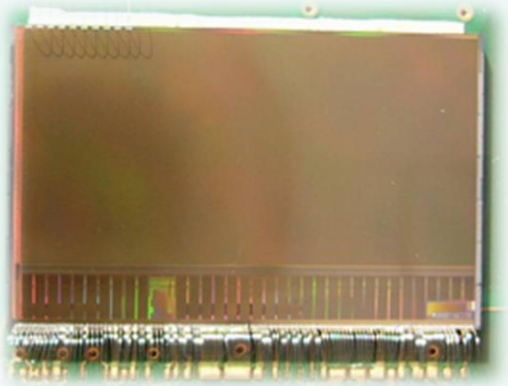
Les journées VLSI - PCB - FPGA - IAOCAO 2018

HDL SOURCE CODE PROTECTION

KIMMO JAASKELAINEN
Groupe Microélectronique
Institut Pluridisciplinaire Hubert Curien
23 rue du Loess - BP28
67037 Strasbourg cedex 2

Why this interest?



MIMOSA-26
CMOS Pixel Sensor
~ 700k pixels, 21.5 x 13.8 mm^2

BEAST Project (KEK)
Plume Ladder,
presentation of
G. Claus

For a XILINX FPGA firmware development: a request from collaborators for the VHDL simulation model of the MIMOSA-26 Slow Control interface (ModelSim)

EXCEPT the simulation model contained VERILOG modules of the **ASIC DESIGN**
- constraint: these VERILOG modules were not foreseen to be distributed!

Alternative solutions

Method	Problems
Netlist, schematics	too tightly related to the orginal implementation or technology
Obfuscation of source code	one way transformation, difficult to verify

IEEE Std 1735-2014 - IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP) (1/3)

Features (source code)
Use Models to perform the protection at the RTL source code level
Definitions embedded in the RTL source code with markup syntaxes (pragmas)
Pragma definition (source code line): Verilog: *`pragma protect*, VHDL: *`protect*
Independent of RTL code, no analysis (HDL syntax error are accepted for encryption)
Broad range of use: from generic RTL Code for multiple Vendor tools …. to the tool/technology specific approach with the IPs
Encrypted RTL code sections encapsulated in "*Digital Envelopes*" in source code
Digital Envelope contains: *Key Block (Encryption Key)* and *Data Block (Source Code)*
Two level of *Recommendations* of usage: Version 1 and Version 2

IEEE Std 1735-2014 - IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP) (2/3)

Features (encryption)
Hybrid public-key encryption scheme with the **standard encryption methods**: Asymmetric encryption(RSA) + Symmetric encryption (AES)
RTL code encrypted with the symmetric AES key (*Session Key*) to *Data Block*
Session Key (AES) encrypted with the Tool Vendor's Public Key (RSA) to *Key Block*
Scheme allows for using Multiple *Key Blocks* (= multiple EDA tools) with one *Data Block*

Asymmetric encryption (2 keys): the key *to decrypt* the data (*private key*) is *different* from the key *to encrypt* the data (*public key*).

Symmetric encryption (1 key): the key (*private key*) *to encrypt* the data is the *same* as the key *to decrypt* the data

IEEE Std 1735-2014 - IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP) (3/3)

Version 1 Recommendations
GOAL: Interoperability across the different EDA tools (Cadence, Mentor, Xilinx, Altera, ..)
Most of EDA vendor tools supports only Version 1 Recommendations
No restrictions on use of the protected code among the users of the same tool

Version 2 Recommendations
Includes Version 1 Recommendations
Adds Rights Management: licensing, code visibility restrictions
Officially supported by Xilinx (VIVADO)

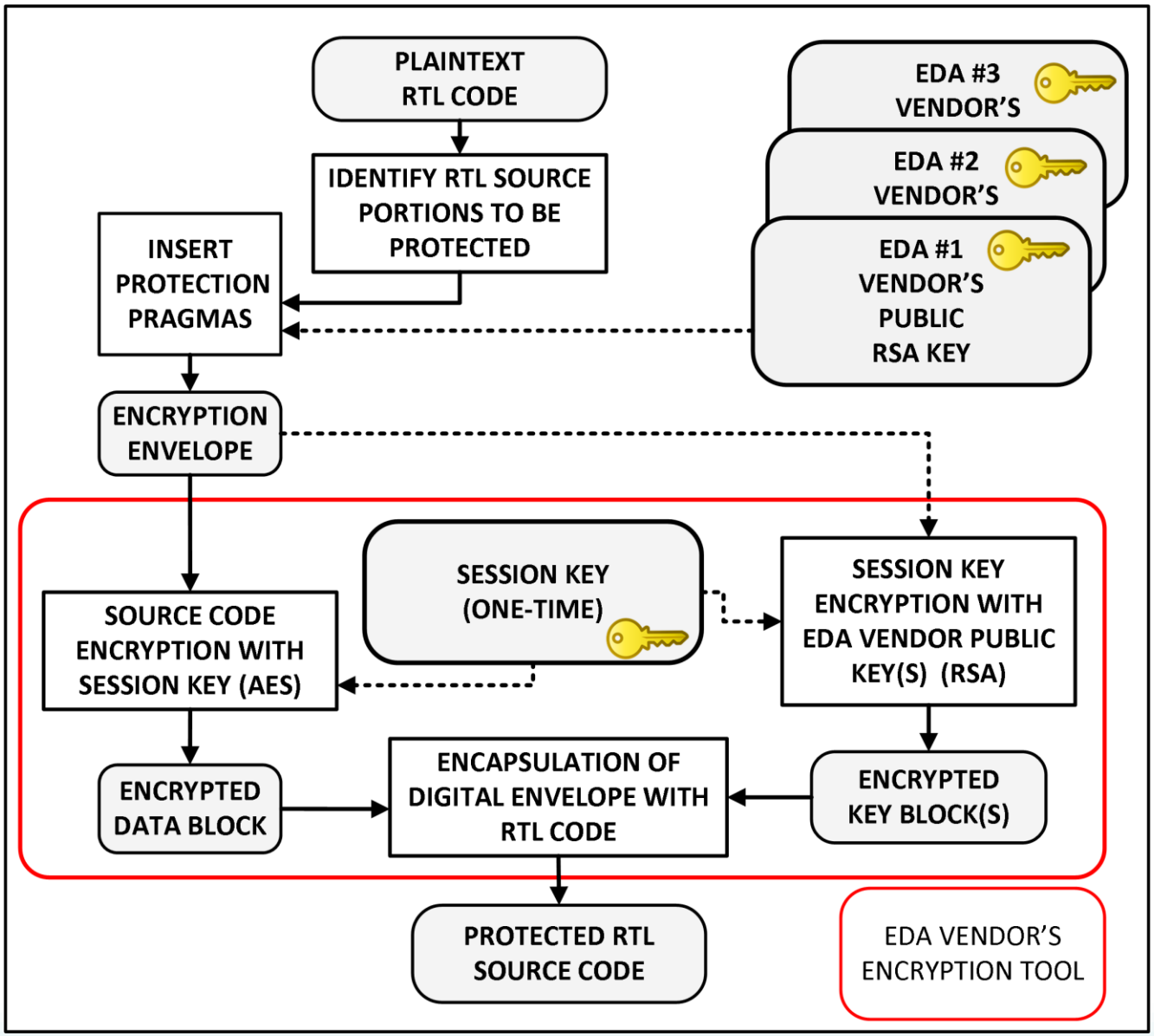
Encryption Process

Easy to use!

Learning Time:
~ 1 Day

RTL Code Overhead:
~ 20 lines of code/
Encryption Envelope

Encryption Time:
~ few minutes



Example of VHDL source code – ENCRYPTION ENVELOPE

Protection pragma lines overhead: 17 lines of code

"Version 1 Recommendations"

"Tool Vendor's Public Key Information" QuestaSim/ModelSim

"Source code to be protected"

```
architecture structure of core_vhdl is
begin
-- removed plain text code .........
`protect version = 1
`protect author = "Kimmo.Jaaskelainen@iphc.cnrs.fr"
`protect key_keyowner = "Mentor Graphics Corporation"
`protect key_method = "rsa"
`protect key_keyname = "MGC-VERIF-SIM-RSA-2"
`protect data_method = "aes128-cbc"
`protect key_public_key
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtNA6tJ1tV/cXF4K5mL4s
4KCuTKWSbN/BnJJ6elRTWr2+s5Baaul0ctIX/3KYzpITmG9ph/4uZBs+jV5DAC+9
WRZQDc11JdIlRi04dEx/bGVbfPs3pdTPFZjA6gfegdW03ZNhjaJChTwEoXL1xIGP
oodJyhX9r1DoxU2lWB19vpwI5Geygh6pYgkPXb0aQzLh6hyUBhH9yMN6eV+imBbO
eax8ZCO6Gz2CJq3ebS/JoMYrikgcIEf6kVhIOiB9LluTp6TZlSd8ilwPhQmfXWH2
w4CaIpN8kADaVHnDWIdqqHlGf3cNQrlWj6FnFpSam6PjmWp5ZD4Jt6UNJxEoKEsn
gwIDAQAB
`protect key_block
`protect begin
ff_B_p: process (clk,clr,dinB)
begin
    if (clr = '1') then
        doutB <= '0';
    elsif (clk'event and clk = '1') then
        doutB <= dinB;
    end if;
 end process;
`protect end
end structure;
```

Example of VERILOG source code – ENCRYPTION ENVELOPE

"Version 1 Recommendations"

"Tool Vendor's Public Key Information" QuestaSim/ModelSim

"Source code to be protected"

```
module core_ver (dinA, dinB, doutA, doutB, clk, clr);
 // removed plain text code .........
`pragma protect version = 1
`pragma protect author = "Kimmo.Jaaskelainen@iphc.cnrs.fr"
`pragma protect key_keyowner = "Mentor Graphics Corporation"
`pragma protect key_method = "rsa"
`pragma protect key_keyname = "MGC-VERIF-SIM-RSA-2"
`pragma protect data_method = "aes128-cbc"
`pragma protect key_public_key
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtNA6tJ1tV/cXF4K5mL4s
4KCuTKWSbN/BnJJ6elRTWr2+s5Baaul0ctIX/3KYzpITmG9ph/4uZBs+jV5DAC+9
WRZQDc11JdIlRi04dEx/bGVbfPs3pdTPFZjA6gfegdW03ZNhjaJChTwEoXL1xIGP
oodJyhX9r1DoxU2lWB19vpwI5Geygh6pYgkPXb0aQzLh6hyUBhH9yMN6eV+imBbO
eax8ZCO6Gz2CJq3ebS/JoMYrikgcIEf6kVhIOiB9LluTp6TZlSd8ilwPhQmfXWH2
w4CaIpN8kADaVHnDWIdqqHlGf3cNQrlWj6FnFpSam6PjmWp5ZD4Jt6UNJxEoKEsn
qwIDAQAB
`pragma protect begin
always @(posedge clr or posedge clk)
begin
          if(clr) begin
            doutB = 0;
          end
          else begin
            doutB = dinB;
          end
end
`pragma protect end
endmodule
```

Example of Protected VHDL source code – DIGITAL ENVELOPE

KEY BLOCK "SESSION KEY"

DATA BLOCK "SOURCE CODE"

```
architecture structure of core_vhdl is
begin
 -- removed plain text code .........
`protect begin_protected
`protect version = 1
`protect author = "Kimmo.Jaaskelainen@iphc.cnrs.fr"
`protect encrypt_agent = "QuestaSim" , encrypt_agent_info = "10.7"
`protect key_keyowner = "Mentor Graphics Corporation" , key_keyname = "MGC-
VERIF-SIM-RSA-2"
`protect key_method = "rsa"
`protect encoding = ( enctype = "base64" , line_length = 64 , bytes = 256 )
`protect key_block
XbqqhNYhSYN/oEKMEiq0Ym+DL6WPOqHX3arpghSRWgZHkiu2ay7i6SfuqJ0k789G
lr53+nGZJzLcY6XqIYCg7k4RY2T45mqkN8INrstolSsjxsemltsynkjj0K33JAXG
PpXVK7queDYuCSgcYQu3p1bLJh7w+c2yy2ByPTeWQoowau0XmVf4zg9sb5Hc1CTJ
MFVIcIll+fDrbhd1ZRCGP57atMIGxtHPtaJcXEddnqVuHJlA9DdQtIS9BUkbJJfi
aS4bmhCR3mRukChztA7YPMjmRRe2U51w8/R6cnVBX8C6upCXEn4n5gd94DkU0ykW
u7VP69iqTHjXN3LGjPGzYw==
`protect data_method = "aes128-cbc"
`protect encoding = ( enctype = "base64" , line_length = 64 , bytes = 208 )
`protect data_block
jBI7shRzPNKDtSkujbKJchlhN9ZKjCyyyIh64rzqFizi1ibJYz4E5nEfeWKGPklu
IiCX3yqOuvP+F4DJWrp2/eia0DRwuiXAp4sQUgOqGINHAJWjfo95XlQg30Dbr+QQ
ziXSWgjaQ1tq9uDGUOwh8fZpoY/w6kF8BqwpxRFQwxv+n8kR3IKrpPNIyGGoWNCj
lHwIErCdmKpxhiWrLsgA1V0g8gIhBQ5kRm9+/VYViMIU8OR6rxwkIvyIZHnrsiic
n+UQtlUVnRuxFqyBXSoRWw==
`protect end_protected
end structure;
```

Example of protected VERILOG source code – DIGITAL ENVELOPE

```
module core_ver (dinA, dinB, doutA, doutB, clk, clr);
// removed plain text code .........
`pragma protect begin_protected
`pragma protect version = 1
`pragma protect author = "Kimmo.Jaaskelainen@iphc.cnrs.fr"
`pragma protect encrypt_agent = "QuestaSim" , encrypt_agent_info = "10.7"
`pragma protect key_keyowner = "Mentor Graphics Corporation" , key_keyname = "MGC-
VERIF-SIM-RSA-2"
`pragma protect key_method = "rsa"
`pragma protect encoding = ( enctype = "base64" , line_length = 64 , bytes = 256 )
`pragma protect key_block
sUE5kbkpRQMF/adtEd/LPF6/X6a5hzFUmDSF3NqEkqmbQYc61JbEAfw6LhECpylp
dWrpsDKKPz+riP2ESwSvteo6xh6p0rJ8AujpqgzbVM/bPSo8XdgH8a21lEr5xIpZ
ZWT/w9OjJBGwv2Q1+ToND0uUiMfydMwDWvOMsGvPRJMNE9Cxbqod+i/iPyUVmc3g
e8NA4OnHyUSK6+THFkxdIAyWoXA7SV6fMgXA1r5HmpOuoY+BfASqCacujFj3io96
9i7Sb1Um4A4duB84EjWTuYYr/TkUDKG1ygGNOXeV7G+Vb1pmMUxMq9p9OSUzpWbI
QGqNVBZMmBIfhYqby5u4UQ==
`pragma protect data_method = "aes128-cbc"
`pragma protect encoding = ( enctype = "base64" , line_length = 64 , bytes = 240 )
`pragma protect data_block
mFXHzBbrCoinBs2uKLtGU77eqgaB6lG2x5W6ubgfijK2wER11GX/OgzjhfFTjvyR
zLknt/7fSX0pJzys8kU129lMYhQCQzAthi2SpNj4QFuyRuELMxe1XUDSmKBgtJjK
6j2NlkTI/8ODOOqY/EA2UW8qcJ1FlcGan8HQBDLXGMKEKQ94xXY5p75N8DS+XSsd
jyPyxmomtAFcFZ1K9Ria/g4N87qLQBECun0m8DRxH58E3ftprrB/K1RFZlpRfB7b
Is3L4q7KSJpDA+KPdxgFUQpTBRwxKGnuNFsPV70ealeAGCGcFYJYU9Btfd3AO2t2
`pragma protect end_protected
endmodule
```

KEY BLOCK

DATA BLOCK

LIST OF SOME COMMONLY USED IEEE-1735 COMPATIBLE EDA TOOLS AT IN2P3

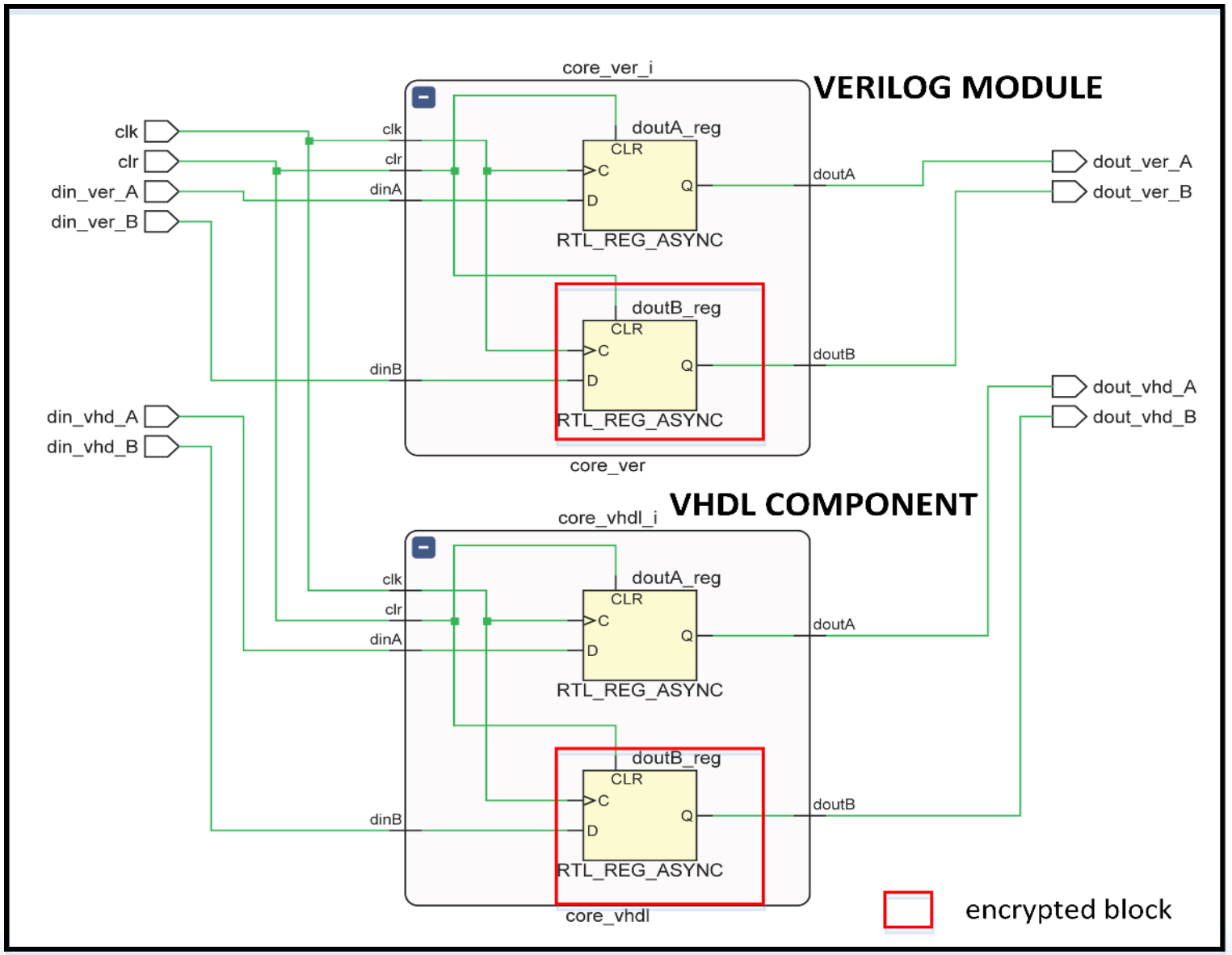
EDA Tool Vendor	Tool
CADENCE	**Incisive**, **Xcelium**, **Genus**
MENTOR GRAPHICS	**QuestaSim**, **ModelSim**
XILINX	**Vivado**
ALTERA (Intel)	**Quartus**

Test Case verified for Simulation **(in RED)**, for Synthesis **(in BLUE)**

RTL TEST CASE FOR TOOL EVALUATIONS (VERILOG/VHDL)

VHDL TOP COMPONENT

source:
XILINX
VIVADO



ENCRYPTION OVERVIEW: CADENCE

Feature, Parameter	Value
Tools version tested	INCISIVE: 15.20-s039 (simulation), XCELIUM: 17.04-s015 (simulation), GENUS: 17.11-S014_1 (synthesis)
RSA Public Key (*key_keyowner, key_keyname*)	"Cadence Design Systems•", "CDS_RSA_KEY_VER_1"
RSA Public Key available	YES
Encryption VERILOG	INCISIVE: "*ncprotect -language vlog <f.v> -outname <f.vp>* " XCELIUM: "*xmprotect -language vlog <f.v> -outname <f.vp>* "
Encryption VHDL	INCISIVE: "*ncprotect -language vhdl <f.vhd> -outname <f.vhdp>* " XCELIUM: "*xmprotect -language vhdl <f.vhd> -outname <f.vhdp>* "
Encryption option	YES
Encryption option license	NO
IEEE 1735 V1 SUPPORT	read: YES, write: YES
IEEE 1735 V2 SUPPORT	read: NO, write: NO

Thanks to G. Bertolone for the technical support!

ENCRYPTION OVERVIEW: MENTOR GRAPHICS

Feature, Parameter	Value
Tools version tested	QuestaSim -64 10.7 (simulation)
RSA Public Key (*key_keyowner, key_keyname*)	"Mentor Graphics Corporation", "MGC-VERIF-SIM-RSA-2"
RSA Public Key available	YES
Encryption VERILOG	vencrypt <f.v> -o <f.vp>
Encryption VHDL	vhencrypt <f.vhd> -o <f.vhdp>
Encryption option	YES
Encryption option license	NO
IEEE 1735 V1 SUPPORT	read: YES, write: YES
IEEE 1735 V2 SUPPORT	read: NO, write: NO

ENCRYPTION OVERVIEW: XILINX

Feature, Parameter	Value
Tools version tested	Xilinx VIVADO 2017.4 (simulation, synthesis)
RSA Public Key (*key_keyowner, key_keyname*)	"Xilinx", "xilinxt_2017_05"
RSA Public Key available	YES
Encryption VERILOG	VIVADO TCL SHELL: "encrypt -lang verilog -ext {.vp} *<f.v>*" (1)
Encryption VHDL	VIVADO TCL SHELL: "encrypt -lang vhdl -ext {.vhdp} *<f.vhd>*" (1)
Encryption option	YES
Encryption option license	"EncryptedWriter_v2" evaluation license required, free of charge
IEEE 1735 V1 SUPPORT	read: YES, write: NO (2)
IEEE 1735 V2 SUPPORT	read: YES, write: YES

(1) **Important!** The options *-ext {.vp} and -ext {.vhdp}* prevents the source file being overwritten.

(2) Reserved. "*Version 1 (V1) of IEEE-1735 -2014 is supported by Xilinx under an early access program.*" *Xilinx UG1118, p.87*

ENCRYPTION OVERVIEW: ALTERA (INTEL)

Feature, Parameter	Value
Tools version tested	Intel (Altera) Quartus Prime Pro 17.1 (synthesis)
RSA Public Key (*key_keyowner, key_keyname*)	"Intel Corporation", "Intel-FPGA-Quartus-RSA-1"
RSA Public Key available	RESERVED. Contact FAE/Altera User support
Encryption VERILOG	For Quartus synthesis: "*encrypt_1735.exe --quartus --language=verilog <f.v>*" For the third Party simulation (Aldec, Cadence, Mentor, Synopsis) : "*encrypt_1735.exe --simulation --language=verilog <f.v>*"
Encryption VHDL	For Quartus synthesis: "*encrypt_1735.exe --quartus --language=vhdl <f.vhd>*" For the third Party simulation (Aldec, Cadence, Mentor, Synopsys) : "*encrypt_1735.exe --simulation --language=vhdl <f.vhd>*"
Encryption option	YES
Encryption option license	NO
IEEE 1735 V1 SUPPORT	read: YES, write: YES
IEEE 1735 V2 SUPPORT	read: NO, write: NO

CONCLUSION

Source code protection allowed us to distribute a simulation model of the slow control interface of CMOS pixel sensor (MIMOSA-26), while preserving its integrity

IEEE-1735 standard defines a convenient method for protecting RTL source code
=> Main Goal : Interoperability across the EDA tools

Source code protection has been tested with multiple EDA tools used at IN2P3
=> Test Case Kit for multiple EDA tools will be available for distribution

Public Research context : source code protection is not the default operation mode
=> Reciprocity: "If you start to provide encrypted RTLs, most likely you will also receive encrypted RTLs."

WARNING, IT IS NOT PERFECT : "Standardizing Bad Cryptographic Practice, A Teardown of the IEEE P1735 Standard for Protecting Electronic-design Intellectual Property", Oct 2017:
"*Full recovery of the plaintext IP without the key*", "*Vector of Hardware Trojans*"

REFERENCES

IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP), IEEE Std 1735™-2014

IEEE Standard VHDL Language Reference Manual, IEEE Std 1076™-2008

IEEE Standard for SystemVerilog— Unified Hardware Design, Specification, and Verification Language, IEEE Std 1800™-2009

XILINX Vivado Design Suite User Guide, *Creating and Packaging Custom IP (UG1118), v2017.2*

Intel® Quartus® Prime Pro Edition Handbook Volume 1, Design and Compilation, QPP5V1 | 2017.12.15

Questa ® SIM User's Manual, Software Version 10.7

Cadence Incisive Enterprise Simulator (ICS) Version 15.20, IP Protection, Cadence Online Documents

Cadence Xcelium Version 17.04, IP Protection, Cadence Online Documents

END

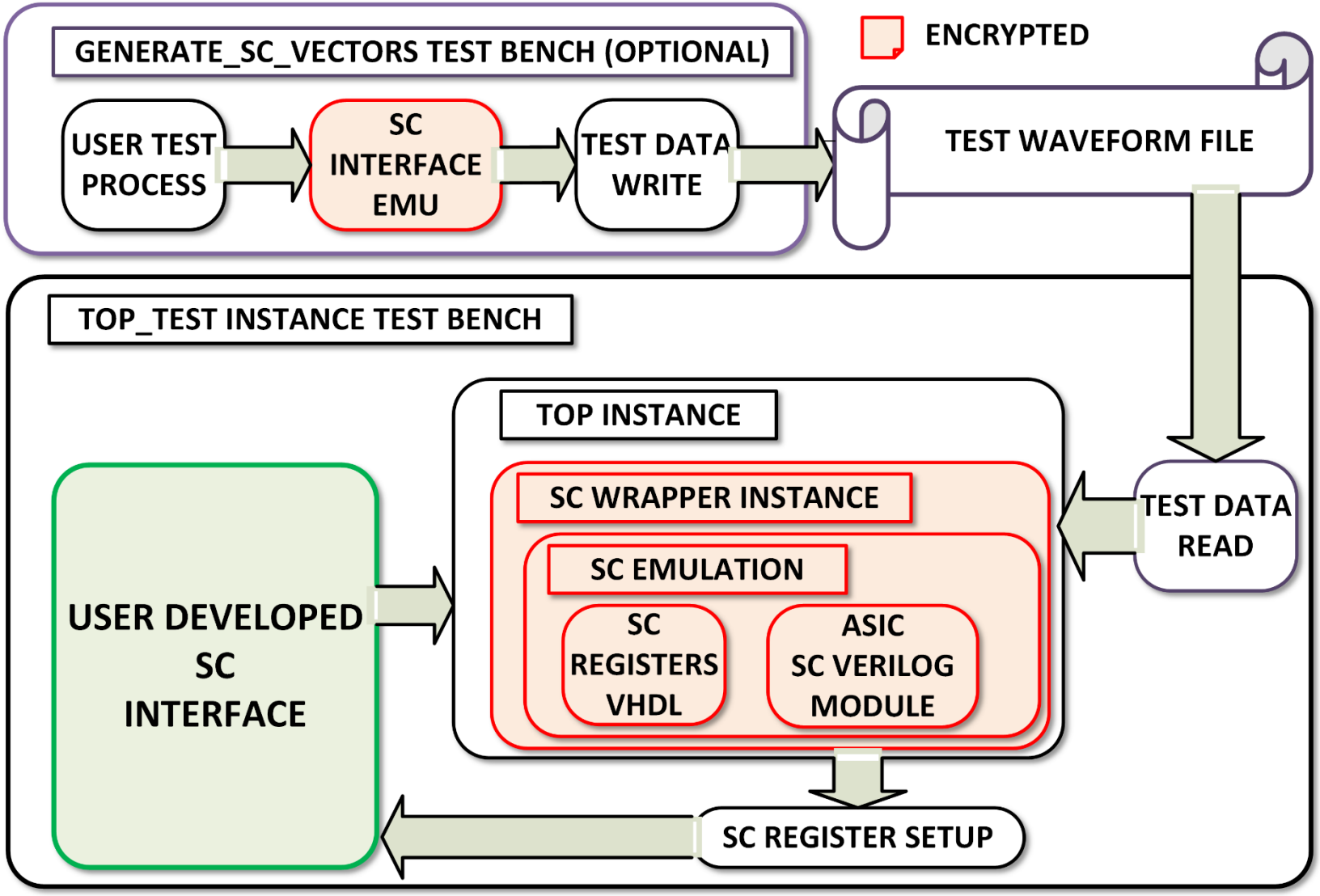
ADDITIONAL SLIDES

IEEE 1735 VENDOR LIST

Vendor	Vendor
AMD	National Semiconductor Corporation
Cadence Design Systems	NXP Semiconductors Inc.
Cisco	QUALCOMM Incorporated
IBM, INC.	Samsung Semiconductor Inc.
Intel Corporation	Synopsys
Marvell Semiconductors	Xilinx
Mentor Graphics	Zuken Inc.
National Instruments	

source: https://www.kb.cert.org/vuls/id/739007

SIMULATION MODEL FOR ASIC SLOW CONTROL



Example of VHDL source file – ENCRYPTION ENVELOPE VERSION 2

”Version 2 Recommendations”

Common Block: “Common Rights”

Simulation: source code can be decrypted

Tool Block: “Tool-specific *Rights and RSA Key*”

Xilinx specific pragmas

Protection pragma lines overhead: ~30 lines of code

```
architecture structure of core_vhdl is
begin
-- removed plain text code .........
`protect version = 2
`protect author = "Kimmo.Jaaskelainen@iphc.cnrs.fr"
`protect encrypt_agent = "XILINX"
`protect encrypt_agent_info = "Xilinx Encryption Tool 2015"
`protect begin_commonblock
`protect control error_handling = "delegated"
`protect control runtime_visibility = "delegated"
`protect control child_visibility = "delegated"
`protect control decryption=(activity==simulation) ? "true" : "false"
`protect end_commonblock
`protect begin_toolblock
`protect rights_digest_method="sha256"
`protect key_keyowner = "Xilinx", key_keyname= "xilinxt_2017_05",
key_method = "rsa", key_public_key
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxngMPQrDv/s/Rz/ED4Ri
j3tGzeObw/Topab4sl+WDRl/up6SWpAfcgdqb2jvLontfkiQS2xnGoq/Ye0JJEp2
h0NYydCB5GtcEBEe+2n5YJxgiHJ5fGaPguuM6pMX2GcBfKpp3dg8hA/KVTGwvX6a
L4ThrFgEyCSRe2zVd4DpayOre1LZlFVO8X207BNIJD29reTGSFzj5fbVsHSyRpPl
kmOpFQiXMjqOtYFAwI9LyVEJpfx2B6GxwA+5zrGC/ZptmaTTj1a3Z815q1GUZu1A
dpBK2uY9B4wXer6M8yKeqGX0uxDAOW1zh7tvzBysCJoWkZD39OJJWaoaddvhq6HU
MwIDAQAB
`protect control xilinx_configuration_visible = "false"
`protect control xilinx_enable_modification = "false"
`protect control xilinx_enable_probing = "false"
`protect control xilinx_enable_netlist_export = "false"
`protect control xilinx_enable_bitstream = "false"
`protect control decryption=(xilinx_activity==simulation) ? "true" :
"false"
`protect end_toolblock = ""
```