情報保護學會論文誌
第17卷 第4號, 2007. 8

동적 파이프 해쉬 함수

김 희 도,[1†] 원 동 호[2‡]
[1]강릉영동대학 부사관과, [2]성균관대학교 정보통신공학부

Dynamic Pipe Hash Function

Hiedo Kim,[1†] Dongho Won[2‡]
[1]Gang Neung Yeong Dong College, Dept. Non-Commissioned Officer,
[2]Shool of Information and Communication Engineering, University Sungkyunkwan

요 약

본 논문에서는 파이프 해쉬 함수를 가진 동적 파이프 해쉬 함수를 제안한다. 안전도를 높이기 위하여, 압축함수를 추가하여 파이프 기반 동적 해쉬 함수를 제안하였다. 제안한 동적 파이프 해쉬 함수는 다중충돌공격에 안전하고 압축 사이즈를 가변할 수 있기 때문에 많은 장점을 가지고 있다. 예를 들어, 디지털 서명 프로토콜에서 사용자가 보다 큰 키 사이즈를 선택하여 높은 안전도를 요구한다면, 동적 해쉬 함수를 사용하여 압축사이즈를 증가시켜 쉽게 실현할 수 있다.

ABSTRACT

In this paper, we proposed a constrution that creates Dynamic Pipe Hash Function with a pipe hash function. To increase security lever, dynamic hash function take and additional compression function. Proposed hash function based on the piped hash function. Our proposed Dynamic Pipe Hash Function is as secure against multi-collision attack as an ideal hash function. And it have advantage for a number of reasons because of variable digest size. For example, in digital signature protocol, If a user requires increased security by selecting a large key size, useing a dynamic hash function in a protocol make implementation much easier when it is mandated that the size of the digest by increased.

Keywords : *Pipe Hash Function, Dynamic Hash Function, Preimage Resistance, Collision Resistance, Multicollision Attacks*

Ⅰ. 서 론

가변적인 해쉬 사이즈를 이용하여 안전도를 증가시키는 방법은 Dunkelmam 과 Biham[1]이 처음 제안하였다. [1]에서 제안한 HAIFA(HAsh Iterative FrAmework)는 기본적인 압축함수의 출력 사이즈와 동일하거나, 더 작게 생성 할 수 있는 가변 사이즈 해쉬 함수 생성에 대하여 제안하였다. 그러나, [1] 에서는 기본적인 압축함수 출력 보다 큰 사이즈를 생성 하지 못했다. William R. Speris II and Samuel S. Wagestaff, Jr.[2]는 [1]를 확장하여 기본압축함수 출력보다 큰 사이즈를 생성하는 방법을 제안 하고 이를 동적 해쉬 함수(dynamic hash function)라 하였다. 그러나 동적 해쉬 함수는 명백한 MD(Merkle-Damgard)구조[3]이므로

접수일: 2007년 4월 3일; 채택일: 2007년 6월 14일
† 주저자, hdkim@gyc.ac.kr
‡ 교신저자, dhwon@security.re.kr

모든 가능한 기본공격, 즉 메시지확장공격, 다중충돌공격 등에 안전 하지 않다. 본 논문에서는 [2]에서 제안한 동적 해쉬 함수 보다 안전하고 마지막 압축 함수를 이용하여 안전도를 증가 시키는 파라미터로 사용할 수 있는 새로운 형태의 동적 파이프 해쉬 함수를 제안 한다. [2]에서 제안한 동적 해쉬 함수는 메시지 외에 안전도 파라미터를 가지며 함수로부터 요구하는 안전도를 설정 할 수 있다.

동적인 변경은 메시지 블록의 수를 변경하거나, 함수의 출력의 크기를 변경함으로서 간단하게 이루어진다.

동적 해쉬 함수는 많은 장점을 가지고 있다. 첫째, 메시지 블록의 수를 줄임으로서 테스트 함수를 쉽게 설계 할 수 있다. 둘째, 압축에 관련된 안전도 파라미터라면, 해쉬 함수를 수정하지 않고 다른 응용들에 많이 사용 할 수 있다.

예를 들어, 디지털 서명에 일반적으로 많이 사용 되어지는 해쉬 후 서명 프로토콜의 경우에는. 만약 서명 알고리즘에 사용되어진 키 비트(RSA, ElGamal, 또는 Polling-Hellman과 같은)의 수가 가변적이라면, 고정된 사이즈를 제한하여 압축할 필요가 없다. 만약 사용자가 보다 큰 키 사이즈를 선택하여 높은 안전도를 요구 한다면, 압축 사이즈를 역시 증가 시켜야 한다. 이때 디지털 서명 프로토콜에서 동적 해쉬 함수를 사용한다면, 압축사이즈를 증가시켜 보다 쉽게 실현 할 수 있다. 동적 압축 해쉬 함수를 이용함으로써 소프트웨어를 수정하는 대신 디지털 서명 프로토콜은 압축사이즈를 변경하여 쉽게 설계 할 수 있다. 동적 해쉬 함수 사용과 압축 사이즈의 변경된 사양을 기술함으로서 공격에 노출된 시스템을 보다 쉽게 재현 할 수 있다. 즉 사용한 안전도 파라미터를 단순히 변경만 하면 된다. 본 논문은 다음과 같이 구성되어 있다. 2장에서는 [2]가 제안한 동적 해쉬 함수를 살펴보고 3장에서는 다중 충동공격에 안전한 동적 해쉬 함수를 제안한다. 4장에서는 제안한 동적 해쉬 함수의 특징과 안전도를 분석하고 5장에서는 결론과 향후 연구방향을 제시하였다.

Ⅱ. 동적 해쉬 함수분석[2]

본 절에서는 [2]에서 제안 한 동적 해쉬 함수를 간단히 소개 한다. 동적인 해쉬 함수는 출력 사이즈 크기와 내부에 적용되는 안전도 파라미터를 제외 하면 Bart Preneel [4]가 정의한 해쉬 함수와 같다.

다음과 같이 동적 해쉬 함수를 정의 한다.

정의 1. 동적 해쉬 함수 $H : \Sigma^* \times [l(n), u(n)] \rightarrow \Sigma^{d(s)}$로 정의 한다.

여기서,

N : 자연수의 집합

$\Sigma = \{0.1\}$

n : 메시지 M 의 길이

Σ^* : 유한이진 스트링들(finite binary strings)의 무한집합

$l(n), u(n), s(n)$: 단조증가함수(monotone increasing function)

$l : N \rightarrow N$

$u : N \rightarrow N$

$d : N \rightarrow N$,

$0 < l(n) \leq u(n)$ 이고

$0 < d(s) < n$, $n > 1$ 이다.

$[a,b] = \{i \in N : a \leq i \leq b\}$.

$s \in [l(n), u(n)]$

동적 해쉬 함수는 메시지 압축 길이를 가변 할 수 있는 2차 파라미터를 가지고 있다.

정의 2. 안전도 파라미터 간격 $[l(n), u(n)]$ 을 가진 동적 해쉬 함수족 $\mathbb{H}$ 는 유한집합(finite sets)

$\mathbb{H} = \{H_n\}_{n=1}^{\infty}$ 의 무한 집합족(infinite set family) 이다.

여기서, H_n 의 멤버들(members)을 크기 n 의 인스턴스들(intanses)이라 한다. 인스턴스 $I = (h_n, D_n, R_n)$ 이다.

여기서, $I \in H_n, D_n = \Sigma^n, R_n \subseteq \Sigma^{d(s)}, s \in [l(n), u(n)]$, $h_n(\cdot, s) : D_n \rightarrow \Sigma^{d(s)}$.

해쉬 함수족 $\mathbb{H}$ 는 세 개의 조건을 가진다.

1) H_n는 접근가능하다(accessable). 즉, H_n는 확률적 다항식 알고리즘이다.
2) H_n는 샘플가능하다(samplable). 즉, H_n는 확률적 다항식 알고리즘이며, 입력 I는 D_n으로부터 균등하게 분포된 원소들(elements)로부터 선택한다.
3) h_n는 다항식 시간 내에서 계산가능하다 즉, 입력 I 와 $x \in D_n$ 은 $h_n(x)$를 계산하는 다항식 시간 알고리즘이다.(n과 $|x|$ 내에서 다항식)

동적 해쉬 함수 구조는 기본적으로 MD 구조[3]를

변경한 것이다. 따라서 명백한 MD 구조는 메시지확장 공격(message expansion attack)에 일반적으로 안전하지 않음이 알려져 있다.

Ⅲ. 제안한 동적 파이프 해쉬 함수의 구조

3.1. NMAC과 파이프 해쉬 함수

NMAC(Nested Message Authentication Code)구조 [5]는 명백한 MD체인(chain)구조 출력에 독립적인 해쉬 함수 g를 추가하여 메시지확장공격에 안전함을 보였다.또한 S. Lucks [6]은 두 개의 압축함수를 파이프 해수 함수로 정의하여 다중충돌공격에 안전함을 보였다.

정의 3. 함수 $\mathrm{NMAC}^{f,g}$ 는 다음과 같이 정의 한다[5].

$\mathrm{NMAC}^{f,g}(m)$:
$let\ m=(m_1,...m_l)$
$y \leftarrow \mathrm{MD}^f(m_1,...m_l)$
$Y \leftarrow g(y)$
return Y
여기서 $f: \{0,1\}^{n+k} \rightarrow \{0,1\}^n$ 이고
$g: \{0,1\}^n \rightarrow \{0,1\}^n$ 이다

정의 4. 두 개의 압축 함수를 파이프 해쉬 함수를 정의 한다[6].

$C' : \{0,1\}^w \times \{0,1\}^m \rightarrow \{0,1\}^w$
$C'' : \{0,1\}^w \rightarrow \{0,1\}^n$

정리 1. 압축함수 C' 와 C''가 독립적인 랜덤 오라클이면, 파이프 해쉬 함수 H에서 $K-$충돌들을 발견하는 시간은

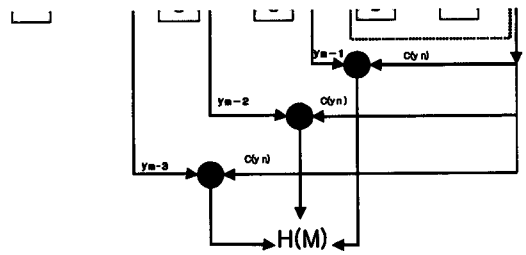
$\Omega(mim\{2^{w/2}, 2^{n(K-1)/K}\})$이다.

위의 정리에서 S. Lucks [6]은 파이프 해쉬 함수에서 $w \geq 2n$ 이면 다중 충돌 공격에 충분히 안전함을 보였다.

3.2. 동적파이프 해쉬 함수

제안한 동적 파이프 해쉬 함수구조는 [2]가 제안 한 구조에 압축 함수 C를 추가하여 [그림 1]과 같이 구성하였다.

첫째, 안전도 파라미터를 좌우하는 초기값 변경이다.



[그림 1] 제안한 동적 파이프 해쉬 함수

초기값은 메시지 블록에 연접한 지정된 초기값으로 생성된다. 초기값은 $IV_s = g(IV, IV \mid s \mid 0,...,0)$이다.

여기서, s는 안전도 파라미터이다. 0은 패딩 값이다. [1],[2] 에서도 같은 방법을 사용 하였다.

둘째, 64bit 메시지 사이즈가 가능하도록 메시지 끝에 1bit를 추가하였다. 모든 메시지는 $10,...0 \mid M \mid s$. 형태이다.

셋째, 압축함수의 출력 사이즈 보다 더 큰 메시지 압축 사이즈이다. 이것은 전단의 체인 값(previous chaining value)과 마지막 체인 값(final chaining value)을 XOR로 구성 한 것이다. [그림 1]은 마지막 세 개의 체인 값(y_{n-3}, y_{n-2}, y_{n-1})을 사용하였다.

이들 체인 각각에 파이프 해쉬값 $C(y_n)$을 XOR 하고 절삭(truncation) 하기 전에 연접하여 메시지 압축을 구성하였다. 원하는 사이즈로 메시지를 압축할 필요가 있다면 절삭 한다. 절삭은 항상 결과의 MSB(Most Significant Bits)에 대하여 한다.

Ⅳ. 제안한 동적 파이프 해쉬 함수의 특징

동적 파이프 해쉬 함수는 다음과 같은 특징을 가지고 있다.

4.1. 원상저항성(Preimage Resistance)

정리 2. 동적 파이프 해쉬 함수에 사용되어진 기본적인 압축 함수가 원상저항성을 가지고 있다면, 동적 파이프 해쉬 함수는 원상저항성을 가진다.

증명 : y_{n-2} 까지 구조는 정확히 MD 구조와 정확히 같으므로, 만약 기본적인 압축 함수가 원상저항성을 가진다면 원상저항성을 가진다. y_{n-1} 의 값이 결과에 영향을 주지 않고 , 메시지 압축에 영향을 미친다. XOR의 특성에 따라, 주어진 y_{n-1}과 $C(y_n)$의 XOR 한 값이다.

그러나 m_n을 발견하는 것은 파이프 해쉬 함수의 원상 저항성과 같다.

4.2. 충돌저항성(Collision Resistance)

정리 3. 만약 파이프 해쉬 함수 구조에 사용한 기본 압축 함수가 원상저항성과 충돌저항성을 가진다면 동적 파이프 해수 함수도 충돌저항성을 가진다.

증명 : 충돌을 발생하는 두 개의 변수는 $n-1$ 메시지 블록과 블록 m_n이다. 이 블록들을 변경할 수 있는 경우는 다음과 같이 4가지이다.

여기서, m_* : $n-1$ 블록들에서부터 블록 m_n까지 모든 메시지 m' : 원 메시지 m이 변경된 메시지라 둔다.

Case 1 : $H(m_* \mid m_n) = H(m_* \mid m_n)$

메시지가 변경 되지 않으므로 충돌이 발생하지 않는다.

Case 2 : $H(m_* \mid m_n) = H(m_* \mid m_n')$

충돌을 발생하는 첫 번째 $n-1$ 메시지변경이 없는 경우이며, 충돌은 블록m_n의 변경에서만 이루어진다. 공격자는 $C(y_n)$와 $C(y_n')$의 같은 값으로부터 두개의 메시지 블록 m_n과 m_n'을 발견 하는 것이다. 이것은 파이프 해쉬 함수가 충돌저항성과 같다.

Case 3 : $H(m_* \mid m_n) = H(m_* \mid m_n)$

충돌을 발생하기 위해서 적어도 하나의 첫 번째 $n-1$ 메시지변경이 있는 경우이다. 따라서 이것은 $y_{n-1} = y_{n-1}'$이다. 파이프 해쉬 함수의 압축함수가 랜덤 오라클과 같이 거동하므로 충돌저항성을 갖는다.

Case 4 : $H(m_* \mid m_n) = H(m_* \mid m_n')$

충돌을 발생하기 위해 마지막 메시지에 따라 첫 번째 적어도 하나의 첫 번째 $n-1$ 메시지변경이 있는 경우이다.

이 경우 $y_{n-1} \oplus C(y_n) = y_{n-1}' \oplus C(y_n')$ 이다. 이는 y_n이나 y_n' , y_{n-1}이나 y_{n-1}', 먼저 계산되어야 한다. 이는 m_n 이나 m_n'이 y_n이나 y_n'에 대응 되는 경우이며, 2차 원상공격에 해당된다. 파이프 해쉬 함수는 이차원상 저항성을 가진다.

4.3. 2차 메시지압축저항성(Second Message Digest Resistance)

o 2차 메시지압축저항성은 같은 메시지 압축을 발견하는데 계산상 불가능 한 것이다.

〔표 1〕 다른 해쉬 함수와 제안한 동적 해쉬 함수 비교

해쉬함수	입력 사이즈	출력사이즈	다중충돌공격 (K충돌)	비고
MD	고정	고정	$2^{n/2}$	
HAIFA[1]	가변	≤ 압축함수	$[log_2 k]2^{n/2}$	
동적 해쉬 함수[2]	가변	가변	$2^{n/2}$	
제안한 해쉬 함수	가변	가변	$2^{n(K-1)/K}$	

4.4. 다중충돌저항성(Multicollision Ressistance)

정리 1로부터 파이프 해쉬 함수는 다중충돌저항성을 갖는다.

4.5. 안전도증대

이 결과는 도메인 확장자(domain extender)이다. 도메인 확장자는 안전도를 증대시키는 충돌저항성 해쉬 함수임을 〔7〕〔8〕등에서 보였다.

정의 5 동적 해쉬 함수 족 $\mathbb{H}$ 에서 동적 원상 발견자(dynamic preimage finder) M, 동적 충돌 스트링 발견자(dynamic collision string finder)F, 동적 압축 생성자(dynamic digest generator)G이라 둔다.

정리 4 기본 압축함수가 랜덤 오라클로 거동한다면, 동적 해쉬 함수구조는 안전도를 증대시킨다.

증명 : $Pr\{h_n(M(n,h_n(x,s)),s) = h_n(x,s)\} \geq$
$Pr\{h_n(M(n,h_n(x,s+1)),s+1) = h_n(x,s+1)\}$
$Pr\{F(n,h_n,s) \neq ?\} \geq$
$Pr\{F(n,h_n,s+1)h_n \neq ?\}$
$Pr\{G(n,s,s',h_n(x,s)) = h_n(x,s')\} \geq Pr\{G(n,s,s'+1,h_n(x,s)) = h_n(x,s'+1)\}$

여기서 $s \neq s'$, $s \neq s' = 1$,이고 $h_n \in H_n, x \in D_n$, $\{s, s+1, s', s'+1\} \in [l(n), u(n)]$이고 M, F, G는 정의 5에서와 같이 각각 랜덤 오라클이다.

V. 결 론

본 논문에서는 파이프 해쉬 함수를 가진 동적 파이프

해쉬 함수를 제안 하였다. 제안한 동적 파이프 해쉬 함수는 마지막에 압축 함수를 추가함으로서, 일반적인 공격으로부터 안전성을 확보하고 메시지확장공격과 다중충돌공격에도 안전함을 보였다. 향후 마지막 압축 함수 거동이 출력 사이즈와 안전도에 미치는 영향에 대하여 좀더 연구가 이루어져야 할 것으로 사료된다.

참고문헌

[1] ELi Biham and Orr Dunkelman, A framework for iterative hash funcitons - HAIFA. Technical report,National Institute for standards and Technology, August, 2006.

[2] William R. Speris II and Samuel S. Wagestaff,Jr,Dynamic Cryptographic Hash Functioneprint.iacr.org/2006/477.pdf

[3] Ivan Damgard, A Design Principle for Hash Functions, Advances in Cryptology Proceedings of CRYPTO 1989, Lecture Notes in Computer Science435, pp. 416-427, Springer-Verlag, 1990.

[4] Bart Preneel, Analysis and Design of Cryptographic Hash function. Thesis Ph.D, Katholieke Universiteit Leuven, Belgium, January 1993. 416-427, Springer-Verlag, 1990.

[5] Navendu Misra, Surey of Message Authentication Code(MAC) construction and funture development University of Texas at Austin, May 2003.

[6] Stefan Lucks, A failure-Friendly Desing Principle for Hash Funtions, Advances in Cryptology, proceedings of ASIACRYPTO 2005, Lecture Notes in Computer Science 3788, pp.474-494, Springer-Verlag, 2005.

[7] Damgard. Collision free hash functions and public key signature schemes. In EUROCRYPTO '87 Proceedings, Lecture Notes in Computer Science304, Pages203-216,1988.

[8] R. Mercle, One way hash function and DES, Advances in Cryptology, Proc. Crypto, '89, LNCS 435, G.Brassard, Ed.,Springer-Verlag, 1990,pp428-446.

〈著者紹介〉

김 희 도 (Hie do Kim) 종신회원

1985년 2월 : 서울산업대학교 전자공업과 졸업
1988년 2월 : 한양대학교 전자통신공학과 석사
2000년 2월 : 성균관대학교 전기전자 및 컴퓨터공학과 수료
1994년 3월~현재 : 강릉영동대학 부사관과 부교수
<관심분야> 정보보호, 암호학

원 동 호 (Dong ho Won) 종신회원

1976년-1988년 : 성균관대학교 전자공학과(학사, 석사, 박사)
1978년-1980년 : 한국전자통신연구원 전임연구원
1985년-1986년 : 일본 동경공업대 객원연구원
1988년-2003년 : 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년-1998년 : 국무총리실 정보화추진위원회 자문위원
2002년-2003년 : 한국정보보호학회장
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장
<관심분야> 암호이론, 정보이론, 정보보호