LILI-II 스트림 암호의 고속화 구현에 관한 연구

정회원 이 훈 재*, 문 상 재**

On a High-speed Implementation of LILI-II Stream Cipher

Hoon-Jae Lee*, Sang-Jae Moon** *Regular Members*

요 약

LILI-II 스트림 암호는 NESSIE 후보로 제안된 바 있는 LILI-128의 성능개선 알고리듬이다. 이 알고리듬은 클럭 조절형 스트림 암호방식이며, 구조적으로 동기식 논리회로 구현시 속도가 저하되는 단점이 있다. 본 논문에서는 이 문제를 보완하고자 4-비트 병렬 LFSR을 제안하였으며, 각 레지스터 비트는 4개의 서로 다른 귀환 또는 이동 경로를 갖게 된다. 그리고 ALTERA 사의 Max+plus II 툴과 FPGA 소자(EPF10K20RC240-3)를 선정하여 하드웨어 구현 및 타이밍 시뮬레이션을 실시하였으며, 최신 Lucent ASIC 소자 기술(LV160C, 0.13μm CMOS & 1.5v technology)로 설계시 지연시간이 1.8ns 이하였고, 500 Mbps 이상의 고속화가 가능함을 확인하였다. 마지막으로 LILI-II 암호를 병렬 구현시 속도가 4, 8, 또는 16 Gbps (m=8, 16 또는 32)로 고속화 가능함을 제시하였다.

Key Words : LILI-128, LILI-II, stream cipher, clock-controlled sequence, keystream generator.

ABSTRACT

LILI-II stream cipher is an upgraded version of the LILI-128, one of candidates in NESSIE. Since the algorithm is a clock-controlled, the speed of the keystream data is degraded structurally in a clock-synchronized hardware logic design. Accordingly, this paper proposes a 4-bit parallel LFSR, where each register bit includes four variable data routines for feedback or shifting within the LFSR. Furthermore, the timing of the proposed design is simulated using a Max+plus II from the ALTERA Co., the logic circuit is implemented for an FPGA device (EPF10K20RC240-3), and apply to the Lucent ASIC device (LV160C, 0.13μm CMOS & 1.5v technology), and it could achieve a throughput of about 500 Mbps with a 0.13μm semiconductor for the maximum path delay below 1.8ns. Finally, we propose the m-parallel implementation of LILI-II, throughput with 4, 8 or 16 Gbps (m=8, 16 or 32).

Ⅰ. 서 론

해킹 등과 같은 정보화 사회의 여러 가지 역기능 문제 해결에 필수 기술인 암호 알고리듬은 공개키 암호(public-key cryptosystem) 및 대칭키 암호(symmetric cipher)로 대별된다. 대칭키 암호는 또 다시 블록 암호(block cipher)와 스트림 암호(stream cipher)로 나뉘어지며, 이 중에서 스트림 암호는 블록 암호보다 빠르고 암호화 과정이 간단하다. 예를 들면, RC4[1-2]는 SSL과 같은 인터넷 보안 응용을 구현함에 있어서 가장 유사한 블록 암호보다 2배 이상 빠르고 구현이 쉬운 것으로 조사되었다[3]. 70~90년대에 발표된 대표적인 키 수열 발생기(스트림 암호)로는 비메모리 형태의 Geffe 발생기[7]와 메모리 형태의 Rueppel 합산 수열 발생기(summation generator)[8~10]를 들 수 있다. 이들

* 동서대학교 인터넷공학부 정보네트워크공학전공(hjlee@dongseo.ac.kr),
** 경북대학교 전자전기공학부(sjmoon@knu.ac.kr)
논문번호 : 030093-0312, 접수일자 : 2003년 3월 12일
※본 연구는 대학 IT지원센터육성 · 지원사업 및 동서대학교 특별연구과제 연구결과로 수행되었습니다.

두 방식은 최대 주기 뿐 아니라 랜덤 특성이 양호하고 구현이 용이한 장점이 있지만, 안전성 측면에서 몇가지 문제가 있다. Geffe 발생기는 선형 복잡도가 작고 상관 면역도가 없기(0) 때문에 상관성 공격(correlation attack)에 취약한 것으로 알려져 있다[11]. 또한 Rueppel 발생기는 2개의 LFSR로 구성될 경우 선형 복잡도 및 상관 면역도가 거의 최대로 만족되지만, 연속되는 "0" 또는 "1"이 출력되는 특수한 경우 Meier등[12]과 Dawson [13]의 상관성 공격에 취약하였으며, LM 발생기 형태[10] 또는 최소한 3개 이상의 LFSR로 구성되어야 한다. 최근에는 여러 종류의 클럭 조절(clock-controlled)형 키 수열 발생기가 제안된 바 있으며, 그 중에는 유럽지역 디지털 셀룰러 폰 (GSM)의 표준 암호인 A5암호[14]와 LILI 패밀리[4]가 대표적이다. 하지만 A5 암호는 선형 복잡도가 낮기 때문에 GSM 암호로는 취약하다고 알려져 있다[15]. 추후로는 각국마다 표준 스트림 암호를 설계(예, 일본의 CRYPTREC 프로젝트, 유럽의 NESSIE 프로젝트 등)하여 이동·무선 암호 등에 적용할 것으로 보이며, 특히 네트워크 기술의 초고속화로 인하여 병렬형 스트림 암호 시스템 (parallel stream cipher system)[6, 16-17]등과 같은 안전성이 높고 고속화 실현이 가능한 알고리듬에 관심이 높아지고 있다.

본 논문에서는 Clark 등[4]이 제안한 LILI-II 암호에 대한 고속 하드웨어 구현 방안에 대하여 연구한다. LILI-II 암호는 유럽 차세대 암호 프로젝트(NESSIE)에서 동기식 스트림 암호분야에 제안 후보인 LILI-128[5] 패밀리의 동기식 스트림 암호 알고리듬이다. 보안성이 취약한 것으로 알려진 유럽 GSM 표준암호 A5[14-15]와 비교할 때 비교적 간단한 구조이면서 보안성이 높고, 하드웨어/소프트웨어 구현이 용이한 특징을 갖고 있어서 A5를 대체할 수 있는 차세대 이동 단말용 암호로 적합하다. 본 논문에서는 LILI-II 암호의 하드웨어 구현에 따른 구조적인 문제점을 발견하고 이를 해결함으로써 차세대 무선 암호로서의 병렬형 고속화 구현 방안에 대하여 접근코자 한다. LILI-II 암호는 255-비트 크기의 클럭 조절형 스트림 암호 방식[2~4]이며, 이러한 형태는 동기식 논리회로 구현 시 구조적으로 속도가 저하되는 단점이 있다. 즉, LILI-II에 사용된 두 개의 LFSR 중에서 하나(LFSRc)는 정상적인 클럭이 공급되지만, 나머지 하나(LFSRd)는 안전성을 높이기 위하여 1에서 4까지의 랜덤 클럭 수만큼 공급한 후에 정상적인 출력 데이터(1 비트)를 얻게 된다. 이에 따라 발생될 데이터는 데이터 비트 간격에 대한 예측이 어렵게 될 뿐 아니라, 키 수열 발생속도(또는 통신속도)를 최대 1/4까지 감소시킨다. 또한 키 수열 발생에서 불균일 클럭 입력에 따른 구조적 문제는 하드웨어 구현시 동기식 통신에 대한 장애요소로 작용하여 암호 시스템의 전체 성능을 저하시킨다. 본 논문에서는 LILI-II를 고속화 구현하기 위하여 귀환/이동에 있어서 랜덤한 4개의 연결 경로를 갖는 4-비트 병렬 LFSRd를 제안한다. 그리고 ALTERA[18] 사의 FPGA 소자 (EPF10K20RC240-3)를 선정하여 그래픽/VHDL 하드웨어 구현 및 타이밍 시뮬레이션한 결과 50MHz 시스템 클럭에서 안정적인 50Mbps (즉, 45 Mbps 수준인 T3급 이상, 설계회로의 최대 지연 시간이 20ns 이하인 조건) 출력 수열이 발생될 수 있음을 확인한다. 또한 FPGA/VHDL 설계회로를 Lucent[19] ASIC 소자 (LV160C, 0.13μm CMOS & 1.5v technology)에 적합하게 설계 변환 및 시뮬레이션을 실시하여 최대 지연시간이 1.8ns 이하에서 500 Mbps 이상의 고속화가 가능함을 확인한다. 그리고 LILI-II 알고리듬을 m-병렬화한 2단계 고속화 속도는 1단계 고속화 속도를 m배 증대시킨 4, 8 또는 16 Gbps (m=8, 16 또는 32) 고속 구현이 가능함을 제안한다.

Ⅱ. LILI-II 고속화 방안

1. 1단계 고속화 방안

LILI-II 암호의 구조는 그림 1과 같다. 사용된 두 개의 선형 귀환 이동 레지스터 LFSR(linear feedback shift register)[5~7]은 128단(LFSRc)과 127단 (LFSRd)으로 구성되며, LFSRc는 정상적인 시스템 클럭을 입력받지만 LFSRd는 함수 f_c에 따라 클럭 수가 랜덤(1~4)하게 변화하는 랜덤 클럭을 입력받는다. 클럭 통제를 위한 랜덤 수를 발생시키는 f_c 함수는 다음과 같다.

$$f_c = 2C[0] + C[126] + 1,$$

여기서 $C[i]$는 LFSRc의 i번째 탭 값이며, "0" 또는 "1"의 값을 갖는다.

f_d 함수는 필터 수열 함수(filtered sequence function)[5]에 따라 출력을 발생시킨다.

LILI-II 암호에서 128단 LFSRc 및 127단

LFSRd의 원시다항식 (primitive poly- nomial)[10~11]은 각각 다음과 같이 정의된다.

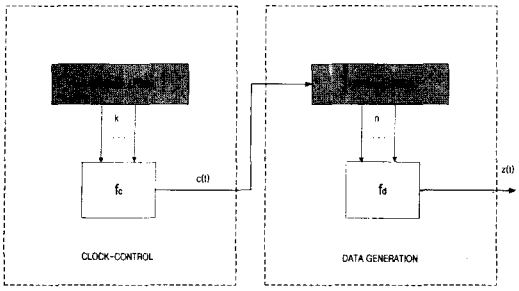

그림 1. LILI-II 스트림 암호

$$g_c(x) = x^{128} + x^{126} + x^{125} + x^{124} + x^{123} + x^{122} + x^{119}$$
$$+ x^{117} + x^{115} + x^{111} + x^{108} + x^{106} + x^{105}$$
$$+ x^{104} + x^{103} + x^{102} + x^{96} + x^{94} + x^{90}$$
$$+ x^{87} + x^{82} + x^{81} + x^{80} + x^{79} + x^{77} + x^{74}$$
$$+ x^{73} + x^{72} + x^{71} + x^{70} + x^{67} + x^{66}$$
$$+ x^{65} + x^{61} + x^{60} + x^{58} + x^{57} + x^{56} + x^{55}$$
$$+ x^{53} + x^{52} + x^{51} + x^{50} + x^{49} + x^{47}$$
$$+ x^{44} + x^{43} + x^{40} + x^{39} + x^{36} + x^{35} + x^{30}$$
$$+ x^{29} + x^{25} + x^{23} + x^{18} + x^{17} + x^{16} + x^{15}$$
$$+ x^{14} + x^{11} + x^{9} + x^{8} + x^{7} + x^{6} + x^{1} + 1$$

$$g_d(x) = x^{127} + x^{121} + x^{120} + x^{114} + x^{107} + x^{106} + x^{103}$$
$$+ x^{101} + x^{97} + x^{96} + x^{94} + x^{92} + x^{89}$$
$$+ x^{87} + x^{84} + x^{83} + x^{81} + x^{76} + x^{75} + x^{74}$$
$$+ x^{72} + x^{69} + x^{68} + x^{65} + x^{64} + x^{62}$$
$$+ x^{59} + x^{57} + x^{56} + x^{54} + x^{52} + x^{50} + x^{48}$$
$$+ x^{46} + x^{45} + x^{43} + x^{40} + x^{39} + x^{37}$$
$$+ x^{36} + x^{35} + x^{30} + x^{29} + x^{28} + x^{27} + x^{25}$$
$$+ x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{14} + x^{10}$$
$$+ x^{8} + x^{7} + x^{6} + x^{4} + x^{3} + x^{2} + x^{1} + 1$$

여기서, "+"는 GF(2) 상에서의 연산이며, 비트별 배타 합(XOR) 논리이다.

LILI-II에 사용된 두 개의 LFSR 중에서 하나(LFSRc)는 정상적인 클럭이 공급되지만, 나머지 하나(LFSRd)는 안전성을 높이기 위하여 1에서 4까지의 랜덤 클럭 수만큼 공급한 후에 정상적인 출력 데이터를 얻게 된다. 이에 따라 발생될 데이터는 데이터 비트 간격에 대한 예측이 어렵게 될 뿐 아니라, 키 수열 발생속도(또는 통신속도)를 최대 1/4까

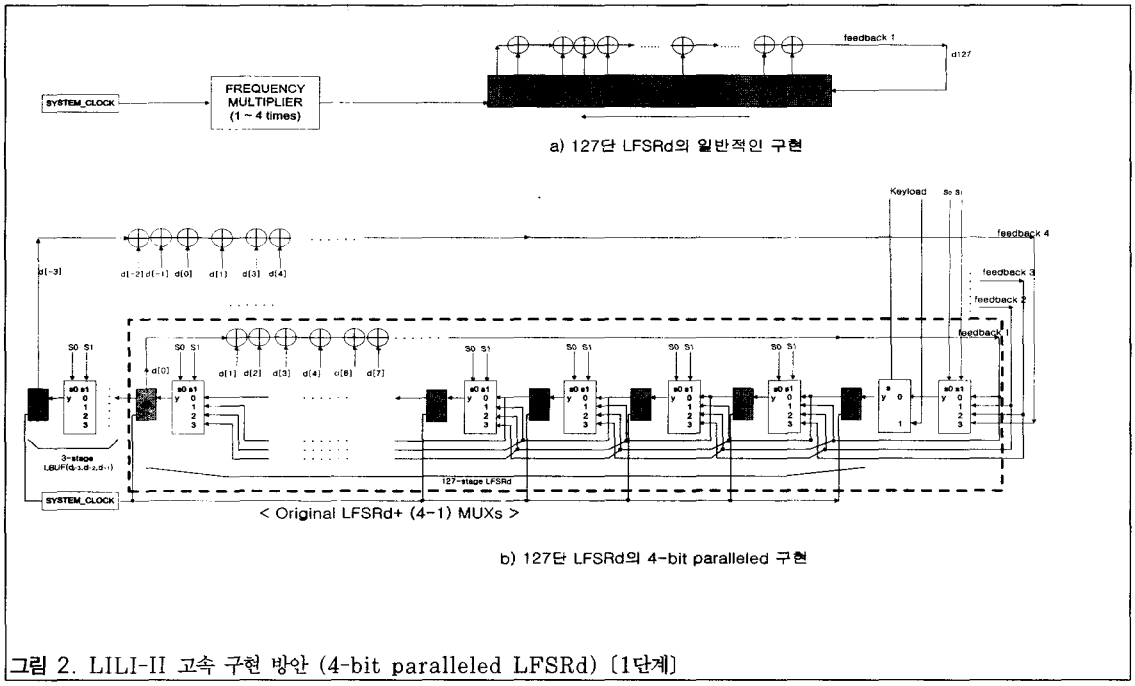

그림 2. LILI-II 고속 구현 방안 (4-bit paralleled LFSRd) [1단계]

지 감소시킨다. 또한 키 수열 발생에서 불균일 클럭 입력에 따른 구조적 문제는 하드웨어 구현시 동기식 통신에 대한 장애요소로 작용하여 암호 시스템의 전체 성능을 저하시킨다.

LFSR의 하드웨어 구현 시에는 시스템의 안정성을 고려할 때 시스템 클럭에 맞추어 레지스터 값을 좌측 이동시키는 클럭 동기식 논리 설계 (clock-synchronized logic design) 방법이 일반적으로 적용된다. 그러나 이 방법으로 LILI-II 암호를 구현함에 있어서 일반형인 LFSRc는 상기의 방법으로 쉽게 구현될 수 있지만, 클럭 조절형인 LFSRd는 1~4배의 고속 클럭이 별도로 요구된다. 또한 별도의 고속 클럭 추가문제를 해결하고자 주파수 채배기 (frequency multiplier)를 도입할 수도 있지만, 초고속 통신에서는 클럭 간격(clock interval)에서의 시간 여유 (time margin)가 작기 때문에 적용이 어렵다.

LILI-II가 갖는 구조적인 문제를 해결하기 위하여 비트 이동 루트가 클럭을 초월하여 1~4 비트 씩 가변적으로 이동할 수 있는 4-비트 병렬 입력 LFSRd의 고속 구현 방안을 그림 2 b)와 같이 제안한다.

그림 2 b)의 일반 LFSR 구현시 D 플립플롭을 사용하여 구성될 수 있지만, 이 때는 기존의 클럭보다 1~4배 빠른 클럭을 필요로 한다. 제안된 그림 b)의 경우 127단 LFSRd 각 비트들은 $d_0, d_1, \ldots, d_{126}$ 으로 나타낸 레지스터에 저장된 후 f_c 값에 따라 1~4 비트 씩 좌측 이동하며, 하나의 레지스터는 좌측으로 4개의 (4-1) 멀티플렉서 (MUX) 회로로 출력된다. 이 부분에 대한 설계 아이디어를 "4-비트 병렬 LFSRd (4-bit paralleled LFSRd)" 라고 부르며, 고속화 구현 회로의 핵심부분이다. 예를 들면, 그림에서 d_{122} 레지스터는 그 이전 4개의 레지스터들($d_{123}, d_{124}, d_{125}, d_{126}$)중에서 랜덤하게 어느 한 입력($f_c = 1$일 때는 d_{123}, $f_c = 2$일 때는 d_{124}, $f_c = 3$일 때는 d_{125}, $f_c = 4$일 때는 d_{126})이 선택되며, 이때 선택 신호들 ($s1, s0$)은 f_c로 구현된 전가산기 출력으로부터 얻어진다. 그리고 127-비트 LFSRd의 좌측에는 3-비트 LBUF가 4개의 귀환 비트 조합을 계산하기 위하여 d_0의 출력을 차례로 보관하고 있다. 4개의 귀환 비트 조합 중에서 feedback 1은 원래의 귀환 비트와 동일한 탭의 XOR 조합을, feedback 2는 feedback 1에 비하여 1-비트씩 좌측 이동된 탭의 XOR 조합을, feedback 3는 2-비트씩 좌측 이동된 탭의 XOR 조합을, feedback 4는 3-비트씩 좌측 이동된 탭의 XOR 조합을 이룬다. 여기에서 원래의 귀환(feedback 1) 탭 XOR 조합들은 LFSRd의 원시 다항식 $g_d(x)$로부터 주어지며, 그 조합은 낮은 차수부터 (0, 1, 2, 3, 4, 6, 7, 8, 10, 14, 18, 19, 20, 21, 22, 23, 25, 27, 28, 29, 30,35, 36, 37, 39, 40, 43, 45, 46, 48, 50, 52, 54, 56, 57, 59, 62, 64, 65, 68, 69, 72, 74, 75, 76, 81, 83, 84, 87, 89, 92, 94, 96, 97, 101, 103, 106, 107, 114, 120, 121) 단으로 구성된다. LFSRc의 탭과 구분하기 위하여 LFSRd의 각 탭의 값을 d_i 또는 $d[i]$로 표기하였다.

2. 1단계 방안 타이밍 분석

제안된 고속화 병렬 구현 방안을 검증하기 위하여 VHDL 회로를 설계하였다. ALTERA사의 FPGA 소자 (EPF10K20RC240-3)를 선정한 후 그림 1, 2와 같이 4개의 세부 블록으로 나누어 VHDL (Very high speed integrated circuit Hardware Description Language) 설계 언어로 구현하였다. 첫 번째 블록은 component LFSRC128 (LILI-c128)로 LFSRc를 구현한 것이고, 두 번째 블록은 component FADD (full_adder)로 $f_c = 2c[0] + c[126] + 1$ 의 함수를 구현한 것이다. 두 번째 블록의 출력은 LFSRd에 대한 클럭 이동 비트를 산출하는 함수로서 임의의 정수 값을 출력한다. 이 부분에 대한 설계는 $f_c - 1$ 을 사전 계산한 후 전 가산기 (full adder)로 간단히 구현하였으며, 계산 결과는 LFSRd로 전달된다. 세 번째 블록은 component LFSRD127로서 LFSRd를 구현한 것이며, 마지막 네 번째 블록은 component fd로 fd 함수를 구현한 것이다.

그림 3은 LILI-II에 대한 타이밍 시뮬레이션 파형이다. 사용된 시스템 클럭 (CLK)은 50 MHz 이며, 리셋 된 후 키 데이터 (KEY_DATA)로 초기화된 LFSRc 출력 신호 (C127, C126, C0)와 LFSRc 메모리 상태값(C)이 클럭에 동기되어 50 Mbps의 속도로 안정된 랜덤 비트를 출력하였다. 이 회로에서 사용된 최장 길이의 지연시간은 9.9ns로 조사되었고, 따라서 50 MHz 클럭(period=20 ns)에 대하여 50% 이상의 시간 여유(margin)를 갖는 안정성 있는

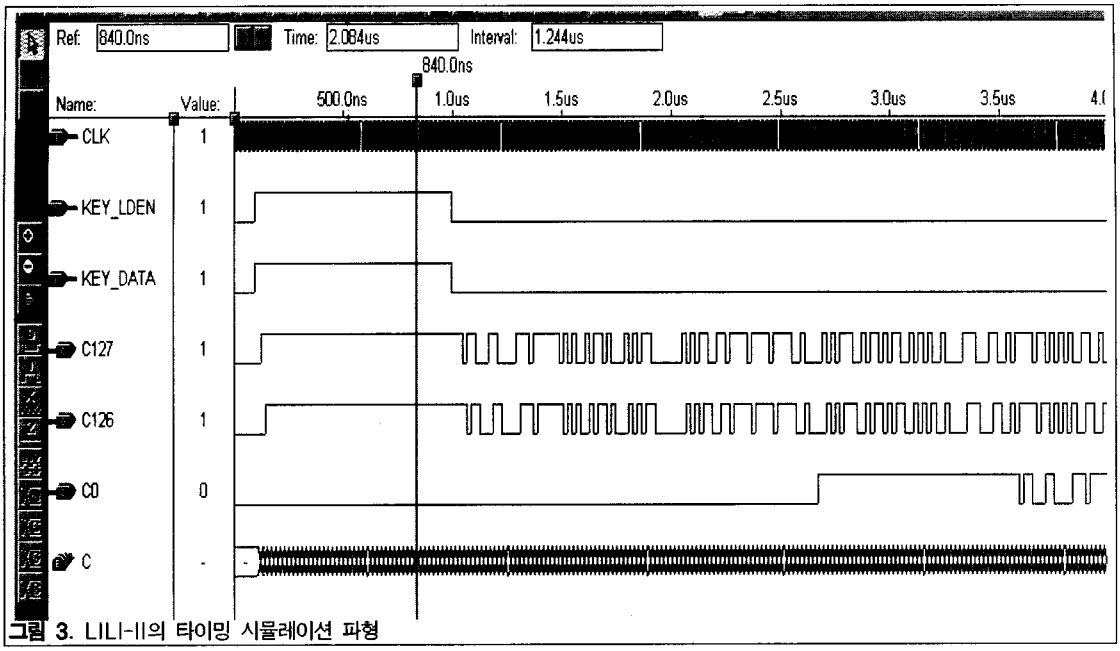

그림 3. LILI-II의 타이밍 시뮬레이션 파형

50 Mbps의 출력을 발생하였다.

그리고 상기 FPGA/VHDL 설계 회로를 Lucent[19] ASIC 소자 (LV160C, 0.13μm CMOS & 1.5v technology)에 적합하게 설계 변환 및 시뮬레이션한 결과 최대 지연시간이 1.8ns 이하였고, 500 Mbps 이상의 고속화가 가능함을 확인하였다.

표 1에서는 제안된 병렬 하드웨어 구현 방안을 기존의 구현방안과 비교하였는데 하드웨어 복잡도 측면에서 소규모 증가가 예상되지만 키 수열 발생기의 안전성을 유지하면서도 그 성능을 최대 4배까지 고속화시킬 수 있었다. 즉, 게이트 수로 살펴본 하드웨어 복잡도가 1.16배 증가되었으며, 출력 키 수열이 최대한 4배의 속도 향상이 가능함을 확인하였다. 마지막으로 50 MHz 시스템 클럭을 인가한 경우 안정적인 50 Mbps의 키 수열 출력을 낼 수 있음을 FPGA 소자를 통하여 확인할 수 있었다. 초고속 암호 통신을 위한 ASIC 설계 변환 및 시뮬레이션에서는 상기 FPGA의 성능을 10배정도 향상시킬 수 있었고, 500 Mbps의 속도가 가능함을 확인하였다. 더 빠른 고속 통신이 요구될 경우 2단계 고속화가 필요하다.

3. 2단계 고속화 병렬형 제안

상기의 1단계 고속화 방안 보다 더 높은 통신 속

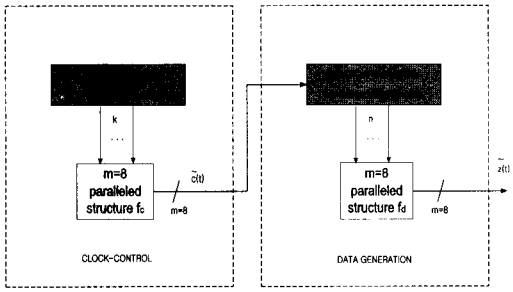

그림 4. m-병렬 구현 방안 (2단계)

도를 위해서는 참고문헌[5]에서 제시된 바와 같이 개별 LFSR에 대하여 각각 병렬형 스트림 암호의 적용이 요구된다. 연구에서는 LILI-II 암호에 대하여 2단계 고속화 방안으로 병렬형 스트림암호 적용방안을 제안하고, 그 성능을 분석한다.

LILI-II 스트림 암호를 병렬형 스트림 암호로 구현하기 위하여 그림 4와 같은 병렬형 구조를 제안한다. 병렬형 스트림 암호를 적용하기 위하여 그림 1의 4개 블록 구성 요소 별로 그림 4와 같이 PS-LFSRc, paralleled-fc, paralleled-LFSRd, paralleled-fd 함수 등 각 블록의 병렬화가 필요하다. 128단 LFSRc는 보통 그림 2 a) 형태로 구성되는데, 이 경우에는 시스템 클럭이 인가될 때 한 클럭당 한 비트의 출력을 발생할 뿐이다. 연구 결과에서는 스트림 암호에서도 블록 암호처럼 클럭 하나에

표 1. LILI-II의 구현 방안 비교표

Items	In general (기존 방법)	Proposed(1st stage)	Proposed(2nd stage)
Hardware implementation	Clock-synchronized logic general implementation.	Multiple configured. (4-bit parallel LFSRd implemented)	parallel configuration
Throughput of data rate for ALTERA FPGA device (EPF10K20RC240-3) with 50MHz system clock	12.5~50 Mbps variable rate.	50 Mbps fixed rate: (maximum four times higher) - Maximum path delay about 18 ns	50×m Mbps fixed rate: (m=8, 16, 32, ...)
Throughput of data rate for Lucent ASIC device (LV160C, 0.13μm, 1.5v technology) with 500MHz system clock	125~500 Mbps variable rate:	500 Mbps fixed rate: (about 1~4 times): - Maximum path delay about 1.8 ns.	500×m Mbps fixed rate: (about 16~64 times) where m= 8, 16, or 32
Number of gates used (if 1 F/F=5 AOI gate)	21,443 gates: - 255 D flip-flops - 2 (2:1) MUXs - 66+61 XORs - 1 FA - 4 kbit RAM	24,783 gates (about 1.16 times): - 255+4 D flip-flops - 127 (4:1) MUXs - 2 (2:1) MUXs - 66+4x61 XORs - 1 FA - 4 kbit RAM	403,716 gates : (about 18.8 times) if m=16 - 128+(16-1) + 127 + (64-4) D flip-flops - 127 (64:1) MUXs - 2 (2:1) MUXs - 35 XORs - 16 FA - 4x16 kbit RAM

〔Note〕 AOI gate : And-Or-Inverter gate

여러 비트(m)의 출력을 낼 수 있는 병렬형 구조[6]가 가능하며, LFSRc와 LFSRd를 병렬형 구조로 개선하였다.

그림 5에서는 128단 LFSRc에 대한 병렬 구조인 (n=128, m=8) PS-LFSRc에 대하여 나타내었다. LFSRc의 병렬형 구조에서는 기존의 일반형 128단 레지스터와 비교할 때 회로 상으로 추가되는 레지스터(7=m-1, D F/F) 및 feedback 함수(XOR 조합 7개)가 단점이지만, 시스템 성능 즉, 출력 속도를 m배 향상시키는 큰 잇점이 있다. m-병렬 fc 함수와 m-병렬 fd 함수는 기존의 fc 함수 및 fd 함수와 동일한 회로를 병렬 구성하였다. m-병렬 LFSRd는 1단계 고속화 기술을 포함하여 4×m 클럭 만큼 이동되는 병렬 구성이 된다.

4. 종합 성능 분석

제안된 1단계 구현 및 2단계 고속화 방안에 대한

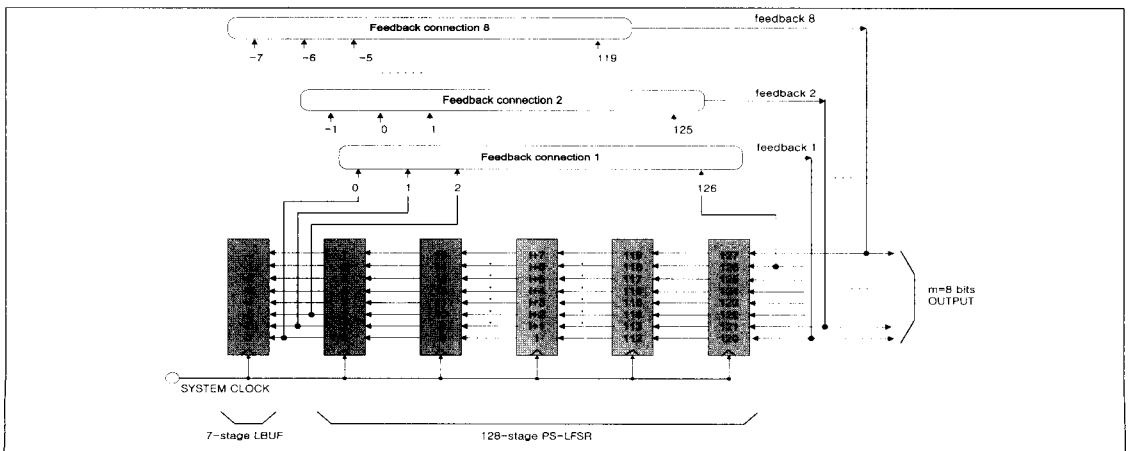

그림 5. 8-paralleled LFSRc의 구현 방안 (2단계)

종합 성능을 요약하면 표 1과 같다. 일반적인 구현 방안(기존 방안)과 비교할 때 1단계 구현에서는 FPGA에 의한 방법으로 50 Mbps, ASIC 방법으로는 500 Mbps의 속도를 출력할 수 있어서 기존의 방법보다 4배 빠른 속도를 보였다. 증가되는 하드웨어 복잡도는 1.16배임이 분석되었으며, 이는 하드웨어 기술의 발전 추세로 보아서 중요한 문제가 아니다. 또한 1단계 뿐 아니라 2단계 고속화 방안을 겸할 경우에는 ASIC 단계에서의 출력 속도는 m=32로 설정했을 때 최대 m배인 500×32 = 16 Gbps 출력이 가능함을 알 수 있·었으며, 이 때에 하드웨어 복잡도는 18.8배 증가하였다. 이 경우에도 대부분의 복잡도가 메모리 때문이었으며, 메모리 대형화가 가능한 시점에는 큰 문제가 아니라고 판단된다.

Ⅲ. 결 론

LILI-II 스트림 암호는 클럭 조절형 스트림 암호 방식으로서 이러한 형태는 동기식 논리회로에 따른 하드웨어 구현에 있어서 속도를 저하시키는 구조적인 문제점을 안고 있다. 본 논문에서는 속도 저하 문제를 해결하는 LILI-II 스트림 암호의 고속화 구현 방법을 연구하여 하드웨어 구현에 따른 구조적인 문제점을 보완하였다. 그 결과 기존의 구현 방안에 비하여 1단계 방안에서 최대 4배의 고속화가 가능하였고, 2단계 방안에서는 m배(8, 16 또는 32 등) 고속화가 가능함을 확인하였다. 또한 하드웨어 설계 검증을 위하여 ALTERA 사의 Max+plus II로 타이밍 시뮬레이션을 실시하였고, FPGA소자 (EPF10K20RC 240-3)를 선정하여 하드웨어로 구현하였다. 구현된 회로는 50MHz 시스템 클럭에서 안정적인 50Mbps 출력 수열이 발생될 수 있음을 확인하였다. 또한 FPGA/VHDL 설계회로를 Lucent ASIC 소자 (LV160C, 0.13μm CMOS & 1.5v technology)에 적합하게 설계 변환 및 시뮬레이션한 결과 최대 지연시간이 1.8ns 이하였기 때문에 500 Mbps 이상의 고속화가 가능함을 확인하였다. 마지막으로 초고속 암호 통신을 위한 ASIC 설계 변환에서 1단계 고속화 방법에서는 500 Mbps의 속도가 가능하였으며, 이를 2단계 고속화에 적용 시에는 4, 8, 또는 16 Gbps (m=8, 16 또는 32)의 출력이 가능함을 알 수 있었다.

참 고 문 헌

[1] B. Schneier, *Applied Cryptography (2nd edition)*, John Wiley & Sons, Inc., 1996.

[2] A.J. Menezes, P.C. Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[3] Wedbush Morgan Securities - Industrial Report, "Access Manage- ment/Internet Security Industry," on http://www.vikasqupta.com, Feb. 28, 2002.

[4] A. Clark, E. Dawson, J. Fuller, J. Golic, Hoon-Jae Lee, W. Millan, Sang-Jae Moon, L. Simpson, "The LILI-II Keystream Generator," *LNCS 2384*, ACISP'2002, pp.25-39, Jul. 2002.

[5] L. Simpson, E. Dawson, J. Dj. Golic and W. Millan, "LILI Keystream Generator," *Proceedings of the Seventh Annual Workshop on Selected Areas in Cryptology SAC'2000* to appear in Springer-Verlag LNCS, 2000.

[6] Hoonjae Lee, Sangjae Moon, "Parallel Stream Cipher for Secure High-Speed Cmmunications," *Signal Processing*, Vol. 82, No.2, pp.259-265, Feb. 2002.

[7] P. R. Geffe, "How to Protect Data with Ciphers that are really hard to Break," *Electronics*, pp. 99-101, Jan. 1973.

[8] R. A. Rueppel, "Correlation Immunity and the Summation Generator," *Advances in Cryptology, Proceedings of CRYPTO'85*, pp. 260-272, 1985.

[9] R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, 1986.

[10] Hoonjae Lee, Sangjae Moon, "On An Improved Summation Genera- tor with 2-Bit Memory," *Signal Processing*, 80(1), pp. 211~217, Jan. 2000.

[11] T. Siegenthaler, " Decrypting a Class of Stream Ciphers Using Ciphertext Only," *IEEE Trans. on Computer*, C-34(1), pp. 81-85, Jan. 1985.

[12] W. Meier and O. Staffelbach, "Correlation Properties of Combiners with Memory in Stream Ciphers," *Journal of Cryptology*, Vol. 5, pp. 67-86, 1992.

[13] E. Dawson, "Cryptanalysis of Summation Generator," *Advances in Cryptology-AUSCRYPT'92, LNCS*, Springer-Verlag, pp. 209-215, 1993.

[14] S.B. Xu, D.K. He, and X.M. Wang, "An Implemenatation of the GSM General Data Encryption Algorithm A5," *CHINACRYPT'94*, Xidian, China, 11-15 Nov. 1994, pp. 287-291.

[15] J. Golic, "Cryptanalysis of alleged A5 stream cipher generator," *LNCS 1233, Eurocrypt'97*, pp. 239-255, Springer-Verlag, 1997.

[16] P.Rogaway and D. Coppersmith, "A Software-Oriented Encryption Algorithm," *FSE'94, Cambridge Security Workshop Proceedings*, Springer- Verlag, 1994, pp. 56-63.

[17] D. Stinson, *Cryptography Theory and Practice(2nd ED)*, CRC Press, 2002.

[18] Altera technical data sheets in http:// www.altera.com.

[19] Lucent technical data sheets in http:// www.lucent.com.

이 훈 재(Hoon-jae Lee) 정회원

1985년 2월 : 경북대학교 전자공학과 졸업(학사)
1987년 2월 : 경북대학교 전자공학과 졸업(석사)
1998년 2월 : 경북대학교 전자공학과 졸업(박사)
1987년 2월~1998년 1월 : 국방과학연구소 선임연구원
1998년3월~2002년 2월 : 경운대학교 컴퓨터전자정보공학부 조교수
2002년3월~현재 : 동서대학교 인터넷공학부 조교수
<주관심분야> 암호이론, 네트워크보안, 디지털 통신

문 상 재(Sang-jae Moon) 정회원

1972년 2월 : 서울대학교 공업교육과 졸업 (전자공학 학사)
1974년 2월 : 서울대학교 대학원 전자공학과 졸업 (전자공학 석사)
1984년 6월 : 미국 UCLA 통신공학과 졸업(통신공학 박사)
1984년 7월~1985년 6월 : UCLA Postdoctor 근무
1974년 12월~현재 : 경북대학교 공과대학 전자전기공학부 교수
2001년 2월 ~2002년 1월 : 한국정보보호학회 회장
1999년 8월 ~현재 : 경북대학교 ITRC 연구센터장
<주관심분야> 정보보호, 이동 네트워크