연결정보의 높은 복원율을 위한 Path-table 기반의 FPGA 역공학

최소연, 유호영
충남대학교 공과대학 전자공학과

FPGA Reverse Engineering based on Path- table for High-coverage of Programmable Interconnect

Soyeon Choi and Hoyoung Yoo
Department of Electronics Engineering
Chungnam National University
E-mail : sychoi.cas@gmail.com, hyyoo@cnu.ac.kr

Abstract

In this paper, we propose a PIP reverse engineering method using a path table to expand the restoration coverage of programmable interconnect points (PIP). The most commonly used SRAM-based FPGA is vulnerable to malicious attacks because it stores circuit information in external memory. Among the attack methods, FPGA reverse engineering has been proposed as a method of restoring a net list of circuits from a bitstream including circuit information, but there are disadvantages that the reverse engineering of the PIP, which is a connecting element, takes a long time or the restoration coverage is limited. In this paper, we propose a PIP reverse engineering method using a path table to enable the restoration of all PIPs in a short time. Using the proposed method, PIP reverse engineering can be performed perfectly in 19 times faster time than previous studies.

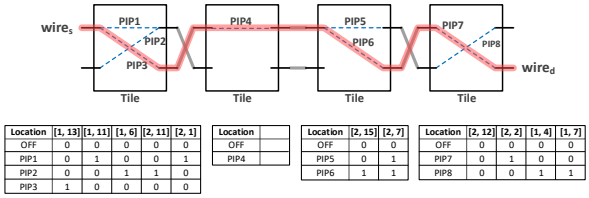
I. 서론

FPGA (Field Programmable gate array)는 내부에 재 구성 가능한 논리 요소들을 포함하는 반도체 소자로 여러 연구/산업 분야에서 사용된다 [1]. 가장 보편적으로 사용되는 SRAM 기반의 FPGA 는 외부 메모리에 회로 정보를 저장하기 때문에 악의적인 공격에 취약하다. 악의적 공격 방법 중 FPGA 역공학은 회로 정보를 포함한 비트스트림으로부터 넷 리스트를 복원하는 방법이다. BIT2NCD 에서 제안된 FPGA 역공학은 비트스트림과 넷 리스트의 연결관계를 정의하는 매핑 테이블을 사용한다 [1]. 이때, FPGA 내 논리 요소인 PLP (programmable logic point)와 연결 요소인 PIP (programmable interconnect point)를 비트 기법을 제안하였으나 PIP 역공학에 필요한 매핑 테이블 만드는 데에 수 백일 이상의 시간이 필요하다. Paar's team 이 PIP 매핑 테이블 생성에 소요되는 시간을 줄이는 방법을 제안하였다 [2]. 그러나 이 경우 복원하지 못하는 PIP 들이 발생해 복원의 범위가 줄어든다. 본 논문에서는 이를 개선하기 위해 path table 을 추가로 만들어 빠른 시간 내에 완벽한 PIP 역공학을 수행하는 방법을 제안한다.

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2021R1I1A3055806)

II. Background

BIT2NCD[1]에서 제안한 방법은 PIP 매핑 테이블을 만들때, PIP 로 구성되는 넷 (net)을 완벽하게 구성한다. 이때 넷은 연결하고자 하는 논리 요소들의 입출력인 wire 들을 연결하는 경로이다. 넷은 $wire_s$ 와 $wire_d$ 를 연결하는 경로의 수에 따라 경로의 수가 2 개 이상인 경우 다중-경로 넷 (multi-path net), 경로가 1 개인 경우 단일-경로 넷 (single-path net)으로 구분된다.



Location	[1, 13]	[1, 11]	[1, 6]	[2, 11]	[2, 1]
OFF	0	0	0	0	0
PIP1	0	1	0	0	1
PIP2	0	0	1	1	0
PIP3	1	0	0	0	0

Location	
OFF	
PIP4	

Location	[2, 15]	[2, 7]
OFF	0	0
PIP5	0	1
PIP6	1	1

Location	[2, 12]	[2, 2]	[1, 4]	[1, 7]
OFF	0	0	0	0
PIP7	0	1	0	0
PIP8	0	0	1	1

그림 1. Paar's team 의 방법으로 만든 PIP 매핑 테이블

Location	[1, 13]	[2, 7]	[2, 15]
OFF	0	0	0
PIP3-PIP4-PIP6	1	1	1

그림 2. PIP4 복원을 위한 경로 테이블

Paar's team [2]은 완전한 넷이 아니더라도 매핑 테이블을 위한 비트스트림을 만드는데 문제가 발생하지 않는다 점을 이용해 PIP 역공학에 소요되는 시간을 줄이는 방법을 제안하였다. Paar' team [2]은 PIP 를 하나만 포함하도록 비트스트림을 만들고, 이를 비교해 PIP 매핑 테이블을 생성한다. 이 방법을 하면 다중-경로 넷의 경우 BIT2NCD [1] 와 같이 모든 PIP 를 역공학 하는 것이 가능하다. 단일-경로 넷의 경우 그림 1 의 PIP 4 와 같이 PIP 양 단의 wire 에 연결된 PIP 가 1 개뿐인 PIP 가 net 상에 존재한다. 이 경우 PIP4 와 같은 PIP 는 [2]의 방법으로 매핑 테이블이 생성되지 않아 역공학이 불가하다.

III. Path-table 을 활용한 PIP 역공학

본 논문에서는 모든 넷에 대해 완벽하게 역공학을 수행할 수 있는 PIP 역공학 방법을 제안한다. 우선, 단일-경로 넷에서 복원이 불가능 했던 그림 1 의 PIP4 와 같은 형태의 PIP 를 전체 FPGA 에서 탐색하였다. 그 결과, FPGA 내에서 PIP 로 정의되어 있으나 항상 연결이 고정되는 PIP 가 이에 해당하며, FPGA 의 전체 PIP 중 약 40%를 차지한다. 이 PIP 들은 연결이 고정되므로 연결되는 PIP 또한 정해져 있기 때문에, PIP 양 단의 wire 에 연결되는 PIP 를 포함하는 경로 또한 특정할 수 있다. 경로를 구성한 후 경로에 대한 매핑 테이블을 만들어 그림 2 처럼 경로 테이블 (path-table)로 정리하면 PIP4 와 같은 PIP 를 역공학 하는 것이 가능하다.

경로 테이블을 이용해 PIP 역공학을 하기 위해서는 매핑 테이블로 복원한 PIP 정보가 필요하다. 따라서 경로 테이블을 사용하기 전 [2]의 방법으로 만든 PIP 매핑 테이블을 이용해 PIP 복원을 수행하는 과정이 선행되어야 한다. 이후 매핑 테이블로 복원하지 못한 PIP 가 있는지 경로 테이블로 확인해 PIP 역공학을 완료한다.

표 1. PIP 역공학 시간과 복원 범위 비교

Method	[1]	[2]	Proposed
Coverage	124 years	229 days	12 days
Time	100%	60%	100%

IV. 실험 결과

본 논문에서 제안하는 방법과 이전 연구 [1, 2]를 비교하기 위해 Xilinx 사의 Spartan-3 S50 칩을 목표로 하여 PIP 역공학을 수행하였다. Xilinx EDA 툴은 ISE Design Suite 14.7 을 사용하였으며, 매핑 테이블과 역공학 수행은 C 언어로 설계한 in-house tool 을 사용하였다. 표 1 은 BIT2NCD [1]과 Paar's team 의 방법 [2], 본 논문에서 제안한 방식의 PIP 복원 범위와 시간을 비교한다. 동일 환경에서 BIT2NCD [1]의 방법으로 PIP 매핑 테이블을 생성하고 PIP 역공학을 수행했을 때에는 모든 PIP 에 대해 복원이 가능하나 124 년의 시간이 소요되며, Paar's team [2]의 방법을 사용하면 복원에 대한 시간은 229 일로 줄일 수 있으나 60%의 PIP 만 복원할 수 있다. 그러나 제안하는 방법을 사용하면 약 12 일만에 모든 PIP 의 역공학이 가능하다.

IV. 결론

본 논문에서는 짧은 시간동안 모든 PIP 의 역공학을 수행하기 위해 경로 테이블을 이용한 PIP 역공학 기법을 제안하였다. 제안하는 방법을 사용하면 기존 연구 [2] 대비 19 배 빠르게 완벽한 PIP 역공학을 수행할 수 있어 FPGA 역공학의 실현 가능성 높이는 것이 가능하다.

참고문헌

[1] Z. Ding, et. al, "Deriving an NCD file from an FPGA bitstream: Methodology, architecture and evaluation," Microprocessors Microsystems-Embedd ed Hardware Des., vol. 37, no. 3, pp. 299–312, 2013.

[2] Maik Ender, et. al, "Insights into the mind of a trojan designer: the challenge to integrate a trojan into the bitstream," the 24th Asia and South Pacific Design Automation Conference (ASPDAC '19), pp. 112–119, 2019.