通信情報保護學會誌
第3卷 第1號, 1993. 3

S-Boxes와 해쉬함수

조한혁* · 황석근**

1. 서 론

정보화 시대를 맞이하여 정보 보호의 문제가 사회적으로 중요한 문제로 부각되고 있다. 특별히 쌍방의 정보 교환시에 생길 수 있는 메시지 도청과 메시지의 수정 그리고 송수신자의 위장등이 중요한 문제이다. 해쉬함수는 메시지 인증 및 사용자 인증 등을 위해 사용되기 시작하였는데, 메시지 인증은 전달된 메시지가 공격받지 않은 원래 그대로의 메시지임을 보증하는 기능이고, 사용자 인증은 사용자 A가 상대자에게 메시지를 보낼 때 그가 바로 A임을 보증하는 기능이다. 이러한 인증의 방법으로 디지탈 서명이 있는데, 해쉬함수는 이러한 디지탈 서명과 인증의 효율성을 높이는데 필수적인 역할을 하고 있는 한 암호학적 도구이다. 해쉬함수는 finger print, MDS(manipulation detection code) 등으로 불리기도 하는데, 해쉬함수의 등장은 일방함수(one way function)와 일방 trapdoor 함수 (one way trapdoor function)의 일반적인 개념을 바탕으로 Rabin[17] 등에 의해 시작된 것으로 본다. 본고에서는 S-Boxes를 이용한 해쉬함수의 설계와 해쉬함수 제작을 위한 S-Boxes의 조건등을 살펴본다.

2. 해쉬함수와 디지탈서명

해쉬함수는 임의의 비트의 string을 일정한 비트의 string으로 바꾸어 주는 함수로서, 인증 및 디지탈 서명에 있어서 인증과 서명을 만드는 시간을 단축시켜준다. 이러한 필요성에 의해 1979년 J. Carter와 M. Wegman이 "Universal Classes of Hash Functions"을 발표한 이 후 100여편의 hash function에 관한 연구가 발표되었으나, 암호화 기술과 연관되어 본격적으로 연구된 것은 최근의 일이다. 그 중에서 Damgard[6]는 임의의 비트를 일정한 비트로 보내는 해쉬함수의 구성에 대한 연구를 했으며, Merkle[14]은 DES의 임의성을 전제로 임의의 비트를 일정한 비트로 보내는 해쉬함수를 제안한 바가 있다. 그 외에도 대칭블럭암호시스템, 공개키 암호시스템등과 결부되어 지금까지 많은 해쉬함수가 제안되어 왔다. 이제 해쉬함수를 보다 형식적으로 정의하기 위하여 $V=\{0, 1\}$일 때, $V^1 \cup V^2 \cup \cdots\cdots \cup V^n$, $V^1 \cup V^2 \cdots$를 각각 V^n, V^*로 나타내기로 한다. 이 때, 함수 $h : V^* \rightarrow V^k$를 해쉬함수라 한다.

"ISO/DP10118, Hash function for digital signatures"에서는 임의의 길이의 String을 k-비트로

* 서울대학교 수학교육과 조교수
** 경북대학교 수학교육과 부교수

축약하는 함수 $h : V^* \rightarrow V^k$가 바람직한 해쉬함수이기 위한 조건을 다음과 같이 제시하고 있다. 가) 계산 효율이 좋을 것. 나) 해쉬함수 H로부터 h(M)=H이 되는 메세지 M을 찾는 일은 계산상 불가능할 것 (약일방향성 : weak one-waynss). 다) 어떤 메세지 M과 그 해쉬값 H가 주어졌을 때, h(M′)=H가 되는 메세지 M′≠M을 찾는 일은 계산상 불가능할 것 (강일방향성 : strong one-wayness). 라) h(M)=h(M′)되는 메세지 M′≠M을 찾는 일은 계산상 불가능할 것(충돌회피성 : collision freeness). 여기서 (가)는 해쉬함수의 계산상의 효율성 조건을 말하고, (나), (다), (라)는 해쉬함수의 안전성에 대한 조건이다. 안전성 조건 (나), (다)는 피압축메세지 H가 나왔을 때, 원래의 메세지 M을 역산 내지는 변조하는 일을 방지하기 위한 기능을 갖게 하기 위함이고, (라)는 이를테면 송신자가 처음 M을 보내놓고 나중에 M′를 보냈다고 주장하는 부정, 이른바 내부부정을 방지하기 위한 제약이다. 여기서 h(x)=h(x′)되는 x≠x′를 발견하는 일은 계산상 불가능할 때, h를 계산상 일대일(computationally one to one) 함수라 하고 이러한 string의 쌍 x, x′를 h에 대한 충돌쌍 (colliding pair)이라 한다. 한편 계산상 일대일 일방해쉬함수를 충돌회피(collision free) 일방해쉬함수라 한다. 이러한 해쉬함수는 다음과 같은 공개키 암호시스템을 써서 디지탈서명에 사용될 수 있다. 먼저 메세지 M의 서명자는 서명비밀키 K와 해쉬함수 h 및 서명생성함수 π를 써서 서명 S를 생성한다. 즉, $S=\pi(h(M), K)$이다. 다음 서명자는 메세지 M과 서명 S를 수신자에게 보낸다. 여기서 해쉬함수는 압축된 메시지 H=h(M)을 생성하므로 π의 계산량을 줄여서 디지탈서명의 효율화를 도모하게 한다. 이 후, 수신자는 서명검증키 P와 서명검증함수 Θ를 써서 조사한다. 즉, $\Theta(h(M), P, S)$로 두고 서명이 옳으면 True 혹은 False로 판단한다.

3. 기초해쉬함수

임의 길이의 스트링을 축약하는 일반적인 법칙을 설정하기는 지극히 어려우므로 해쉬함수 $h : V^* \rightarrow V^k$는 보통 하나의 기초함수 $f : V^{m+k} \rightarrow V^k$를 바탕으로 다음과 같이 정의되며, 이때 다음의 정리 A가 성립한다.

1. 메세지 M을 m-bits string의 concatenation으로 나타낸다.
   즉, $M=M_1\|M_2\|\cdots\|M_N$.
2. $H_0=I \leftarrow$ k-bits 초기치
3. $H_i=f(M_i, H_{i-1}) \oplus H_{i-1}$ (i=1, 2, ···, N)
4. $H=h(M, I)=H_N \leftarrow$ k-bits 해쉬값

정리 A [2]。 h가 f를 기초함수로 하는 해쉬함수할 때, h가 충돌회피일 필요충분조건은 f가 충돌회피인 것이다.

이와 같이, 기초함수의 안전성은 그것을 바탕으로 정의된 해쉬함수의 안전성에 직결되어 있는 것이다. 뿐만 아니라 다음 정리에서 보는 바와 같이 충돌회피인 기초 일방함수가 하나 있으면 이를 바탕으로 임의의 길이의 메세지를 축약하는 일방해쉬함수를 만들 수 있다.

정리 B [2]。 충돌회피 일방해쉬함수 $f : V^{m+k} \rightarrow V^k$가 주어져 있다면, 임의의 자연수 i에 대하여 충돌회피 일방해쉬함수 $F : V^{m+k+i} \rightarrow V^k$를 만들 수 있다.

기존의 많은 해쉬함수는 (m+k)-bit string을 k-bit string으로 보내는 기초함수 f가 대칭블락 암호키 e에 의해 $f(M, H)=eM(H)\oplus H$ (단 M은 m-bits, H는 k-bits)로 정의되고 있다. 이 때, 초기치 H_0에 의하여 $M=M_1\|M_2\|\cdots\|M_N$의 해쉬값은 $F_N(M_1\|M_2\|\cdots\|M_N, H_0)$이 된다. 여기서 $F_N(M_1\|M_2\|\cdots\|M_N, H_0)$은 점화식을 써서 $f(M_N, F_{N-1}(M_1\|M_2\|\cdots\|M_{N-1}, H_0))$으로 정의한다. 이 때, f의 보수속성에 의하여 $f(M^c, H^c)=eM^c(H^c)$ $H^c=(eM(H))^c\oplus H^c=eM(H)\oplus H=f(M, N)$이 된다. 따라서 f는 충돌회피가 아니며, 정리 A에 의해 F_N은 충돌회피가 아니다. 이제 이와 같은 충돌쌍에 대한 개선책을 살펴보자. (1) 실제 사용에 있어서 $f(M, H)=eM(H)\oplus H$의 보수속성에 의해 만들어진 (M, H)와 (M^c, H^c) 이외의

충돌쌍은 만들기가 용이하지 않다고 본다. 그렇다면 정다한 사용자 양측이 그들만의 비밀키 H_0를 공유하여 사용할 수도 있다. 이때 H_0를 항상 저장해 둘 필요는 없다. 왜냐하면 송수신자는 수신자에게 먼저 초기치를 공개키 시스템을 이용하여 보낼 수 있기 때문이다. (2) M을 $M_1 \| M_2$로 확장하여 (이를테면 M_1은 M의 길이, M_2는 M자신) $f(M, H)=F(M_1 \| M_2, H)$로 하면 $(M_1 \| M_2)^c$에 의해 M_1의 값이 바뀌므로 이러한 종류의 충돌은 막을 수 있다. (3) 기초함수를 $f(M, H)=eM(H)+H$ (여기서 +는 modulo 2^k의 합)와 같이 정의한다. 그러면 e의 보수속성이 앞에서와 같은 종류의 충돌쌍을 제공하는 데에 아무런 도움을 줄 수 없다.

4. S-Boxes를 통한 해쉬함수의 설계

1989년 Merkle이 DES를 사용하여 수 개의 해쉬함수를 제안하였고, 1990년에는 안전한 S-Box에 기초한 해쉬함수 알고리즘을 제안하기도 했다[13]. 이러한 연구와 Adams and Tavares[3]가 제안한 Structured Design of Cryptographically Good S-Boxes의 방법등은 안전한 해쉬함수의 제작에 응용할 수 있다. 예를 들어, DES는 56비트의 키와 64비트의 블락을 64비트로 보내므로 DES를 120비트에서 64비트로 가는 기초해쉬함수로 볼 수 있는데, 이제 DES의 S-Boxes를 SBox[4][8]과 같이 정리한 후 이를 사용한 기초해쉬함수 f()의 주요 알고리즘을 살펴보자.

다음의 f()를 실행시키면 pass가 0부터 1까지 변하며 루프를 두 번 반복 실행하게 되는데, 루프에서는 64비트의 input이 4비트씩 16조각을 나누어지어 last 블럭은 rotl로 다음 블럭은 rotn으로 그리고 현재 위치의 블럭은 roth로 표현되게 된다. 다음 A : 에 가면 roth가 가르키는 4비트의 하위 3비트에서 0부터 7까지의 수를 얻어 SBox[4][8]에서 S-Box 하나를 선택할 때 사용한다. B : 에서는 이렇게 얻어진 수 num과 pass의 값등을 통해 S-Box 하나를 취하게 되고 이 값이 sbox에 저장된다. 다음, C : 에서는 sbox의 값이 rotl 블럭 및 rotn 블럭과 XOR되게 된다. 여기서 rotn이 가르키는 블럭에서 다음

```
for(pass=0 ; pass<2 ; pass++)
{  for(rot=1 ; rot<17 ; rot++)  {
       rotl=4*(rot-1) ;
       roth=4*(rot % 16) ;
       rotn=4*((rot+1) % 16) ;

A :    num=input[roth+1]*4+
           input[roth+2]*2+
           input[roth+3]  ;

B :    sbox=SBox[2*pass+((int)rot/2)%2][
                  17*num+input[roth]*8] ;

C :    for(i=0 ; i<4 ; i++) {
           input[rotl+i]^=(sbox & 0x01) ;
           input[rotn+i]^=(sbox & 0x01) ;
           sbox>>=1 ;  }
}
```

일이 벌어지므로 XOR하는 일은 다음의 S-Box를 선택하는데 영향을 주게된다.

이제 구현된 해쉬함수를 분석하자. 먼저 같은 S-Box에 의한 두 번의 XOR가 문제를 일으킬 수 있기에, 적어도 두 번 이상의 반복 시행이 있어야 한다. 이를 위해 DES의 32개 S-Boxes를 SBox[2*2][8]와 같이 정렬시켰고, Sbox는 SBox[2*j+(i/2 mod 2)][3-bits of block[i]]으로 뽑아진다. 다음, 한 방향으로만 XOR를 하면 circuit-depth가 감소될 수 있기에, 두 방향으로 XOR를 하여 circuit-depth를 보존시켰다. 이 때, 두 방향으로 XOR를 하기에 parity가 보존되지만, f()로 부터 만들어질 수 있는지는 암호시스템은 적당하지는 않다. 마지막으로 Output bit가 128정도 되어야 birthday Paradox Attack에 안전하기에 큰 S-Boxes를 사용하여 위의 기초해쉬함수를 보완하여야 한다.

5. 해쉬함수를 위한 S-Boxes의 설계

DES의 S-Boxes등의 기존의 S-Boxes에는 어떤

trapdoor가 있을 수도 있다. 또한 meet-in-the-middle-attack을 견디기 위해서는 큰 S-Boxes가 필요하게 되며, 요사이 바람직한 S-Box의 조건이 새롭게 발표되고 있다. 따라서 해쉬함수 등을 위해 설계 방법이 공개된 안전한 S-Box를 제작하는 연구가 요청된다. 그런데 n비트에서 n비트로 가는 S-Box는 n개의 부울함수로 나타내어지는데, 안전한 S-Box의 제작은 이를 구성하는 부울함수의 모임에 의해 결정된다. 이제 해쉬함수의 설계를 위한 큰 S-Boxes를 위해 부울함수의 조건을 Walsh-Hadamard 변환등을 이용하여 알아보자.

부울함수는 본래 부울대수 위에서 정의되는데, 논리적인 연산을 대수적인 연산으로 바꿀 수 있기에 편의상 유한체인 $GF(2)$에서 정의되며, n개의 변수를 갖는 부울함수는 $f: GF(2)^n \rightarrow GF(2)$이 된다. 이제 n개의 변수를 갖는 부울함수 $f: GF(2)^n \rightarrow GF(2)$에 대해서, v(f)를 f의 truth table을 나타내는 길이가 2^n인 벡터라 하자. 이 때, 부울함수는 2^n 길이의 (0, 1)-벡터 또는 유한기하의 측면에서 $GF(2)^n$의 부분집합으로도 이해될 수 있다. n-비트에서 n-비트로 가는 S-Boxes는 n개의 변수를 갖는 부울함수 n개가 모여 만든 함수로서 $GF(2)^n \rightarrow GF(2)^n$인 함수가 된다. 따라서 S-Boxes도 $n \times 2^n$인 (0, 1)-행렬로 표현될 수 있다. 이러한 표현은 유용한데, 예를 들어 S-Box의 전단사 성질은 S-Box가 $n \times 2^n$인 (0, 1)-행렬로 표현될 때 row들을 일차결합한 벡터의 weight가 항상 2^{n-1}인 것이다.

$f: GF(2)^n \rightarrow GF(2)$인 부울함수에 대해서 v(f)가 f의 truth table을 나타낼 때, 모든 아핀부울함수 f들의 v(f)를 모아 놓은 공간을 1차 리드-뮬러 코드(Reed-Muller Code)라 하는데, 이를 R(n)으로 표시하자. 이때 $m=2^n$이라면 R(n)은 $GF(2)^m$의 부분공간이 된다. 이제 $B(n)=\{f \mid GF(2)^n \rightarrow GF(2)\}$의 원소 f와 g의 거리 $d(f, g)$는 $v(f)$와 $v(g)$의 *Hamming* 거리로 정의된다. 또한 f의 비선형거리 $\delta(f)$는 $\min_{l \in R(n)} d(f, l)$으로 정의된다. 일반적으로 k에 대해 $\delta_k(f)$는 min {d(f, g) | g ∈k차 리드-뮬러 코드 R(k, n)}으로 정의된다. 비선형거리는 $\delta(f)=2^{n-1} - \frac{1}{2} \max_{w \in GF(2)^n} |\hat{F}(w)|$ 과 같이 해다마드 변환을 통해 구할 수도 있다.

이제 R(n)의 covering radius를 γ_n이라 하면 다음의 사실이 성립한다.

(1) : n이 짝수이면 γ_n은 $2^{n-1}-2^{n-2/2}$이다.

(2) : n이 홀수이면 $2^{n-1}-2^{n-1/2} \leq \gamma_n \leq 2^{n-1}-2^{n-2/2}$이다.

참고로 9이상의 홀수인 n에 대한 γ_n의 값은 아직 미해결 문제로 남아있다. 이제 $m=2^n$이라 할 때, $GF(2)^m$을 R(n)으로 짜른 coset C의 weight를 max {wt(v) | v ∈C}로 정의하고, 이러한 weight를 갖는 C의 원소를 C의 coset-leader라 한다. 짝수인 n과 f ∈B(n)에 대해 f의 비선형거리 $\delta(f)$는 f를 포함하는 coset의 weight로 정의된다. 특히 $\delta(f)=2^{n-1}-2^{n-2/2}$인 함수 f를 벤트함수 (bent function)이라 한다. 벤트함수의 비선형위수 (대수적 표준형의 차수)가 n/2로 제한되어 있으며, 또한 (0, 1)-balanced가 아니다. 그러나 벤트함수는 이상적인 비선형성을 갖고 있기에, 어떤 암호학적 성질을 갖는 함수가 벤트함수와 가까울수록 그 함수는 바람직하다고 말할 수 있다. bent함수 f의 성질은 n이 짝수일 때 $\delta(f)=2^{n-1}-2^{n-2/2}$과 같이 해다마드 변환을 통해 확인할 수 있다.

이제 부울함수 f ∈B(n)가 선형함수이고 a ∈GF $(2)^n$를 임의의 벡터라 하자. 그러면 임의의 x에 대해 f(x+a)=f(x)+f(a)가 되며, 따라서 임의의 x값에 대해 f(x+a)-f(x)는 일정한 값 f(a)를 갖는다. 이제 이러한 성질을 일반화하여 다음과 같이 의사아핀함수를 정의하자. 즉, 임의의 벡터 a ∈$GF(2)^n$에 대해서, f(x+a)-f(x)의 값이 x값에 상관없이 일정한 값을 가질 때 함수 f를 의사아핀함수라 한다. 임의의 벡터 a ∈$GF(2)^n$에 대해서, f(x+a)=f(x)인 x의 개수와 f(x+a) ≠ f(x)인 x의 개수가 같은 함수 f를 완전비선형함수라 한다. 또한 weight가 d이하인 임의의 벡터 a ∈$GF(2)^n$에 대해서, f(x+a)=f(x)인 x의 개수와 f(x+a) ≠ f(x)인 x의 개수가 같은 함수 f를 완전비선형위수가 d인 함수라 하다. 이에 대해 다음에 제시되는 정리를 보자.

정리 C. 완전비선형위수에 대한 다음의 명제는 서로 동치이다.

(1) : 부울함수 $f: GF(2)^n \rightarrow GF(2)$의 완전비선형 위수가 d이다.

(2) : weight가 d이하인 임의의 벡터 c에 대해,

$$\sum_{x \in GF(2)^n} f(x) \oplus f(x \oplus c) = 2^{n-1}.$$

(3) : weight가 d이하인 임의의 벡터 c에 대해,
$F(x) = (-1)^{f(x)} : GF(2)^n \rightarrow \{1, -1\}$ 이면

$$\sum_{x \in GF(2)^n} F(x) \cdot F(x \oplus c) = 0.$$

(4) : weight가 d이하인 임의의 벡터 c에 대해,
$\hat{F}(w) = \sum_{x \in GF(2)^n} F(x)(-1)^{x \cdot w}$이면

$$\sum_{x \in GF(2)^n} \hat{F}^2(w)\,(-1)^{w \cdot c} = 0.$$

이제 A(n)은 집합 {f ∈B(n) | f는 의사아핀함수}을 나타내며, $\pi(n)$은 집합 {f ∈B(n) | f는 완전비선형함수}을 나타내며, $\rho(f) = \min\{d(f, g) \mid g \in A(n)\}$을 나타낸다고 하자. 이 때, 의사아핀함수의 집합 A(n)은 위수가 n인 1차 Reed-Muller 코드 R(n)을 당연히 포함한다. 따라서 $\delta(f) \geq \rho(f)$이 된다. 다음 정리는 주어진 f ∈B(n)이 완전비선형함수일 조건이다.

정리 D. 다음은 f ∈B(n)이 완전비선형함수일 필요충분조건이다.

(1) 0이 아닌 임의의 벡터 c ∈GF(2)^{n}에 대해 $f * f(c) = 0$

(2) 임의의 벡터 c ∈GF(2)^{n}에 대해 $|\hat{F}(c)| = 2^{n/2}$.

(3) 임의의 벡터 c ∈GF(2)^{n}에 대해 $\Sigma \hat{F}^2(w)\,(-1)^{w \cdot c} = 0$.

(4) 임의의 아핀함수 g ∈R(n)에 대해 d(f, g)의 값은 $2^{n-1} \pm 2^{n-2/2}$

(5) $\delta(f) = 2^{n-1} - 2^{n-2/2}$

(6) $\rho(f) = 2^{n-2}$

(7) f는 bent함수이다.

(8) 임의의 아핀함수 g ∈R(1, n)에 대해 c(f, g)의 절대값은 $2^{-n/2}$.

증 명 : $f(x)$를 이용하여 $F(x) = (-1)^{f(x)} : GF(2)^n \rightarrow \{1, -1\}$를 정의하자.

만일 F가 {+1, −1}로 가는 부울함수라 하면, F*F의 해다마드 변환은 $\hat{F}^2$이다. 따라서 f가 완전비선형함수이면 $\hat{F}^2$은 상수함수이고 $F*F(0) = 2^n$이므로 $|\hat{F}(c)| = 2^{n/2}$이다. 이제 L_w : x->xw라 하자. 여기에서

$$F(w) = \#\{x \mid f(x) = L_w(x)\} - \#\{x \mid f(x) \neq L_w(x)\}$$
$$= 2^n - 2\,d(f, L_w(x)).$$

따라서 $L_w^*(x)$를 $L_w(x)+1$로 잡으면

$d(F, L_w(x)) = 2^{n-1} - \frac{1}{2} F(w)$이며,

$d(F, L_w^*(x)) = 2^{n-1} + \frac{1}{2} F(w)$이다.

따라서 f가 완전비선형함수이면, 임의의 아핀함수 g ∈R(1, n)에 대해

$d(f, g) = 2^{n-1} \pm 2^{n-2/2}$이다.

이제 $d(f, g) = 2^{n-1} + \frac{1}{2} F(w)$라는 사실에서 $\delta(f) = 2^{n-1} - 2^{n-2/2}$이 된다. 그런데 임의의 f에 대해 Parseval의 정리에 의해

$\Sigma \hat{F}^2(w) = 2^{2n}$이다.

따라서 만일 f가 완전비선형함수가 아니라면 어떤 c에 대해

$|\hat{F}(c)| > 2^{n/2}$이다.

$\max\{\delta(f) \mid f \in B(n)\}$의 값은 $2^{n-1} - 2^{n-2/2}$이다. 따라서 f ∈B(n) 이 벤트함수일 필요충분조건은 $\delta(f) = 2^{n-1} - 2^{n-2/2}$이다. 또한 $\max\{\rho(f) \mid f \in B(n)\}$의 값은 2^{n-2}이다. 따라서 f ∈B(n)이 벤트함수일 필요충분조건은 $\rho(f) = 2^{n-2}$이다. 여기서 f가 완전비선형함수가 아니면 $\delta(f) < 2^{n-1} - 2^{n-2/2}$이다. 이제 주어진 두개의 부울함수 f와 g에 대해 f와 g에 교차상관계수 c(f, g)는 $(\#\{x \mid f(x) = g(x)\} - \#\{x \mid f(x) \neq g(x)\})/2^n$으로 정의된다. 따라서 $g = L_w$라면 $c(F, L_w) = \hat{F}(w)/2^n = 2^{n-2/2}$이다.

주어진 두개의 부울함수 f와 g의 교차상관계수 c(f, g)는 $(\#\{x \mid f(x) = g(x)\} - \#\{x \mid f(x) \neq g(x)\})/2^n$이기에 c(f, g)는 $2^n - 2 * d(v(f), v(g))$를 2^n으로

나눈 것이다. 그런데 g가 L_w일 경우 c(f, L_w)는 정의에 의해 $F(w)/2^n$임에 유의하자. 이러한 이유등에 의해 f가 완전비선형함수일 필요충분조건은 f가 모든 아핀함수와 최소의 상관계수를 갖을 때이다. 따라서 어떠한 암호학적 조건에 맞는 함수는 완전비선형함수에 가장 가까이 있으면 바람직하다. 예를 들어 스트림 블락시스템에 유용한 correlation immune 함수를 보자. 그런데 완전비선형함수의 성질은 correlation immune 함수의 성질과 위배된다. 위수가 m인 correlation immune 함수 f는 weight가 m이하인 임의의 벡터 w에 대해서 F(w)=0이 된다. 따라서 그러한 벡터 w에 대해 c(f, L_w)는 0이 된다. 따라서 Parseval's 정리에 의해 다른 아핀 함수와 f와의 상관계수가 높게 된다. 여기서 f와 제로함수 0와의 상관계수 c(f, 0)는 정의에 의해 함수 f의 ±1-균형도를 표시해준다. 따라서 완전비선형함수의 ±1-균형도는 $2^{-n/2}$이다. 그런데 이것은 n이 커짐에 따라 0으로 수렴해간다. 따라서 완전비선형함수(n이 짝수일 때 Bent함수)는 0/1 balance를 갖지 않지만 n이 커짐에 따라 balance 성질과 비슷한 성질을 갖게 되고, 또한 비선형성이 우수하므로 암호학적인 부울함수가 가져야할 조건중에 하나라고 할 수 있다.

6. 결 론

지금까지 조사된 바의 대부분의 디지탈 서명용 해쉬함수들은 충돌회피함수가 아니므로 완벽하게 안전하다고는 볼 수 없거나 또는 실행시간이 너무 길다는 결점을 갖고 있다. 다음 imprint가 짧은 모든 해쉬함수는 meet-in-the-middle attack에 약하므로 확률적으로 충돌회피가 불가피하다. 한편 실용성의 관점에서 대칭블락암호키를 atomic operation으로한 해쉬함수가 중요하다. 그러나 지금까지 제안된 거의 모든 해쉬함수는 대칭블럭암호키의 보수성이나 weak key property와 같은 함수적 구조로 인한 취약점을 가지고 있다. 그렇지만 이런 종류의 해쉬함수가 대단히 효율적이므로 이와 같은 취약점을 극복하는 연구가 요구된다. 따라서 새로운 해쉬함수의 구성에는 이같은 성질을 갖지 않는 블럭암호(예 : Knapsack Problem 또는 Modular squaring을 이용한 암호)를 사용하든지, 또는 이런 성질들이 전혀 작용할 수 없는 구성법을 고안해야 할 것이다. 최근에 S-Box를 바탕으로 소개된 해쉬함수는 계산 속도 및 안전성의 문제점만 보완되면 상당히 안전하고 효율적인 hashing tool이 될 것이다. 따라서 이러한 S-Box를 바탕으로 하는 종합적인 해쉬함수의 개발이 필요할 것으로 본다.

해쉬함수의 연구도 스트림암호시스템에서 주기등의 수학적 피라메타로 안전성을 표시할 수 있는 것처럼, 안전성을 수식화 하여야 할 것이다. 그러한 점에서 S-Boxes를 이용한 해쉬함수는 S-Boxes들을 이루는 부울함수들의 성질을 수식화 하여 암호학적 이론을 수학적으로 표현할 수 있는 것이다. 본 연구를 위해 만일 안전한 S-Boxes가 있다면, 그것을 통해 해쉬함수를 만들 수 있는 알고리즘을 프로그램으로 구현하였다. 또한 S-Boxes의 설계를 위한 부울함수들의 암호학적 성질을 해드마드 행렬을 이용한 해마마드 변환으로 표현하여 프로그램으로 만들고, 이를 활용하여 구체적으로 DES의 부울함수에 대해 실험해 보았다. 그 결과 DES의 128개 부울함수 가운데 15개만이 1차의 Correlation-immune 함수였으며, 2차 이상의 Correlation-immune 함수는 없었다. 또한 데스의 모든 부울함수는 1 보다 큰 m에 대해 m차의 완전비선형함수가 아니었다. 따라서 모든 부울함수는 SAC 조건을 만족하지 않았고, 물론 m(>0)차의 SAC 조건도 만족하지 않았다. 또한 DES의 S-Box S_{ij}의 비선형거리를 S_{ij}를 이루는 부울함수의 비선형거리의 합으로 정의할 때, S_{74}의 비선형거리는 8이고, S_{23}, S_{33}, S_{34}, S_{64}, S_{63}, 그리고 S_{83}의 비선형거리는 12였다. 그 외의 S-Box S_{ij}의 비선형거리는 대부분 14와 16이었다. 이러한 알고리즘을 효율화 시키면 큰 S-Boxes와 이를 통한 해쉬함수를 만드는데 활용할 수 있을 것이다.

Bent함수는 본래 조합론의 이론에서 나온 것인데, 이것이 비선형성을 갖는 좋은 암호학적 대상으로 활용되고 있다. 따라서 Reed-Muller 코드와 부울함수에 대한 체계적인 연구가 필요하다. 그런데 Bent함수이며 어떤 암호학적 성질을 만족시키는 부울함수를 찾는 일은 확률적으로 0퍼센트에 가깝다고 한

다. 따라서 벤트함수에 가장 가까이 있으며 또한 주어진 암호학적 성질을 갖는 부울함수의 연구가 요청된다. 또한 바람직한 조건을 모두 갖는 큰 부울함수를 찾는 일을 시간이 많이 걸리는 작업이므로 Random Number 등을 응용하여 S-Box를 제작하는 연구도 요청된다.

참 고 문 헌

1. 김광조, Bent 함수의 암호학적 성질에 관한 고찰, 통신정보보호학회논문지, 1권 1호 (1991), pp.85-90.

2. 황석근 & 조한혁, 디지탈 서명과 해쉬함수, 통신정보보호학회지, 2권 1호 (1992), pp.23-29.

3. C. Adams and S. Tavares, The structured Design of cryptographically good S-Boxes, J. Cryptology 3 (1990), pp.27-41.

4. Carter and Wegman, Universal clases of hash functions, J. computer and System Sci. 18 (1979), pp.91-110.

5. D. Coppersmith, Another birthday attack, Proc. of Crypto'85, LNCS 28 (1986), pp.14-17.

6. I. B. Damgard, A design principle for hash functions, Proc. of Crypto'89 (1990), pp. 416-427.

7. D.W. Davies, Applying the RSA digital signature to electronic mail, IEEE Computer 16, No. 2, (1983), pp.55-62.

8. W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Trans Inform. Theory, IT22. 6 (1976), pp.644-654.

9. R. Forre, The strict avalanche criterion : spectral properties of Boolean functions and an extended definition, in Advances in Cryptology : Proc. of CRYPTO'88 (1989), pp.450-468.

10. S. Goldwasser, S. Micali and R. L. Rivest, A 'paradoxical' solution to the signature problem, IEEE (1984), pp.441-448.

11. Godlewski and Camion, Manipulation and errors, Localization and detection, Processdings of Erocrypt'88, Springer.

12. ISO/DP 10118, Hash functions for digital signatures, 1989.

13. R. C. Merkle, A fast software one-way hash function, J. Cryptology, 3 (1990), pp.43-58.

14. R. C. Merkle, one way hash functions and DES, proc. of CRYPTO'89 (1990), pp.428-445.

15. W. Meier and O. Staffelbach, Nonlinear criteria for cryptographic functions, Proc. of EUROCRYPT'89, pp.549-562.

16. J. Pieprzyk and G. Finkelstein, Toward effective nonlinear cryptosystem design, IEE Proc. 135 (1988), pp.325-335.

17. M. Rabin, Digitalize signatures, In R. Demillo et al., editor, Foundation of Secure Computation, Academic Press, 1978, pp.155-166.

18. O. S. rothaus, On "Bent" functios, J. Combi. Theroy (A) 20 (1976), pp.300-305.

19. A. F. Webster and S. E. Tavares, On the design of S-boxes, Proc. of CRYPTO'85 (1986), pp.523-534.

20. D. Welsh, Codes and Cryptography, Clarendon Press, Oxford, 1989.

21. G. Z. Xiao and J. L. Massey, A spectral characterization of correlation-immune combining functions, IEE Trans. Info. Theory 34 (1988), pp.569-571.

□ 著者紹介

趙 漢 赫(正會員)

1979年 2月 서울大學校 師範大學 數學教育科 卒業(理學士)
1981年 2月 서울大學校 大學院 數學科 卒業(理學碩士)
1988年 8月 Univ. of Wisconsin-Madison 大學院 數學科 卒業(Ph. D.)
1988年 9月～1989年 2月 Bowling Green State Univ. 專任講師
1989年 3月～현재 서울大學校 助教授

黃 石 根(正會員)

1972年 2月 慶北大學校 師範大學 數學教育科 卒業(理學士)
1977年 2月 慶北大學校 大學院 數學科 卒業(理學碩士)
1985年 8月 Univ. of Wisconsin-Madison 大學院 數學科 卒業(Ph.D.)
1979年 4月～1990年 2月 慶北大學校 專任講師-助教授
1990年 3月～1991年 3月 成均館大學校 副教授
1991年 3月～現在 慶北大學校 副教授