신뢰할 수 있는 플랫폼 모듈 (TPM; Trusted Platform Module) 연구의 암호기술 분석

문상국

목원대학교 전자공학과

Analysis of Security Technology of Trusted Platform Modules

Sangook Moon

Mokwon University, Department of Electronic Engineering

E-mail : smoon@mokwon.ac.kr

요 약

보안 관련 설계 기술 개발에 대해서는 국내와 국외의 현황이 거의 차이가 나지 않는다. 현재 2048 비트 RSA 처리 모듈이 개발되고 있는 추세이긴 하지만 처리 비트폭이 넓은 이유로 연산 처리 속도가 빠르지 않아 효율적 자원을 소모하면서 고속으로 동작되는 RSA 처리부의 설계가 필요하다. RNG (Random Number Generator) 개발 측면에서는 PRNG (Pseudo Random Number Generator)에서 TRNG (True Random Number Generator)로 바뀌는 추세이며 소면적 고속의 전용 RNG가 요구된다. 칩 레벨 보안 관련해서는 국내외 제조사별로 특허권 침해를 받지 않는 보안 칩 고유의 안전장치를 개발하고 있으며, 독자적인 칩 레벨의 안전장치가 필요하다.

ABSTRACT

As for the technology developed for network security, there is little difference of design ability between the domestic and the foreign studies. Although the development of 2048 RSA processor has been undergone, the processing speed does not meet the requirement due to its long width. These days, an RSA processor architecture with higher speed comsuming less resource is necessary. As for the development of RNG (Random Number Generator), the technology trend is moving from PRNG (Pseudo Random Number Generator) to TRNG (True Random Number Generator), also requiring less area and high speed.

키워드

Trusted Platform Module, RSA, 암호, TRNG

Ⅰ. 서 론

네트워크 기술의 발달로 현대사회는 유무선 네트워크와 같은 거대한 공통매체로 정보를 공유하게 되었다. 필요에 따라 이러한 정보들은 암호화되어 보호되어야 하기에, 개인의 정보를 인증해 줄수 있는 IC카드와 같은 정보 보호 기술이 반드시 필요하게 되었다. 이러한 정보보호기술은 암호학적인 알고리즘에 의해 복잡한 연산을 거쳐 이루어진다. 데이터를 암호화하는 기술은 암호에 사용되는 많은 수학연산을 처리하기 위해 높은 컴퓨팅 파워를 요구한다. 이러한 이유로 인해 지난 수년 동안 웹사이트에서의 신용카드 구매와 같은 경우를 제외하고는 대부분의 비즈니스에서 사용되지 않았으나, 최근에는 자신들이 가지고 있는 서버에 간단하게 add-on 보드 혹은 appliance 고속암호연산 프로세서 제품들을 장착하여 암호화의 수행을 빠르게 연산 가능하도록 할 수 있게 되었다. 회사의 경영자들은 업무가 네트워크 의존적이 되어감에 따라 더 나은 보안을 요구할 것이며 동시에 많은 소비자들은 보안 허점이 많은 인터넷을 안전하게 만들도록 요구하고 있다. 이에 따라 IDC는 2005년에는 모든 인터넷 트래픽이 암호화되는 수준으로 발전할 것이라 예측하고 있다. 물론, 하드웨어의 미래는 아직도 불투명하지만, PC에 암호연산 프로세서가 기본적으로 탑재되는 날도 멀지 않을 것으로 예측하고 있다.

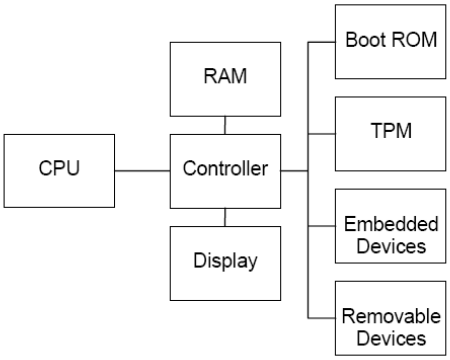

그림 1. PC 플랫폼에서 CPU 및 주변장치들과 TPM과의 구성 관계.
Fig. 1. Hierarchical organization of TPM in PC platform.

II. STPM (Secure Trusted Platform Module) 개요

STPM이란, 보다 안전한 TPM (Trusted Platform Module)의 뜻이다. TPM은 TCG (Trusted Computing Group)라는 컴퓨팅 환경의 보안 측면을 개선하고자 하는 비영리 산업 표준 단체에서 제안하는 모델로, 컴퓨터 시스템에 주변 장치의 형태로 연결된, 보안 처리를 담당하는 모듈을 말한다. TPM은 그림 1과 같이PC, PDA, 휴대전화와 같은 CPU 중심의 개인용 정보 인증을 필요로 하는 기기에 구성 요소로 작용한다. Secure TPM을 구현하는 방법은 하드웨어 혹은 소프트웨어 모두 가능하겠지만, RSA와 같은 복잡한 연산 처리부 같은 경우는 하드웨어로 구현하는 것이 바람직하다. TPM에서는 인증 및 암호 처리에 관련하여 임의 난수 발생기 (RNG; random number generator)와 암호 연산 처리부를 요구하는데, 기본적인 암호 시스템으로 RSA를 지원하며, 키의 범위는 2048 비트까지의 길이를 제안한다. TPM의 구성요소는 그림 2와 같이 I/O를 통한 시스템 버스에 유기적으로 연결되는 구조를 가질 수 있다. 범용 프로세서가 전자상거래에 필요한 암호화를 효율적으로 다룰 수 있도록 지원하지 못하는 반면, STPM 기반의 프로세서는 암호연산을 빠르게 수행하도록 특별하게 디자인되어 전자상거래 서버들이 암호연산 프로세서를 이용하지 않을 때보다 90% 가량 늘어난 처리를 할 수 있게 한다. 또한 암호 연산 프로세서는 서버의 성능을 향상시키고 처리 지연을 줄일 뿐만 아니라, 새로운 하드웨어 투자를 늘릴 수 있으면서 서버의 안전성에 도움을 준다. 즉 항상 많은 작업을 하는 서버는 불안정하기 때문에, 서버에 큰 부하가 되는 암호 기능을 분리하여 STPM이 처리함으로써 전체 시스템의 수명을 개선해 주는 경제적 이점이 있다. 또한 암호연산 프로세서는 OS나 응용프로그램 대신에 전용하드웨어가 알고리즘의 정확한 구현을 보장할 뿐만 아니라, 암호키와 중요한 데이터를 물리적으로 보호함으로써 높은 안전성을 보장한다. 따라서 STPM 기반의 보안 프로세서를 구현한다는 것은 상당히 중요한 가치를 가진다.

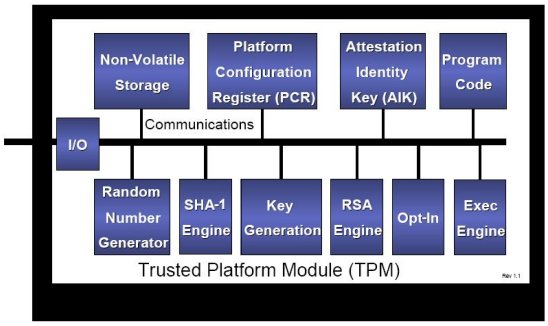

그림 2. TPM의 구성요소 구조도.
Fig. 2. TPM components diagram.

미국에서는 1996년 IP를 이용한 SoC 설계의 표준화 작업 수행을 목적으로 VSIA라는 단체를 설립하였다. VSIA는 IP quality, IP protection, IP transfer, R&D 등 4개 워킹그룹으로 구성되어 있으며, IP 품질 표준, IP 보호 표준, IP 전달물 표준, IP 설계 표준 등을 표준화 대상으로 활발히 운영되고 있다. SPIRIT은 세계 주요 EDA 개발 회사들이 주축이 되어 만든 단체로 IP core의 통합과 검증을 EDA 툴에서 용이하게 하기 위한 규격을 책정하는 것을 목적으로 2006년도에 IP 인터페이스 표준안을 발표하였다. 또한 IP 거래를 위한 유통기관으로는 프랑스의 D&R (Design & Reuse)이 있으며, 대만의 IP mall, 일본의 IPTC 등이 있어 양질의 IP들이 지적 재산권의 보호를 받으며 정당한 가치를 인정받는다 [1][2].

III. RSA 알고리즘 이슈

가. 인수분해 (factoring)와의 관계

공격자 (passive adversary)는 암호문 c로부터 그에 상응하는 평문 m을 얻어내려고 하는데 이는 A에게서 주어진 공개정보인 (n, e)를 이용한다. 이를 RSA problem (RSAP) 라 하는데 실제적으로 이런 문제에 대해 어떤 효과적인 알고리즘도 존재하지 않는다. 공격자가 RSAP를 해결하기 위해 얻을 수 있는 가능한 하나의 방법은 첫째 요소 n에 있는데 이는 A가 한 것처럼 ϕ와 d를 계산한다. d를 알아내면 복호화 할 수 있다. 한편 공격자가 만약 d를 계산한다면 factor

n도 따라 구할 수 있다. 공개키 (n, e)로부터 RSA 복호화 지수 d를 계산하는 문제와 n의 인수분해 문제는 계산적으로 동일하다. RSA 키 생성시 $n = pq$ 의 인수분해를 통해 계산적으로 소수 p, q를 얻기 불가능함은 필수적인 요소이다.

나. 작은 암호화 지수 (small encryption exponent) e

암호화 지수 e가 작은 정수이면 계산 시 효율적이긴 하나 쉽게 평문을 복구할 수 있기 때문에, 이를 막기 위해 일반적으로 일정 크기 이상 (최소 64bit)의 임의적으로 생성된 비트열을 사용한다. 또한 이 비트열 각각의 암호화 과정마다 독립적으로 이루어져야 한다. 이런 과정을 소금치기 (salting message)라고 말하기도 한다. 작은 암호화 지수는 작은 크기의 메시지 m에 대해서도 문제를 일으키는데 이는 만약 $m < n^{1/e}$ 이면 m을 단순히 c의 e^{th} 정수의 제곱근에 의해 $c = m^e \bmod n$으로부터 계산할 수 있다. 메시지 소금치기 기법은 이런 문제를 막을 수 있다.

다. 전수 탐색 공격 (forward search attack)

만약 메시지 공간이 너무 작거나 예상 가능하다면 공격자는 c가 나타날 때까지 모든 가능한 평문 메시지를 암호화 해봄으로써 암호문을 복호화 할 수 있다. 일종의 소금치기와 같은 방법을 사용함으로써 이런 공격을 막을 수 있다.

라. 작은 복호화 지수 (small decryption exponent) d

암호화 지수 e처럼 작은 복호화 지수 d도 복호화의 효율성을 높일 수 있다. 그러나 만약 $\gcd(p-1, q-1)$가 작고 d가 모듈러스 n의 4분의 1의 개수에 해당하는 비트를 갖는다면 효과적인 알고리즘에 d는 공개 정보인 (n , e) 로부터 계산할 수 있다. 그러나 d와 n의 크기가 같다면 d의 계산이 불가능하다. 그러므로 이런 공격을 피하기 위해 복호화 지수 d는 반드시 n과 같은 크기를 가져야 한다.

마. 곱셈에 대한 특성 (multiplicative properties)

m_1, m_2를 두개의 평문 메시지라 하고, c_1, c_2를 그것의 기대되는 RSA 암호화된 메시지라고 할 때 $(m_1 m_2)^e \equiv m_1^e m_2^e \equiv c_1 c_2 \pmod n$이다. 이와 같이 $m = m_1 m_2 \pmod n$ 의 상응하는 암호문이 $c_1 c_2 \pmod n$이 되는 것을 RSA 의 유사 특성 (homomorphic property)라 한다. 이런 특징은 적응 선택 암호문 공격 (adaptive chosen - ciphertext attack)을 가능하게 한다.

바. 공통 모듈러스 공격 (common modulus attack)

각각의 개체가 모듈러스 n에 대한 RSA를 가져야 하는 필요성에 대한 것이다. 때때로 중앙의 신용할 수 있는 권위자가 하나의 모듈러스 n에 대한 RSA를 가지고 네트워크 상에서 각각의 개체에게 서로 구별되는 암호화/복호화 지수를 분배하는 방법이 제안되곤 한다. 그러나 위의 인수분해와의 관계에서처럼 (ei, ni) 쌍에 대한 지식은 모듈러스 n에 대한 인수분해가 가능하고, 그것에 따라 네트워크 상에서 모든 개체들은 복호화 지수를 연속적으로 결정하게 된다. 또한 만약 하나의 네트워크 상에서 하나의 메시지가 암호화되고 둘 이상의 개체에게 보내진다면 공격자들이 공개된 정보로부터 메시지를 회복할 수 있는 기술을 가질 가능성이 높아지게 된다 [3].

IV. TRNG 테스트 기술

TRNG (True Random Number Generator)는 전기적 장치의 일종으로 컴퓨터 장치와 연동되어 순수한 난수를 발생시킨다. 이는 컴퓨터 프로그램에서 난수와 비슷하나 한계가 존재하는 결정적 (deterministic) 주기를 가지는 의사 난수를 발생시키는 PRNG (Pseudo Random Number Generator)와 상대되는 개념을 가지고 있다. TRNG의 사용 용도로는 암호화에 사용되는 키의 생성, 복권추첨, 혹은 통계적인 시뮬레이션의 응용 방면으로 사용되며, 저항 소자, 혹은 반도체 다이오드, 혹은 방사능물질로부터의 전기적인 잡음을 난수 발생의 근거로 삼는다.

이러한 TRNG를 테스트하는 방법은 PRNG나 산술연산기를 비롯한 결정적 소자에 대한 테스트와는 많이 틀려서, 새로운 개념과 방법론이 제시되어야 한다. 이를테면, TRNG가 어떤 테스트를 통과했다고 하더라도 이 TRNG가 좋은 TRNG라는 보장이 없으며, 그 TRNG가 어떤 테스트를 실패했다 하더라도 그 TRNG가 반드시 나쁜 TRNG라는 보장이 없다는 것이다 [4].

George Marsaglia는 PRNG의 테스트를 위하여 Diehard tests 라는 일련의 통계적인 테스트 방법을 제안하였는데, 이를 TRNG에 적용하기 위해서는 테스트 패턴에의 상당한 변화를 주면서 연속적인 패턴의 변화를 주면서 통계적으로 관찰하는 방법을 사용하여야 한다. 이상적인 하드웨어와 소프트웨어가 결합된 TRNG의 블록 다이어그램은

다음 그림 3과 같다. 그림 3에서 A에서 F까지의 레이블은 각 단계에서의 테스트 포인트를 지정해 놓은 것이다. D, E, F 포인트에서의 테스트는 난수성 측면에서는 특별한 의미가 없으며, 최소한 교정되지 않은 출력인 B 포인트에서의 테스트가 가장 큰 의미를 가진다. 난수 테스트 시 고려해야 할 사항들은 표 1과 같다.

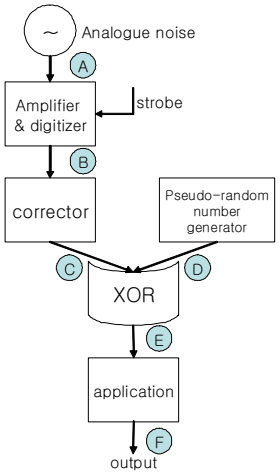

그림 3. TRNG 블록 다이어그램.
Fig. 3. TRNG block diagram.

표 1. 난수 특성 고려 이슈.
Table 1. Consideration issues in random number generation.

– Bias – Drift – Short term auto-correlation – Other short term dependencies	– 1/*f* noise – Other non-whiteness – Bad spots – Back door – Discrete frequencies

V. 결 론

본 고에서는 신뢰할 수 있는 플랫폼 모듈 기반의 암호기술에 대한 분석을 수행하였고, 각 기술에 대한 구현 시 이슈에 대하여 분석하였다. 본 조사에 의해 STPM 적용 시스템의 보안 및 신뢰성을 위한 데이터 처리 기술과 물리적인 보호기술이 학술적으로 접근되었고, 차후 개발에 필수적인 연구가 될 것이다. STPM에 적용 가능한 RSA 암호 처리부에서 키의 길이는 2048비트가 제안되며, 소면적, 고속 2048 RSA 처리부에 대한 설계 기술 확보는 매우 시급하다. 본 고에서는 이러한 RSA 설계시 이슈, 또한 TRNG에 대한 동향과 이슈에 대해 살펴보아 TPM에 적용 가능한 RSA 암호 모듈 연구에 적용이 가능하다.

참고문헌

[1] TCG Architecture Overview, http://www.trustedcomputinggroup.org
[2] TCG TPM Specification v1.2 part1, http://www.trustedcomputinggroup.org
[3] Cetin Kaya Koc, "Analyzing and Comparing Montgomery Multiplication Algorithms," *IEEE MICRO*, pp. 26~33, June 1996.
[4] Robers Davies, "Hardware random number generators," http://www.robertnz.net