FPGA 역 공학 도구 분석

Soyeon Choi, Jiwoon Park, Hwasoo Shin, and Hoyoung Yoo
Department of Electronics Engineering, Chungnam National University, Korea
E-mail: hyyoo@cnu.ac.kr

FPGA 는 칩 내부 회로 구현을 자유롭게 변경할 수 있어 디지털 회로를 사용하는 다양한 산업분야에서 사용된다. 대표적으로 사용되는 SRAM-기반 FPGA 는 SRAM 이 휘발성 메모리이므로 외부의 비휘발성 메모리에 비트스트림을 저장하여야한다. FPGA 에 전원이 인가되면 외부의 PROM 으로부터 비트스트림이 FPGA 로 전송되는데, 이때 비트스트림에 손상이 발생할 수 있으며, 이는 군사방어, 범죄수사 등의 분야에서 심각한 문제를 야기할 수 있다. 이를 방지하기 위하여 비트스트림으로부터 넷리스트 파일을 복원하는 역 공학 도구들이 개발되었다.

Xilinx 사의 FPGA 는 RTL 코드를 합성할 때 ISE 디자인 도구를 이용하며, ISE 디자인 도구는 합성 과정에서 여러가지 파일을 생성한다. RTL 코드를 매핑하고 Place&Route 한 넷리스트 정보를 가지고 있는 NCD (Netlist Circuit Description) 파일은 바이너리 형식의 파일로 읽을 수 없다. NCD 파일은 바이너리 형식이므로 넷리스트를 문자 형태로 표현한 XDL (Xilinx Design Language) 파일로 변환할 수 있다. XDL 파일은 전체 칩의 정보가 아닌 RTL 코드가 매핑 된 부분의 정보만 나타내기 때문에 전체 칩의 정보를 알기 위해서 XDLRC (XDL report) 파일을 생성해야 한다.

1. Debit : Xilinx FPGA 의 역 공학 도구로 Debit 이 최초로 개발되었으며, Debit 은 비트스트림 파일과 XDL 파일의 교차 상관관계 알고리즘을 제안하고 이를 적용하여 외부 메모리로부터 전송된 비트스트림 파일을 XDL 파일로 복원한다. 전체 PLP (Programmable logic point), PIP (Programmable Interconnect Point)가 아닌 일부 PLP, PIP 에 대한 복원만 가능하여 불완전한 형태의 XDL 파일이 생성된다.

2. BIL : BIL 은 PIP 의 복원만 수행하는 역 공학 도구로, XDLRC 파일을 추가적으로 사용하여 복원된 XDL 파일의 정확도를 개선하고자 하였다. FPGA 분석을 먼저 수행하여 필요한 PIP 의 구성 데이터베이스를 생성하고 생성된 데이터베이스를 바탕으로 역 공학을 수행한다. PIP 에 대한 역 공학만 수행하기 때문에 복원되는 XDL 파일은 완전한 형태가 아니다.

3. Bit2ncd : Bit2ncd 는 XDL, XDLRC, 비트스트림을 이용하여 NCD 파일까지 복원하는 역 공학 도구이다. Bit2ncd 를 실행하기 전에 PIP 와 PLP 에 대한 수학적 분석 도구인 PK-분석과 PUK-분석을 사용하여 비트스트림의 매핑 테이블을 생성한다. 매핑 테이블을 이용하여 bit2ncd 툴을 실행시키면 완전한 형태로 복원된 XDL 파일을 생성할 수 있고, XDL 의 형태가 완전하므로 ISE 디자인 도구의 기본 명령어 xdl2ncd 를 사용하여 NCD 파일까지 복원할 수 있다.

4. BRET : BRET 은 BIL 를 기반으로 BIL 을 개선하고 PLP 의 복원도 가능한 역 공학 도구이다. XDL 파일 하나와 비트스트림 파일 하나만 사용하여 PIP 를 복원하는 BIL 과 달리 여러 개의

XDL 파일들과 비트스트림 파일들을 사용하기 때문에 BIL 에서 복원하지 못한 PIP 도 복원할 수 있다.

5. Bit2RTL : Wang 연구팀은 XDL 파일을 완벽하게 복원하여 RTL 코드까지 복원하는 역 공학 도구를 개발하였다. 세 단계로 구성되어 있으며, 첫 번째로 FPGA 를 분석하여 비트스트림 매핑 정보를 생성하고, 다음 단계에서 매핑 정보를 바탕으로 비트스트림 파일을 넷리스트로 복원하고, 마지막으로 복원한 넷리스트를 RTL 로 생성하는 과정으로 구성되어 있다.

표 1 은 5 가지의 역 공학 도구 Debit, BIL, Bit2ncd, BRET, Bit2RTL 을 비교한 내용을 나타내며, Bit2RTL 은 100% 정확도로 XDL 파일을 복원할 수 있으며, Bit2ncd 도 FPGA 의 모델에 따라서 100%에 가까운 정확도로 XDL 을 복원할 수 있다. Debit 과 BIL 은 일부 정보만 복원할 수 있어 나머지 역 공학 도구에 비하여 정확도가 낮다.

본 논문에서는 현재까지 개발된 FPGA 역 공학 도구들을 분석하고 비교하였다. 역 공학 도구는 하드웨어 유지 보수 및 손상 여부 파악에 필요하나 현재까지 개발된 역 공학 도구들은 최신 FPGA 칩은 지원하지 못한다. 따라서 최신 FPGA 에 적용가능한 역 공학 도구를 개발할 필요성이 있다.

	Input			**Output**	**Supported FPGA**	**Accuracy (%)**	
	BIT	XDL	XDLRC			PLP	PIP
Debit[1]	○	○	×	XDL	Vertex-2,3,4,5/Spartan-3	76.3	69.5
BIL[2]	○	○	○	XDL	Vertex-5	-	54.4
Bit2ncd[3]	○	○	○	XDL, NCD	Spartan-3,3E/Vertex-2,4,5	100	99.5
BRET[4]	○	○	○	XDL	Vertex-5	98.4	95.9
Bit2RTL[5]	○	○	○	RTL	Spartan-3	100	100

표 1. FPGA 역 공학 도구 비교

Acknowledgments 이 논문은 정부(과학기술정보통신부)의 재원으로 국가보안기술연구소의 지원(2019-0424-01)을 받아 수행된 연구임. EDA 툴은 IDEC의 지원을 받음.

References

[1] J.-B. Note and É. Rannaud, "From the bitstream to the netlist," in FPGA, 2008, vol. 8, pp. 264-264.

[2] F. Benz, A. Seffrin, and S. A. Huss, "Bil: A tool-chain for bitstream reverse-engineering," in 22nd International Conference on Field Programmable Logic and Applications (FPL), 2012: IEEE, pp. 735-738.

[3] Z. Ding, Q. Wu, Y. Zhang, and L. Zhu, "Deriving an NCD file from an FPGA bitstream: Methodology, architecture and evaluation," Microprocessors and Microsystems, vol. 37, no. 3, pp. 299-312, 2013.

[4] J. Yoon et al., "A Bitstream Reverse Engineering Tool for FPGA Hardware Trojan Detection," presented at the Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security - CCS '18, 2018.

[5] T. Zhang, J. Wang, S. Guo, and Z. Chen, "A Comprehensive FPGA Reverse Engineering Tool-Chain: From Bitstream to RTL Code," IEEE Access, vol. 7, pp. 38379-38389, 2019.