情報保護學會論文誌
第 21 卷 第 2 號, 2011. 4

상용 FPGA 클러스터 시스템 기반의 최적화된 DES 코어 설계

정 은 구,†‡ 박 일 환
ETRI 부설연구소

Optimized DES Core Implementation for Commercial FPGA Cluster System

Eun-Gu Jung,†‡ IlHwan Park
The Attached Institute of ETRI

요 약

기존의 FPGA기반 DES 전수조사 시스템은 비용대비 높은 성능을 가지고 있으나, 단일 FPGA에서 DES 알고리즘의 최적화 설계에 대한 연구는 미흡하다. 본 논문에서는 77개 Xilinx Virtex5-LX50 FPGA로 구성된 상용 FPGA 클러스터 시스템의 단일 FPGA에 최적화된 하드웨어 DES를 제안한다. 이를 위해서 DES 코어의 파이프라인 수, DES 코어 수, DES 코어의 동작 주파수 등에 따른 설계 공간 탐색을 수행하여 단일 FPGA에 333MHz로 동작하는 16개의 DES 코어를 집적했다. 또한, 각 FPGA에 공급되는 전력의 제한으로 인한 성능 하락을 줄이기 위해서 저전력 설계를 적용하여 333MHz로 동작하는 8개의 DES 코어를 집적했다. 제안된 DES을 상용 시스템에 적용할 경우, 각각 최대 2.03일과 4.06일안에 DES 키를 찾을 수 있을 것으로 판단된다.

ABSTRACT

The previous FPGA cluster systems for a brute force search of DES keyspace have showed cost efficient performance, but the research on optimized implementation of the DES algorithm on a single FPGA has been insufficient. In this paper, the optimized DES implementation for a single FPGA of the commercial FPGA cluster system with 77 Xilinx Virtex5-LX50 FPGAs is proposed. Design space exploration using the number of pipeline stages in a DES core, the number of DES cores and the maximum clock frequency of a DES core is performed which leads to integrating 16 DES cores running at 333MHz. Also low power design is applied to reduce the loss of performance caused by limitation of power supply on each FPGA which results in fitting 8 DES cores running at 333MHz. When the proposed DES implementations would be used in the FPGA cluster system, it is estimated that the DES key would be found at most 2.03 days and 4.06 days respectively.

Keywords: DES, FPGA, COPACOBANA, BRUTE-FORCE ATTACK

I. 서 론

DES 암호알고리즘[1]은 64비트 평문과 56비트 키를 이용하여 64비트 암호문을 생성하며, 16개 라운드를 가지는 Feistel 구조의 블록 암호이다. 키 길이는 56비트에 불과하여 전수 조사 공격[2]에 대한 취약점을 가지고 있다. 즉, 알려진 64비트 평문과 거기에 대응하는 64비트 암호문이 있을 경우에, 알려진 평문과 키 공간 전부에 대해서 DES 암호화를 수행하여 64비트 암호문과 일치하는 키를 찾는다. 키를 찾으면 같은 키로 암호화된 암호문을 모두 평문으로 복호화할 수 있다.

한편, 급격한 반도체 기술의 발달로 DES 전수조사

접수일(2011년 1월 18일), 게재확정일(2011년 4월 4일)
† 주저자, egjung@ensec.re.kr
‡ 교신저자, egjung@ensec.re.kr

공격은 고비용의 전용칩[3]을 이용하는 단계에서 저비용의 FPGA[4-8]를 이용하는 단계로 발전하고 있다. 최근에 제작된 COPACOBANA 5000[6, 7]의 경우에는 128개의 FPGA 칩을 이용하여 최대 3.58일 안에 키를 찾을 수 있을 것으로 예측하고 있고, 176개의 FPGA로 구성된 상용 FPGA 클러스터 시스템[8]은 최대 2.98일안에 DES 키를 찾을 수 있을 것으로 발표했다. 특히, 상용 FPGA 클러스터 시스템의 개발은 FPGA 시스템 개발 및 검증, 그리고 소프트웨어 드라이버 및 API 개발 시간을 생략할 수 있어서, 연구 개발 시간을 단축할 수 있는 장점이 있다. 그러나 기존 연구들은 FPGA 클러스터 시스템의 장점인 비용대비 높은 성능과 빠른 개발에 초점을 맞추고 있어서, DES 전수조사를 위한 DES 하드웨어의 최적화 설계에 관한 연구는 부족한 실정이다. 비록 [4, 5]에서 4개의 코어를 하나의 FPGA에 집적해서 최대의 성능을 얻었다고 설명했지만 그 방법론에 대한 자세한 설명은 없다.

본 논문에서는 검증된 상용 FPGA 클러스터 시스템인 PICO Computing사의 SuperCluster-3[9]을 이용하여 단일 FPGA에 최적화된 하드웨어 DES를 제안한다. 이를 위해서 DES 코어의 파이프라인 수, DES 코어 수, DES 코어의 동작 주파수 등에 따른 설계 공간 탐색을 수행하여 최적화된 DES를 설계하였다. 또한, 개별 FPGA에 공급되는 전력제한으로 인한 성능 하락을 줄이기 위해서 저전력 설계도 적용하였다. 제안된 DES를 77개의 FPGA로 구성된 상용 클러스터 시스템에 적용할 경우, 최대 2.03일안에 DES 키를 찾을 수 있을 것으로 예측된다.

본 논문은 다음과 같이 구성된다. 2장에서는 ASIC 및 FPGA기반 DES 전수조사 시스템에 관한 기존 연구와 DES 알고리즘에 대해서 살펴보고, 3장과 4장에서는 상용 FPGA 클러스터 시스템인 SuperCluster-3과 단일 FPGA에 최적화된 DES 설계에 대해서 설명한다. 5장에서는 설계된 DES의 성능을 평가하고 6장에서 결론을 맺는다.

II. 관련 연구

2.1 DES 전수조사 시스템

DES 전수조사 시스템 설계에는 크게 2가지 방법이 사용되었다. 첫 번째는 ASIC 설계 기술을 이용하여 DES 전용 칩을 개발하고 이를 기반으로 시스템을 설계하는 것이다. 전용 칩 개발에는 많은 시간과 비용이 들지만, DES 연산 속도가 매우 빠르다는 장점이 있다. 두 번째 방법은 FPGA를 기반으로 해서 시스템을 설계하는 것이다. FPGA는 전용 칩에 비해서는 느리지만, 칩을 제조할 필요가 없어서 개발 시간이 짧은 장점이 있다.

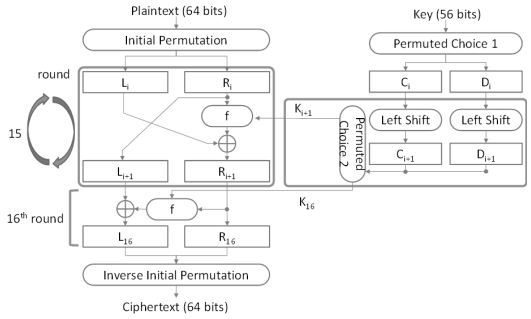
DES 전용 칩 기반의 DES 전수조사 시스템의 설계는 1977년에 2천만 달러의 비용으로 전용 칩 백만 개를 이용하여 12시간 안에 키를 찾을 수 있을 것으로 예측했고[10], 1992년에 백만 달러의 비용으로 57,600개의 DES 전용 칩으로 3.5시간 안에 가능할 것으로 예측했다[11]. 이후 1998년에 25만 달러의 비용으로 1,800개의 DES 전용 칩으로 최대 9일안에 키를 찾을 수 있는 EFF DES Cracker 시스템이 실제 제작되었다[3].

FPGA 기반 DES 전수조사 시스템의 설계는 2000년 3,248개의 FPGA를 이용하여 최대 14.9일 안에 DES 키를 찾을 수 있는 RASH 시스템이 개발되었고[12], 2006년에 1만 달러의 비용으로 120개의 FPGA를 이용하여 최대 12.8일안에 DES 키를 찾을 수 있는 COPACOBANA[4, 5] 시스템이 제작되었고, 후속 시스템인 COPACOBANA 5000[6, 7]이 2009년에 개발되었다. 이 시스템은 128개의 FPGA를 포함하고 있으며, 최대 3.58일안에 키를 찾을 수 있을 것으로 예측했다. 이 예측값은 FPGA의 용량 증가를 기반으로 해서 계산된 값이다. 최근 2010년에 FPGA기반 슈퍼클러스터 시스템 개발회사인 PICO Computing사에서 176개의 FPGA를 이용하여 최대 2.98일안에 DES 키를 찾을 수 있음을 발표했으나, 구체적인 설계 내용은 공개하지 않았다[8].

2.2 DES 알고리즘

DES 알고리즘은 64비트 평문과 56비트 키를 이용하여 64비트 암호문을 생성하는 Feistel 구조의 블록 암호로써, 16개의 라운드로 구성된다[1]. [그림 1]과 같이 암호화 과정에서 평문은 초기 치환을 거친 후 각각 32비트의 L값과 R값으로 나누어진다. 이 값에 대해서 16번 라운드 연산을 수행한다. 즉, 다음 라운드의 L값은 현재의 R값이고, 다음 라운드의 R값은 현재 L값과 f 함수의 출력의 XOR 연산 결과이다. 이때, f 함수는 현재 R값과 라운드 키를 이용하여 비트 선택 테이블, XOR 연산 그리고 S-BOX 연산을 수행한다. 마지막 라운드는 이전 라운드와 다르게 R값과

L값을 서로 바꾸지 않는다. 그리고 최종적으로 역 치환을 수행한 후, 64비트 암호문을 얻는다. 각 라운드에서 필요한 라운드 키는 입력 56비트 키의 치환을 거친 후, 각각 28비트의 C값과 D값으로 나누어지고 각각에 대해서 왼쪽 쉬프트를 수행한다. 이때, 쉬프트 양은 각 라운드마다 1 혹은 2로 고정되어 있다. 그리고 쉬프트된 값을 다시 치환하여 라운드 키를 얻는다.

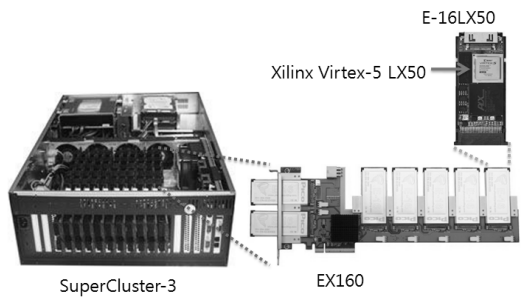


〔그림 1〕 DES 알고리즘의 암호화 과정

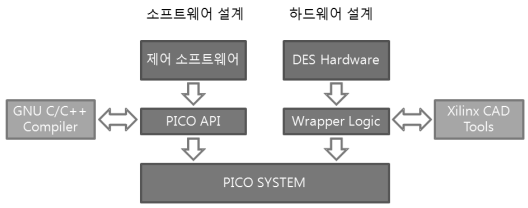
III. FPGA 클러스터 시스템

PICO Computing사의 FPGA기반 슈퍼 클러스터 시스템인 SuperCluster-3(이하 SC-3)는 〔그림 2〕와 같이 4U랙마운트 높이에 2개의 인텔 제온 프로세서 및 11개 이상의 PCIe 카드를 장착할 수 있는 메인보드로 구성되어있다. PCIe 카드인 EX160은 Xilinx사의 고성능 FPGA인 Virtex-5 LX50 (XC5VLX50-2- FF324)이 포함된 E-16 카드를 7개까지 장착할 수 있기 때문에, SC-3은 최대 77개의 FPGA를 장착할 수 있다.

SC-3을 이용하여 시스템을 개발하기 위해서는 〔그림 3〕과 같이 하드웨어 설계 및 소프트웨어 개발이 필



〔그림 2〕 PICO Computing사의 FPGA기반 슈퍼클러스터인 SC-3의 구조



〔그림 3〕 SC-3을 이용한 시스템 개발 과정

요하다. 먼저, PICO Computing사에서 제공된 레퍼 로직(wrapper logic)을 포함한 DES 하드웨어를 Xilinx사의 ISE 캐드툴을 사용하여 설계한다. 이때, 레퍼 로직은 PICO Com`puting사에서 개발된 API와 관련된 하드웨어가 포함되어 있어, 설계된 하드웨어 입출력은 모두 레퍼 로직을 통해서만 가능하다. 개발된 시스템을 제어하기 위해서 PICO Computing사에서 제공된 API를 이용하여 제어 소프트웨어를 개발하며 GNU C/C++ 컴파일러가 사용된다.

IV. DES 하드웨어 설계

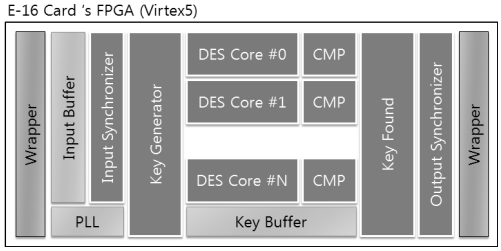
4.1 DES 하드웨어 구조

DES 하드웨어 구조는 〔그림 4〕와 같이 레퍼 로직을 통해서 DES 하드웨어에 데이터를 전송하고 결과를 받는다. 이때, 레퍼 로직은 66.67MHz로 동작하며, 32 비트의 데이터 폭을 가진다. 레퍼 로직을 통해서 전송된 입력값은 버퍼 블록인 Input Buffer에 저장되고, 이들 값들은 고속으로 동작하는 내부 DES 코어에 전송하기 위해서 동기화 블록인 Input Synchronizer를 경유하게 된다. 입력값 중에서 키의 시작값은 Key Generator 블록에 전송되어 매 클록마다 새로운 키를 발생하여 DES 코어에 공급한다. 나머지 입력값인 평문은 DES 코어에 전달되고, 암호문은 비교 연산을 수행하는 CMP 블록에 전송된다. 이때, 생성된 키는 Key Buffer 블록에 함께 저장된다. 한편, DES 코어 블록등 고속 동작이 필요한 블록의 클록은 PLL 블록에서 공급한다. DES 코어에서 암호문이 출력되면, CMP 블록에서 DES 코어의 출력과 찾고자 하는 암호문이 맞는지 비교한다. 키가 맞을 경우에 Key Buffer 블록에서 해당하는 키값을 찾는다. 이 과정은 Key Found 블록에서 이루어진다. 찾은 키값을 저속의 래퍼 로직으로 전송하기 위해서 동기화 블록인 Output Synchronizer를 경유한다.

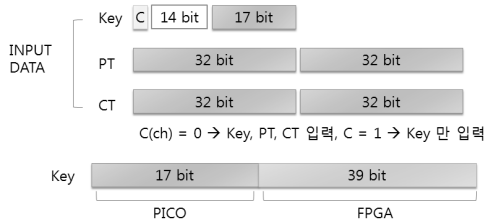
FPGA에 전송되는 입력 데이터는 〔그림 5〕와 같이

64비트 평문(PT), 64비트 암호문(CT), 17비트 키 시작주소와 1비트 채널 값으로 구성되어 있다. DES 키는 56비트이므로 나머지 39비트만큼 FPGA 내부에서 조사하게 된다. 데이터 전송 순서가 키 시작주소, 평문, 암호문이기 때문에 1비트 채널 값을 이용하여 평문과 암호문 데이터의 전송여부를 파악할 수 있고, 이 정보를 바탕으로 Input Buffer 블록이 저장해야할 데이터를 미리 결정할 수 있다. 즉, 평문과 암호문은 키 값을 찾을 때까지 한번만 전송하지만 키 시작주소는 계속 공급한다.

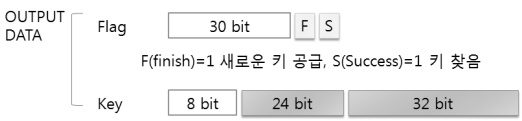
출력 데이터의 구조는 〔그림 6〕과 같이 주어진 키 시작주소에서 키를 찾는 과정이 끝났음을 나타내는 1비트 F 플래그와 키를 찾았음을 나타내는 1비트 S 플래그로 구성된 플래그와 찾은 56 비트 키값으로 구성되어 있다.



〔그림 4〕 DES 하드웨어 구조



〔그림 5〕 입력 데이터 구조



〔그림 6〕 출력 데이터 구조

4.2 DES 코어

DES 하드웨어 구조에서 DES 코어 수 및 동작 주파수는 DES 키 탐색 시간에 반비례하기 때문에 단일 FPGA에서 DES 코어 수와 동작 주파수의 곱이 최대가 되도록 DES 코어를 구현해야 한다. 먼저, 지금까지 발표된 하드웨어 DES 〔13, 14〕 중에서 현재까지 FPGA상에서 면적 대비 최대의 성능을 보인 DES 코어〔13〕를 기본 DES 코어로 선택했고, E-16 카드의 FPGA에 구현했다. 구현된 DES 코어는 파이프라인과 루프 언롤링을 적용하였고, 라운드 키는 on-the-fly 형식으로 생성하도록 설계하였다.

〔표 1〕과 같이 DES 코어에 적용된 파이프라인 수에 따라서 4개의 DES 코어를 각각 구현하였고, 각 파이프라인 수에 따른 동작 주파수와 E-16카드에서 구현할 수 있는 이론상 최대 DES 코어 수를 계산했다. 이때, E-16 카드의 FPGA에서 사용할 수 있는 면적인 슬라이스〔15〕 수는 7,200개이다. 비록 룩업테이블(Look-Up Table, LUT)과 레지스터로 구성된 슬라이스는 구현시에 룩업테이블과 레지스터를 동시에 모두 사용하는 경우가 100%가 되지 않기 때문에, 슬라이스 기준에 비해서 더 많은 DES 코어를 집적할 가능성은 있다. 그러나 이 경우 셀의 배치 및 라우팅의 복잡도가 급격히 증가하여 DES 코어의 동작 주파수가 급격히 떨어지는 문제가 있기 때문에 여기서는 고려하지 않는다.

〔표 1〕에서 단일 FPGA의 성능을 DES 코어의 동작 주파수와 DES 코어 수의 곱의 값을 기준으로 할 때, DES 코어의 파이프라인 수가 17인 경우에 최대 성능을 나타내었다. 따라서 DES 하드웨어 구조에서 DES 코어는 17단 파이프라인을 가지도록 설계했다. 이때, 파이프라인 수가 17인 경우는 각 라운드마다 파이프라인 단계를 적용할 때, 34는 S-BOX를 기준으로 라운드마다 2개의 파이프라인 단계를 적용할 때, 그리고 8과 5는 각각 2개와 4개의 라운드를 하나의 파이프라인 단계로 적용할 때이다.

〔표 1〕 파이프라인 수에 따른 DES 코어 성능 비교

파이프라인 수	면적 (슬라이스)	동작 주파수 (MHz)	DES 코어 수	동작 주파수 x DES 코어 수
5	465	203.7	15.4	3,136
8	484	293.5	14.8	4,343
17	716	525.4	10.0	5,254
34	911	544.1	7.9	4,298

4.3 DES 하드웨어 구현

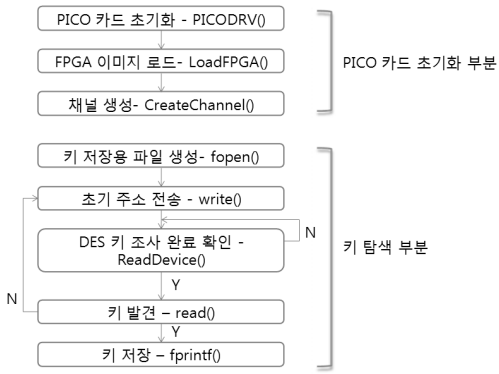
앞 소절에서 선택된 DES 코어는 17단 파이프라인

을 가지며, 1단 파이프라인의 임계 경로의 시간은 연속된 2개의 CLB(Configurable Logic Block)〔15〕를 지나는 시간과 같다. 이때, 라우팅에 의한 지연시간은 무시한다. 이것은 DES 하드웨어 전체가 구현되어야 정확한 값을 알 수 있기 때문이다. 여기서 CLB는 FPGA에서 순차 및 조합논리회로를 구성하기 위한 기본 리소스로써 Virtex-5는 2개의 슬라이스로 구성되고 있다. 각 슬라이스 6개의 1비트 입력을 가지는 4개의 룩업테이블과 4개의 1비트 레지스터로 구성된다. 따라서 〔그림 4〕에서 DES 하드웨어 구조의 나머지 블록의 구현에서 임계 경로는 2개의 CLB를 지나는 시간과 같도록 설계해야한다. 이것은 VLSI 설계에서 파이프라인을 연속된 게이트 수를 기준으로 적용하는 것과 마찬가지로 FPGA 설계에서는 연속된 CLB 수를 기준으로 적용해야 하기 때문이다. 이를 위해서, 각 블록 구현시에 2개의 CLB를 기준으로 파이프라인을 적용했다.

블록 구현에서 Key Generator 블록은 키값을 증가시키기 위해서 사용된 덧셈기로 인해서 임계 경로를 2개의 CLB로 맞추기가 어려운 블록이다. 이를 해결하기 위해서 고속 구현이 가능한 LFSR을 이용해서 키 주소를 생성하도록 설계했다. 이때, LFSR에서 생성할 수 없는 0값은 마지막 LFSR 값을 출력한 뒤, 상수 0값이 출력하도록 제어로직을 추가했다.

한편, DES 하드웨어의 설계를 단순화 및 고속화하기 위해서 DES 코어의 수를 2의 지수승이 되도록 설계했다. 즉, 8개의 DES 코어를 가지는 경우와 16개의 DES 코어를 가지는 경우로 각각 설계했다. 앞 소절에서 설명한 것처럼 이론상 DES 코어가 10개밖에 집적할 수 없지만, 남아있는 룩업테이블 혹은 레지스터를 이용해서 DES 코어를 더 집적할 여지가 있다. 따라서 17단 파이프라인을 가지는 경우에는 최대 16개의 DES 코어를 집적할 수 있다. 그러나 이것은 셀의 배치와 라우팅의 복잡도를 급격히 증가시켜 DES 코어의 최대 동작 주파수를 낮추는 단점이 있고, 캐드툴에 의한 DES 코어의 면적을 줄이기 위한 시도에 의해서 성능이 더욱 하락할 수 있다. 이러한 영향에 의한 성능 하락은 5장에서 설명한다.

또한, 2의 지수승인 DES 코어 수는 Key Generator 블록에서 키값의 마지막 비트값을 고정시킬 수 있어서 Key Generator 블록의 설계를 단순화시킨다. 즉, 8 코어일 때는 3비트를, 16코어일 때 4비트를 고정할 수 있다. 또한 Key Found 블록에서는 CMP 블록의 결과값으로 찾아진 키의 마지막 비트값을 쉽게 알 수 있다. 즉, 8 코어일 경우에는 8-to-3 인코더, 16 코어일 경우에는 16-to-4 인코더를 사용하면 된다. 마찬가지로 DES 하드웨어 내부구조를 래퍼로직의 동작주파수의 배수배가 되도록 했다. 이렇게 함으로써 입력값과 출력값의 동기화 블록의 설계를 단순화할 수 있다.



〔그림 7〕 DES 하드웨어의 제어 소프트웨어 구조

4.4 제어 소프트웨어

DES 하드웨어 제어 소프트웨어는 〔그림 7〕과 같이 PICO API를 이용하여 크게 PICO카드 초기화 부분과 키 탐색 부분으로 나눌 수 있다. PICO 카드 초기화 부분은 PICODRV()함수를 이용하여 E-16 카드를 초기화시키고 설계된 하드웨어의 비트 파일을 LoadFPGA()함수를 이용해서 다운로드한다. 그 다음 각 카드와 호스트 PC가 서로 데이터를 전송하기 위해서 CreateChannel()함수를 이용하여 채널을 만든다.

PICO 카드의 초기화 부분이 끝난 다음 DES 키 탐색을 수행한다. DES 키 조사 부분은 찾은 키를 저장할 파일 생성, 초기 주소 전송, FPGA의 DES 키 조사 완료 확인, 그리고 찾은 키를 FPGA에서 읽어서 파일에 저장 등으로 구성된다. 초기 주소는 초기화 파트에서 생성된 채널과 write()함수에 의해서 각 FPGA로 전송된다. 이때, 평문과 암호문이 함께 전송되고, 두 번째 전송부터는 주소만 전송된다. DES 키 조사 완료 확인은 폴링 방식으로 FPGA의 F비트 값이 1인지 확인하는 작업이다. 만약 0이면 DES 키 조사가 완료되지 않는 것이고, 1이면 완료된 것이다. DES 키 조사가 완료되면 S비트 값을 이용하여 FPGA가 키를 찾았는지 확인한다. 만약에 찾았다면 FPGA에 저장된

키값을 read() 함수를 이용해서 읽어서 fprintf() 함수를 이용하여 파일에 저장한다. 만약에 발견되지 않았다면 다음 주소를 생성해서 DES 키 조사를 수행한다.

V. 성능 평가

DES 하드웨어 설계는 하드웨어 언어인 Verilog을 이용하여 기술하였고 Xilinx ISE 10.1 캐드툴을 이용하여 합성 및 P&R을 수행하였다. 이때, 필요한 constraint file, 합성 및 P&R 스크립트는 PICO Computing사에서 제공된 것을 이용하였다.

앞장에서 설명한 것처럼 8개의 DES 코어를 가지는 경우와 16개의 DES 코어를 가지는 경우의 설계 결과는 〔표 2〕와 같다. 코어 수가 8개일 때의 최대 동작 주파수가 400MHz이며, 16개일 때는 최대 333MHz의 동작 주파수를 기록하였다. 이것은 77개의 FPGA를 이용하여 전수조사를 수행할 경우, 8 코어의 경우에는 최대 3.38일이 필요하고 16 코어의 경우에는 최대 2.03일이 필요할 것으로 예측된다. 이때, 전수조사시간은 단일 FPGA의 성능으로부터 계산된 값이다. 여기서, DES 하드웨어의 속도가 4장에서 설계된 단일 DES 코어의 속도보다 떨어지는 것은 FPGA 내부의 자원을 대부분 사용함으로써 셀의 배치와 라우팅 복잡도가 급격한 증가했기 때문이다. 또한, 코어수가 10개보다 많이 집적될 수 있는 이유는 4장에서 설명한 것처럼 슬라이스에서 남는 룩업테이블과 레지스터를 추가로 사용하기 때문이다. 그러나 이것은 셀 배치와 라우팅의 복잡도를 급격히 증가시켜 동작 주파수를 하락시킨다. 즉, 16 코어의 최대 동작주파수는 8 코어에 비해서 20%정도 낮다.

비록 16 코어의 동작 주파수는 단일 DES 코어보다 36.6% 낮지만, 단일 FPGA의 성능을 의미하는 동작 주파수와 DES 코어 수의 곱에서는 16 코어가 5,328로, 단일 DES 코어의 이론값인 5,254보다 약 1.4% 약간 높다. 이것은 설계된 DES 하드웨어가 최적의 지점에 도달했다는 것을 의미한다.

한편, SC-3의 E-16 카드에서 발생하는 열과 각 FPGA로 공급되는 전력의 제한으로 앞에서 설계된 3가지 모두 정상적인 동작을 하지 못했다. 〔그림 8〕과 같이 FPGA로 공급되는 전원 부분을 수정하고 FPGA에 방열판을 추가로 더 장착하면 〔표 2〕에서 설계된 3가지 모두 동작시킬 수 있다. 그러나 E-16 카드의 하드웨어 수정 없이 사용하려면 DES 하드웨어의 저전력 설계가 필요하다.

〔표 2〕 DES 하드웨어 구현 결과 비교

코어 수	면적 (슬라이스)	동작주파수 (MHz)	동작 주파수 x DES 코어 수	전수조사시간 (77 FPGAs)
8	4,532	333	2,664	4.06 일
8	6,036	400	3,200	3.38 일
16	6,720	333	5,328	2.03 일

〔그림 8〕 수정된 E-16카드

FPGA의 저전력 설계를 위해서 Xilinx사의 백서〔16〕와 저전력 FPGA 설계 논문〔17, 18〕을 참조하여 저전력 설계를 수행하였다. 특히, Xilinx ISE 캐드툴에서 제공하는 저전력 설계를 위한 여러 가지 옵션을 함께 이용하였다. 〔표 3〕과 같이 8 코어일 때는 같은 성능을 유지하면서 면적이 약 7.8% 감소하였다. 16 코어일 때는 동작 주파수가 267MHz로 감소하였고 면적은 8.2% 감소하였다. 그러나 E-16 카드에서 동작하는 것은 DES 코어가 8개이고 동작주파수 333MHz인 경우이다. 따라서 E-16 카드의 하드웨어 수정이 없을 경우에 DES 전수조사 시간은 최대 4.06일안에 가능할 것으로 예상된다.

〔표 3〕 저전력 DES 하드웨어 구현 결과 비교

코어수	면적 (슬라이스)	동작 주파수 (MHz)	전수조사시간 (77 FPGAs)	동작여부
8	4,371	333	4.06 일	O
8	5,561	400	3.38 일	X
16	6,164	267	2.54 일	X

VI. 결 론

본 논문에서는 검증된 상용 FPGA 클러스터 시스템인 PICO Computing사의 SuperCluster-3 (SC-3)에 최적화된 하드웨어 DES를 제안한다. 이를

위해서 DES 코어의 파이프라인 수, DES 코어 수, DES 코어의 동작 주파수 등에 따른 설계 공간 탐색을 수행하여 단일 FPGA에 최대 16개의 DES 코어를 집적할 수 있었다. 이때, DES 코어의 최대 동작 주파수는 333MHz를 기록하였다. 이 결과를 77개의 FPGA로 구성된 SC-3에 적용할 경우에는 최대 2.03일안에 DES키를 찾을 수 있을 것으로 판단된다. 또한, 설계된 DES 하드웨어를 이용하기 위해서는 FPGA에 공급되는 전원부의 수정이 필요하기 때문에, 저전력 설계 기법을 적용하여 하드웨어 변경 없이 사용할 수 있는 저전력 DES 하드웨어도 설계하였다. 단일 FPGA에 333MHz의 동작 주파수를 가지는 8개의 DES 코어를 집적할 수 있었고, 같은 FPGA 클러스터 시스템에 적용할 경우에 최대 4.06일안에 DES 키를 찾을 수 것으로 예상된다.

참고문헌

〔1〕 FIPS PUB 46-3, "Data Encryption Standard (DES)," December 1999.

〔2〕 M. Stamp, Information Security: Principles and Practice, Wiley-Interscience, October 2005.

〔3〕 Electronic Foundation, Cracking DES, O'Reilly Media, July 1998.

〔4〕 S. Kumar, C. Paar, J. Pelzl, G. Pfeiffer, A. Rupp, and M. Schimmler, "How to Break DES for € 8,980," Proceedings of Special-purpose Hardware for Attacking Cryptographic Systems, October 2006.

〔5〕 T. Guneysu, T. Kasper, M. Novotny, C. Paar, and A. Rupp, "Cryptanalysis with COPACOBANA," IEEE Transactions on Computers, vol. 57, no. 11, pp.1498-1513, November 2008.

〔6〕 T. Guneysu, G. Pfeiffer, C. Paar, and M. Schimmler, "Three Years of Evolution: Cryptanlaysis with COPACOBANA," Proceedings of Special-purpose Hardware for Attacking Cryptographic Systems, pp. 1-16, September 2009.

〔7〕 L. Wienbrandt, S. Baumgart, J. Bissel, C. M. Y. Yeo, and M. Schimmler, "Using the reconfigurable massively parallel architecture COPACOBANA 5000 for applications in bioinformatics," Proceedings of Internationals Conference on Computational Science, ICCS 2010, pp. 1027-1034, May 2010.

〔8〕 Pico Computing, Inc., "FPGA Cluster Demonstrates Massively Parallel, Hardware-Accelerated DES Cracking," January 2010. Available: http://www. picocomputing.com/pdf/PR_Pico_DES_BH_Jan_29_2010.pdf

〔9〕 Pico Computing, Inc., SC-Series Clusters. Available: http://www.picocomputing.com/ sc_series.html.

〔10〕 W. Diffe and M. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," Computer, 10, pp.74-84, June 1977.

〔11〕 M.J. Wiener, "Efficient DES Key Search," TR-244, School of Computer Science, Carleton University, Ottawa, 1994.

〔12〕 T. Katsumi, M. Iida, and K. Nkakjima, "Time-Memory Trade-off Cryptanalysis on FPGA-based Parallel Machine RASH," Proceedings of 4th IEEE AP-HPC, May 2000.

〔13〕 G. Rouvroy. "Efficient Uses of FPGAs for Implementations of DES and Its Experimental Linear Cryptanalysis," IEEE Transactions on Computers, 52, pp.473-482, April 2003.

〔14〕 한승조, "VHDL을 이용한 고속 DES 암호칩 설계 및 구현," 정보보학회논문지, 8(3), pp.79-94, 1998년 9월.

〔15〕 Xilinx, Virtex-5 FPGA User Guide, UG190 (v5.3) May 17, 2010. Available: http:// www.xilinx.com/support/documentation/user_ guides/ug190.pdf

〔16〕 Peggy A. "Virtex-5 FPGA System Power Design Considerations," Xilinx White Paper, WP285 Feb. 2008. Available: http://www.xilinx.com/support/documentation/white_papers/wp285.pdf

〔17〕 G. Sutter and E. Boemo, "Experiments

in Low Power FPGA Design," Proceedings of Latin American Applied Research, vol. 37, no. 1, pp. 99-104, January 2007.
[18] F. Sun, H. Wang, F. Fu, and X. Li, "Survey of FPGA low power design," Proceedings of 2010 International Conference on Intelligent Control and Information Processing (ICICIP), pp. 547-550, Oct. 2010.

〈著者紹介〉

정 은 구 (Eun-Gu Jung) 정회원
2000년 2월: 경북대학교 전자전기공학부 졸업
2002년 2월: 광주과학기술원 정보통신공학과 석사
2006년 2월: 광주과학기술원 정보통신공학과 박사
2007년 3월~2008년 2월: 미국 카네기멜론대학교 박사후 연구원
2008년 4월~현재: 한국전자통신연구원 부설연구소
〈관심분야〉 암호알고리즘 하드웨어 설계, 컴퓨터 구조, 비동기 VLSI 설계

박 일 환 (IlHwan Park) 정회원
1988년 2월: 고려대학교 수학과 졸업
1990년 2월: 고려대학교 수학과 석사
1996년 2월: 고려대학교 수학과 박사
1996년 5월~1999년 12월: 한국전자통신연구원
2000년 1월~현재: 한국전자통신연구원 부설연구소
〈관심분야〉 정보보호이론