Tamper Resistant Module을 이용한 암호시스템에서의 인증방식과 다중 마스터 키의 운용에 관한 연구

조 주 연, 이 필 중

포항공과대학 전자전기공학과

A Study of Authentication Scheme and Operating Method of Multi Master Keys for Cryptosystem using Tamper Resistant Module

Joo Yeon Cho, Pil Joong Lee

Dept. E. E., Pohang Institute of Science and Technology

요약 본 논문에서는 TRM을 이용한 사용자의 ID를 기초로 하는 암호시스템을 구현하고 안전성 유지를 위해 반드시 필요한 TRM과 사용자 사이의 쌍방인증방식을 설명하였다. 그리고 이의 개선된 방식으로서 키 생성키인 마스터 키를 다중화하여 TRM 내에 국소분배함으로써 TRM 내의 마스터 키를 시스템 상에서 보호하는 방안과 TRM Identity (TID)를 이용한 디지탈 서명방식을 제안하였다. 제안된 방식은 암/복호화의 속도가 빠른 관용 암호알고리듬을 사용하면서도 디지탈 서명을 비롯한 공개키 암호알고리듬이 가지고 있는 장점들을 모두 구현하고 있다.

1. 서론

정보화를 추구하는 현대사회에서는 컴퓨터 통신망의 급속한 확장과 사용자의 급증으로 원거리에서도 대량정보를 신속하고 정확하게 교환할 수 있게 되었다. 그러나 이에 따른 타인의 도청이나 정보의 불법변경 등에 대한 정보보안의 요청 또한 증가하고 있으며 암호시스템이 이에 가장 잘 부응한다는 것은 주지의 사실이다. 널리 알려진 관용 암호시스템 (conventional cryptosystem) 은 암/복호화 속도가 빠른 대신 공통의 키를 공유하는 문제와 낮은 안전도가 문제시되어 왔고 이에 반하여 공개키 암호시스템 (public key cryptosystem) 은 이런 문제를 극복한 반면 암/복호화 속도가 상대적으로 느리고 공개키 디렉토리 관리가 어려운 점이 문제점으로 지적되어 왔다.

1986년 Desmedt 와 Quisquater 가 CRYPTO '86 에서 제안한 tamperfree device (TFD) 를 이용한 암호시스템 [1] 은 암/복호화 속도가 빠른 관용 암호알고리듬 [6][7] 을 사용하면서도 공개키 암호시스템의 특성을 구현할 수 있게 함으로써 위의 두 암호시스템의 장점을 모두 살린 것으로 평가될 수 있다. 그러나 각 TFD 내에 단일 마스터 키를 사용함으로써 이 키가 노출되면 전체 암호시스템이 파괴된다는 위험을 안고 있으며 또한 이런 형태의 암호시스템에 반드시 필요한 사용자와 TFD 사이의 인증 protocol 이 제시되지 않았다는 점 등이 그 실현가능성에 있어 문제점으로 지적될 수 있겠다.

1987년 J.J. Quisquater 는 다중 마스터 키 분배를 통해 TFD 내에 개별적인 마스터 키 소유를 가능하게 하는 방식 [2] 을 제안함으로써 문제해결에 접근했으나 사용자와 TFD 간의 인증방식과 송신자의 디지탈 서명방식은 여전히 미해결의 과제로 남아 있었다.

본 논문에서는 실제적으로 구현이 가능하다고 생각되는 tamper resistant module (TRM) 을 이용하여 앞에서 제기한 문제들의 해결방안을 제시하고자 한다. TRM 내에 단일 마스터 키를 사용할 경우에 사용자와 TRM 간의 상호 신분인증 문제는 이미 [3] 에서 연구가 있었으며 본 연구는 이를 더욱 개선시킨 것이다. 먼저 기존의 TRM 을 이용한 암호시스템에 대하여 살펴보고 이의 변형인 사용자의 ID 를 기초로 하는 암호시스템의 구현에 관하여 설명한다. 그리고

TRM 내에 단일한 마스터 키를 사용했을 경우에 필요한 사용자와 TRM 간의 쌍방인증 protocol 에 관하여 [3] 에서 제안된 방식을 설명한다. 또한 다중 마스터 키를 TRM 내에 국소분배하는 Quisquater 의 개념에 기초하여 TRM 내에 다중 마스터 키를 사용했을 경우에 앞에서 제기한 문제들의 해결방안을 제시한다. 즉 어느 하나의 TRM 의 마스터 키가 불법적으로 노출되어도 전체 암호통신망은 유지될 수 있으며 노출된 TRM 의 마스터 키의 교체만으로 전체 통신망은 완전히 원래대로 회복가능하다. 또한 사용자와 TRM 간의 쌍방인증 protocol 을 제시함으로써 불법적인 사용자 사칭이나 가장 (forgery) 을 방지하도록 하였으며 송신하고자 하는 목적지의 TRM의 ID 를 알면 송신자의 디지탈 서명이 가능하도록 설계하였다. 그리고 제안된 방식의 응용으로서 하나의 TRM 을 이용하는 그룹 모두에게 한번의 암호화로 비밀전송이 가능하게 하는 방안을 제안하였다.

2. TRM 을 이용한 ID 를 기초로 하는 암호시스템

2.1 기존의 방식

1986년 Desmedt 와 Quisquater 는 관용 암호알고리듬과 TRM 을 이용하여 아래 그림과 같은 새로운 형태의 공개키 암호시스템을 제안하였다.

이 방식은 관용 암호알고리듬을 이용하면서도 공개키 암호시스템의 장점을 모두 살릴 수 있는 간단하면서도 응용이 광범위한 암호시스템이라 할 수 있다. 사용자는 다음과 같은 방법으로 비밀통신을 수행할 수 있다.

(1) 사용자 A 는 자신의 비밀키 SK_A 를 선택한다.

(2) 사용자 A 는 SK_A 를 센타에 제출하고 센타는 키 생성키인 마스터 키 K_M 을 이용하여 A 의 공개키인 PK_A ($= E''_{K_M}(SK_A)$) 를 계산하여 일반에게 공개한다.

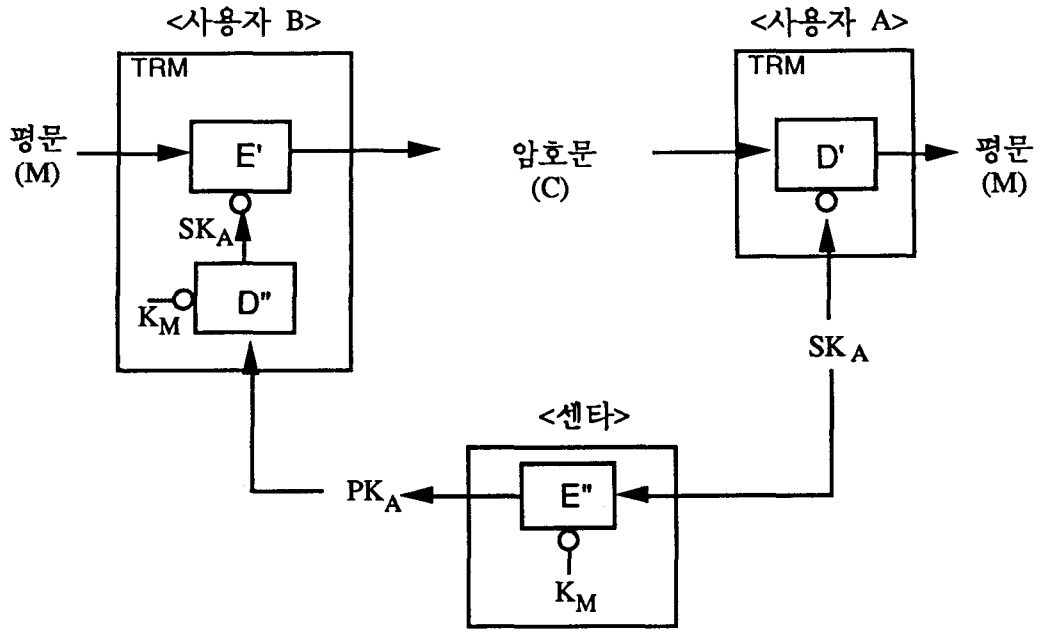


그림 1. TRM을 이용한 공개키 암호시스템

(3) 사용자 B는 사용자 A에게 암호통신을 하고자 할 때 PK_A를 암호키로 이용하여 평문을 암호화한다. A는 전달된 암호문 C를 자신의 비밀키인 SK_A를 이용하여 메시지 $M (= E_{SK_A}(C))$을 복원한다.

위의 방식에서 특이한 점은 TRM 안에서 마스터 키 K_M을 이용하여 사용자 A의 공개키인 PK_A가 A의 비밀키인 SK_A로 계산되어 암호키로 이용된다는 점이다. 그러나 SK_A는 TRM 안에서만 이용되어 외부에 노출되지 않고 다른 사람들은 SK_A를 알 수 없으므로 암호시스템의 안전이 유지된다. 따라서 TRM의 물리적 안전성은 위의 암호시스템의 가장 기본이 되는 것이다.

또한 공개키 디렉토리 관리 문제를 해결하기 위해 그림 2와 같은 ID를 기초로 하는 암호시스템으로 변환하여 구성할 수 있다. TRM을 이용하는 암호시스템은 TRM 제작 및 키관리를 관장할 신뢰할 수 있는 센타를 필요로 하므로 사용자가 간편하게 쓸 수 있고 공개키 인증문제를 해결한 ID를 기초로 하는 암호시스템이 TRM을 이용하는 암호시스템에 보다 적합하리라고 본다.

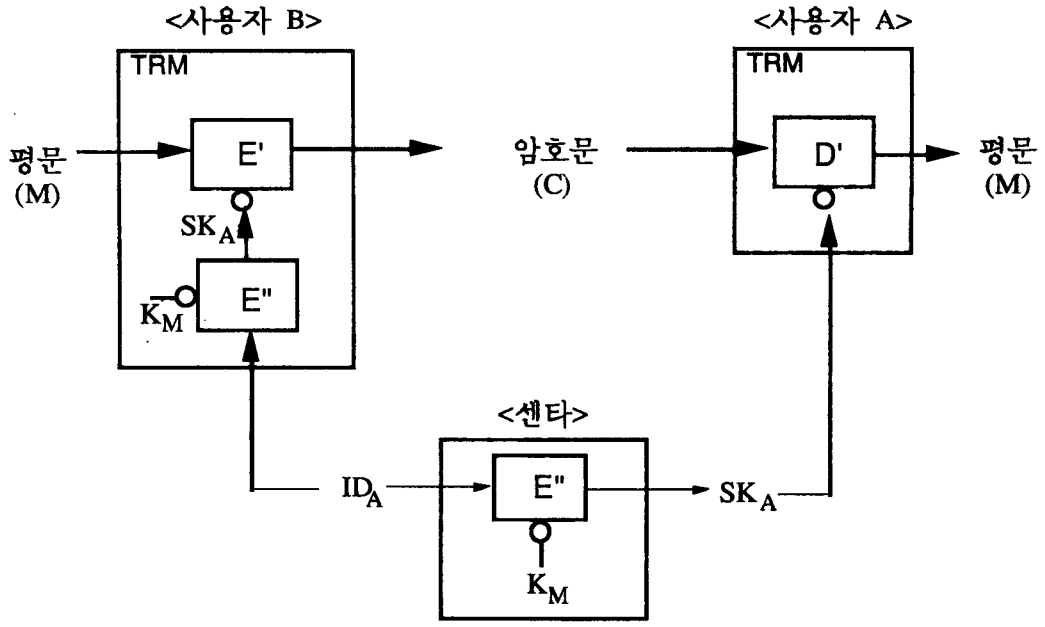


그림 2. TRM을 이용한 ID를 기초로 하는 암호시스템

2.2 인증방식

TRM을 이용하는 암호시스템에서 반드시 필요로 하는 것이 바로 TRM 접근 제어로서 사용자와 TRM 간에 상호 신분인증이 이루어져야 한다[3]. 이를 위해 다음과 같은 protocol이 필요하다.

가. 등록

사용자는 암호통신을 이용하기 전에 신뢰할 수 있는 키분배 센타에 등록을 해야하며 다음과 같은 절차를 거친다.

(1) 사용자 A는 센타에 자신의 ID인 ID_A와 자신이 선택한 비밀번호 SN_A를 제출한다.

(2) 센타는 카드의 유효기간 T_A를 정하고 $E_{K_M}(SN_A, T_A)$를 계산하여 ID_A와

함께 사용자 A의 메모리 카드 C_A에 저장하여 사용자 A에게 전달한다. 그리고 PIN_A를 안전한 채널을 이용하여 사용자 A에게 전달한다. PIN_A는 $g(SK_A)$이며 SK_A는 사용자 A의 비밀키로서 $E_{K_M}(ID_A)$이다. g는 길이가 4~6정도 길이의 알파뉴메릭(alpha-numeric) 문자를 출력하는 간단한 일방함수를 이용한다.

이 때 SN_A는 사용자가 TRM의 적법성 여부을 확인하기 위해 기억하고 있는 비밀번호이며 PIN_A는 사용자 자신의 적법성을 TRM에게 증명하기 위해 사용되는 개인번호이다.

나. TRM 접근제어

사용자는 자신이 소유한 카드 속의 개인정보와 기억하고 있는 비밀번호를 이용하여 다음과 같은 과정을 거쳐 상호신분인증을 수행한다.

(1) 사용자 A는 자신의 메모리 카드 C_A를 TRM에 입력한다.

(2) TRM은 C_A로부터 ID_A를 읽고 $E_{K_M}(SN_A, T_A)$을 복호하여 SN_A, T_A를 알아낸 후 T_A로부터 유효기간을 검사한다. 카드가 유효기간 내의 것임이 확인되면 TRM은 ID_A를 이용하여 A의 비밀키 $SK_A (= E_{K_M}(ID_A))$를 계산하고 A의 $PIN_A (= g(SK_A))$를 구한다. 그리고 SN_A를 터미널에 출력한다.

(3) 사용자 A는 화면에 나타난 SN값이 자신이 기억하고 있는 SN_A와 같은지를 확인하고 같으면 TRM이 마스타 키 K_M을 가졌음을 믿는다. 그리고 자신의 패스워드인 PIN_A를 컴퓨터의 키보드를 통하여 TRM에 입력한다.

(4) TRM은 입력된 PIN이 (2)에서 계산된 PIN_A와 같은지를 검사하고 같으면 사용자 A의 신원을 확인한다.

2.3 다중마스터 키를 이용한 방식

앞 절에서 제안된 방식은 각 TRM 내에 단일 마스터 키를 사용함으로써 이 키가 노출되면 전체 암호시스템이 파괴된다는 위험을 여전히 안고 있다. 이를 해결하기 위해 이 절에서는 각 TRM 이 가지고 있는 마스터 키를 다중화하고 이를 몇 개의 그룹으로 나누어 각 TRM 에 분배하는 방식을 제안한다. 제안된 방식은 사용자의 ID 를 기초로 한 암호시스템으로서 일정한 수의 마스터 키를 소유한 신뢰할 수 있는 키분배센타가 존재하며 각 사용자는 자신의 개인정보가 저장된 메모리 카드를 소유한다고 가정한다.

가. 등록

키분배 센타는 키 생성키인 마스터 키를 n 개 소유한다고 가정한다. 변수 n 은 제안된 암호시스템의 응용분야에 따라 달라지는 안전변수이다.

(1) 사용자 A 는 자신의 고유한 비밀번호 SN_A 를 정하고 이를 자신의 ID_A와 함께 키분배센타에 제출한다.

(2) 센타는 n 개의 마스터 키 $K_M = (K_{M_1}, \cdots, K_{M_n})$ 으로 ID_A 를 암호화하여 이를 사용자 A 의 비밀키 $\mathbf{SK}_A = (SK_{A_1}, \cdots, SK_{A_n})$ 로 정하고 제출된 비밀번호 SN_A 로 암호화하여 사용자 A 에게 분배한다($\mathbf{ESK}_A = E_{SN_A}(\mathbf{SK}_A)$). 또한 사용자 A 의 비밀번호 SN_A 와 카드의 유효기간인 T_A 를 마스터 키로 암호화한 값 $\mathbf{ESN}_A = E_{\mathbf{K}_M}(SN_A, T_A)$ 도 함께 그림 3 과 같이 사용자 A 에게 분배한다.

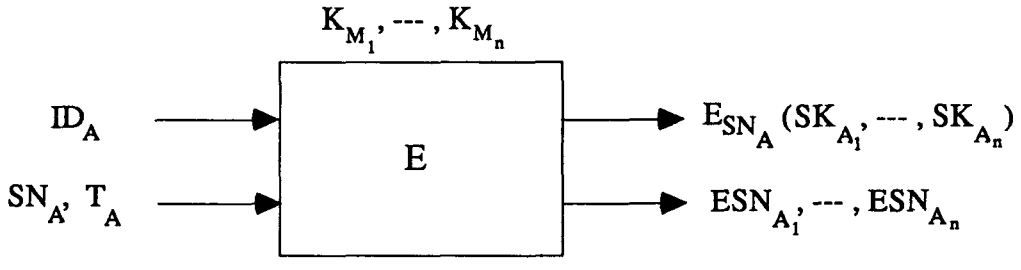


그림 3. 다중키 생성과 분배

(3) 센타는 간단한 트랩도어 일방함수 g(.)를 이용하여 $g(SN_A \oplus ID_A)$를 계산하고 이를 사용자 A의 개인 번호 PIN_A로 부여한다.

(4) 센타는 자신이 보유한 마스터 키 중에서 일부(예: 3개)를 랜덤하게 선택하여 간단한 변형함수 f(.)와 함께 각 TRM에 부여한다. 또한 부여된 각 마스터 키의 지표(index)들을 하나의 숫자로 합쳐 함수 f(.)에 대입하여 얻은 값을 TRM의 Identity(TID)로 공개한다. 이 때 함수 f(.)는 공개된 TID가 TRM이 소유한 미스터 키의 지표들을 직접적으로 가리키는 것을 방지하기 위하여 사용되는 함수이며 안전한 관용 암호알고리듬을 이용하여야 한다.

(5) 결과적으로 각 사용자와 TRM이 가진 정보는 다음과 같다.

$$\text{Card A} = \{ID_A,\ \mathbf{ESN_A} = (ESN_{A_1}, \cdots, ESN_{A_n}),\ \mathbf{ESK_A} = (ESK_{A_1}, \cdots, ESK_{A_n})\}$$

$$TRM_a = \{TID_a,\ K_{M_{a_1}},\ K_{M_{a_2}},\ K_{M_{a_3}},\ g(.),\ f(.)\} \quad \text{단 } TID_a = f(a_1 || a_2 || a_3)$$

나. TRM 접근제어 protocol

사용자 A가 TRM을 이용한 암호통신시스템을 통하여 메세지 전달을 원할 경우 사용자와 TRM 모두 제안된 시스템에 적법한가를 서로간에 인증받을 필요가 있다[4]. 이를 위하여 앞 장에서 제안된 인증방식을 응용하여 다음과 같은 사용자와 TRM 간의 쌍방인증 protocol을 제안한다.

(1) 사용자 A는 자신의 메모리 카드를 TRM에 입력한다.

(2) TRM은 자신이 가진 마스터 키 중의 하나로 카드로부터 받은 $\mathbf{ESN_A}$를 n개 모두 복호한다. 이 때 만약 등록 초기에 SN_A를 48비트, T_A를 8비트 정도로 정하였다면 복호된 SN_A와 T_A를 그 비트 크기만큼 각각 분리하여 저장해두고 SN_A에 해당하는 부분만을 작은 수부터 번호를 매겨 순서대로 출력한다. 이 때 응용되는 시스템에 따라 n의 크기가 커질경우 모든 SN_A 후보들을 출력하는 것은 번거로울 수 있다. 그러므로 등록 시에 미리 비밀번호의 입력

문자를 상용하는 문자들로 제한해두고 인증 시에 SN_A 후보들 중에서 그 범위 내에 속한 것들만 사용자에게 출력하게 한다. 이 방법으로 거의 대부분의 SN_A 후보들을 걸러낼 수 있다.

(3) 사용자 A는 출력된 값들 중에 자신의 비밀번호를 확인할 수 있으면 마스터 키를 가진 적법한 TRM이라고 믿고 자신의 비밀번호에 해당하는 순서번호를 입력한 다음 자신의 개인번호인 PIN_A을 입력한다.

(4) TRM은 선택된 비밀번호로부터 이에 해당하는 유효기간 T_A를 찾아 사용자의 카드가 적법한 유효기간 중인가을 확인한다. 그런 다음 사용자의 카드 내의 ID_A와 확인된 비밀번호 SN_A를 이용하여 PIN_A을 계산한 후 사용자 A가 입력한 값과 비교하여 같으면 카드의 소유자가 적법한 사용자 A임을 확인한다.

다. 메세지 송수신 시스템

사용자 A는 TRM 접근제어를 거친 후 그림 4와 같은 시스템을 통하여 사용자 B에게 원하는 메세지를 안전하게 전달할 수 있다. 메세지는 관용 암호시스템을 통하여 암/복호화되며 각 사용자의 비밀키는 사용자의 ID를 TRM 내의 마스터 키로 암호화하여 생성된다. 또한 각 TRM은 3개의 마스터 키를 가지고 있다고 가정한다.

(1) 송신자 A가 수신자 B의 ID_B를 TRM에 입력하면 송신 TRM은 자신이 가진 마스터 키 a_1, a_2, a_3를 이용하여 수신자의 비밀키의 일부 (SK_{a_1}, SK_{a_2}, SK_{a_3})를 생성하고 이를 통하여 메세지를 암호화한다.

(2) 송신 TRM은 암호화에 사용된 비밀키의 지표를 간접적으로 나타내는 TID_{TX}를 암호화된 메세지와 함께 수신자 B에게 전송한다.

(3) 수신 TRM은 우선 수신자 B와 상호인증과정을 통하여 적법성을 인증한다. 그런 다음 전송되어 온 TID_{TX}를 역변형함수 $f^{-1}(.)$에 대입하여 송신 TRM의 마스터 키의 지표를 알아내고 수신자 B의 개인정보가 담긴

메모리 카드로부터 그 지표에 해당되는 수신자 B 의 비밀키를 추출한다. 그리고 이를 이용하여 전달된 메세지를 복원한다.

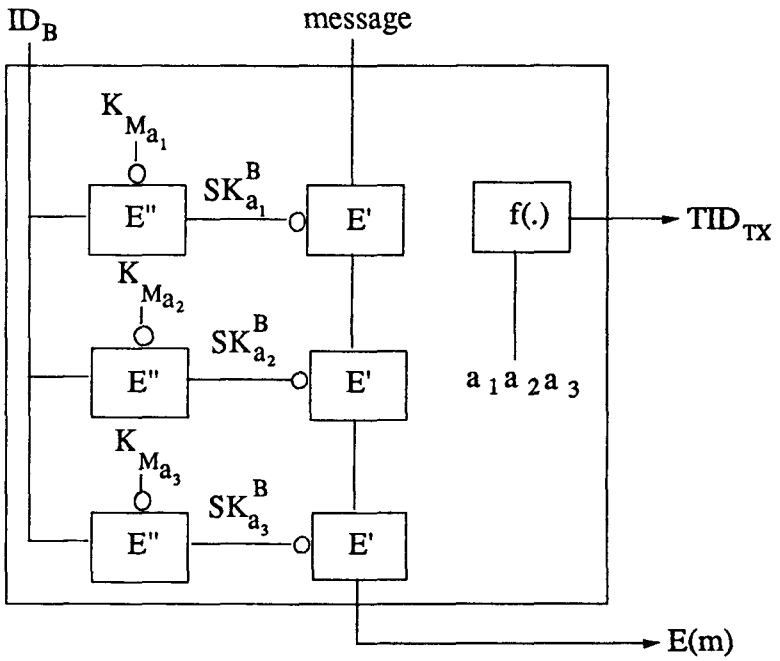
라. 디지탈 서명

제안된 방식에서 송신자는 수신 TRM 의 Identity 인 TID_{RX} 를 이용하여 다음과 같이 디지탈 서명을 할 수 있다. 우선 TRM 을 이용한 통신보안시스템 구현을 위하여 센타는 모든 TRM 의 마스터 키의 지표를 간단한 변형함수를 거쳐 TRM Identity 인 TID 로 공개하며 각 사용자는 메세지 송수신을 위한 주소에 자신의 메일박스에 부착된 TRM 의 공개된 TID 를 첨부시킨다. 송신자가 전송할 메세지에 디지탈 서명을 하고자 할 경우 우선 수신자의 메일박스에 부착된 TRM 의 TID_{RX} 를 TRM 에 입력하여 TRM 내에서 수신 TRM 의 마스터 키지표를 계산하게 하고 그 지표에 해당하는 자신의 비밀키로 메세지에 디지탈 서명을 할 수 있다. 수신자는 자신의 메일박스에 부착된 TRM 내의 마스터 키로 디지탈 서명에 사용된 송신자의 비밀키를 생성할 수 있으므로 송신자의 서명을 확인할 수 있다. 그림 5 는 송신자 A 가 수신자 B 에게 보내는 메세지에 디지탈 서명을 하는 예이다. 여기에서 m 은 메세지 또는 메세지를 해쉬한 값을 나타내며 분쟁 시에 제 3자에게 공증할 수 있게 하기 위하여 디지탈 서명된 값 D(m) 을 m 과 함께 인증자에게 전달한다.

마. 원거리 수신

제안된 방식에서는 송신자는 임의의 곳에서 메세지를 암호화하여 송신할 수 있으나 수신자는 자신의 메일박스를 관리하는 TRM 에서만 송신된 메세지를 복호할 수 있다. 그러나 만약 수신자가 원거리에서도 자신에게 송신된 메세지를 보기를 원한다면 다음과 같은 과정을 거친다.

♦ Transmitter



$a_1 a_2 a_3$: Concatenated index of master keys

♦ Receiver

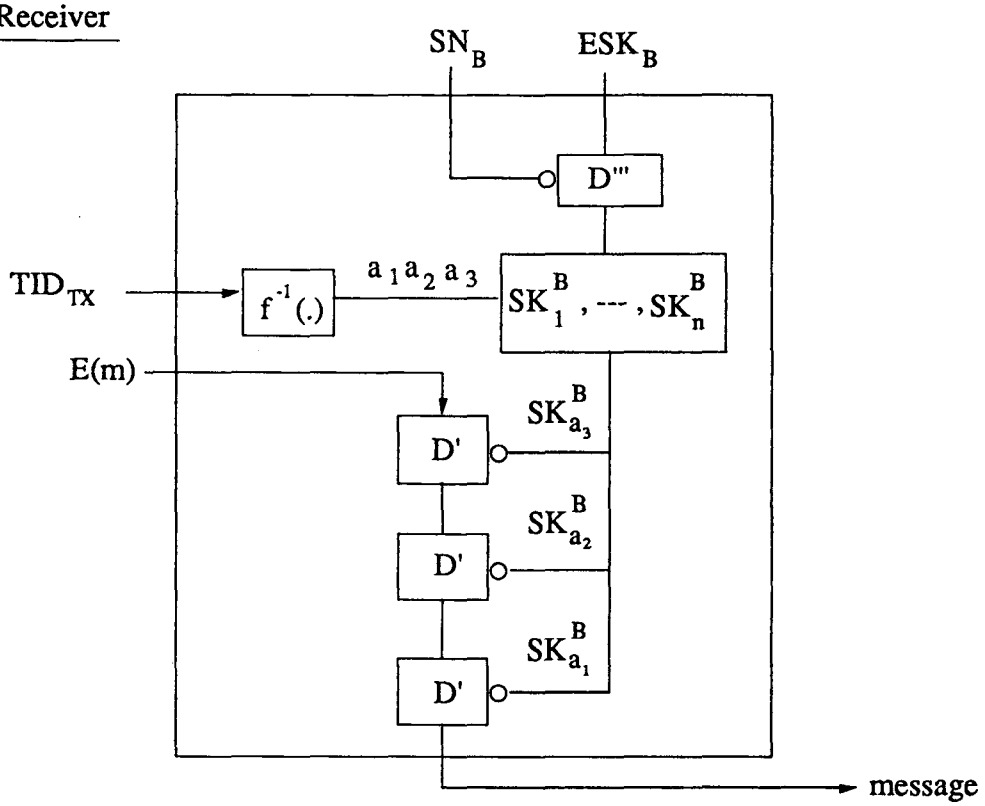
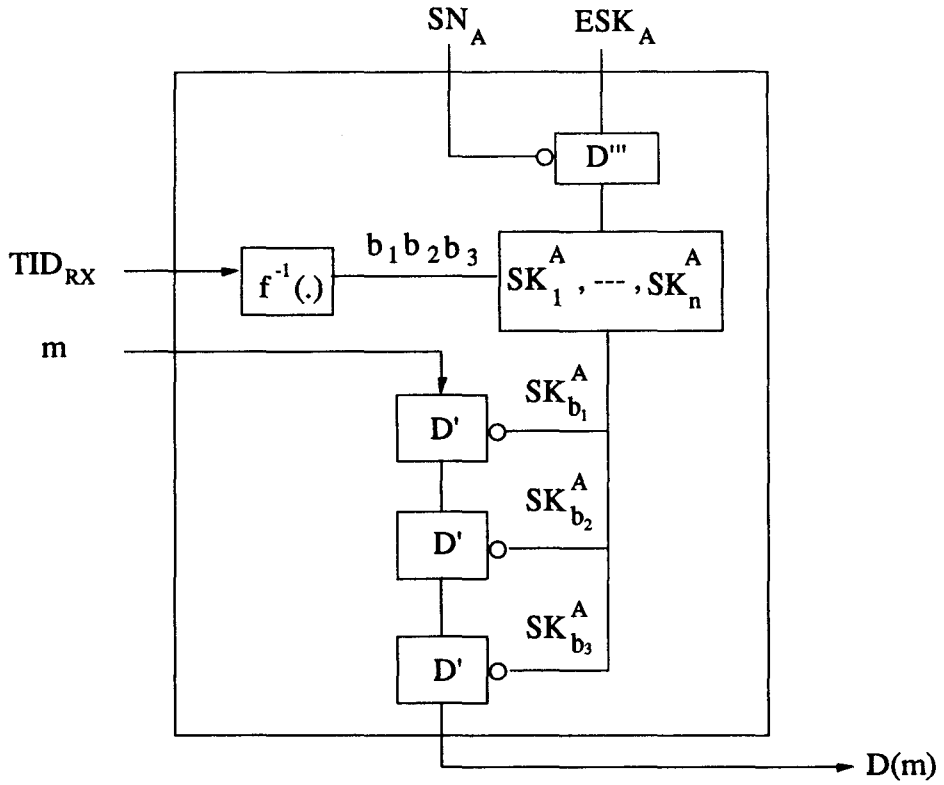


그림 4. 다중키를 이용한 메세지 송수신 시스템

♦ Signer



♦ Verifier

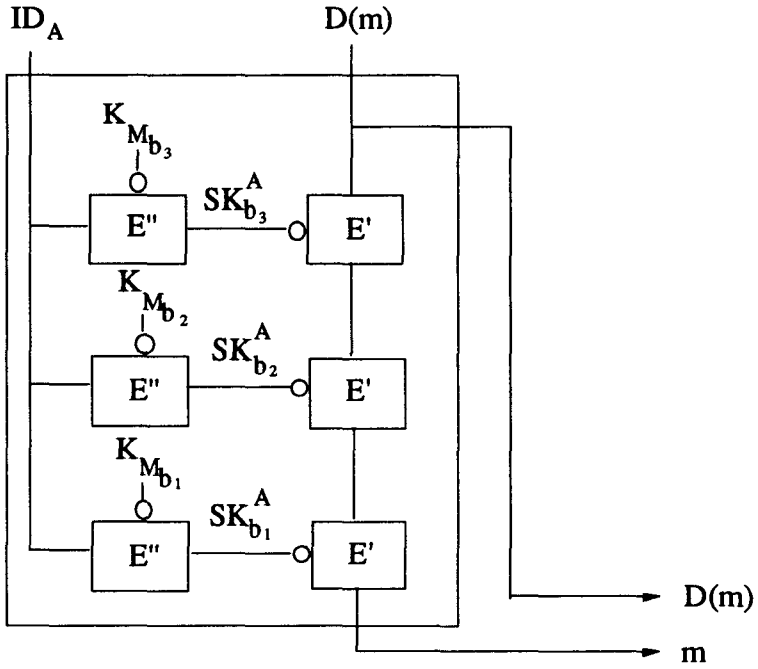


그림 5. 다중키를 이용한 디지탈 서명방식

(1) 수신자 B는 현재의 위치에서 가까운 TRM_A에 가서 적법한 인증절차를 거친다.

(2) 수신자 B는 원거리 수신모드를 선택하고 자신의 메일박스를 관리하는 TRM_B의 TID_B와 수신을 원하는 메세지 이름을 입력한다. TRM_A는 TID_B를 통하여 TRM_B가 가진 마스터 키의 지표를 알아내고 수신자 B의 개인 카드로부터 이에 해당하는 비밀키를 추출한다.

(3) TRM_A는 송신된 메세지와 송신 TRM의 TID가 담긴 정보를 수신자가 위치한 TRM_A로 재송신하기를 요구하는 메세지를 다음과 같은 형식으로 TRM_B에게 발송한다.

$$\{RT, E_{SK_B}(TID_B), ID_B, TID_A, \text{name of message}\}$$

RT : 재전송 요구신호

$E_{SK_B}(TID_B)$: TRM_B의 TID_B를 수신자 B의 비밀키로 암호화한 값

ID_B : 수신자의 ID

TID_A : 수신자가 위치한 TRM의 TID

이 때 수신자의 비밀키로 암호화하는 이유는 수신자 B가 자신의 적법성을 자신의 메일박스를 관리하는 TRM_B에게 인증하기 위함이다.

(4) TRM_B는 수신자 ID_B를 자신이 가진 마스터 키로 암호화하여 수신자 B의 비밀키를 생성한다. 그리고 이를 이용하여 $E_{SK_B}(TID_B)$를 복호하여 복원된 TID_B가 맞는지 확인함으로써 수신자 B의 적법성을 인증한다. 그런 다음 TID_A를 수신 TID로 하여 송신된 메세지와 송신 TRM의 TID가 담긴 정보를 수신자가 위치한 TRM_A로 전송한다.

(5) TRM_A는 송신 TRM의 TID를 이용하여 메세지를 암호화한 비밀키의 지표를 알아내고 수신자의 개인카드로부터 그 지표에 해당하는 비밀키를 추출하여 메세지를 복원한다.

이와 같은 방법으로 수신자는 자신의 비밀키가 저장된 메모리 카드를 가지고 있으면 어디서든지 수신이 가능하게 된다. 그러나 디지탈 서명인증은 원거리 TRM

에서 확인할 수 없으므로 자신의 메일박스를 관리하는 TRM 에서 확인한 후 그 결과를 비밀전송해 주어야 한다.

바. 그룹별 전송

만약 송신자가 같은 메세지를 동시에 여러사람에게 보내고자 할 때 매번 각 수신자의 비밀키로 메세지를 암호화하여 전송하는 것보다는 한번의 암호화로 원하는 수신자들에게 모두 전달할 수 있다면 송신자는 전송비용과 시간을 훨씬 절약할 수 있을 것이다. 제안된 보안시스템에서는 하나의 TRM 이 다수의 사용자들이 이용하는 호스트 컴퓨터에 설치되어 있다고 가정하므로 하나의 TRM 이 관리하는 모든 사용자들을 하나의 그룹이라고 할 수 있다. 이 때 송신자가 어떤 그룹 A의 모든 사용자들에게 같은 메세지를 발송하고 싶다면 한 명의 사용자에게 메세지를 발송하는 경우와 마찬가지의 과정을 거쳐 그룹키 GK_A 를 생성할 수 있다. 즉 센타는 그림 6 과 같이 TRM 의 ID 인 TID 를 이용하여 각 TRM 이 관리하는 그룹의 비밀키 GK_A 를 생성하고 이를 각 TRM 에게 그룹키로 분배한다. 각 TRM 은 자신이 가진 마스터 키의 지표에 해당하는 그룹키를 소유한다.

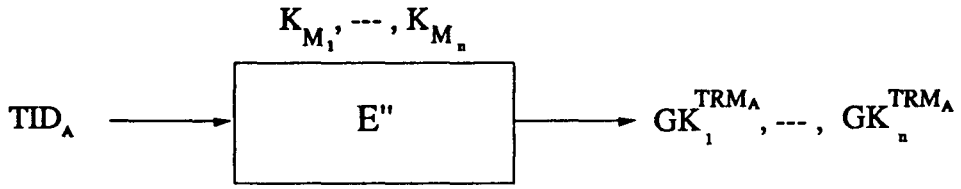


그림 6. 그룹별 전송을 위한 키생성 및 분배

만약 어떤 사용자가 TRM_A 를 사용하는 그룹 A 모두에게 동시에 같은 메세지를 송신하고자 한다면 우선 그룹송신 모드를 선택하고 수신 TRM_A 의 TID_A 를 입력하여 이에 해당하는 그룹키 $GK_A = (GK_{a_1}, GK_{a_2}, GK_{a_3})$ 를 생성시키고 송신 TRM 은 이를 이용하여 보내고자 하는 메세지를 암호화하여 전송한다. 수신은 앞에서

설명한 절차를 똑같이 거치면 된다. 이와 같은 방법을 이용하면 한 번의 암호화로 TRM_{RX}가 관리하는 모든 사용자에게 비밀전송이 가능하다.

3. 안전성 분석

제안된 방식은 물리적 안전성에 바탕을 둔 TRM이라는 암호장비와 사용자의 메모리 카드를 이용하여 구현된 ID를 기초로 하는 암호시스템이다. 사용자의 카드는 메모리와 I/O 포트만으로 구성되어 저장된 정보를 보호할 능력이 없으나 사용자가 기억하는 비밀고유번호와 결합하여 적법한 사용자에게 충분한 안전성을 보장한다. 그리고 사용자가 자신을 인증하기 위해 사용하는 개인번호인 PIN은 불법한 자의 사칭을 막기 위하여 사용자의 기억력이 허락하는 한 충분히 길 필요가 있으며 4~6 정도의 알파뉴메릭 문자가 적당하리라고 본다. 또한 사용자가 일정한 수(예: 3번) 내에 PIN 을 정확히 입력하지 못하면 카드를 파괴하는 것도 사칭을 막는 한 방법일 수 있다. 사용자의 TRM 인증의 경우에도 TRM이 터미날에 비밀번호인 SN를 다른 여러 수들과 같이 출력하므로 주위의 노출의 위험은 없으나 불법 TRM을 설치하여 사용자의 SN을 알아내는 의도는 항상 가능하므로 이에 대비하여 SN을 PIN과 비슷한 충분한 길이로 보호하는 것이 바람직하다.

또한 제안된 방식은 TRM의 물리적 안전성에 기반을 두고 있으나 어느 하나의 TRM이 공격자의 어떤 공개적인 물리적, 화학적 훼손으로 마스터 키가 노출될 가능성을 배제할 수는 없다. 다중 마스터 키를 이용하는 방식에서는 일단 노출된 TRM의 마스터 키를 이용하면 모든 사용자로 사칭이 가능하므로 키분배센타는 노출되거나 분실된 TRM이 가졌던 마스터 키의 TID를 광고하여 각 TRM이 메시지를 수신할 때에 마스터 키의 지표를 조사하여 노출된 TRM이 가진 마스터 키이면 수신거부할 수 있게 해야 한다. 제안된 시스템에서는 어느 하나의 TRM이 마스터 키를 노출하더라도 전체 암호통신망은 그대로 유지되며 노출된 TRM을 센타에서 회수하여 마스터 키만을 교체함으로써 원래의 시스템은 완전히 복구가능하다. 교체되는 마스터 키는 기존의 센타가 보유한 n개의 마스터 키

중에서 다시 랜덤하게 선택하되 노출된 마스터 키와 중복되지 않도록 선택하여 TRM에 분배함으로써 추가되는 정보없이 기존의 시스템은 그대로 유지될 수 있다. 그러나 기존의 시스템이 영구적일 수는 없으며 제안된 시스템도 일정기간(예: 1년)마다 시스템을 새로 초기화하는 것이 바람직하다고 하겠다. 그리고 여기에서 고려하지 않은 위협은 공격자가 TRM을 흔적없이 비밀리에 분석하여 불법적으로 마스터 키를 알아낸 다음 적법한 사용자로 가장하는 것인데 이는 제안된 시스템이 이미 TRM이라는 암호장비를 가정하였고 또 실제로 직접적인 훼손없이 정보노출이 불가능하게 물리적 안전성을 부여하는 것이 가능하므로 위의 위협은 여기에서는 고려하지 않는다.

한편 키분배센타가 n개의 마스터 키를 가지고 각 TRM에게 그 중 일부의 마스터 키를 분배하도록 암호시스템을 설계한다고 가정할 때, 각 TRM이 가지는 마스터 키의 수와 시스템의 안전도와는 어느 정도의 trade-off가 있다. 만약 각 TRM에 마스터 키를 하나씩 분배한다고 하면 전체 시스템의 파괴를 위해서는 모든 TRM을 분석해야만 하지만 대신 마스터 키를 분배할 수 있는 TRM의 수는 n개로 제한된다. 그러나 만약 n개의 마스터 키 중에서 k개의 마스터 키를 임의로 선택하여 각 TRM에 분배한다면 분배가능한 TRM의 수는 ${}_nC_k$로 확장되는 반면 키지표 변환함수 f(.)를 알아낸 최악의 경우 n/k개만의 TRM을 분석함으로써 전체 시스템의 마스터 키를 모두 알아낼 수 있게 된다. 또한 변수 n을 크게 할수록 사용자가 가지는 개인정보량이 늘어나게 되므로 이 점 역시 시스템 설계시에 고려해야 할 것이다. 그러므로 암호시스템이 구현된 컴퓨터 통신망의 규모와 성격에 따라 n과 k의 크기를 적절하게 결정하여야 한다. 그러나 대체로 n을 크게 하고 k를 3~4 개로 제한하는 것이 적당한 선택이라고 보아진다. 그리고 원하는 안전도를 제공할 수 있는 크기의 n을 수용할 수 있는 수준에서 개인이 휴대하는 메모리 카드의 용량을 정하는 것이 바람직하다. 그리고 k를 n/2 보다 크게 한다는 것은 아무런 이득이 없으므로 제외시켜야 한다.

이상에서 보듯이 제안된 시스템은 일정한 수 이상의 TRM을 분석하여야 시스템이 완전히 파괴되며 그 전에는 일단 성립한 암호시스템을 계속 유지시킬

수 있으므로 Desmedt 와 Quisquater 가 제안한 방식 [1] 보다 훨씬 실현가능성에 접근했다고 할 수 있다. 그러나 TRM 이라는 특수한 성격의 암호장비를 가정하는 이상 개방통신 시스템보다는 TRM 관리가 용이한 폐쇄그룹 내의 통신시스템으로 구현되는 것이 바람직하다고 생각된다.

4. 결론

현대의 발달해 가는 하드웨어 기술로 첨단 암호화 장비를 구현하고 이를 기반한 암호시스템을 구축하는 것은 현대암호학의 또 하나의 요구이다. 본 논문에서는 TRM 을 이용하여 사용자의 ID 에 기초한 암호시스템을 구현하고 안전성 유지를 위해 반드시 필요한 TRM 과 사용자 사이의 쌍방인증방식을 제안하였으며 또한 키생성키인 마스터 키를 다중화하여 TRM 내에 국소분배함으로써 시스템의 마스터 키를 보호하는 방안과 TRM Identity (TID) 를 이용한 디지탈 서명방식을 제안하였다. 제안된 방식은 1984년 Shamir 가 처음 제안한 ID 를 기초로 하는 암호시스템의 원래의 의미를 모두 구현하고 있다고 생각된다 [8]. 제안된 암호시스템은 사용자의 ID에 기초한 공개키 암호시스템을 근간으로 하고 메세지 암/복호화는 빠른 속도를 낼 수 있는 관용 암호알고리듬을 이용하되 이를 TRM 이라는 암호장비에 결합시켜 안전도를 높혔다. 또한 사용자는 자신의 개인정보를 간단한 메모리 카드에 저장하고 자신이 기억하는 정보와 결합하여 TRM 과 사용자 간의 쌍방인증을 간편하고 안전하게 할 수 있도록 하였다. 그러므로 제안된 암호시스템은 대량정보의 고속처리와 고도의 안전성, 그리고 사용자의 편이성을 함께 요구하는 현대사회에 보다 적합한 암호시스템이라고 생각된다.

[참고문헌]

[1] Y. Desmedt and J. J. Quisquater, "Public key system based on the difficulty of tampering," in *Proc. of Crypto '86*, 1986, pp. 111-117

[2] J. J. Quisquater, "Secret distribution of keys for public key systems", in *Proc. of Crypto '87*, 1987, pp. 203-208

[3] 문 희철, 이 필중, "Tamper Resistant Module 을 이용한 ID를 기초로 하는 암호시스템과 MHS 보안 서비스에 관한 연구," *91동계 컴퓨터통신 Workshop*, 1991, pp. 243-250

[4] P. J. Lee, "Secure access control for public networks," in *Proc. of Auscrypt' 90*, 1990, pp. 25-37

[5] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, IT-22, 6, 1976, pp.644-654.

[6] NBS, "Data Encryption Standard," FIPS PUB 46, Jan. 1977

[7] A. Shimizu and S. Miyaguchi, "Fast Data Encryption Algorithm FEAL," in *Proc. of EUROCRYPT' 87*, April, 1987

[8] A. Shamir, "Identity based cryptosystems and signature schemes", in *Proc. of Crypto '84*, 1984, pp. 47-53