Secure Encryption Schemes의 구축에 따른 One-Way 함수의 연구

유 승 재*

요 약

one-way 함수는 패스워드와 같이 compute는 쉽고 invert는 어렵다는 의미를 갖는 함수로서 암호기법에서 매우 중요한 역할을 하고 있으며, 특히 encryption schemes의 존재성은 바로 one-way 함수의 존재성을 필요로 하고 있음은 잘 알려진 사실이다. 본 연구에서는 기존 암호기법에 존재하는 one-way 함수들을 분석하고 또한 one-way 함수가 될 수 있는 여러 가지 형태의 함수들을 조사·연구함으로써 다양하고 안전한 encryption schemes을 갖추기 위한 근원을 제공한다. one-way 함수의 종류, 역할과 그 특성을 살펴보고 one-way 함수의 일반적인 조건을 통하여 one-way 함수가 될 수 있는 여러 가지 함수들을 조사하고, one-way 함수와 trapdoor 함수에 대한 이론적 특성을 논하였다.

Study on One-Way Functions for the Construction of Secure Encryption Schemes

Seung-Jae Yoo*

ABSTRACT

One way Functions are similar to the passwords in the sense that are easy to compute and hard to invert. So they are the most basic primitive for cryptographic applications. Especially, it is well-known that it needs to exist of one way functions for the existence of the encryption schemes. In this note, we devote to study the various properties of the one way functions to give the base for the construction of the secure encryption schemes. They include the study for a sort and part of one way functions. Also, we deal with the theoretical relationship between one way function and trapdoor function.

* 중부대학교 정보보호학과

1. 서 론

현대 암호는 정보보호의 근간으로서 그 중요성이 매우 크며, 최근 20년 동안 많은 학자들의 관심과 연구가 진행되고 있다. one-way 함수는 패스워드와 같이 compute는 쉽고 invert는 어렵다는 의미를 갖는 함수로서 암호기법에서 매우 중요한 역할을 하고 있으며, 특히 encryption schemes의 존재성은 바로 one-way 함수의 존재성을 필요로 하고 있음은 잘 알려진 사실이다. 따라서 본 연구를 통하여 기존 암호기법에 존재하는 one-way 함수들을 분석하고 또한 one-way 함수가 될 수 있는 여러 가지 형태의 함수들을 조사·연구함으로써 다양하고 안전한 encryption schemes을 갖추기 위한 근원을 제공하는데 본 연구의 목적이 있다.

안전한 데이터 전송을 위한 암호화 작업(encryption schemes)에서 합법적인 사용자만이 메시지 해독이 가능해야 한다. 즉 안전한 encryption schemes이 존재하기 위한 필요조건은 NP가 BPP에 포함되지 않는 것(따라서 P≠NP)이다. 그러나 이것은 필요조건이지 충분조건이 아니다. P≠NP은 단지 최악의 경우 encryption schemes이 침입되는 것은 어렵다는 것을 의미한다. 실제로 침입문제는 NP-완비로 가능하기 때문에 encryption schemes의 구축은 쉬운 문제이다. 따라서 보안은 최상의 혹은 평균 이상의 견고함을 요구한다.

그러므로 안전한 encryption schemes의 존재를 위한 조건은 NP에서 견고한 language가 존재한다는 것이다. 이와 같은 문제를 이용하기 위해서는 그와 같은 단계를 빠르게 해결할 수 있는 보조의 정보와 더불어 견고한 단계를 만들 수 있어야 한다. 반면에 그 견고한 단계는 합법적인 사용자에게도 어려움을 준다. 따라서 안전한 encryption schemes의 존재는 '주어진 보조의 입력단계의 해결이 쉽다' 또한 '보조 입력이 주어지지 않는 경우는 이런 단계의 해결이 어렵다' 등과 같은 보조의 입력과 연관된 단계의 생성의 효과적인 방법의 존재를 의미하는 것이다.

이와 같은 조건을 함축하는 것이 바로 one-way 함수인데, 본 연구에서는 우선 고급수학의 이론을 통하여 one-way 함수의 종류, 역할과 그 특성을 살펴본다. 또한 one-way 함수의 일반적인 조건을 통하여 one-way 함수가 될 수 있는 여러 가지 함수들의 source를 조사하고, one-way 함수와 trapdoor 함수에 대한 이론적 특성을 살펴본다.

2. One-way 함수

암호 응용의 가장 기본적인 원시함수가 되는 one-way 함수는 PPT(propabilistic polynomial time) 알고리즘과 복잡성 이론의 암호법에서 널리 이용되는 negligible 함수의 쌍으로 정의된다. 그리고 그 특성에 따라 SOW(strong one-way) 함수와 WOW(weak one-way) 함수로 분류된다. 즉 함수 $f:\{0,1\}^* \rightarrow \{0,1\}^*$이 SOW 함수라 함은 입력 x와 출력 $f(x)$인 PPT가 존재하고, 모든 PPT 알고리즘 A에 대해서 negligible 함수 $\nu_A(x)$가 존재하여 충분히 큰 k에 대해서

$$\Pr[f(z)=y : x \leftarrow \{0,1\}^k ;\ y \leftarrow f(x);\ z \leftarrow A(1^k, y)] \le \nu_A(k)$$

가 성립함을 의미한다. 여기서 함수 ν_A가 negligible이라 함은 모든 상수 $c \ge 0$에 대해서 적당한 정수 k_c가 존재해서 $k \ge k_c$인 모든 k에 대해서 $\nu_A(k) < k^{-c}$를 만족하는 것을 의미한다.

그리고 WOW 함수라 함은 입력 x와 출력 $f(x)$인 PPT가 존재하고, 모든 PPT 알고리즘 A와 충분히 큰 k에 대해서

$$\Pr[f(z)\neq y : x \leftarrow \{0,1\}^k ; y \leftarrow f(x) ; z \leftarrow A(1^k, y)] \geq \frac{1}{Q(k)}$$

을 만족하는 다항식 Q가 존재하는 것이다.

예를 들면, 정수 x, y에 대해서 $f(x, y) = x \cdot y$로 정의된 함수는 적어도 짝수들에 대해서 역변환을 쉽게 구해질 수 있으므로 SOW 함수가 아니다. 그러나 x, y가 대략 같은 크기의 소수(prime number)일 경우라면 라 한다면 $x \cdot y$의 역변환을 구하는 것은 매우 어렵다. 실제로 이 함수는 WOW 함수가 된다.

SOW 함수와 WOW 함수의 차이점은 WOW 함수상에서는 역변환하기 어려운 입력의 어떤 non-negligible 요소를 필요로 하는 반면 SOW 함수는 negligible 요소를 가진 입력을 제외한 모든 것을 역변환하기 어렵다는 것이다.

그러나 WOW 함수의 존재와 SOW 함수의 존재와는 서로 필요충분의 관계가 있으며, 하나의 WOW 함수로부터 새로운 SOW 함수를 만들 수 있다는 특성이 있다.

실제로 함수 f가 WOW 함수라 하고 Q를 WOW 함수 정의에서 언급된 다항식이라 하자. 이 때, 함수 g를

$$g(x_1 \cdots x_N) = f(x_1) \cdots f(x_N)$$

이라 정의하면 g는 SOW 함수가 된다. 여기서 $N = 2kQ(k)$이고 각각의 x_i는 길이가 k인 정수이다.

위에서 언급한 SOW 함수와 WOW 함수의 모두 역연산 알고리즘은 PPT인데 이보다 더 강력한 버전의 비일양 one-way 함수를 알아보자.

함수 f가 비일양(non uniform) one-way(**NUOW**) 함수라 함은 다음 두 조건을 만족해야 한다.

(1) 함수 f에 대한 계산 PPT 알고리즘이 존재해야 하고

(2) 임의의 polynomial-size 알고리즘 $A = \{M_k\}_{k \in N}$에 대해서 negligible 함수 $\nu_A(x)$가 존재하여 충분히 큰 k에 대하여

$$\Pr[f(z)\neq y : x \leftarrow 0,1^k ; y \leftarrow f(x) ; z \leftarrow M_k(y)] \leq \nu_A(k)$$

을 만족하다.

두 조건에서 조건 (1)과 조건 (2)는 각각 계산의 편리성과 역변환의 어려움이라는 one-way 함수의 근본적인 요구사항을 보장한다.

다음은 함수 $f : \{0,1\}^* \rightarrow \{0,1\}^*$ 뿐만 아니라 유한차원의 정의역과 치역을 가진 다양한 형태의 one-way 함수들에 대해서 알아본다. 우선 유한차원의 정의역 D_i와 치역 R_i에 대해서 SOW 함수들의 모음은 다음의 4조건을 만족하는 합수들의 집합 $F = \{f_i : D_i \rightarrow R_i\}_{i \in I}$이다.

(1) 입력 1^k에 출력 $i \in \{0,1\}^k \cap I$인 PPT S_1이 존재한다.

(2) 입력 $i \in I$에 출력 $x \in D_i$인 PPT S_2이 존재한다.

(3) 모든 $i \in I$와 $x \in D_i$에 대해서

$$A_1(i, x) = f_i(x)$$

인 PPT A_1가 존재한다.

(4) 모든 PPT A에 대해서 적당한 negligible 함수 $\nu_A(x)$가 존재하여 충분히 큰 k에 대해서

$$\Pr[f_i(z)\neq y : i \leftarrow I ; x \leftarrow D_i ; y \leftarrow f_i(x) ; z \leftarrow A(i, y)] \leq \nu_A(k)$$

을 만족한다.

one-way 함수가 존재한다면 one-way 함수들의 모음은 따라서 존재하고 또한 그 역도 성립한다. 실제로 f를 one-way 함수라 하고, $I = \{0,1\}^*$,

$i \in I$, $D_i = R_i = \{0, 1\}^*$ 그리고 $f_i(x) = f(x)$이라 할 때, 함수들의 모음 $F = \{f_i : D_i \rightarrow R_i\}_{i \in I}$을 살펴보자. 여기서 S_1은 입력 1^k, $k \in \{0, 1\}^*$으로 택하고, S_2은 입력 i, $x \in D_i = \{0, 1\}^{|i|}$ 그리고

$$A_1(i, x) = f_i(x) = f(x)$$

로 택한다. 또한 f가 one-way라는 조건에 의해 위 조건 (4)의 만족은 자명하다. 따라서 모음 F는 One-Way 함수의 모음이 된다.

3. Trapdoor 함수와 Trapdoor 함수의 모음

이 절에서 언급할 trapdoor 함수는 특별한 특성을 갖는 one-way 함수이다. 이 함수 역시 계산은 간단하지만 역함수에 관한 정보를 갖지 않고는 역변환은 불가능한 성질을 갖는데 여기서 역함수에 관한 정보란 그것을 소유한 자가 임의로 선택한 점에서 f의 역변환을 가능하게 하는 비밀역함수를 갖는 것을 의미한다.

임의의 k에 대해서 $t_k \in \{0, 1\}^*$가 존재하여 $|t_k| \leq p(k)$을 만족하고 또한 모든 $x \in \{0, 1\}^*$, $I(f(x), t_k) = y$ 에 대해서 $f(y) = f(x)$을 만족시키는 적당한 다항식 P와 PPT 알고리즘 I가 존재하는 one-way 함수

$$f : \{0, 1\}^* \rightarrow \{0, 1\}^*$$

을 trapdoor 함수라 한다.

유한 정의역 $D_i (i \in I)$에 대하여 SOW trapdoor 함수들의 모음은 다음의 다섯 조건을 만족하는 집합 $F = \{f_i : D_i \rightarrow D_i\}_{i \in I}$이다.

(1) $i \in \{0, 1\}^k \cap I$이고 $|t_k| \leq p(k)$일 때 입력 1^k, 출력 (i, t_i)인 다항식 P와 PPT S_1이 존재한다. 정보 t_i는 i의 trapdoor로서 참조된다.

(2) 입력 $i \in I$이고 출력 $x \in D_i$인 PPT S_2가 존재한다.

(3) $i \in I$, $x \in D_i$에 대해서

$$A_1(i, x) = f_i(x)$$

인 PPT A_1이 존재한다.

(4) 모든 $x \in D_i$와 모든 $i \in I$에 대해서 $A_2(i, t_i, f_i(x)) = x$인 PPT A_2가 존재한다.

(5) 모든 PPT A에 대해서 negligible 함수 $\nu_A(x)$가 존재하여 충분히 큰 k에 대하여

$$\Pr[f_i(z) \neq y : i \leftarrow I ; x \leftarrow D_i ; y \leftarrow f_i(x) ; z \leftarrow A(i, y)] \leq \nu_A(k)$$

을 만족한다.

두 소수 p와 q에 대해서 $n = pq$라 하자. 그러면 곱셈군

$$Z_n^* = \{x : 1 \leq x \leq n, (x, n) = 1\}$$

의 원소의 개수는 $\varphi(n) = (p-1)(q-1)$이고, $e \in Z_{p-1}$과 $\varphi(n)$은 서로소이다. 이 때,

$$I = \{\langle n, e\rangle : n = pq, |p| = |q|\}$$

라하고, I의 특정한 원소인 $\langle n, e\rangle$을 인덱스로 하는 trapdoor를 $ed = 1 \bmod \varphi(n)$인 d라 하자. 그러면

$$RSA = \{RSA_{\langle n, e\rangle} : Z_n^* \rightarrow Z_n^* | \langle n, e\rangle \in I\}$$

는 trapdoor 함수들의 모음이 된다.

4. One-Way 함수와 Trapdoor 함수의 Predicates

이 절에서는 secure encryption과 프로토콜 디

자인에 매우 유용한 one-way predicate의 의미와 특성을 살펴본다.

우선 그 정의를 보면 one-way predicate는 다음 두 조건을 만족하는 boolean 함수 $B:\{0,1\}^* \rightarrow \{0,1\}$이다.

(1) 입력 $v\in\{0,1\}$과 1^k에서 $B(x)=v$이고, $|x| \leq k$를 만족하는 PPT 알고리즘이 존재한다.

(2) 모든 $c>0$과 충분히 큰 k에 대해서 주어진 $x\in\{0,1\}^k$에 대한 어떠한 PPT 알고리즘도 확률이 $\frac{1}{2}+\frac{1}{k^c}$보다 큰 $B(x)$를 계산할 수 없다.

또한 one-way predicate가 다음 조건을 만족한다면 이것을 trapdoor predicate라 한다. 즉, 주어진 k에 대해서 크기가 k에서의 trapdoor 다항식에 의해 유계이고 또한 $|x|<k$인 모든 x에 대해서 $B(x)$의 polynomial-time 계산을 가능하게 해주는 trapdoor 정보 t_k가 존재한다.

Q_n을 법 n에 대한 모든 2차 잉여류(square)의 집합이라 하고 $(J_n(x))$를 $x\in Z_n^*$에 대해서 정의된 Jacobian이라 하자. 그러면 소수 n에 대해서

$$x\in Q_n \Leftrightarrow (J_n(x))=1$$

임을 알 수 있고, 만약 n이 합성수이면

$$x\in Q_n \Rightarrow (J_n(x))=1$$

임을 알 수 있다. 또한,

$$J_n^{+1}=\{x : x\in Z_n^* \wedge ((J_n(x))=1\}$$

이라 하고, $\widetilde{Q_n}$을 법 n에 관한 의사 이차잉여류의 집합이라 하자. 그러면 n이 두 소수의 곱일 때, $|Q_n|=|\widetilde{Q_n}|$이고, 임의의 의사 이차잉여류 y에 대해서 $f_y(x)=y\cdot x$으로 정의된 함수는 Q_n에서 $\widetilde{Q_n}$으로의 일대일대응이 된다.

주어진 합성수 n과 $x\in J_n^{+1}$에 대해서, x가 법 n에 관한 2차 잉여류인지 아니면 의사 이차잉여류인지를 결정하는 것은 2차 잉여성문제로서 암호체계의 수의 기저가 되는 매우 어려운 문제이다.

이와 관련된 이차잉여류에 관한 다음 성질은 매우 의미 있는 특성이다.

소수 p, q에 대해서 $S\subset\{ns.\ t.\ n=pq\}$라 하자. 만약 $n\in S$에 대하여 $O(n, x)$가 $x\in J_n^{+1}$ 여부를 정확하게 결정할 확률이 $\frac{1}{2}+\varepsilon$ 보다 크다는 것을 만족시키는 PPT 알고리즘 O가 존재한다면, 모든 $n\in S$와 $x\in J_n^{+1}$에 대해서 $B(x, n)$이 $x\in Q_n$ 여부를 정확하게 결정할 확률이 $1-\delta$보다 크다는 것을 만족시키는 ε^{-1}, δ^{-1}와 $|n|$에서 running time polynomial을 갖는 probabilistic 알고리즘 B가 존재한다.

이 성질에 의하면 2차 잉여성을 해결하기 매우 어렵다면 이것은 이차잉여류와 비잉여류를 구별하기 어렵다는 것을 의미하는 매우 가치있는 특성이다.

참 고 문 헌

[1] M. Blum and S. Micali, "How to generate cryptographically strong sequencew of pseudo-random bits", SIAM J. Computing, Vol. 13, No.4, pp.850-863, November 1984.

[2] S. Goldwasser and M Bellare, "Lecture Notes on Cryptography. Cambridge", Mass., August 2001.

[3] S. Goldwasser and S. Micali, "Probabilistic encryption and how to play mental poker keeping secret all partial information. In Proc. 14th ACM Symp. on Theory of Computing", pp.365-377, San Francisco, 1982.

ACM.

[4] _____, "Probabilistic encryption", JCSS, Vol.28, No.2, pp.270-299, April 1984.

[5] L. Rivest, Adi Shamir and M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol.21, No.2, pp.120-126, 1978.

유 승 재

1988년 동국대학교 수학과(이학사)

1990년 동국대학교 수학과(이학석사)

1998년 동국대학교 수학과(이학박사)

1997년~현재 중부대학교 정보보호학과 부교수