BIL: A Tool-Chain for Bitstream Reverse-Engineering

Florian Benz, André Seffrin, Sorin A. Huss
Center for Advanced Security Research Darmstadt (CASED)

CASED

INTRODUCTION

- Goal: Reversal of Xilinx Virtex-5 bitstreams, i.e., conversion of a .bit file into a netlist.

- XDL files are text files which can be obtained from the Xilinx design flow: Conversion from NCD files by means of a tool provided by Xilinx.

- The Debit project[1] presents a method for correlating XDL files with bitstream files, making various assumptions about connectivity.

- In this work, we extend the approach by taking into account data from XDLRC files.

[1]Jean-Baptiste Note and Eric Rannaud, "From the Bitstream to the Netlist", 16th international ACM/SIGDA symposium on field programmable gate arrays (FPGA'08)

XDLRC

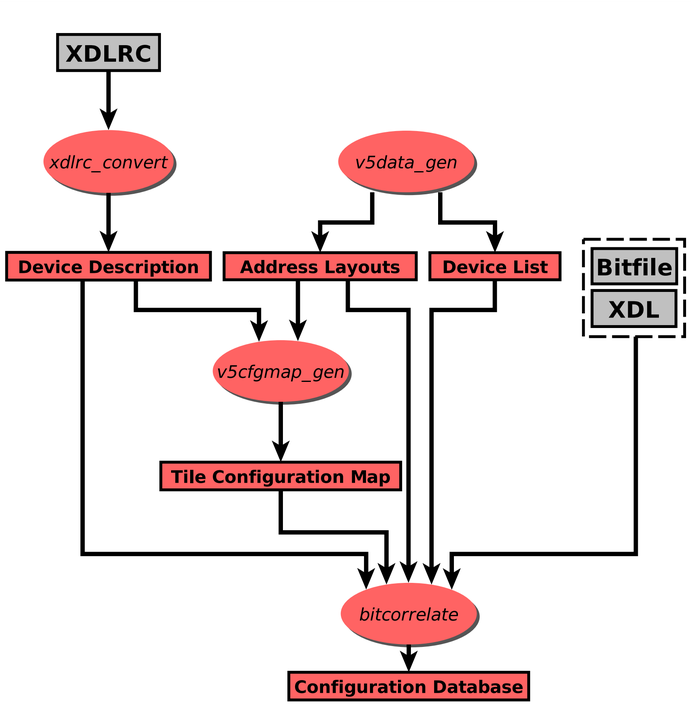
- XDLRC files contain information on fixed and reconfigurable resources on the FPGA device (primitive sites, wires, pips).

- XDLRC files tend to be rather large (up to 15 GB for some Virtex-5 devices). Exploiting regularities in the file format, we achieve a compression ratio of up to 1000:1. This allows for better handling of the data.

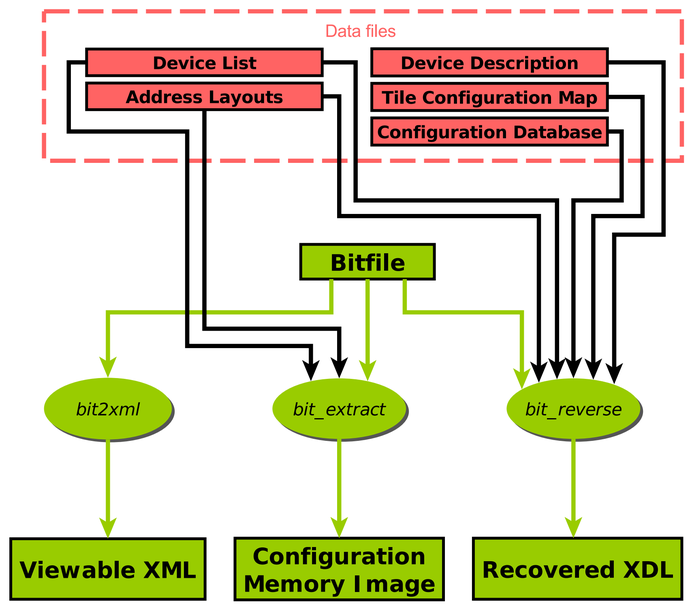
- The extracted data allows to map address data from the bitstream to resources identified within the XDLRC file.

- XDL files only show active resources, while XDLRC files show all device resources. This allows to determine whether a correlation run has identified all resources.

CORRELATION STEPS



REVERSAL STEPS



BITSTREAM DISASSEMBLY VIEW

Disassembly of jpegenc.bit

File meta data:

Source file: jpegenc.ncd;UserID=0xFFFFFFFF
Target device: 5vlx30ff324
Creation date: 2012/02/14
Creation time: 16:43:44

Packet stream:

Index	Packet type	Opcode	Register	Word count	Data
0	Dummy word				0xffffffff
1	Dummy word				0xffffffff
2	Dummy word				0xffffffff
3	Dummy word				0xffffffff
4	Dummy word				0xffffffff
5	Dummy word				0xffffffff
6	Dummy word				0xffffffff
7	Dummy word				0xffffffff
8	Buswidth pattern				
9	Dummy word				0xffffffff
10	Dummy word				0xffffffff
11	Sync word				
12	Type 1 packet	NO_OP			
13	Type 1 packet	REGISTER_WRITE	WBSTAR	1	0x00000000
14	Type 1 packet	REGISTER_WRITE	CMD	1	NULL
15	Type 1 packet	NO_OP			
16	Type 1 packet	REGISTER_WRITE	CMD	1	RCRC
17	Type 1 packet	NO_OP			
18	Type 1 packet	NO_OP			
19	Type 1 packet	REGISTER_WRITE	TIMER	1	0x00000000
20	Type 1 packet	REGISTER_WRITE	REG19	1	0x00000000
21	Type 1 packet	REGISTER_WRITE	COR0	1	0x00003fe5
22	Type 1 packet	REGISTER_WRITE	COR1	1	0x00000000
23	Type 1 packet	REGISTER_WRITE	IDCODE	1	0x0286e093
24	Type 1 packet	REGISTER_WRITE	CMD	1	SWITCH

RESULTS

- Correlation of PIP information according to the approach from the Debit project was performed, but in a tile-wise manner.

- This reveals that correlation according to Debit can only be successfully applied to two tile types: INT and HCLK. This means that full bitstream reversal remains difficult without any known correlation approach for the other tile types.

- Future work may include looking at performing correlation for other tile types and primitive site settings, as well as actual netlist reconstruction.

- The project has been released as open source for further development: http://florianbenz.github.com/bil/

TECHNISCHE UNIVERSITÄT DARMSTADT
Fraunhofer SIT
h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES
LOEWE – Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz