CDMA 시스템 인증을 위한 암호 해쉬 함수의 구현

황 재 진, *채 현 석, 최 명 렬
한양대학교 전자전기제어계측공학과, *동원대학 모바일컨텐츠과
전화 : 031-400-4036

Implementation of Cryptographic Hash Function for CDMA System Authentication

Jae-Jin Hwang, *Hyen-Seok Chae, Myung-Ryul Choi
Dept. of EECI, HanYang University
*Dept. of Mobile Contents and Internet, TongWon College
E-mail : heyjin25@asic.hanyang.ac.kr

Abstract

In cellular communication, subscriber authentication is an essential technique. The mobile station should operate in conjunction with the base station to authenticate the identity. In CDMA system, authentication is the process by which information is exchanged between a mobile station and base station for the purpose of confirming the mobile station. A successful authentication process means that the mobile station and base station process identical sets of shared secret data(SSD). SSD can be generated by authentication algorithms. The cryptographic hash function is a practical way of authentication algorithms. In this paper, we propose and implement MD5 and SHA-1 with modified structure.

I. 서론

무선 이동통신 시스템은 가입자에게 이동성을 지원하고 통신망에 무선 접속을 가능하게 한다. 하지만, 이러한 특성은 보안적 측면에서 불법적인 도청과 접속을 용이하게 하고 가입자의 현재 위치의 노출 등의 문제점을 내포한다. 모든 셀룰러(cellular) 단말기는 처음 서비스에 가입할 때, 내장된 메모리 칩에 이동국 식별 번호 MIN (Mobile Identification Number)과 단말기 제조회사에서 부여하는 단말기 고유번호 ESN(Electronic Serial Number)이 저장된다. MIN과 ESN을 통해 가입자에게 무선 접속 서비스가 제공되기 때문에, 이것을 도청하여 단말기에 불법 복제하면 가입비와 사용료를 지불하지 않고도 서비스를 제공받을 수 있다. 그러므로, 가입자 신분 확인 또는 가입자 인증은 필수적인 보안 서비스이다.

CDMA 시스템 인증을 위한 암호 인증 알고리즘 (Cryptographic Authentication Algorithms)으로 암호 해쉬 함수(Cryptographic Hash Function)를 이용할 수 있다. 원래, 해쉬 함수(Hash Function)는 전산과학 분야에서 사용되는 것으로 임의의 길이의 데이터를 일정한 길이의 값으로 전환하기 위해 사용되는 함수인데, 암호학 분야에서 암호 해쉬 함수라는 명칭으로 인증 및 디지털 서명 분야에 응용되고 있다.

본 논문에서는 CDMA 시스템의 인증을 위해 사용되고 있는 암호 해쉬 함수 MD5와 SHA-1의 효율적인 구현 방안을 제안하고, 하드웨어적으로 구현하였다. Xilinx사의 ISE 5.2i를 사용하여 VHDL로 설계하였으며, 시뮬레이션 검증을 위해 Mentor Graphics의 ModelSim v5.6e를 사용하였다. 하드웨어적인 동작 검증을 위해 Xilinx사의 Vertex xcv300을 이용하였다.

II. CDMA 통신에서의 인증

이동국(Mobile Station)은 기지국(Base Station)에 접속하여 서비스를 제공받게 되고, 기지국은 접속하는 이동국의 신원(Identity)을 확인하기 위한 절차를 수행한다. CDMA 시스템에서의 인증은 이동국의 신원을 확인하기 위한 이동국과 기지국간의 정보 교환이라 할 수 있다. 인증 절차가 성공했다는 것은 이동국과 기지국이 동일한 SSD(Shared Secret Data)를 가지고

있음을 의미한다.

SSD는 SSD-A와 SSD-B로 구성되는데, SSD-A는 인증 절차에 사용되고, SSD-B는 음성보안(Voice Privacy)과 메시지 기밀성을 지원하기 위해 사용된다. SSD는 암호 해쉬 함수에 의해 생성되며, 그림 1에 SSD의 생성의 예를 나타내었다.

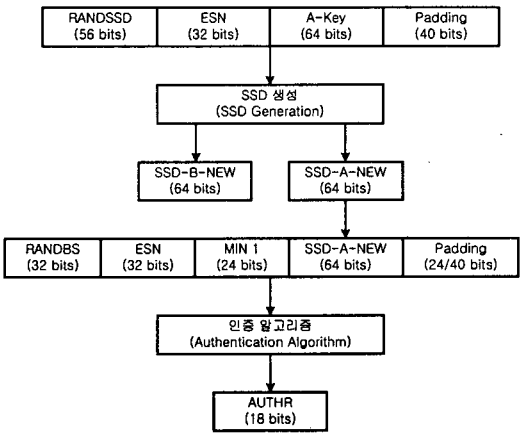

그림 1. SSD(Shared Secret Data)의 생성

III. MD5

3.1 MD5의 개요

MD5는 메시지 축약(Message-Digest) 알고리즘으로 임의의 길이의 메시지를 입력받아 128-bit의 해쉬코드(Hash Code)를 출력한다. 입력 메시지는 16개의 32-bit 서브블록으로 구성된 512-bit 단위로 처리된다.

3.2 MD5 메시지 축약 알고리즘

입력 메시지는 512-bit의 배수가 되도록 패딩(Padding)된다. MD5는 4개의 32-bit 버퍼 A, B, C, D를 가지고 있으며 그림 2의 값으로 초기화된다. 또한, 4개의 보조함수(Auxiliary Function) F, G, H, I로 기본적인 연산을 수행한다. 보조 함수는 그림 3에 나타내었다. 그리고, 그림 4와 그림 5에 MD5의 기본 연산 과정과 전체 구조를 각각 나타내었다.

A = 01 23 45 67
B = 89 AB CD EF
C = FE DC BA 98
D = 76 54 32 10

그림 2. MD5의 버퍼 초기값

$$F(X,Y,Z) = (X \cdot Y) + (\overline{X} \cdot Z)$$
$$G(X,Y,Z) = (X \cdot Z) + (Y \cdot \overline{Z})$$
$$H(X,Y,Z) = X \oplus Y \oplus Z$$
$$I(X,Y,Z) = X \oplus (Y + \overline{Z})$$

그림 3. MD5의 보조함수(Auxiliary Function)

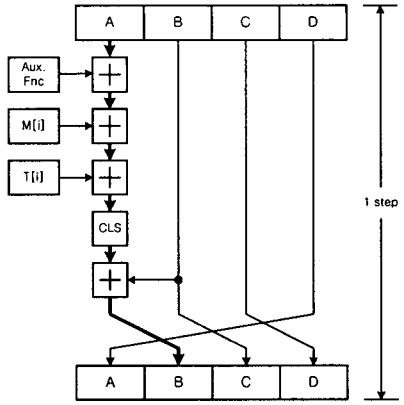

그림 4. MD5의 기본 연산 과정

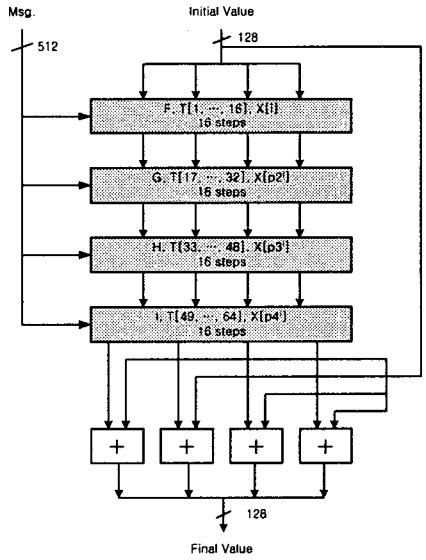

그림 5. MD5의 전체 구조

IV. SHA-1

4.1 SHA-1의 개요

NIST에 의해 제안된 SHA(Sesure Hash Algorithm)는 FIPS 180-1을 통하여 SHA-1으로 해쉬 함수 표준으로 채택되었다. SHA-1은 임의의 길이의 메시지를 입력받아 160-bit의 해쉬코드를 출력한다.

4.2 SHA-1 알고리즘

MD5와 동일한 방법으로 메시지 패딩이 이루어진다. SHA-1은 5개의 32-bit 버퍼를 가지고 있으며, 그림 6의 값으로 초기화된다. 사용되는 함수와 상수는 그림 7과 그림 8에 각각 나타내었다. 그림 9을 이용하여 W_t를 구한다. 그림 10과 그림 11에 SHA-1의 기본 연산 과정과 전체 구조를 각각 나타내었다.

A = 67 45 23 01
B = EF CD AB 89
C = 98 BA DC FE
D = 10 32 54 76
E = C3 D2 E1 F0

그림 6. SHA-1의 버퍼 초기값

$$f_t(B,C,D) = (B \cdot C) + (\overline{B} \cdot D), \quad 0 \le t \le 19$$
$$f_t(B,C,D) = B \oplus C \oplus D, \quad 20 \le t \le 39$$
$$f_t(B,C,D) = (B \cdot C) + (B \cdot D) + (C \cdot D), \quad 40 \le t \le 59$$
$$f_t(B,C,D) = B \oplus C \oplus D, \quad 60 \le t \le 79$$

그림 7. SHA-1에 사용되는 기본 함수

$$K_t = \text{5A827999}, \quad 0 \le t \le 19$$
$$K_t = \text{6ED9BA1}, \quad 20 \le t \le 39$$
$$K_t = \text{8F1BBCDC}, \quad 40 \le t \le 59$$
$$K_t = \text{CA62C1D6}, \quad 60 \le t \le 79$$

그림 8. SHA-1에 사용되는 상수 K_t

$$W_t = S^1(W_{t-16} \oplus W_{t-16} \oplus W_{t-16} \oplus W_{t-16})$$

그림 9. W_t의 계산

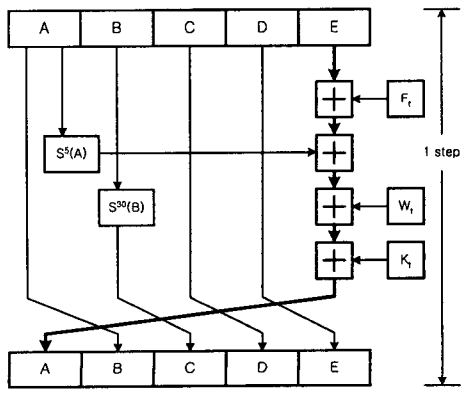

그림 10. SHA-1의 기본 연산 과정

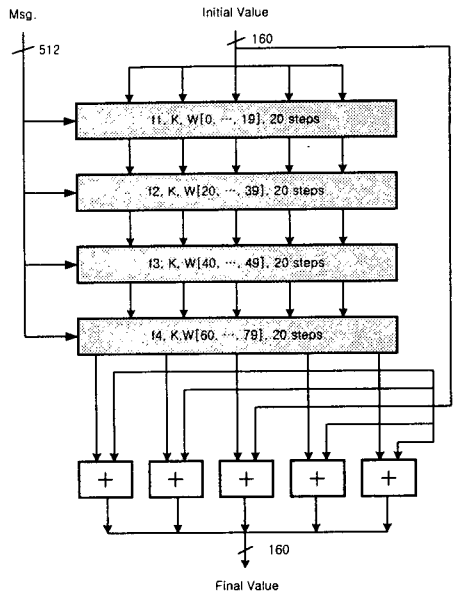

그림 11. SHA-1의 전체 구조

V. 제안한 암호 해쉬 함수의 구현

본 논문에서는 CDMA 시스템에 적용 가능한 인터페이스를 갖는 암호 해쉬 함수를 설계하였다. 그림 4와 그림 10에서 굵은 선으로 나타낸 부분이 가장 긴 연산 시간을 필요로 한다. MD5와 SHA-1이 data-dependent rotation 구조를 갖기 때문에, 이 부분은 병렬 연산 처리가 곤란하다. 본 논문에서는 굵은 선으로 나타낸 부분의 연산들을 각각의 state로 분리하여 수행했다. 이것은 조합회로(Combinational Logic)를 작게 하고 지연(Delay)을 감소시켜 최대 동작주파수를 증가시킨다. 하지만, state가 늘어나 클럭 수가 증가된다. 그러나, 그림 12와 그림 13과 같이 병렬 처리를 하면, 클럭 수를 감소시킬 수 있고 두 단계의 연산이 한 번에 가능하다. 하지만, 제안한 구조는 복잡도가 증가하여 게이트(Gates) 수를 증가시킬 수 있다. 그러나, 다음절에서 알 수 있듯이 게이트의 수는 소형화하는데 무리가 없다. 그림 12와 그림 13에 제안한 방식을 나타내었다.

V. 성능 분석

표 1과 표 2에 각각의 성능과 비교한 결과를 나타내었다. 참고논문과 비교했을 때, 비슷한 처리량(Throughput)에 2배 정도의 최대 동작주파수를 얻을 수 있다. 게이트 역시 23,000 게이트 정도이므로 소형화에 크게 무리가 없음을 알 수 있다.

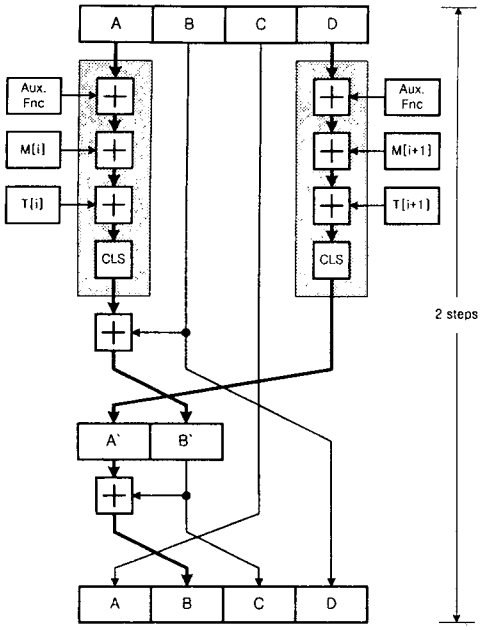

그림 12. 제안한 MD5의 연산 구조

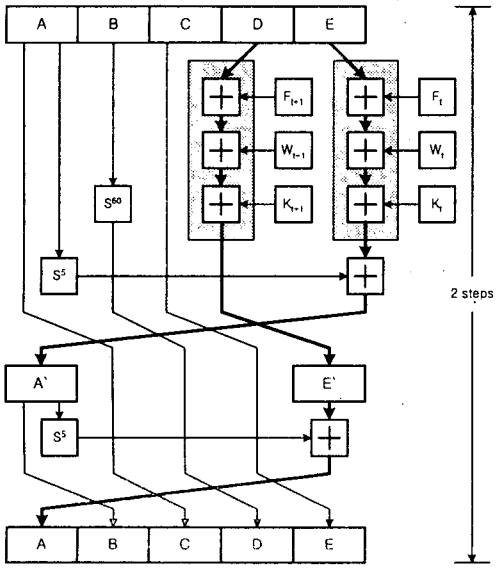

그림 13. 제안한 SHA-1의 연산 구조

표 1. MD5의 성능 분석 및 비교

	Gates	Max. Freq.	Throughput
제안한 구조	27,502	50.418 MHz	171 Mbps
참고문헌[7]	-	21 MHz	165 Mbps
참고문헌[8]	-	26.43 MHz	200 Mbps

표 2. SHA-1의 성능 분석 및 비교

	Gates	Max. Freq.	Throughput
제안한 구조	22,832	51.854 MHz	157 Mbps
참고문헌[9]	-	23.15 MHz	144 Mbps

V. 결론

본 논문에서는 CDMA 시스템 인증에 적용 가능한 MD5와 SHA-1의 효율적인 하드웨어 구현 방안을 제안하고 구현하여 보았다. 향후, 다른 암호 알고리즘을 계속 구현할 예정이며, AMBA Multi-Layer AHB를 이용하여 모듈화 할 계획이다.

참고문헌

[1] M. Y. Rhee, "Internet Security : Cryptographic Principles, Algorithms, and Protocols", John Wiley & Sons, 2003.

[2] W. Stallings, "Cryptography and Network Security : Principle and Practice", Third Edition, Prentice Hall, 2003.

[3] M. Y. Rhee, "CDMA Cellular Mobile Communication Network Security", Prentice Hall, 1998.

[4] FIPS PUB 180-1, "Secure Hash Standard", NIST, US Department of Commerce, Washington D.C., April 1995.

[5] R. Rivest, "The MD5 Message-Digest Algorithm", RFC 1321, MIT LCS & RSA Data Security, Inc., April 1992.

[6] D. Eastlake, P. Jones, "US Security Hash Algorithm 1 (SHA-1)", RFC 3174, Motorla and Cisco Systems, September 2001.

[7] J. Deeparkumara, H. M. Heys, R. Venkatesan, "FPGA Implementation of MD5 Hash Algorithm", Electrical and Computer Engineering, IEEE Canadian Conference on, Volume:2, pp.919-924, 2001.

[8] 윤희진, 정용진, "CSA를 이용한 MD5 프로세서 구현", 한국정보처리학회 춘계학술대회논문집, 2002.

[9] D. Zibim, Z. Ning, "FPGA Implementation of SHA-1 Algorithm", ASIC, 2003. Proceedings. 5th International Conference on, Volume: 2, pp.1321-1324, 2003.