SUM compares MAC_{SD} and MAC_{SUM}

5) If the MAC matching process succeeds, it validates the bitstream

TAG modification (1/2)



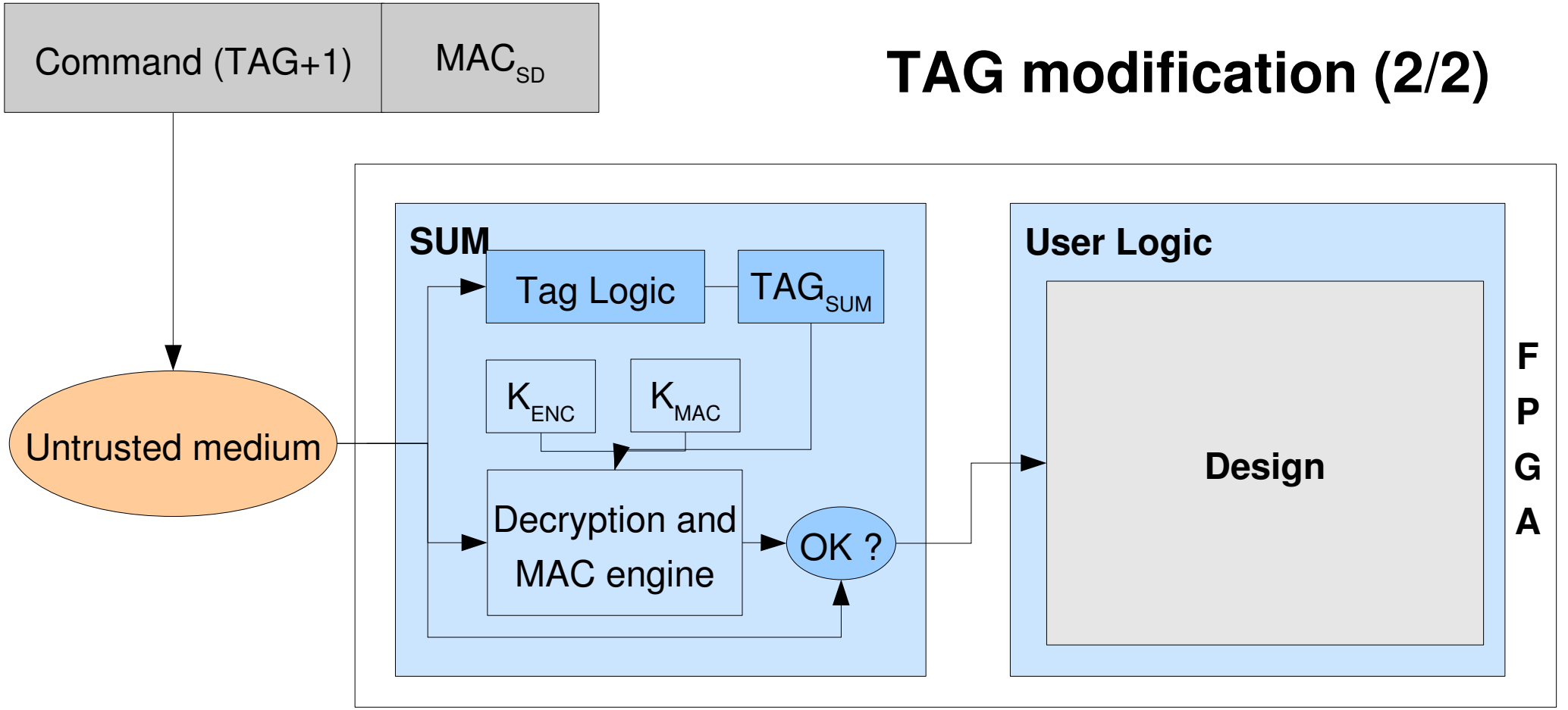
1) SD computes :

$MAC_{SD2} : MAC_{KMAC} (CmdUp || TAG_{SD})$

2) SD sends :

Command (TAG+1)	$MAC_{SD\ 2}$

TAG modification (2/2)

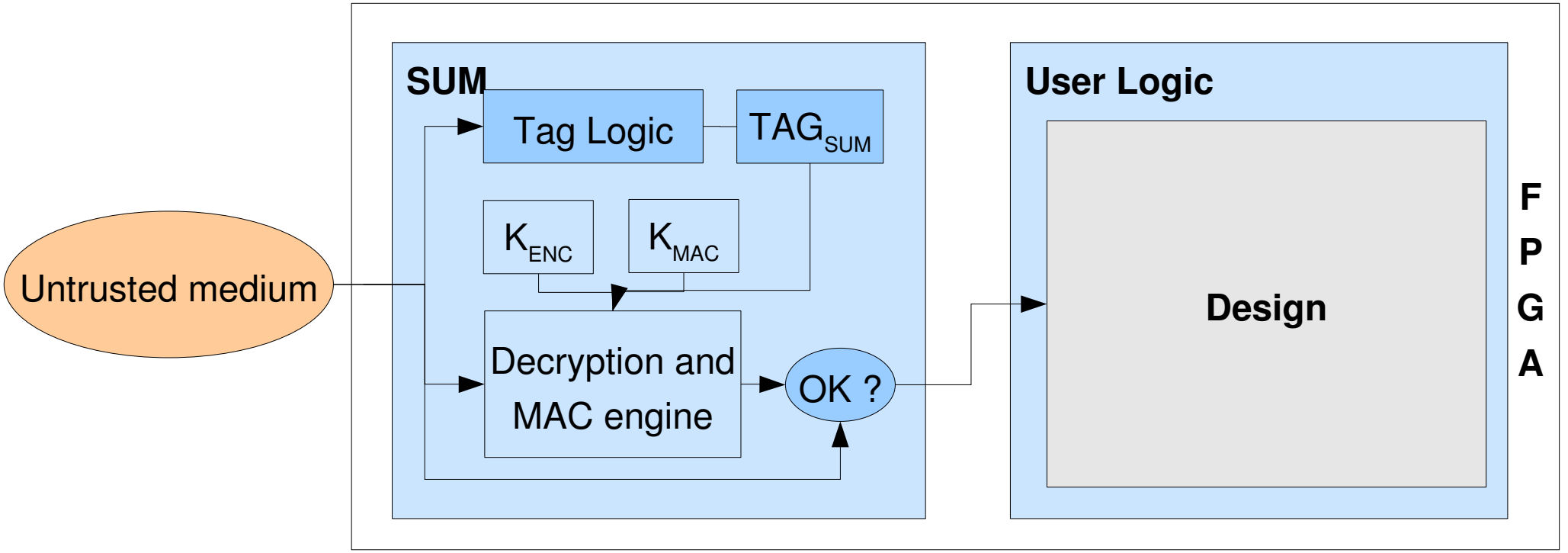


3) FPGA SUM computes $MAC_{SUM2} = MAC_{KMAC}(CmdUp \ || \ TAG_{SUM})$

4) FPGA SUM compares MAC_{SUM2} and MAC_{SD2}

5) If the MAC matching process succeeds, $TAG_{SUM} = TAG_{SUM} + 1$

Acknowledgment (1/2)

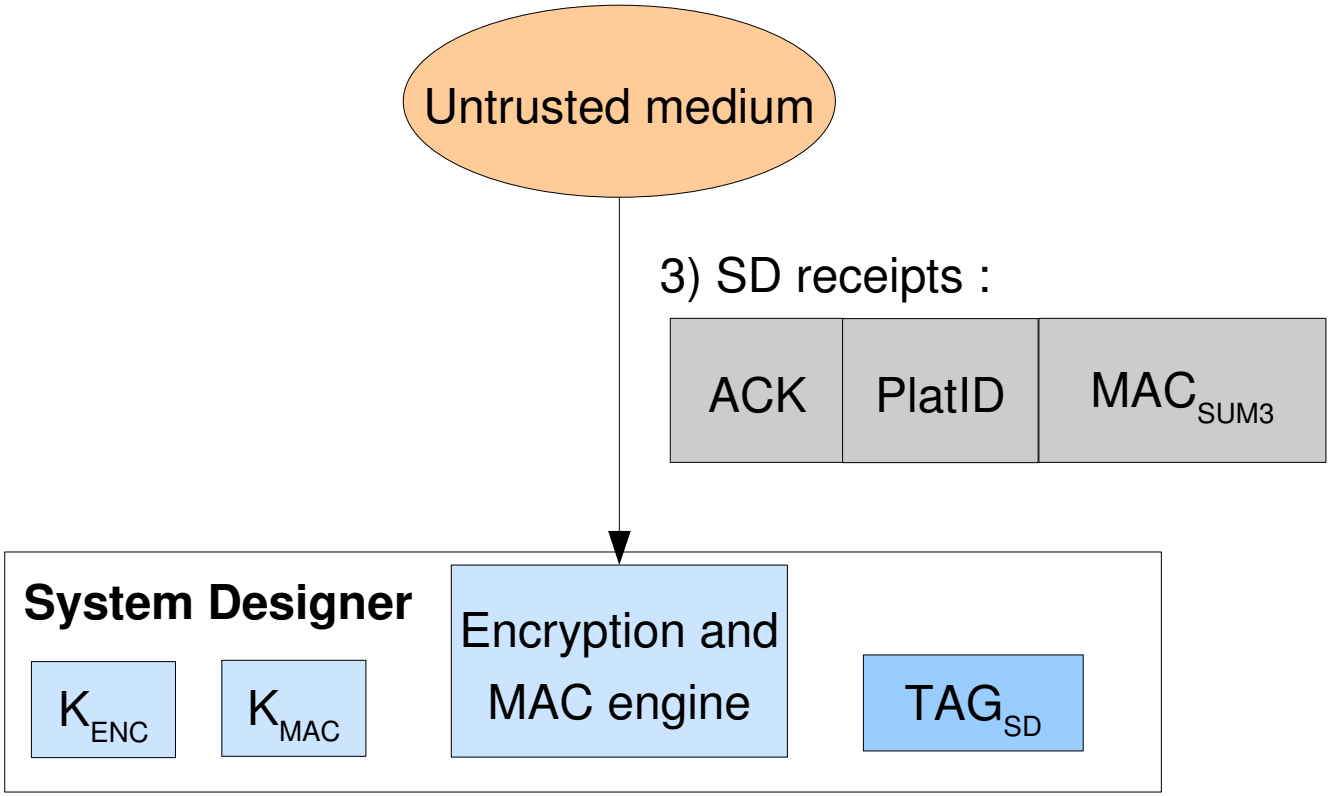


1) FPGA SUM computes $MAC_{SUM3} = MAC_{KMAC}$ (ACK || TAG_{SUM} || Plateform ID)

2) **FPGA SUM sends** (using user logic) :

ACK	PlatID	MAC_{SUM3}

Acknowledgment (2/2)

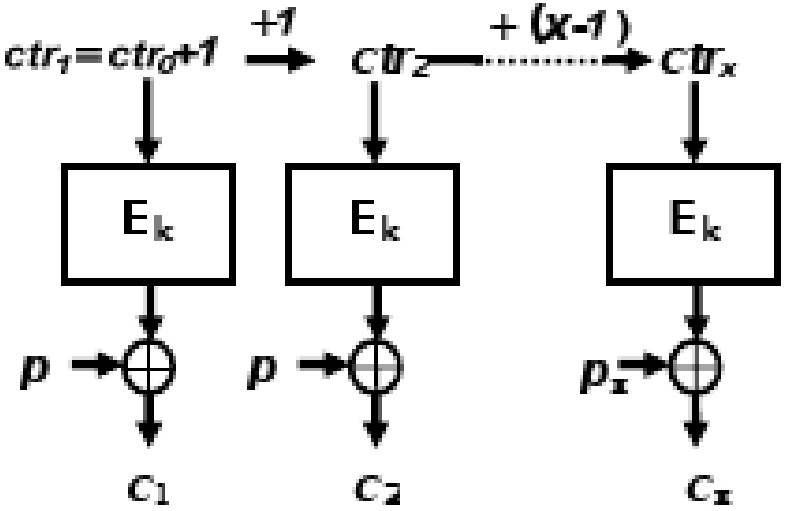


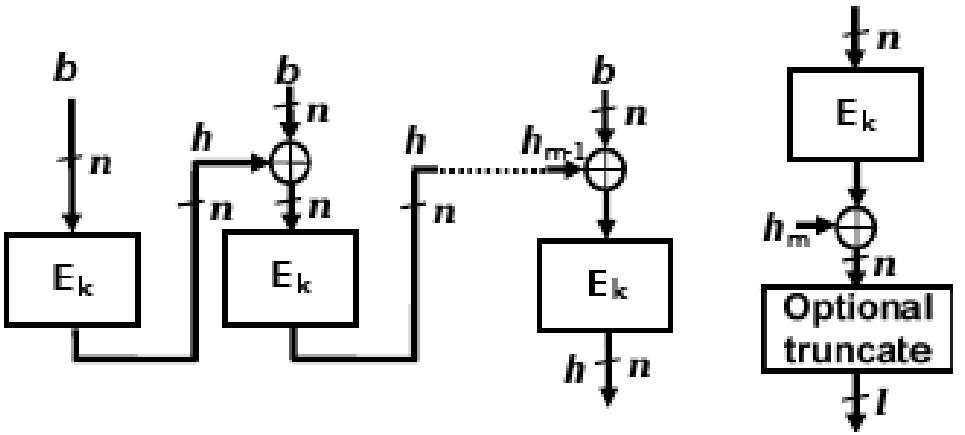
4) SD computes MAC_{SD3} : MAC_{KMAC} (ACK || TAG_{SD} || Plateform ID)

5) FPGA compares MAC_{SD3} and MAC_{SUM3}

6) If the MAC matching process succeeds, remote system has been upgraded

CCM Mode





- Recommended by NIST
- Authenticated encryption
- Only encryption mode of AES used
- Two pass algorithm

Configuration throughput estimation with CCM

AES engine characteristics : 11,6 bits per clock cycle / ~30kGates[1]

CCM performances : 5.8 bits per clock cycle

		Encryption Only		SUM with CCM		
FPGA vendor / FPGA Family	Configuration interface width	Max. loading Freq. (MHz)	Throughput (Mb/s)	Max. Loading Freq. (MHz)	Throughput (Mb/s)	Overhead
Xilinx / Virtex-5	8	100	800	100	580	37%
	32	N/A	N/A	N/A	N/A	N/A
	1	100	100	100	100	0%
Altera / Stratix-III	16	40	640	40	232	64%
	1	40	40	40	40	0%
Lattice / ECP2M	8	45	360	45	261	28%
	1	45	45	45	45	0%

[1]*heliontech IP core for ASIC (http://www.heliontech.com/aes.htm)*

Configuration throughput estimation with CCM

AES engine characteristics : 11 cycles per encryption / ~30kGates[1]

CCM performances : 5.8 bits per clock cycle

		Encryption Only		SUM with CCM		
FPGA vendor / FPGA Family	Configuration interface width	Max. loading Freq. (MHz)	Throughput (Mb/s)	Max. Loading Freq. (MHz)	Throughput (Mb/s)	Overhead
Xilinx / Virtex-5	8	100	800	100	580	37%
	32	N/A	N/A	N/A	N/A	N/A
	1	100	100	100	100	0%
Altera / Stratix-III	16	40	640	40	232	64%
	1	40	40	40	40	0%
Lattice / ECP2M	8	45	360	45	261	28%
	1	45	45	45	45	0%

[1] *heliontech IP core for ASIC (http://www.heliontech.com/aes.htm)*

Configuration throughput estimation with CCM

AES engine characteristics : 11 cycles per encryption / ~30kGates[1]

CCM performances : 5.8 bits per clock cycle

		Encryption Only		SUM with CCM		
FPGA vendor / FPGA Family	Configuration interface width	Max. loading Freq. (MHz)	Throughput (Mb/s)	Max. Loading Freq. (MHz)	Throughput (Mb/s)	Overhead
Xilinx / Virtex-5	8	100	800	100	580	37%
	32	N/A	N/A	N/A	N/A	N/A
	1	100	100	100	100	0%
Altera / Stratix-III	16	40	640	40	232	64%
	1	40	40	40	40	0%
Lattice / ECP2M	8	45	360	45	261	28%
	1	45	45	45	45	0%

External flash memory is generally slower than FPGA capabilities

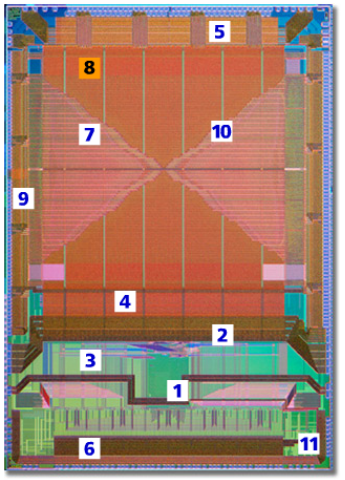
[1] *heliontech IP core for ASIC (http://www.heliontech.com/aes.htm)*

Conclusion

- Encryption is not sufficient to entirely trust FPGA plateform
- FPGA needs an authenticated encryption of the bitstream (CCM, EAX) not only CRC
- SUM protects against replays with a negligible area and throughput overhead with CCM
- Acknowledgment feature provides an alert system if update is not correctly installed

Perspectives

- Implement a variant of our scheme on Actel fusion FPGA



- Propose our scheme to FPGA vendors (FPL'08)

Thank you

Benoît Badrignans
Benoit.Badrignans@lirmm.fr

LIRMM / NETHEOS

Reouven Elbaz
David Champagne

Princeton University

Lionel Torres

LIRMM