通信情報保護學會誌
第8卷 第4號, 1998. 12

공개키 암호 방식의 안전성 개념에 관한 연구

A Study on the Notion of Security for Public-key Encryption Schemes

강 주 성*, 박 춘 식*

요 약

본 논문에서는 공개키 암호 방식에 대한 안전성 개념들을 종합적으로 조사하고 분석한다. 의미론적 안전성(semantic security), 구별불능 안전성(indistinguishable encryption), NM-안전성(non-malleability) 등에 대한 개념을 소개한다. 그리고 이들 개념에 공격(attack) 관점의 안전성을 결합한 정의에 대해서 고찰하며, 소개한 개념들 사이의 수학적 관계를 규명한다.

1. 서 론

암호 방식에 대한 최소한의 안전성 요구 조건은 통신로 상의 정보를 도청할 수 있는 수동적인 공격자에게는 암호문으로부터 평문을 복호화 해내는 과정이 본질적으로 어려워야 한다는 것이다. 그러나 몇몇 환경에서는 이보다 훨씬 강한 안전성이 요구될 때가 있다. 이 때 암호 방식의 안전성 개념을 잘 정립함으로써 암호 방식이 어떠한 의미로 안전성을 보장하는지 알아보는 것은 중요한 일이다.

본 논문에서는 공개키 암호 방식의 안전성 개념에 대하여 살펴본다. 이 글에서 소개하는 안전성 개념은 기존의 결정적(deterministic) 공개키 알고리즘에서는 달성하기 힘든 강한 안전성 개념들이다. 예를 들면, RSA 방식에서 고정된 공개키에 대하여 임의의 메시지 m은 항상 같은 암호문 c로 암호화 된다. 이러한 시스템에서는 같은 메시지를 두 번 이상 보내게 되면 이 사실이 쉽게 탐지될 수 있다. 또한, RSA 방식에서 0과 1은 항상 자기 자신으로 암호화 되고, 암호문과 평문의 Jacobi 심볼이 일치하게 된다. 이러한 사실은 안전성 관점에서는 취약한 부분으로 볼 수 있다.

안전성 측면에서 약점을 안고 있는 결정적 알고리즘의 대안으로서 확률적(probabilistic) 암호화 방식이 사용된다. 확률적 공개키 암호 방식에서는 같은 메시지일지라도 송신할 때마다 서로 다른 암호문으로 암호화된다. 확률적 공개키 암호 방식은 어떤 안전성 개념에 대하

* 한국전자통신연구원 부호기술연구부 부호1팀

여 증명 가능한 안전성을 확보하기 위해서 랜덤성을 이용하는 방식이다. 대표적인 확률적 공개키 암호 방식으로는 Goldwasser와 Micali[6], Blum과 Goldwasser[4], Bellare와 Rogaway[2]가 제안한 방식등이 있다.

우리는 먼저 Goldwasser와 Micali[6]가 소개한 의미론적 안전성(semantic security)과 구별불능 안전성(indistinguishable encryption)을 살펴볼 것이다. 의미론적 안전성은 Shannon이 정의한 완전 안전성(perfect secracy) 개념을 polynomially bounded시킨 버전으로 볼 수 있으며, 구별불능성 암호화 성질은 의미론적 안전성과 수학적으로 동치인 개념이다. 다음으로 Dolev, Dwork, Naor[4]에 의해서 제안된 좀 더 강한 개념의 안전성인 NM-안전성(non-malleability)에 대해서 알아본다.

한편, Bellare 등[1]은 이들 안전성 개념에 공격 관점을 첨가한 정의를 발표하였다. 일반적으로 암호학에서 공격은 암호문 단독 공격, 기지 평문 공격, 선택 평문 공격, 선택 암호문 공격 등으로 대별한다. 공개키 암호 방식에서는 모든 사용자가 공개된 정보인 공개키를 사용하여 임의의 메시지를 암호화할 수 있으므로 암호문 단독 공격이나 기지 평문 공격은 실질적인 공격이 될 수 없다. 그래서 공개키 암호 방식에서는 공격을 선택 평문 공격, 선택 암호문 공격, 능동적 선택 암호문 공격(adaptively chosen ciphertext attack)으로 분류한다. 능동적 선택 암호문 공격은 선택 암호문 공격보다 더 강력한 공격법으로서 도전 암호문을 제외한 모든 암호문에 대해서 공격자가 복호화 시킬 수 있다고 가정한다.

본 논문은 서론을 포함하여 총 5개의 절로 구성된다. 2절에서는 공개키 암호 방식을 엄밀하게 정의하고, 3절에서는 여러 가지 안전성 개념들을 소개한다. 4절에서는 안전성 개념들 사이의 관계를 규명하며, 5절은 결론부이다.

2. 공개키 암호 방식의 정의

암호 방식이란 간단히 말해서 주어진 평문을 해독 불가능한 형태로 변형하거나 암호화된 통신문을 해독 가능한 형태로 변환시키는 방법이다. 그리고 암호화에 사용되는 키와 복호화에 사용되는 키가 동일한 지의 여부에 따라서 대칭키 방식과 공개키 방식으로 구분한다. 본 절에서는 공개키 암호 방식의 안전성을 정의하기 위한 준비 과정으로 암호화 키와 복호화 키가 서로 다른 공개키 암호 방식의 기본적인 메카니즘을 수학적으로 엄밀히 분석한 정의를 소개한다.

정의 1 (공개키 암호 방식)

$\Pi=(K, E, D)$가 다음의 조건을 만족할 때 우리는 Π를 공개키 암호 방식(public-key encryption scheme)이라 부른다.

1. 키 생성 알고리즘 K는 확률적(probabilistic) 알고리즘으로 1^n을 입력으로 하여 공개키와 비밀키 쌍 (k_p, k_s)를 출력한다.
2. 암호화 알고리즘 E는 확률적 알고리즘으로 공개키 k_p와 평문 $x\in\{0, 1\}^*$를 입력으로 하여 암호문 y를 출력한다.
3. 복호화 알고리즘 D는 결정적(deterministic) 알고리즘으로 비밀키 k_s와 암호문 y를 입력으로 하여 메시지 $x\in\{0, 1\}^*$ 또는 결점있는 암호문을 나타내는 기호 "?"를 출력한다.
4. 임의의 평문 $x\in\{0, 1\}^*$에 대하여 $E(k_p, x)=y$인 모든 암호문 y는 $D(k_s, y)=x$를 만족한다.
5. K, E, D는 모두 다항식 시간 안에 계산되는 알고리즘들이다.

여기에서 1^n은 각 비트 값이 모두 1인 n-비트 벡터를 의미하고, 정수 n은 암호 방식의

안전성 파라메타로서의 역할을 한다. 그리고 $E(k_p, x)$는 공개키 k_p로 평문 x를 암호화 하는 것을, $D(k_s, y)$는 비밀키 k_s로 암호문 y를 복호화함을 각각 의미한다.

위 정의에서 키 생성 알고리즘 K는 1^n을 입력으로 해서 첫 번째 성분인 공개키 k_p와 두 번째 성분인 비밀키 k_s를 출력하는데 이를 기호로

$$K(1^n) = (K_1(1^n), K_2(1^n)) = (k_p, k_s)$$

로 표현하기로 하자.

3. 여러 가지 안전성 개념의 정의

본 절에서는 공개키 암호 방식에 대한 몇가지 안전성 개념을 살펴본다. 의미론적 안전성, 구별불능 안전성, NM-안전성의 개념을 소개하고, 이들 개념에 공격 관점의 안전성을 결합한 정의를 고찰한다.

3.1 의미론적 안전성(semantic security)

의미론적 안전성은 Goldwasser와 Micali[6]에 의해 소개된 개념으로서 공개키 암호 방식의 증명 가능한 안전성을 제공하기 위한 효시가 된 정의라고 볼 수 있다. 대략적으로 말해서 의미론적 안전성은 암호문으로부터 효율적으로 계산 가능한 것은 모두 단지 평문의 길이만 주어졌을 때에도 효율적으로 계산 가능한 것이라는 사실을 의미한다. 즉, 평문의 길이 이외에 다른 정보가 없다면 암호문은 평문을 유추해 내는 데에 아무런 역할도 하지 못한다는 개념이 의미론적으로 안전하다는 뜻이다. 의미론적으로 안전한 암호 방식을 사용하는 통신로 상에서 암호문을 도청하는 공격자는 평문에 대해서 아무런 정보도 얻지 못한다. 의미론적 안전성의 엄밀한 정의는 다음과 같다.

정의 2 (의미론적 안전성)

공개키 암호 방식 $\Pi=(K, E, D)$가 의미론적으로 안전(semantically secure)하다는 뜻은 다음을 만족하는 다항식 시간 변환 T가 존재한다는 것이다. 즉, 임의의 다항식 크기 순환족 $\{C_n\}$, $|X_n| = poly(n)$인 임의의 확률 과정 $\{X_n\}$, 임의의 polynomially-bounded 함수들 f, $h:\{0, 1\}^* \rightarrow \{0, 1\}^*$, 그리고 임의의 다항식 $p(\cdot)$와 충분히 큰 모든 n에 대하여,

$$P(C_n(K_1(1^n), E(K_1(1^n), X_n), 1^{|X_n|}, h(X_n)) = f(X_n)) < P(C'_n(K_1(1^n), 1^{|X_n|}, h(X_n)) = f(X_n)) + \frac{1}{p(n)}$$

을 만족한다. 여기에서 $C'_n = T(C_n)$이다.

위 정의에서 함수 h는 평문 X_n에 대한 부분 정보를 제공하는 것으로서 보통 궤적(*history*)이라고 부른다. 알고리즘 C_n과 C'_n은 평문 X_n에 대한 정보 $f(X_n)$을 추론해 내기 위한 도구들이다. 의미론적으로 안전한 암호 방식에서는 암호문이 이러한 추론 과정에 실질적인 도움을 주지 못한다.

3.2 구별불능 안전성(indistinguishability of encryptions)

의미론적 안전성과 함께 암호 방식의 안전성을 판별하기 위한 방법으로 Goldwasser와 Micali[6]가 제안한 개념이 구별불능성(indistinguishability)이다. 임의의 두 평문에 대한 각각의 암호문을 식별해내는 것이 계산적으로 불가능할 때 이 암호 방식은 구별불능성을 소유한다고 말한다. 구체적이고 엄밀한 정의는 다음과 같다.

정의 3 (구별불능 안전성)

임의의 다항식 크기 순환족 C_n, 다항식 $p(\cdot)$, 충분히 큰 n과 $x, y \in \{0, 1\}^{poly(n)}$ ($|x| = |y|$)

에 대하여,

$$|P(C_n(K_1(1^n), E(K_1(1^n), x)=1) - P(C_n(K_1(1^n), E(K_1(1^n), y))=1)| < \frac{1}{p(n)}$$

을 만족할 때 공개키 암호 방식 $\Pi=(K, E, D)$는 구별불능 암호화 성질을 갖는다고 말한다.

3.3 공격 관점의 안전성

기존 안전성의 개념에 공격 관점을 결합시켜서 좀 더 다양하게 안전성을 분류한 논문이 Bellare, Desai, Pointcheval, Rogaway[1]에 의해 Crypto'98에서 발표되었다. 그들은 공격자(adversary) A를 확률적 알고리즘의 순서쌍 $A=(A_1, A_2)$로 정의하였다. 기본적으로 A_1에는 공개키가 주어지고, A_1은 이를 입력으로 하여 시험 정보(test instance)를 출력한다. 다음 단계인 A_2는 A_1의 출력인 시험 정보의 확률적 함수로 생성되는 도전 암호문 y에 대하여 공격 목표에 맞는 결과를 출력한다. 공개키 암호 방식에 대한 공격은 다음 세가지로 분류할 수 있다. 첫째, 선택 평문 공격(CPA)에서 공격자는 그가 선택한 평문을 공개키로 암호화할 수 있다. 이 공격에서 공격자에게는 공개키에 접속할 권한을 부여한 것 이외의 아무런 권한도 주어지지 않는다. 둘째, 선택 암호문 공격(CCA)은 A_1 에게 복호화 오라클을 접속할 수 있도록 허락해주고, A_2 에게는 그 접속을 허락하지 않는 공격을 의미한다. 즉, 복호화 오라클은 시험 정보를 생성하는 데만 쓰이고, 도전 암호문이 나타나기 전에 제거된다. 셋째, 능동적 선택 암호문 공격(ACCA)은 가장 강력한 공격 방식으로 A_1과 A_2 모두에게 복호화 오라클 접속을 허락한다. 그러나 A_2가 도전 암호문 y를 입력으로 해서 복호화 오라클을 사용하는 행위는 금지된다.

위에서 열거한 세가지 공격 방법에 대한 견고성을 조사함으로써 공개키 암호 방식의 안전성을 점검할 수 있다. 공개키 암호 방식이 적절한 선택 암호문 공격에 대하여 안전할 때 그 암호 방식은 공격 관점에서는 가장 높은 차원의 안전성을 제공하는 것이다.

공격 관점의 안전성을 구별 불능 안전성에 결합한 정의를 살펴보도록 하자. A가 확률적 알고리즘일 때 $A(x_1, x_2, \cdots; r)$은 입력 $x_1, x_2, \cdots$와 내부 동전 r을 가지고 A를 실행한 결과라 하고, $y \leftarrow A(x_1, x_2, \cdots)$는 내부 동전 r을 선택하여 A를 실행한 결과를 y로 놓는 시행이라 하자. 그리고 S가 유한 집합일 때 $x \leftarrow S$는 S로부터 균등한 가능성으로 한 원소를 선택하는 시행을 나타낸다고 하자.

한편, 임의의 상수 $c \geq 0$에 대하여, $n \geq n_c$인 모든 n이 $f(n) \leq n^{-c}$을 만족하는 정수 n_c가 존재할 때 함수 $f : N \rightarrow R$은 negligible하다고 말한다.

정의 4 (공격 관점을 결합한 구별불능 안전성 : IND-ATK)

$\Pi=(K, E, D)$가 어떤 공개키 암호 방식이고, $A=(A_1, A_2)$를 공격자라고 하자. 임의의 ATK$\in$\{CPA, CCA, ACCA\}에 대하여,

$$\Gamma_{\Pi,A}^{\mathrm{IND-ATK}}(n) = 2P((k_p, k_s) \leftarrow K(1^n), (x_0, x_1, s) \leftarrow A_1^{O_1}(k_p), b \leftarrow \{0, 1\}, y \leftarrow E(k_p, x_b), A_2^{O_2}(x_0, x_1, s, y)=b) - 1$$

로 놓고,

ATK=CPA일 때 $O_1(\cdot)=0$, $O_2(\cdot)=0$

ATK=CCA일 때 $O_1(\cdot)=D(k_s, \cdot)$, $O_2(\cdot)=0$

ATK=ACCA일 때 $O_1(\cdot)=D(k_s, \cdot)$, $O_2(\cdot)=D(k_s, \cdot)$

이라 하자. 여기에서 A_1은 $|x_0|=|x_1|$인 x_0과 x_1을 출력하고, ACCA인 경우 A_2는 복호화 오라클에 y를 복호화 하라고 요구하지 못한다. 위와

같은 가정하에서 공개키 암호 방식 Π가 IND-ATK sense로 안전하다는 뜻은 A가 $\Gamma_{\Pi,A}^{IND-ATK}(\cdot)$이 negligible한 다항식 시간 알고리즘이라는 것이다.

위 정의에서 A_1이 출력하는 (x_0, x_1, s)중 s는 공개키 k_p를 포함한 상태 정보(state information)를 나타내고, y는 도전 암호문으로서 x_b를 암호화한 결과이다.

3.4 NM-안전성(non-malleability)

NM-안전성 개념은 Dolev, Dwork, Naor[4]에 의해서 처음 소개된 것으로 이들의 머리글자를 인용하여 DDN-안전성이라 부르기도 한다. 앞에서 소개했던 의미론적 안전성과 구별불능 안전성 개념의 정의에서와는 다르게 NM-안전성을 정의할 때는 공격자의 공격 목표가 낮아진다는 것이 큰 특징이다. 이전의 두 안전성 개념에서 공격자의 목표는 주어진 도전 암호문 y로부터 평문 x를 찾아내는 것이었다. 그러나 NM-안전성 개념 정의에 나타나는 공격자의 목표는 도전 암호문 y의 평문 x를 찾는 것이 아니고 단지 그것의 평문이 x와 알려진 방법으로 관계지워진 어떤 암호문을 얻어내는 것이다. 즉, 다른 안전성 개념에서 보다 공격 성공의 목표치가 약하기 때문에 NM-안전성에서 고려되는 공격자는 그만큼 공격을 쉽게 성공시킬 수 있는 것이다.

Dolev, Dwork, Naor[4]는 시뮬레이터라는 개념을 이용하여 NM-안전성을 정의하였다. 그리고 최근에 Bellare, Desai, Pointcheval, Rogaway[1]는 DDN-안전성 개념을 개선시키고 공격 관점의 안전성을 결합시킨 정의를 발표하였다. 여기에서는 후자인 최근의 NM-안전성 개념 정의를 소개하기로 한다. 먼저 NM-안전성을 정의하기 위해서 필요한 몇가지 기호를 약속하기로 하자. $\boldsymbol{x}=(x_1, \cdots, x_{|x|})$는 임의의 벡터를 나타내고, $|x|$는 벡터의 성분들 개수를 의미한다. $x \in \boldsymbol{x}$의 의미는 x가 벡터 $\boldsymbol{x}$의 한 성분이란 것이며, $x \leftarrow D(k, y)$는 벡터 $\boldsymbol{y}$ 각각의 성분들에 대해서 $x_i \leftarrow D(k, y_i)$인 시행들을 수행한다는 뜻이다. 그리고 집합론에서 자주 쓰이는 관계(relation)는 R로 표현하기로 한다.

정의 5 (공격 관점을 결합한 NM-안전성 : NM-ATK)

$\Pi=(K, E, D)$가 공개키 암호 방식이고, $A=(A_1, A_2)$를 공격자라고 하자. 임의의 ATK $\in$ {CPA, CCA, ACCA}와 자연수 n에 대하여

$$\Gamma_{\Pi,A}^{IND-ATK}(n) = |\Lambda_{\Pi,A}^{NM-ATK}(n) - \Lambda_{\Pi,A,\$}^{NM-ATK}(n)|$$

으로 정의하자. 여기에서

$$\Lambda_{\Pi,A}^{NM-ATK}(n) = P((k_p, k_s) \leftarrow K(1^n) : (M, s) \leftarrow A_1^{O_1}(k_p) : x \leftarrow M : y \leftarrow E(k_p, x) : (R, y) \leftarrow A_2^{O_2}(M, s, y) : x \leftarrow D(k_s, y) : y \notin \boldsymbol{y}, ? \notin \boldsymbol{x}, R(x, \boldsymbol{x}))$$

이고,

$$\Lambda_{\Pi,A,\$}^{NM-ATK}(n) = P((k_p, k_s) \leftarrow K(1^n) : (M, s) \leftarrow {}_1O_1(k_p) : x, \tilde{x} \leftarrow M : y \leftarrow E(k_p, x) : (R, y) \leftarrow A_2^{O_2}(M, s, y) : x \leftarrow D(k_s, y) : y \notin \boldsymbol{y}, ? \notin \boldsymbol{x}, R(\tilde{x}, \boldsymbol{x}))$$

이며,

ATK = CPA일 때 $O_1(\cdot) = 0$, $O_2(\cdot) = 0$

ATK = CCA일 때 $O_1(\cdot) = D(k_s, \cdot)$, $O_2(\cdot) = 0$,

ATK = ACCA일 때 $O_1(\cdot) = D(k_s, \cdot)$, $O_2(\cdot) = D(k_s, \cdot)$

이라 하자. 여기에서 메시지 공간 M은 항상 길이가 일정한 메시지를 출력하고, ACCA인 경우 A_2는 복호화 오라클에 y를 복호화 하라

고 요구하지 못한다. 위와 같은 가정하에서 공개키 암호 방식 Π가 NM-ATK sense로 안전하다는 의미는 임의의 다항식 $p(n)$에 대하여, A가 $p(n)$시간 내에 동작하고, 관계 R이 $p(n)$ 시간 내에 계산 가능할 때, $\Lambda_{\Pi, A}^{NM-ATK}(\cdot)$이 negligible하다는 것이다.

공격자 A_1은 공개키 k_p가 주어진 조건에서 메시지 공간 M과 상태 정보 s를 출력한다. A_2는 M으로부터 뽑은 메시지 x의 암호화된 값 y를 받아서 관계 R과 $y \notin \boldsymbol{y}$인 벡터 $\boldsymbol{y}$를 출력한다. 공격자는 $\boldsymbol{x} \leftarrow D(k_s, \boldsymbol{y})$일 때 $R(x, \boldsymbol{x})$가 성립하기를 희망한다. 공격자 (A_1, A_2)가 공격에 성공한다는 뜻은 이와 같은 시행을 랜덤한 $\tilde{x} \leftarrow M$에 대하여 관계 $R(\tilde{x}, x)$가 성립하는 것보다 상당히 큰 확률로 수행할 수 있다는 것이다.

위 정의 5에서 $\Lambda_{\Pi, A}^{NM-ATK}(\cdot)$은 직관적으로 공격자가 선택한 평문 x에 대하여 관계 R이 성립하여 공격이 성공할 확률을 나타내고, $\Lambda_{\Pi, A}^{NM-ATK}(\cdot)$은 랜덤한 평문 $\tilde{x}$에 대해서 원하는 관계 R이 성립함으로써 공격이 성공할 확률을 의미한다. $y \notin_y$라는 조건은 공격자에게 도전 암호문을 단순히 복사하기만 하면 되는 것과 같은 사소한 공격은 허용하지 않기 위한 것이다. 그리고 만일 $? \in \boldsymbol{x}$라면, 수신자는 간단히공격자의 메세지를 거절해서 공격이 실패하는 또다른 사소한 경우 이므로 $? \notin \boldsymbol{x}$라는 조건이 삽입되었다.

4. 안전성 개념들 사이의 관계

3절에서 우리는 공개키 암호 방식의 안전성 개념 정의들을 살펴보았다. 살펴본 안전성 개념은 크게 의미론적 안전성, 구별불능 안전성, NM-안전성이며, 여기에 공격 관점의 안전성을 첨가한 정의를 소개하였다. 본 절에서는 이 개념들 상호간의 관계를 정리하고자 한다.

먼저 Goldwasser와 Micali가 소개한 의미론적 안전성과 구별불능성 암호화 개념은 수학적으로 서로 동치임이 증명되었다[5, 6].

정리 1

공개키 암호 방식이 의미론적으로 안전(semantically secure)할 필요 충분 조건은 그것이 구별불능 안전성(indistinguishable encryption)을 갖고 있다는 것이다.

정리 1에 의해서 서로 다른 언어로 표현된 두가지 안전성 개념인 의미론적 안전성과 구별불능 안전성은 서로 수학적으로 동치이다. 그러므로 이 두가지 안전성 개념은 같은 개념으로 인식해야 한다. 어떤 학자들은 두가지를 완전히 동일한 것으로 취급하여 본 논문에서 소개한 정의를 필요에 따라서 다르게 표현하기도 한다. 현재는 표현의 용이성 때문에 구별불능 안전성을 대표로 많이 사용하는 추세이다.

한편, 공격 관점이 결합된 안전성 개념들 사이의 상호 관계는 Bellare, Desai, Pointcheval, Rogaway에 의해서 잘 규명되었다[1]. 다음에 열거하는 정리들이 이 관계들을 잘 나타내주는 사실들이다.

정리 2

임의의 ATK∈CPA, CCA, ACCA에 대하여, 공개키 암호 방식 Π 가 NM-ATK sense로 안전하다면, Π는 IND-ATK sense로도 안전하다.

정리 2는 공격의 종류에 상관없이 NM-안전성이 구별불능 안전성을 갖는다는 개념보다 강력하다는 뜻이다. 이는 공격자의 목표를 낮추어서 공격 성공을 용이하게 한 NM-안전성이 보다 더 강력할 것이라는 직관을 잘 반영해 준다.

정리 3

공개키 암호 방식 Π가 IND-ACCA sense로 안전하다면, Π는 NM-ACCA sense로도 안전하다.

정리 3은 정리 2에 의해서 일반적으로 더 약한 안전성 개념으로 알고있는 구별불능 안전성이 능동적 선택 암호문 공격(adaptively chosen ciphertext attack)이 가능한 공격자 관점에서는 NM-안전성과 동치라는 뜻이다.

정리 4

IND-CCA sense로 안전한 공개키 암호 방식 Π가 존재한다고 가정하면, IND-CCA sense로 안전하지만 NM-CPA sense로는 안전하지 않은 공개키 암호 방식 Π^*가 존재한다.

정리 4가 의미하는 바는 IND-CCA sense로 안전한 공개키 암호 방식이 존재한다는 전제하에 IND-CCA sense의 안전성은 NM-CPA sense의 안전성을 함축(imply)하지 못한다는 사실이다.

정리 5

NM-CPA sense로 안전한 공개키 암호 방식 Π가 존재한다고 가정하면, NM-CPA sense로 안전하지만 IND-CCA sense로는 안전하지 않은 공개키 암호 방식 Π^*가 존재한다.

정리 5의 내용은 일반적으로 더 강한 안전성 개념인 NM-안전성이 공격 종류에 따라서 구별불능 안전성을 소유한다는 사실을 함축하지 못할 수 있음을 보여준다. 즉, 선택 평문 공격(CPA)만이 가능한 공격자에 대하여 NM-안전성을 갖는 공개키 암호 방식은 좀 더 강한 공격 종류인 선택 암호문 공격(CCA)을 할 수 있는 공격자에게 항상 구별불능 안전성을 갖도록 보장하지는 못한다는 뜻이다.

정리 4와 정리 5를 종합해 보면 IND-CCA sense의 안전성과 NM-CPA sense의 안전성 사이에는 수학적으로 아무런 관계가 없음을 알 수 있다.

정리 6

NM-CCA sense로 안전한 공개키 암호 방식 Π가 존재한다고 가정하면, NM-CCA sense로 안전하지만 NM-ACCA sense로는 안전하지 않은 공개키 암호 방식 Π^*가 존재한다.

정리 6은 수학적으로 NM-CCA $\not\Rightarrow$ NM-ACCA라는 사실을 나타낸다. 즉, NM-안전성 개념에서는 공격 종류에서 능동적 선택 암호문 공격(adaptively chosen ciphertext attack)이 선택 암호문 공격(chosen ciphertext attack)에 비해서 항상 더 강한 공격 방법이라는 것이다.

정리 2부터 정리 6까지의 내용을 종합적으로 표현하면 그림 1과 같다. 그림에서 화살표는 수학적 함축성(implication)을 나타내고, 화살표 위의 사선은 이 함축성이 성립하지 않음을 표현한 것이다.

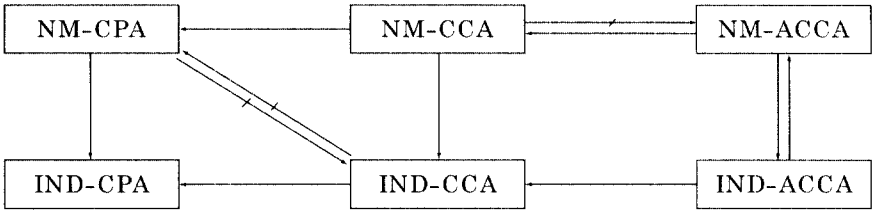

그림 1. 안전성 개념들 사이의 관계

우리는 그림 1에서 NM-CPA와 IND-CCA가 수학적으로 관계가 없다는 사실로부터 NM-CPA는 NM-CCA를, IND-CPA는 IND-CCA를 각각 함축하지 못함을 알 수 있다. 그리고 IND-CPA는 NM-CPA를, IND-CCA는 NM-CCA를 각각 함축하고 있지 못한다는 사실도 자연스럽게 얻을 수 있다.

또한, NM-CCA가 NM-ACCA를 함축하고 있지 못한다는 사실을 얻을 수 있으므로 그림 1은 안전성 개념을 사이의 관계를 완벽하게 규명한 것으로 볼 수 있다.

5. 결 론

우리는 Goldwasser와 Micali가 제안한 의미론적 안전성과 구별불능 안전성 개념, Dolev, Dwork, Naor가 정의한 NM-안전성, 그리고 이들 개념에 공격 관점을 첨가하여 Bellare 등이 소개한 개념들을 종합적으로 고찰해 보았다.

이 글에서 소개한 공개키 암호 방식의 안전성 개념 외에도 정보 이론을 배경으로 한 Yao[7, 8]의 정의와 랜덤 오라클 모델에서 성취될 수 있는 Bellare와 Rogaway[2]의 평문 인식성(plaintext awareness) 등의 개념들이 있다. 이 개념들은 본 논문에서 소개한 개념들과는 그 배경이 조금 다른 관계로 언급하지 않았다.

공개키 암호 방식의 안전성 개념에 대한 연구는 상당히 추상적이고 난해한 분야라는 이유 때문인지 국내에서는 이에 대한 연구가 활발하지 못한 것 같다. 그러나 공개키 암호 시스템에 증명 가능한 안전성을 부여하고자 할 때에는 반드시 선행되어야 할 중요한 연구 분야이다. 앞으로 국내의 독자적인 공개키 알고리즘 개발의 필요성과 함께 공개키 시스템의 안전성을 분석하는 다양한 연구가 필요하다고 생각된다.

참고문헌

[1] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among notions of security for public-key encryption schemes", Advances in Cryptology-CRYPTO '98(LNCS 1462), 1998, 26-45.

[2] M. Bellare and P. Rogaway, "Optimal asymmetric encryption", Advances in Cryptology-EUROCRYPT '94(LNCS 950), 1995, 92-111.

[3] M. Blum and S. Goldwasser, "An efficient probabilistic public-key encryption scheme which hides all partial information", Advances in Cryptology-CRYPTO '84(LNCS 196), 1985, 289-299.

[4] D. Dolev, C. Dwork, and M. Naor, " Non-malleable cryptography" , Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, 1991, 542-552.

[5] O. Goldreich, " Foundations of Cryptography(Fragments of a Book - 2nd Edition)", Weizmann Institute of Science, Rehovot, Israel, 1998.

[6] S. Goldwasser and S. Micali, "Probabilistic encryption", Journal of Computer and System Sciences, 28, 1984, 270-299.

[7] R. H. Sloan, "The notion of security for probabilistic public-key cryptosystems", MIT/LCS/ TR-379, 1986.

[8] A. C. Yao, "Theory and applications of trapdoor functions(extended abstract)", Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, 1982, 80-91.

□ 著者紹介

강 주 성

1989년 2월 고려대학교 이과대학 수학과 (학사)
1991년 2월 고려대학교 대학원 수학과 (이학석사)
1996년 2월 고려대학교 대학원 수학과 (이학박사)
1997년 12월 ~ 현재 한국전자통신연구원 선임연구원

※ 주관심 분야 :

□ 著者紹介

박 춘 식

광운대학교 전자통신과 졸업
한양대학교 대학원 전자통신과 졸업
일본 동경공업대학 전기전자공학과 졸업 (암호학전공, 공학박사)
1989년 10월 ~ 1990년 9월 일본 동경공업대학 객원 연구원
1982년 3월 ~ 현재 한국전자통신연구소 책임연구원
1997년 한국통신정보보호학회 편집이사, 종신회원

※ 주관심 분야 : 암호이론, 정보이론, 통신이론