논문 2010-6-28

안전한 이중 파이프 해쉬함수에 관한 연구

A Study on the Secure Double Pipe Hash Function

김희도*

Hie-Do Kim

요 약 고전적인 반복 해쉬함수는 다중 충돌 공격에 취약점을 가지고 있다. Gauravaram등은 일반적인 Merkle-Damgard Chain에 accumulation chain을 추가한 3C와 3C+ 해쉬함수를 제안하였다. 이 해쉬함수의 목표는 Joux의 일반적인 공격에 저항성을 갖도록 설계하는 것이다. 그러나 Joux's와 Tuma는 엄격하지 않다는 가정 하에서 다중 충돌 공격에 3C와 3C+ 스킴이 MD 스킴보다 안전성을 갖고 있지 않음을 보였다. 논문에서는 3C 해쉬함수의 안전성을 증대하기 위하여 accumulation chain에 메시지 블록 당 XOR와 XNOR연산을 효과적으로 사용하는 해쉬함수를 제안하였다. 이 방법은 Lucks의 이중 파이프 해쉬함수를 개선한 것이다. 또한, 제안한 이중 파이프 해쉬함수는 다중블록 충돌 공격, 고정점 공격, 그리고 원상공격에 저항성을 갖는다.

Abstract The classical iterated hash function is vulnerable to a multi-collision attack. Gauravaram et al. proposed 3C and 3C+ hash functions, in which an accumulation chain is added to usual Merkle-Damgard changing. Their goal is to design composition schemes resistant to generic attacks of Joux's type, but Joscak and Tuma have shown that 3C and 3C+ schemes are not better than Merkle-Damgard scheme in term of security against multi-collision attacks under some mild assumptions. In this dissertation, in order to increase security of 3C hash function, we proposed secure double pipe hash function which was effectively using XOR and XNOR operations per blocks of message. We seek to improve on the work of Lucks in a way. Proposed secure double pipe hash function takes resistance to multi-block collision, fixed point and pre-image attacks.

Key Words : 압축 함수(Compress function), 해쉬 함수(hash function), 랜덤 오라클(Random Oracle), 충돌 저항성(collision resistant), 다중 블록 충돌 공격(multi-block collision attacks)

Ⅰ. 서 론

암호시스템에서 해쉬함수는 임의의 입력크기에 대한 입력들은 m비트 블록의 메시지로 분할하고 압축함수 $C: \{0,1\}^n \times \{0,1\}^n$을 반복함으로서 실현할 수 있다. 1989년 Merkled[1]과 Damgard[2]는 독립적으로 고정길이 입력에 대하여 충돌 저항성을 가진 압축함수 $C: \{0,1\}^n \times \{0,1\}^n$를 사용 하여 암호학적 해쉬 함수 $H: \{0,1\}^* \rightarrow \{0,1\}^n$를 구성하였다. 그러나 MD 해쉬함수는 다중 충돌 공격에 안전하지 않다. Praveen et al[3]이 다중 충돌 공격에 저항성을 갖기 위해 3C, 3C+ 해쉬함수를 제안하였다. Joscak과 Tuma[4]는 엄격하지 않는 가정에 기초하여 이 함수의 취약점을 제시하였다. 본 논문 은 Lucks[5]가 제안한 이중 파이프 해쉬함수와 Praveen et al이 제안한 3C구조를 조합한 새로운 형태이다. Lucks는 MD 해쉬함수의 일반적인 공격에 저항성을 갖기 위해 광역 파이프 해수함수와 안전한 이중 파이프 해쉬함수를 제안하였다. 제안한 이중 파이프 해쉬 함수는 Lucks가 제안한 이중 파이프 해쉬함수에 선형

*정회원, 강릉영동대학 통신/부사관과
접수일자 : 2010.11.18, 수정완료일자 : 2010.12.10
게재확정일자 2010.12.15

XOR와 XNOR로 구성된 accumulator chain을 추가 하였다. 또한 초기 값과 O(Offset)를 XOR하여 입력으로 사용하였다. Praveen et al은 다중 충돌 공격에 저항성을 갖기 위해 3C와 3C+ 해쉬함수를 제안 하였다. 그러나 Joscak과 Tuma는 3C와 3C+ 해쉬함수 구조가 다중 충돌 공격에 안전하지 않음을 보였다. 제안한 논문은 선형 XOR와 XNOR로 accumulator chain을 추가 구성함으로서 이중 파이프 해쉬함수가 갖는 일반적인 공격의 저항성과 다중 충돌 공격에도 안전성을 동시에 갖는 장점을 가지고 있다. 또한 초기 값과 O(Offset)를 XOR하여 첫 번째 압축함수를 입력으로 사용함으로서 충돌 확률을 낮게 하였다. 따라서 확장 공격 안전성 증대 및 안전한 키 값으로 사용할 수 있다. 반복된 해쉬함수 및 최종 압축함수의 입력을 3개 사용함으로서 일반적인 공격에 대한 안전도를 증대시키고 고정점 공격에도 저항성을 갖는다. 본 논문의 구성은 다음과 같다. 2장에서는 기존의 Lucks가 제안 이중 파이프 해쉬함수를 간단히 소개하고, 3장에서는 Praveen et al이 제안한 3C 해쉬함수 구조에 대하여 알아보고, 제안한 구조와 Lucks가 제시한 이중 파이프 해쉬함수와 Praveen et al이 제시한 3C구조를 조합한 새로운 형태의 이중 파이프 해쉬함수를 제안하였다, 마지막 5장은 결론에 대하여 기술하였다.

Ⅱ. 이중 파이프 해쉬함수 구조

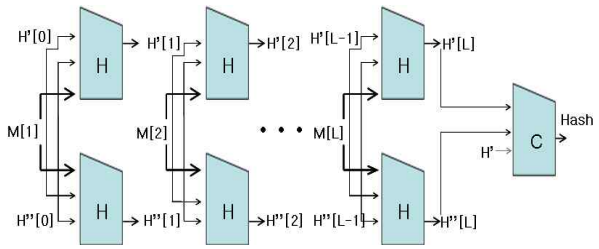

그림 1. 이중 파이프 해쉬함수 구조
Fig. 1. Dual Pipe Hash Function Structure

정리 1. 이중 파이프 해쉬함수 H을 고찰한다.

가. H의 한개 원상을 발견하는 것은 $\Omega(P^{''}(1))$시간을 갖는다.

나. H의 하나의 K-way 원상을 발견하는 것은 $\Omega(min\{T_S, T_X, P^{''}(K)\})$시간을 갖는다.

정리 2. 이중 파이프 해쉬함수 H을 고찰한다.

가. 압축함수 C을 Random Oracle 모델로 적용한다면 하나 또는 K-way 원상과 하나 또는 K-way 2차 원상을 발견하는 것은 $\Omega(2^n)$ 시간을 갖는다.

나. Joux[6]의 원상공격은 K-way 원상을 찾는데 $\Omega(k2^n)$시간이 필요하다.

1. Joux의 공격에 대한 안전성 분석

이 공격은 MD 해쉬함수에서 다중 2차 원상 충돌을 매우 효과적으로 발견할 수 있다. 이중 파이프 해쉬함수에 대한 다중 충돌 공격에서 공격자는 생일공격을 이용하여 cascade chain에서 모든 H 해쉬함수에 대하여 충돌을 발견 하는 것이다. 이중 파이프 해쉬함수의 cascade chain에서 함수 H가 Random Oracle 모델 이라면2^n-충돌을 발견하는데 전체 시간 복잡도는 $O(k * 2^{n/2})$가 상한 경계이다.

공격자는 $H_n = H(M^1) = ...H(M^{2^k})$인 n블록 메시지에 대하여 충돌을 발견한다. 주어진 Y의 결과인 마지막 두 압축함수를 실행함으로서 M_{n+1}의 블록을 발견 하는 것이다. 두 압축함수에서 마지막 실행은 시간 $O(2^n)$을 갖는다. 따라서 이중 파이프 해쉬함수에서 K-원상을 발견하는데 전체 시간 복잡도는 $O(k * 2^{n/2} + 2^n)$이다. 공격자는 주어진 메시지 M으로부터 K-way 2차 원상을 발견하기 위하여 메시지 M의 해쉬 값 $H(M)$을 계산하고 $H(M)$에 모든 충돌로서 K-원상을 발견 한다.

2. 2차 원상 공격에 대한 안전성 분석

Dean[7]는 고정점을 가진 압축함수에서 2차 원상을 발견하는데 복잡도가 2^n보다 작음을 제시하였다. Kelsey와 Schneier[8]는 임의의 압축함수에 기초한 해쉬함수에서 2차 원상을 발견하는데 Joux의 다중 충돌 공격을 사용하여 복잡도가 2^n보다 작음을 보였다. 이들 공격은 다른 길이의 확장 가능한 메시지 패턴을 사용 했으며 모든 과정의 내부 해쉬 값은 MD 강도를 고려하지 않았다. 이중 파이프 해쉬함수에서 cascade chain의 압축함수의

고정점은 두 압축함수의 해쉬 값 $H(M_i)$에 의해 정의되고 이것은 $H(0, M_i) = 0$일 때만 어떤 메시지 블록 M을 얻을 수 있으며 2^{-n}확률을 가지고 발생한다. 따라서 제안한 이중 파이프 해쉬함수에서 고정점을 가지는 압축함수가 2차 원상을 발견하는데 시간 복잡도가 2^n과 같다.

Ⅲ. 3C 해쉬함수 구조

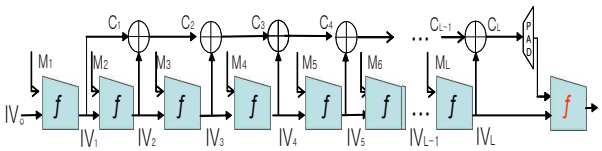

그림 2. 3C 해쉬함수 구조[6]
Fig. 2. 3C Hash Function Structure

3C 해쉬함수 구조는 그림 2과 같다. 3C 해쉬함수 구조는 2개의 chain을 갖고 있다. 하나는 accumulation chain이고 다른 하나는 cascade chain이다.

accumulator chain은 XOR 함수를 선형 결합 한 것이다. cascade chain은 MD 구조와 같다.

IV_0 = 초기 값

$C_1 = IV_1$

$C_i = C_{i-1} \oplus IV_i = IV_1 \oplus IV_2 \oplus, ... \oplus IV_i \quad i = 2, ..., L$

여기서 L 은 메시지 블록수이다.

1. 3C 해수함수의 취약점

최근 Tuma[4]에서 IV_1이 엄격하지 않는 조건에서 같은 압축함수f 을 사용한 3C 해쉬함수는 아래 정리 3에서 $2n$-블록 충돌을 발견할 수 있음을 제시 하였다.

정리 3. H가 압축함수 f 에 기초한 MD 해쉬함수라 하자. $n \geq 2$이라 하고 어떤 초기 벡터 IV_0를 적용하고 $IV_i \oplus IV_i' = IV_{n+i} \oplus IV_{n+i}' \; i = 1, ..., L$는 IV_0와 실제 충돌 메시지들과 상수 독립인(i 에는 종속) 특성을 가진 H에서 n블록 충돌을 발견하는 하나의 알고리즘이 존재한다. 따라서 같은 압축함수를 사용한 3C 해쉬함수 구조에서 $2n$-블록 충돌을 발견하는 어떤 알고리즘이 존재함을 알 수 있다.

증명 : $(M_1 \mid M_2 \mid M_3 \mid M_4 \mid ... \mid M_n)$와 $(M_1' \mid M_2' \mid M_3' \mid M_4' \mid ... \mid M_n')$을 H에서 충돌 발견 알고리즘의 첫 번째 실행에서 얻은 2개의 충돌 메시지라 하자.

$IV_n = IV_n', \quad (M_{n+1} \mid M_{n+2} \mid M_{n+3} \mid M_{n+4} \mid ... \mid M_{n+n}), \quad (M_{n+1}' \mid M_{n+2}' \mid M_3' \mid M_{n+4}' \mid ... \mid M_{n+n}')$ 충돌 메시지의 또 다른 짝(pair)을 얻을 수 있다. $IV_{n+i} (i = 1, ..., L)$와 $IV_{n+i}' (i = 1, ..., L)$를 두 번째 알고리즘 실행에서 초기 값 변화 값이라 둔다. $IV_i \oplus IV_i' = IV_{n+i} \oplus IV_{n+i}' \quad i = 1, ..., L$따라서 다음 식을 얻는다.

$C_{2n} = \oplus_{i=1}^{2n} IV_i$, $C_{2n}' = \oplus_{i=1}^{2n} IV_i'$ **그러므로** $C_{2n} \oplus C_{2n}' = \oplus_{i=1}^{2n} IV_i \oplus_{i=1}^{2n} IV_i' = \oplus_{i=1}^{2n} (IV_i \oplus IV_i') = \oplus_{i=1}^{n} (IV_i \oplus IV_i') \oplus (IV_i \oplus IV_i') = 0$, $IV_n = IV_n'$이기 때문에 $(M_{n+1} \mid M_{n+2} \mid M_{n+3} \mid M_{n+4} \mid ... \mid M_{n+n})$ $(M_{n+1}' \mid M_{n+2}' \mid M_3' \mid M_{n+4}' \mid ... \mid M_{n+n}')$는 3C와 3C+ 해쉬함수 구조에서 어떤 충돌이 존재한다.

Ⅳ. 제안한 안전한 이중 파이프 해쉬함수

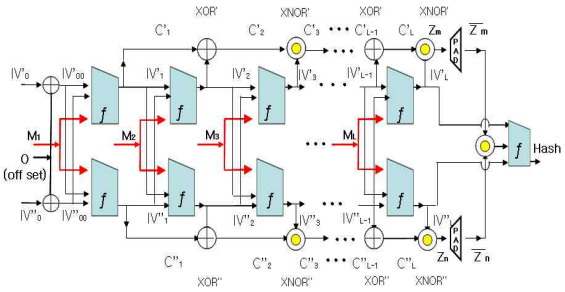

그림 3. 제안한 안전한 이중 파이프 해쉬함수 구조
Fig. 3. Proposed Secure Dual Pape Hash Function Structure

1. "제안한 이중 파이프 해쉬함수은 다음 과 같은 특징을 갖는다."

가. Ⅳ 초기 값과 O(Offset를 XOR하여 첫 번째 압축함수를 입력으로 사용함으로서 충돌 확률을 낮게 하였다. 따라서 확장 공격 안전성 증대 및 안전한 키 값으로도 사용 할 수 있다.

나. accumulator chain에 XOR과 XNOR을 교번 사용하여 내부 다중 블록 충돌을 회피 하였다.

다. 반복된 MD구조 입력과 최종 압축함수의 입력을 3개 사용함으로서 일반적인 공격에 대한 안전도를 증대시키고 고정점 공격에 저항성을 갖는다.

라. n비트 해쉬함수를 병렬로 사용하여 속도를 증가시킴과 동시에 광역 파이프 해쉬함수와 같은 안전도를 갖는다.

2. OMD(Offset MD)

첫 번째 압축함수에서 충돌 확률을 낮게 하기위해 초기값과 (Offset)를 XOR하여 사용하였으며 안전한 PRF(Pseudo Random Function)으로 주어진다[9].

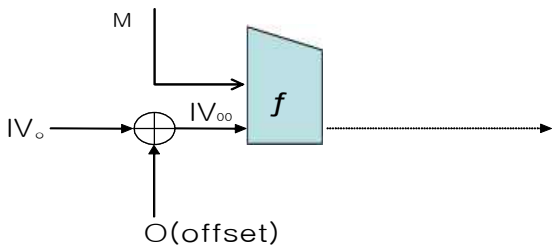

그림 4. OMD(Offset MD)
Fig. 4. OMD(Offset MD)

여기서 서로 다른 초기값으로서 IV_{11}, IV_{22} IV_{00}, , $IV_{33},.., IV_{mm}$에서 m개의 다른 초기값을 random하고 독립적으로 선택한다. 이것은 고정된 초기값이 키라면 보다 더 안전한 키로 사용 할 수 있다.

$IV_0 = \{iv_0, iv_1, iv_2, ..., iv_m\}$ 여기서

$O = \{O_0, O_1,)_2, ..., O_m\}$ 이고

$IV_{00} = O_0 \oplus iv_o$

$IV_{11} = O_1 \oplus iv_1$

$IV_{22} = O_2 \oplus iv_2$

.

$IV_{mm} = O_m \oplus iv_m$

$IV_{00} \neq IV_{11}$ 이다.

다음 $2m$-tuple함수의 확률적인 분산은 서로 다르다.

$(f(IV_0), f(IV_{00}), ...$

$f(IV_m), f(IV_{mm}))$ 따라서 엄격하게 $IV_1 \neq IV_1^{'}$이다.

3. 혼란 해쉬함수

혼란(Dithering) 해쉬함수[10]는 입력이 3개인 해쉬함수이다. 제안한 이중 파이프 해쉬함수도 이러한 형태이며 Dean의 공격과 확장 공격에 저항성을 갖는다. 혼란 해쉬함수는 MD 해쉬함수 구조에 하나의 추가적 입력을 사용하고 이 입력은 각 단계마다 변화 값을 변경할 수 있다. 이것은 결국 어떠한 환경에서도 확장 공격과 Dean의 공격에 대하여 더욱 안전하게 하고 고정점 발견을 훨씬 어렵게 한다. 이 구조는 HAIFA(HAsh Iterative FrAmework)[11]구조와 유사하다. 단지 차이점은 입력으로 사용한 가염 값(Salt Value)이 없는 것이다. 혼란 값은 비 제곱 수열(squre-free sequence) 또는 Abelian 비 제곱 수열을 사용한다.

혼란해쉬함수에서$M = M_1, ..., M_L$일때i^{th}변화값 $IV_i = f(IV_{i-1}, M_i, d_{i-1})$이다.

여기서 $i \in 1, 2, ...L$ $IV_0 =$초기 값 $d_0 =$ 초기 혼란 값

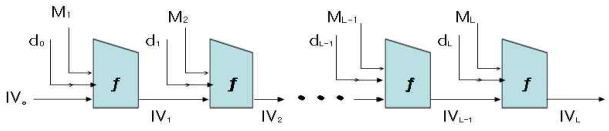

그림 5. 혼란 해쉬함수[10]
Fig. 5. Dithering Hash Function

4. 고정점 공격에 대한 저항성

압축함수 고정점은 (IV_{i-1}, M_i)이다

$$f(IV_{i-1}, M_i) = IV_i$$

$$f(IV_{i-1}, M_i) = IV_{i-1}$$

$IV_i = IV_{i-1}$ 이것은 메시지 블록 M_i가 해쉬함수의 변화 값에 독립적임을 의미한다. 따라서 공격자는 (IV_{i-1}, M_i)가 동일하게 반복 할 때 마다 임의의 다른 메시지를 삽입하여 공격할 수 있다.

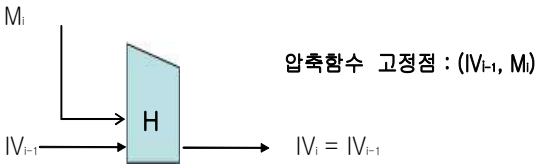

그림 6. 압축함수 고정점
Fig. 6 Compressed Function Fixed Point

공격자는

$IV_i = IV_{i-1} = f(IV_{i-1}, M_i, d_{i-1})$로 부터 고정점을 발견하지 못하도록 혼란 값을 선택해야 한다. 따라서 Dean의 공격과 확장 공격은 혼란 해쉬함수 구조에서 제한된다.

5. 내부 다중 블록 충돌 회피

본 논문에서는 accumulator chain에서 XOR와 XNOR를 교번 사용 하여 내부 다중 블록 충돌을 회피함으로서 다중 블록 충돌 공격에 저항성을 가진다.

정의 1 cascade chain에서 하나의 충돌은 H에서 하나의 충돌을 의미한다.

$(H_i^M, M_i) \neq (H_i^{M'}, M_i) H(H_i^M, M_i) = H(H_i^{M'}, M_i)$ 여기서 H_i^M과 $H_i^{M'}$은 내부해쉬 값.

정의 2 해쉬함수 H를 사용하여 $H(M)$과 $H(M')$이 두개의 다른 메시지 M과 M'의 압축이라 하고 어떤 고정된 함수 T에서 $H(M) = T(H(M'))$이면 $H(M)$과 $H(M')$은 상대 충돌이라 한다.

정리 4 H를 압축함수 f를 사용하여 설계한 해쉬함수라 하자. cascade chain의 상대 충돌이 다중 블록 충돌로 되기 위해서는 accumulation chain에서 충돌 발생이 필요충분조건이다.

여기서

c_i : 메시지 M에 대하여 accumulation chain변화 값

c_i' : 메시지 M'에 대하여 accumulation chain의 변화 값 $i \in \{2, ..., L\}$이다.

$$c_i = c_{i-1} \oplus f(c_{i-1}, M_i)$$

$$c_i' = c_{i-1}' \oplus f(c_{i-1}', M_i')$$

증명 : cascade chain상의 내부 충돌로서 accumulator chain상의 다중 블록 충돌을 고찰한다. $c_L \neq c_L'$일 때 최종 충돌 $H_L^M = H_L^{M'}$, $f(H_L^M, c_L) = f(H_L^{M'}, c_L')$을 가정 한다. 위로부터 $H_i^M = H_i^{M'}$은 t^{th} 데이터 블록이 진행 후 cascade chain상에서 하나의 내부 블록 충돌이 있다. ($c_L \neq c_L'$)이때 해쉬함수 H에서 충돌은 최종 충돌이 아닌 것을 의미한다. cascade chain에서 내부 블록 충돌은 최종 충돌 전에 t^{th} 데이터 블록에서 상대 충돌이 발생 할 수 있다. 이것은 ($c_i \neq c_i'$) $i \in \{2, .., t-1\}$, ($c_i \neq c_i'$) $i \in \{t, ..., L-1\}$을 의미한다. t^{th} 데이터 블록에서 상대 충돌은 블록 $i \in \{t+1, ..., L\}$로 진행 후 최종 충돌로 주어진다. 따라서 내부 다중 블록 충돌은 최종 충돌로 이어진다. t^{th}블록에서 상대 충돌이 내부

충돌이라 하자.

$H(M_t) = T(H(M_t^{'}))\rightarrow$

$H(M_t) = H(M_t^{'})$

$f(H(M_{t+i}), c_{t+j}) = f(H(M_{t+i}^{'}), c_{t+j}^{'})$

$i, j \in [1, 2, ..., l\}$ 내부 충돌은 (H_i^M, M_i)

$\neq (H_i^{M'}, M_i)$일 때$H(H_i^M, M_i) = H$

$(H_i^{M'}, M_i)$이므로$H_i^M = H_i^{M'}$

$(H_i^M \oplus H_i^{M'}) = 0$ 이다.

$(H_i^M \oplus H_i^{M'}) \oplus (c_{j-1} \oplus c_{j-1}^{'}) = 0$를 accumulator chain에서 충돌은 만족해야한다. 따라서 $(c_{j-1} \oplus c_{j-1}^{'}) = 0$은필요충분조건이다.

$c_{j-1} = c_{j-1}^{'}$ 이다. 메시지 M과 $M^{'}$에서 t^{th}블록에서 cascade chain이 충돌하기위해 $(H_i^M \oplus H_i^{M'}) = 0$ 조건을 만족해야하고 내부 블록 충돌 조건은 $(H_i^M \oplus H_i^{M'}) \oplus (c_{j-1} \oplus c_{j-1}^{'}) = 0$이다. 이것은 t^{th}블록에서 하나의 내부 충돌은 t^{th}블록에서 accumulation chain과 cascade chain에서 동시 충돌이다. 이 조건은 $(c_{j-1} \oplus c_{j-1}^{'}) = 0$와 $(H_i^M \oplus H_i^{M'}) = 0$이 동시 일 때만 발생하고 accumulation chain에서 XOR 연산의 출력 값이 0을 만족해야 한다. 이것은 t^{th}블록 일 때 accumulation chain에서 기본적으로 하나의 충돌이다. $(H_i^M, H_i^{M'})$과 $(c_{j-1}, c_{j-1}^{'})$는 cascade chain과 accumulation chain으로부터 얻을 수 있다. 해쉬함수의 전체 충돌은 accumulation chain이 초기 다중 블록 충돌이나 최종 압축함수에서 충돌하는 것이 필수적이다. 위 결과 $(H_i^M \oplus H_i^{M'}) = \delta$와 $(c_{j-1} \oplus c_{j-1}^{'}) = \delta$ 발생 할 경우 accumulator chain 연산을 XOR대신 XNOR를 사용하여 $(H_i^M \oplus H_i^{M'}) \odot (c_{j-1} \oplus c_{j-1}^{'}) = \delta$를 만들어$(c_{j-1} \oplus c_{j-1}^{'}) = 0$과$(H_i^M \oplus H_i^N) = 0$이 동시에 0이 되는 것을 회피 하였다. 그림7은 다음 식을 얻는다.

$C_1 = IV_1 = \delta$

$C_2 = C_1 \oplus IV_2$

$C_3 = C_2 \odot IV_3 = C_1 \oplus IV_2 \odot IV_3$

$C_4 = C_3 \oplus IV_4 = C_1 \oplus IV_2 \odot IV_3 \oplus IV_4$

$C_5 = C_4 \odot IV_5 = C_1 \oplus IV_2 \odot IV_3 \oplus IV_4 \odot IV_5$

$C_n = C_{n-1} \oplus IV_n = C_1 \oplus IV_2 \odot IV_3 \oplus IV_4 \odot IV_5, ..., \odot IV_n = \delta(H_i^M \oplus H_i^{M'}) \odot (c_{j-1} \oplus c_{j-1}^{'}) = \delta$

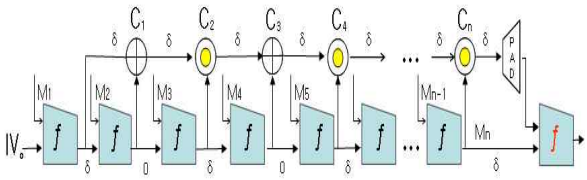

그림 7. 충돌 값 δ 회피

Fig. 7. Collision δ Value Avoid

위 그림 7에서와 같이 accumulator chain 어떤 점에서도 0값이 아니다. 따라서 제안한 해쉬함수는 내부 충돌을 회피함으로서 다중 충돌 공격에 저항성을 갖는다.

표 1. 제안한 논문과 다른 해쉬함수의 압축함수 비교

Table 1. Comarision of Proposed Paper and Other Hash Function of Compression Function

해쉬함수 구조	첫번째압축함수입력크기	압축함수/블록	최종압축함수입력
MD 구조	n	1	n
Wide-pipe Hash	w > n	1	w > n
Double-pipe Hash	2n	2	2n
3C	1n	1+XOR	2n
3C+	1n	1+2×XOR	2n
제안한 해쉬함수	2n	2+2×XOR (XNOR)	3n

표 2. 제안한 논문과 다른 해쉬함수의 안전성 비교
Table 2. Comarision of Proposed Paper and Other Hash Function of Security

Attacks	MD	Wide Pipe hash	Double Pipe Hash	3C, 3C+	Proposed Hash
Message expansion Attack	A	NA	NA	NA	NA
Joux's Multi-collision Attacks	A	A	A	A	NA
Multi-Blocks Attack	A	A	A	A	NA
Dean's Attack	A	NA	NA	NA	NA

NA : Not Applicable, A : Applicable

V. 결 론

본 논문에서는 다중 충돌 공격에 보다 안전한 이중 파이프 해쉬함수를 제안하였다. 내부 해쉬함수 값 n비트를 병렬로 하여 속도는 증가시키고 안전성은 광역 파이프 함수($w \geq n$ 비트)와 같은 효과를 얻기 위해 이중 파이프 해쉬함수로 구성하였다. 만약 $2^{n/2}$ 시간을 가진 모든 공격에 저항성을 가지려면 n을 충분히 크게 해야 한다. 제안한 이중 파이프 해쉬함수는 Lucks가 제시한 이중파이프 해쉬함수에 선형 XOR와 XNOR로 구성된 accumulator chain을 추가 하여 보다 안전하게 하였다. accumulator chain은 다중 충돌 공격을 회피하고 3개의 입력은 고정점 발견을 훨씬 더 어렵게 한다. 이는 이중 파이프 해쉬함수가 갖는 일반적인 공격의 저항성과 다중 충돌 공격에도 안전성을 동시에 갖는 장점을 가지고 있다. 따라서 본 논문은 다중 충돌 저항성과 내부 충돌 저항성을 가지므로 Joux의 공격에 보다 안전하다. 그러나 공격자가 무한계산능력을 가졌다면 어떠한 해쉬함수도 Joux의 다중 충돌 공격으로부터 안전 할 수 없다. 또한 입력에 O(Offset) 값을 가지고 있기 때문에 높은 안전도를 요구하는 디지털서명 및 인증 등에 다양하게 응용 할 수 있다.

참 고 문 헌

[1] Ralph Merkle. One way hash functions and DES. In Gilles Brassard,editor, Aduances in Cryptology: CRYPTO 89,volume 435 of Lecture Notes in Computer Science, pages 428-446. Springer-Verlag, 1989.

[2] Ivan Damgard, A design principle for hash functi ons. In Gilles Brassard, editor, Aduances in Cryp tology: CRYPTO 89, volume 435 of Lecture Notes in Computer Science, pages 416-427. Springer-Verlag, 1989.

[3] Praveen Gauravaram, William Millan, ED Dawson, and Kapali Viswanathan. Constructing Secure Hash Function by En hancing Merkle-Damgard Constructions. IN Lynn Batten, Reihaneh Safavi-Naini, editors, Information Security and Privacy, volume 4058 of Lecture Notes in Computer Science, pages 407-420. Springer-Verlag, 2006.

[4] D. Joscak and J. Tuma. Multico-block Colisions in Hash Functions based on 3C and 3C+Enhancements of Merkle-Dam gard Construction. Information Security and Cryptology. ICISC 2006, volume 4296 of Lecture Notes in Computer Science, pages 407-420.Springer-Verlag, 2006.

[5] Stefan Lucks. A Failure-Friendly Design Prin ciple for Hash Functions. In Bimal Roy,ditr, Aduances in Cryptology-ASI ACRYPT 2005, volume 3788 of Lecture Notes in Computer Science, pages 474-494. Springer-Verlag, 2005

[6] A.Joux. Multicollisions in iterated hash functions, application to cascaded constructions. Crypto 04, volume 3152 of Lecture Notes in Computer Science, pages 306-316. Springer-Verlag, 2004.

[7] Richared D. Dean, Formal Aspects of Mobile Code Security, Ph.D. dissertation, Princeton University, 1999.

[8] J. Kelsey. A long-message attack on SHAx, M Dx, Tiger, N-Hash, Whirlpool, and Snefru.

Draft. Unpublished Manuscript.

[9] M. Bellare and T. Kohno. A theoretical treatment of related-key attacks : RKA-PRPs, RKA-PRFs and Applications, A dvances in Crytology -EUROCRYPTO 2003, volume 2656 of Lecture Notes in Computer Science, pages 492-506. Springer-Verlag, 2003.

[10] Rivest, R. L. : Abelian Square-Free Dithering for Iterated Hash Functions. Presented at ECrypt Hash Function Works hop, June 21, 2005, Cracow, and at the Cryptographic Hash workshop, November1, 2005, Gaithersburg, Maryland(August 2005).

[11] Eli Biham, Orr Dunkelman, A Framework for Iterative Hash Functions - HAIFA, NIST 2nd hash function workshop,Santa Barbara, August 2006.

저자 소개

김 희 도(정회원)

- 1985년 8월: 국립 서울과학기술대학교 전자공학과(학사)
- 1988년 8월: 한양대학교 전자통신과(석사)
- 2008년 2월: 성균관대학교 전기·전자 및 컴퓨터공학과(박사)
- 경력

- 1985년 1월~1989년 1월 동양통신전자(주) 기술연구소 주임연구원
- 1989년 2월~1994년 2월 한국통신기술(주) 대전세계과학 EXPO'93파견 근무 기술과장
- 1994년 3월~현재 강릉영동대학 통신/부사관과 부교수

<주관심분야 : 정보보호기술, 암호이론, 통방융합기술>