블록암호화 알고리즘 KASUMI의 하드웨어 설계 및 응용

최현준* · 서영호** · 문성식*** · 김동욱****

Hardware Design and Application of Block-cipher Algorithm KASUMI

Hyun-Jun Choi* · Young-Ho Seo** · Sung-Sik Moon*** · Dong-Wook Kim****

본 연구는 지식경제부 및 한국산업기술평가관리원의 IT산업원천기술개발사업의 일환으로 수행하였음.
[KI002058, 대화형 디지털 홀로그램 통합서비스 시스템의 구현을 위한 신호처리 요소 기술 및 SoC 개발]

요 약

본 논문에서는 KASUMI 암호화 알고리즘을 하드웨어로 구현하였다. 이는 ASIC이나 코어-기반 설계와 같은 여러 응용분야에 적합하도록 범용적으로 구현하였다. 또한 기밀성 알고리즘과 무결성 알고리즘을 모두 수행할 수 있도록 설계하였으며, 파이프라인 구조를 사용하여 높은 동작 주파수에서도 구동될 수 있도록 하였다. 본 논문에서 설계한 하드웨어를 Altera사의 EPXA10F1020C1을 타겟으로 구현한 결과 최대 동작 주파수 36.35MHz에서 안정적으로 동작함을 확인하였다. 따라서 구현된 하드웨어는 현재 중요한 문제로 대두되고 있는 종단간(end-to-end) 보안에 대한 좋은 해결책으로 유용하게 사용될 수 있을 것으로 생각된다.

Abstract

In this paper, we implemented the kasumi cipher algorithm by hardware. In this work, kasumi was designed technology-independently for application such as ASIC or core-based design. The hardware is implemented to be able to calculate both confidentiality and integrity algorithm, and a pipelined KASUMI hardware is used for a core operator to achieve high operation frequency. The proposed block cipher was mapped into EPXA10F1020C1 from Altera and used 22% of Logic Element (LE) and 10% of memory element. The result from implementing in hardware (FPGA) could operate stably in 36.35MHz. Accordingly, the implemented hardware are expected to be effectively used as a good solution for the end-to-end security which is considered as one of the important problems.

키워드

하드웨어 설계, 블록 암호화, 암호화 시스템, 카즈미

Key word

Hardware Design, Block cipher, Cryptosystem, Kasumi

* 정회원 : 안양대학교 정보통신공학과
** 중신회원 : 광운대학교 실감미디어 연구소
*** 정회원 : 한국폴리텍 II 대학 컴퓨터응용기계과
**** 정회원 : 광운대학교 실감미디어 연구소 (dwkim@kw.ac.kr)

접수일자 : 2010. 08. 13
심사완료일자 : 2010. 10. 11

I. 서 론

최근 이동통신은 3세대를 거쳐 초고속 멀티미디어 서비스를 지원하는 수준까지 놀라운 속도로 진화하고 있다. 이러한 이동통신 기술의 눈부신 발전은 사용자 하여금 PDA나 휴대폰과 같은 이동통신 단말기를 이용해서 단순한 통화뿐만 아니라 전자 상거래와 같은 금융 서비스 및 동영상 서비스까지도 제공받게 하였다. 이처럼 21세기는 이동통신 기술과 통신망 기술의 빠른 발전으로 인해서 유무선 복합 네트워크 환경에서 모든 사용자들의 정보의 획득 및 일상 업무 처리를 가능하게 함으로써 보다 편리해진 삶을 제공하고 있다. 그러나 이러한 기술을 통한 정보화 사회가 제공하는 편리함에는 인터넷 망, 시스템 등에 대한 해킹과 같은 악의적이고 불법적인 위협들이 존재하고 있다. 이러한 위협은 개인의 신상정보의 유출에 의한 범죄에 이용될 수 있을 뿐 아니라, 전자상거래와 같은 유용한 정보통신 서비스의 저변확대에 커다란 장애로 대두되고 있다[1].

편리한 유무선 복합 네트워크 환경을 안전하게 이용하고, 널리 활성화시키기 위해서는 사용자 개인의 정보 유출 방지와 적법한 사용자에게만 서비스를 제공할 수 있도록 하는 사업자 측면에서의 사용자 인증, 권한 검증, 과금 서비스 기능은 매우 중요하고, 이러한 기능을 제공하는 시스템 개발의 필요성과 사용자측면에서 무선 네트워크 환경을 고려한 사용자 개인정보를 보호할 정보보호 알고리즘 개발의 필요성이 점차 높아지고 있다.

1960년대 이전까지만 하더라도 암호는 주로 국방이나 외교 분야의 전유물이었으나 1970년대 중반 미국에서 민간분야에서 사용될 암호화 알고리즘인 DES(data encryption standard)가 개발되면서부터 전 세계적으로 암호화에 대한 관심이 높아지게 되었다. 이러한 DES를 시작으로 각국의 대학, 연구소 및 정부에서 암호관련 연구가 진행되었고, 이로 인하여 현대 암호학의 본격적인 발전이 시작되었다. 이 현대 암호학은 1976년 공개키 암호(public-key cryptography)의 개념이 등장하면서 비약적인 발전을 거듭하여 현재에는 군사 및 외교적 일은 물론, 금융, 개인 프라이버시 보호 등에서 암호화기술이 널리 사용되고 있다.

최근 고속 인터넷의 확산에 따른 기존의 보안 제품으로 인한 속도 저하문제가 대두됨에 따라서 기존의 소프트웨어 기반의 보안제품에서 하드웨어 기반의 보안제품으로 시장의 경향성이 변화되고 있고 관련된 제품과 연구결과들이 다수 발표되고 있다[2-4]. 암호화 알고리즘을 소프트웨어로 구현할 경우, 쉽게 구현이 가능하며 적은 양의 데이터를 암호화할 경우에는 빠른 속도로 처리할 수 있다. 하지만 전자상거래나 무선인터넷 보안시스템에서의 사용과 같은 실제 암호화 알고리즘을 응용할 경우 동시에 수십 건에서 수백 건의 암호화 작업을 수행해야 하며, 만약 이 때 소프트웨어로 암호화를 처리할 경우 시스템 과부하에 의해 처리속도가 현저히 떨어지게 된다. 이는 유/무선 인터넷을 이용한 적용에 암호화 알고리즘을 소프트웨어로 처리하는 것이 부적합함을 의미한다. 또한 해킹 등에 의한 암호화 알고리즘의 불법 접근 및 분석도 가능하여 암호화 알고리즘 자체의 안전 문제도 고려해야 한다. 또한 이러한 암호화 알고리즘을 다른 시스템에 쉽게 이식하고 설치 및 유지/보수가 용이하도록 암호화 시스템을 단일 회로로 구현하는 것이 바람직하다. 따라서 빠른 속도의 암호화와 보다 안전한 암호화 처리를 위해 암호화 알고리즘의 하드웨어 구현이 절실히 요구되고 있다[5].

본 논문에서는 UMTS(universal mobile telecommunication system) 핵심망에 기반한 이동통신망의 무선 접속 기술을 바탕으로 한 시스템의 보안 구조에서 기밀성과 무결성을 제공하는 KASUMI 암호화 알고리즘의 하드웨어 구현결과를 보인다. 또한 구현결과를 영상데이터에 적용하여 응용 가능성을 살펴본다.

본 논문의 구성은 다음과 같다. 2장에서는 KASUMI 암호화 알고리즘에 대해 살펴보고 3장에서 구현한 하드웨어의 설계결과와 실제로 영상데이터에 적용한 실험결과를 보여 다양한 분야에의 응용 가능성을 살펴본다. 마지막으로 4장에서 결론을 맺는다.

II. KASUMI: 블록암호 알고리즘

2.1 암호화 알고리즘의 정의 및 분류

넓은 의미에서 암호화 알고리즘이란 비밀성 및 인증을 제공하기 위한 암호학적 알고리즘을 통칭하는 것으로서 암호화 알고리즘, 전자서명 알고리즘, 해쉬 알고리

증 및 메시지 인증 알고리즘 등이 여기에 속한다. 그러나 본 논문에서는 비밀성 기능을 제공하는 알고리즘으로 국한시켜 좁은 의미인 암호화 알고리즘을 암호화 알고리즘이라 한다. 좁은 의미에서 암호화 알고리즘이란 암호화 및 복호화에 사용되는 수학적 함수를 말하며, 키 스케줄 알고리즘, 암호화 알고리즘 및 복호화 알고리즘의 세 요소로 구성된다. 이를 그림 1에서 보이고 있다.

그림 1. 일반적인 암호화 알고리즘 모델
Fig. 1. Model of conventional cipher algorithm

일반적으로 암호화 알고리즘은 암호화와 복호화에 서로 다른 연관된 키의 쌍을 사용하는 공개키 암호화 알고리즘(public key algorithm)과 암호화와 복호화 키가 동일한 대칭키 암호화 알고리즘(symmetric key algorithm)으로 나뉜다. 대칭키 암호화 알고리즘은 다시 의사난수 생성기 등을 이용해 생성된 키 스트림을 평문 스트림과 XOR을 하는 스트림 암호화와 평문을 일정한 크기의 블록으로 나누어 각 블록을 암호화하는 블록암호로 나눌 수 있다. 따라서 한 번에 처리되는 데이터 단위도 스트림 암호 알고리즘은 한 번에 평문의 한 비트 단위로 연산을 수행하며, 블록암호 알고리즘은 고정된 크기의 블록 단위로 연산을 수행한다.

2.2 KASUMI 알고리즘

KASUMI 암호화 알고리즘은 8라운드 Feistel 구조를 갖고 있다. 기본 구조를 그림 2에서 보이고 있다[4,5]. 이는 64비트 입력 데이터 블록에 대해 동작하고 128비트 키 값을 갖는다. KASUMI 알고리즘에 들어가는 입력 데이터는 각각 32비트 길이를 가지는 L_0 와 R_0 로 나뉜다. 입력(I)는 두 32-bit L_0 와 R_0 로 나뉜다. 그리고 각 I에 대해 $1 \leq I \leq 8$ 이라 정의하면,

$$\begin{aligned} R_i &= L_{i-1} \\ L_i &= R_{i-1} \oplus f_i(L_{i-1}, RK_i) \end{aligned}$$

여기서, f_i 는 라운드 함수이며, RK_i 는 I번째 라운드의 라운드 키 값이다. KASUMI 알고리즘의 최종 출력은 64 비트 길이의 $L_8 \parallel R_8$ 로 만들어진다.

그림 2의 각 라운드 내 하위 함수들의 자세한 동작은 kasumi 알고리즘 명세서[6]를 참고하기 바란다.

III. 하드웨어 설계 및 응용

본 장에서는 전체적인 하드웨어 구조를 설명하고 내부적으로 중요한 구조를 가지는 하드웨어 구성요소에 대해 구조를 나타내고 기본적인 동작을 설명한다.

그림 2. KASUMI 암호화 알고리즘의 기본 구조
Fig. 2. Basic structure of kasumi cipher algorithm

3.1 하드웨어 설계 및 구현결과

본 논문에서 제안하는 전체적인 하드웨어의 구조를 그림 3에 나타냈다. 전체적인 하드웨어는 데이터 패스부(data-path part)와 제어부(controller)로 구성되는데 데

그림 3. 전체적인 하드웨어 구조
Fig. 3. Global hardware block diagram

이터 패스부는 블록 암호화 및 복호화를 수행하는 부분, 인터페이스를 위한 입력 및 출력부, 초기값을 저장하는 레지스터 및 카운터 등으로 구성된다. 그리고 전체 하드웨어를 제어하는 제어기는 외부 호스트로부터 동작을 프로그래밍 받고 저장하여 이를 디코딩하는 명령어 레지스터(instruction register)와 디코더(decoder), 동작 순서를 결정하는 유한상태 기계블록(FSMs)과 상태신호를 이용해서 제어신호를 생성하는 제어신호 발생기(control signal generator), 내부적인 칩의 상태를 외부로 알려주는 상태 레지스터(status register)로 구성된다.

설계한 하드웨어는 유/무선으로 입력되는 데이터를 최소의 대기시간만을 가지면서 실시간으로 데이터를 암호화 혹은 복호화시킬 수 있는 특징이 있다. 직렬 입력 버퍼를 통해 직렬로 입력된 데이터는 최대 64 비트 단위로 버퍼링되어 입력버퍼 혹은 초기값버퍼/카운터에 저장된다.

그림 4에서는 설계한 하드웨어의 최상위 블록도를 보

이고 있다. 세부적인 구조는 그림 3의 전체적인 하드웨어 구조와 동일하다. 제안한 암호화 시스템은 VHDL을 이용하여 하드웨어로 설계하였다. 설계는 VHDL 하향식 설계기법을 통해서 이루어졌으며 특정 구현 대상에 국한하지 않는 범용적인 설계를 이루고자 오직 IEEE 표준 라이브러리만을 사용하였다. 각각의 모듈들은 RTL(register transfer level) 수준으로 설계되었고, 구조적 수준(structure-level)에서 서로 연결되었다. 설계된 하드웨어를 검증하기 위해 Synopsys의 Design Compiler로 논리합성을 수행하였다. 암호화 알고리즘은 일반적인 회로들에 비해 데이터 버스가 크기 때문에 합성 시 팬아웃(fanout), 배선지연(wire delay), CTS(clock tree synthesis) 등에 주의해야 한다.

본 논문에서는 제안한 하드웨어는 Altera사의 EPXA10F1020C1을 타겟으로 구현한 결과 최대 동작 주파수 36.35MHz에서 안정적으로 동작함을 확인하였다. 표 1에서 하드웨어 구현시 사용한 FPGA의 자원 사용율을 보이고 있다.

그림 4 전체적인 하드웨어 구조
Fig. 4. Global hardware block diagram

표 1. 사용된 하드웨어 자원
Table 1. Used hardware resource

Resource name	Amount of used resource
Total logic elements	8,328/38,400 (22%)
Total pins	532/715 (74%)
Total virtual pins	0
Total memory bits	32,768/327,680 (10%)
Total PLLs	0

설계한 하드웨어의 검증을 위한 시뮬레이션 결과를 그림 5, 6에서 보이고 있다. 그림 5에서 보는 바와 같이, 데이터가 직렬로 입력되면 일정 대기 지연시간을 지나고 나서부터 암호화된 데이터가 출력되는 것을 볼 수 있다.

표 2에서는 구현한 하드웨어의 성능을 비교하고 있다. 이전 연구결과의 경우 Xilinx사의 FPGA를 타겟으로 구현되었기에 본 논문의 결과와 직접 비교하기에는 어려움이 있다. 하지만 표에서 보이는 바와 같이 사용 가능

한 하드웨어 자원대비 실제 사용율과 동작주파수의 비교분석은 가능하다. 동작 주파수의 경우 큰 의미는 없지만 이전 결과와 비교해 약 10%정도 빨라졌다. 하드웨어 자원 사용률의 경우 이전 논문에서는 전체 하드웨어 자원의 99%를 사용하였지만 본 논문의 하드웨어는 22%만을 사용하였다. 또한 이전 논문에서는 내부 메모리의 50%를 사용하였지만, 본 논문에서는 10%만을 사용하여 하드웨어 자원 사용율을 크게 줄였다.

표 2. 다른 H/W와의 비교
Table 2. Comparison of other H/W

Item	Our	[7]
Operation frequency	36.35 MHz	33 MHz
Total logic element or Slice	8,328/38,400 (22%)	6825/6912 (99%)
Memory	32,768/327,680 (10%)	12/24 (50%)

그림 5. 암호화 모드의 시뮬레이션 결과
Fig. 5. Simulation result of encryption mode

3.2 구현결과의 응용

본 논문에서 구현한 KASUMI 암호화 알고리즘의 구현결과를 영상데이터에 적용하여 다양한 응용 가능성을 살펴보았다. 적용한 기법은 영상데이터의 일부분을 KASUMI 알고리즘을 이용해 은닉하는 것이다. 이 방법은 영상의 DWT(discrete wavelet transform) 영역에서 주파수 변환된 데이터의 특정 부대역을 암호화하는 것이다[7,8].

영상정보를 숨기는 작업은 영상정보가 전송되는 동안 허락되지 않은 사람이 영상정보를 포획하여 그 영상의 내용을 파악하거나 다시 사용하지 못하게 하는 것이 목적이다. 따라서 암호화 결과 영상을 인식하지 못하거나 영상을 다시 사용하지 못할 정도로 왜곡된다면 반드시 영상 전체를 암호화할 필요는 없다. 더구나 암호화 알고리즘이 복잡한 과정을 거쳐 수행되므로 암호화를 위

한 처리시간 때문에 전체 영상처리시간에 큰 영향을 줄 수 있으며, 특히 무선통신의 경우 암호화 및 복호화 과정으로 인한 지연시간(latency time)과 전력소모는 큰 장애요소가 될 수 있다. 따라서 가능하며 암호화 양을 최소화하는 것이 바람직하다.

영상데이터의 주파수 영역에서 암호화 과정을 적용하기 전에 공간 영역에서 화소값을 대상으로 암호화를 수행하였다. 그 결과를 그림 7에서 보이고 있다. 그림 7(a)는 원영상, (b)는 모든 화소값들을 암호화 한 결과, (c)는 영상에서 중요한 부분만을 선택하여 암호화한 결과를 비교하였다. 암호화된 영상들의 PSNR(peak signal to noise ratio)값을 측정한 결과 그림 7(b)는 9[dB], (c)는 20[dB]로 전체 데이터를 암호화한 경우가 훨씬 낮은 값을 보였다. 하지만 영상의 중요영역만을 암호화한 (c)의 경우에도 암호화 방법으로써 충분한 가치가 있다고 판

그림 6. 복호화 모드의 시뮬레이션 결과
Fig. 6. Simulation result of decryption mode

단된다. 그림 8의 (a)에서 보이는바와 같이 DWT 결과의 부대역들은 서로 다른 주파수 성분들을 포함하고 있다. DWT 레벨이 증가할수록 저주파 성분이 강하며, 따라서 인간의 눈에 대한 중요도가 증가한다. 또한 서로 다른 주파수 성분일 뿐 전체 영상에 대한 정보를 포함하고 있다.

인간의 눈에 가장 큰 영향을 주고 가장 많은 영상정보를 담고 있는 부대역이 최저주파수 부대역인 LL4이다. 따라서 부대역을 선택하는데 있어서 가장 우선이 되어야 하는 부대역은 LL4이다. 그림 8(b)는 Lena 영상의 4-레벨 DWT 후 데이터 전체를 암호화한 결과이고, (c)는 LL4만을 선택하여 암호화한 결과 영상이다. 그림 8(b), (c) 영상은 DWT 영역에서 계수값들을 암호화한 후 IDWT(Inverse-DWT)를 수행하여 복원한 영상들이다. 그림 8(c)의 경우 전체 데이터량의 0.3906%만을 암호화하여 원 영상을 거의 인식할 수 없을 정도의 충분한 효과를 얻을 수 있다.

그림 7. 공간 영역에서의 암호화; (a) 원영상, (b) 전체데이터, (c) 중요영역

Fig. 7. Encryption of spatial domain; (a) original image, (b) whole data, (c) region of interest

그림 8. 주파수 영역에서의 암호화;

(a) 4-레벨 DWT 결과, (b) 전체데이터, (c) LL4

Fig. 8. Encryption of frequency domain; (a) result of 4-level DWT, (b) whole data, (c) LL4

IV. 결론

본 논문에서는 UMTS(universal mobile telecommunication system) 핵심망에 기반한 비동기방식의 무선 접속 기술을 바탕으로 한 시스템의 보안 구조에서 기밀성과 무결성을 제공하는 KASUMI 암호화 알고리즘을 FPGA를 기반으로 하드웨어로 설계하였다. 또한 구현결과를 영상 데이터에 적용하여 다양한 응용분야의 가능성을 살펴보았다. 설계한 하드웨어는 부가적인 소프트웨어나 하드웨어가 없이 암호화와 복호화를 단일 칩에서 수행할 수 있도록 하였고, 면적의 효율성을 높여 FPGA에 성공적으로 사상되었다.

이 설계결과의 일부분을 수정하여 ASIC을 타겟으로 구현할 경우 더 높은 동작속도를 보일 것으로 예상되어 본 논문의 결과는 초고속/초경량 암호화 및 복호화가 필요한 많은 응용분야에서 효율적으로 사용될 것으로 기대된다.

참고문헌

- [1] 정보통신 중점기술 표준화로드맵 Ver.2010, 한국정보통신기술협회, 2009년 12월
- [2] SW시장 분석, “국내 정보보호 시장 동향과 전망”, KIPA, 2008년 1월
- [3] 하준수, 최현준, 서영호, 김동욱, “암호화 알고리즘 ARIA의 FPGA기반 하드웨어 구현”, 한국해양정보통신학회 논문지, 제 10권 제 7호, pp. 1237-1245, 2006년 7월
- [4] 최용제, 김호원, 김무섭, 정교일, “IMT-2000 시스템을 위한 기밀성 및 무결성 하드웨어 구현”, 한국통신학회논문지, 제 27권 제 11호, pp. 1028-1038, 2002년 11월
- [5] 서영호, 박성호, 최성수, 정용진, 김동욱, “네트워크 보안을 위한 다중모드 블록암호시스템의 설계”, 한국통신학회 논문지, 제 28권 제 11C호, pp. 1077-1087, 2003년 11월
- [6] IMT2000 3GPP-보안-비밀성과 무결성 알고리즘 명세, TTA, 2000년 12월
- [7] 서영호, Sujit Dey, 김동욱, “웨이블릿 영역에서의 선택적 부분 영상 암호화”, 한국통신학회 논문지, 제 28권 제6C호, pp. 648-658, 2003년 6월
- [8] 서영호, 최현준, 김동욱, “이산 웨이블릿 패킷 변환을 이용한 디지털 홀로그래프의 암호화”, 한국통신학회 논문지, 제 33권 제 11호, pp. 905-916, 2008년 11월

문성식(Sung-Sik Moon)

1998년 목포대학교 기계공학과
(공학석사)

1983년 ~현재 : 한국폴리텍Ⅱ대학
컴퓨터응용기계과 부교수

※관심분야: H.264/AVC, Stereo Matching, FPGA/ASIC

김동욱(Dong-Wook Kim)

한국해양정보통신학회논문지
제13권 제8호 참고

저자소개

최현준(Hyun-Jun Choi)

한국해양정보통신학회논문지
제13권 제8호 참고

서영호(Young-Ho Seo)

한국해양정보통신학회논문지
제13권 제8호 참고