(19) 대한민국특허청(KR)
(12) 특허공보(B1)

(51) Int. Cl.[6]
H04L 9/32

(45) 공고일자 1996년03월22일
(11) 공고번호 96-003846

(21) 출원번호	특1987-0015758	(65) 공개번호	특1989-0011272
(22) 출원일자	1987년12월30일	(43) 공개일자	1989년08월14일

(71) 출원인 뷜 쎄 뻬 8 쟝-루이 꿀롱
프랑스공화국 78190 트라쁘 뤼 위젠느 애나프

(72) 발명자 미셸 아자르
프랑스공화국 78124 마래이유/몰 드르 뤼 데 아리아스 27

(74) 대리인 김승호, 이태희

심사관 : 임영희 (책자공보 제4384호)

(54) 전송로에 의해 원격적 또는 국부적으로 연결된 송,수신장치사이의 데이터 전송을 확실히 식별하는 방법

요약

내용 없음.

대표도

도1

명세서

[발명의 명칭]

전송로에 의해 원격적 또는 국부적으로 연결된 송,수신장치사이의 데이터 전송을 확실히 식별하는 방법

[도면의 간단한 설명]

본 도면의 전기적 또는 광학적인 표준 전송 루우트(L)를 통해 국부적 또는 원격적으로 연결되어 있는 전송장치(2)와 수신장치(1)를 보이는 본 발명에 따른 전체적인 개략도.

* 도면의 주요부분에 대한 부호의 설명

1 : 카드 또는 휴대용 물체 또는 수신장치 2 : 외부장치 또는 전송장치

T1,T2 : 처리회로 M1,M2 : 메모리 장치

Z1,Z2,Z3 : 메모리 영역 I1,I2 : 인터페이스

b2 ; 버스 P1,P2 : 프로그램

S1,S2 : 키이 CL : 키보드

[발명의 상세한 설명]

본 발명은 전송로에 의해 원격적 또는 국부적으로 연결되며 적어도 하나 이상의 메모리회로와 처리회로를 포함하는 송,수신장치사이의 데이터 전송을 확실히 식별하는 방법에 관한 것이다.

본 발명은 특히 외부장치에 의해 전송된 데이터를 카드를 통해 확실히 식별하거나 또는 카드에 의해 전송된 데이터를 외부장치를 통해 확실히 식별하기 위하여 외부장치와 원격적으로 결합된 메모리 카드에 적용된다.

메모리 카드를 사용하는 대다수의 애플리케이션에서는 카드 내의 메모리 회로내에 기록된 테이터를 판독하거나 기록하는데 표준 동작을 사용한다. 이러한 동작은 카드와 외부장치 사이의 테이터 전송의 유효성을 가정한다. 즉, 수신된 데이터가 전송한 데이터와 동일한 것으로 가정한다. 그러나 이러한 표준 전송로를 통해 원격적으로 연결된 카드와 외부장치사이에의 테이터 전송의 유효성은 테이터 전송중 사취인에 의해 데이터가 사취되기가 쉽기 때문에 완전히 보장 받을 수가 없다. 이러한 문제점은 특히 데이터의 전송을 돈의 계산에 관한 신용이나 또는 차변에 관한 은행업무에 응용할 때 중요한 문제점으로 발생한다.

이러한 문제점의 한 해결책으로 전송될 데이터를 암호화하는 방법을 고려할 수 있으나, 이러한 방법은 완전한 해결책을 제시하지 못한다. 즉, 수신기가 명문의 데이터를 얻기 위하여 데이터를 해독하지만, 이 해독된 데이터가 전송된 데이터와 상응하는 지가 확실하지 않기 때문에 문제점으로 대

두된다.

본 발명은 상술한 결점을 해소하며, 수신된 데이터가 전송된 데이터와 동일한지 뿐만 아니라, 공인된 전송장치에 의해 데이터가 전송되었는지를 확인가능하게 한다. 따라서, 본 발명은 전송중에 데이터가 수정되었는지와 공인되지 않은 전송장치에 의해 데이터가 전송되었는지를 체크하는 것을 가능하게 해준다.

본 발명은 표준 루우트를 통해 상호 연결되며, 적어도 하나이상의 메모리 장치의 처리회로를 포함하는 전송장치(2)와 수신장치(1) 사이에 데이터 전송을 확실히 식별하기 위한 방법에 있어서, 전송장치(2)에서, 처리회로(T2)에 의해 수행된 프로그램(P2)에 의한 흔히 있는 알고리즘의 암호함수(f2)의 실행에 의해, 식 "M=f2(S2,X)"(여기서, S2는 상기 전송장치(2)의 메모리장치(M2)내에 미리 기록된 알고리즘의 암호키이며, X는 테이터(d)의 값(V)을 나타내는 한 구역(X2) 및 소정 조건을 만족하는 적어도 하나이상의 구역(X1)으로서 형성된 파라메타를 나타냄)와 같은 암호 메시지(M)를 형성하는 단계 ; 상기 메세지(M)를 수신장치(1)에 전송하고, 상기 알고리즘의 해독함수(f1)의 실행에 의해 "X'=f1(M,S1)"(여기서, S1은 상기수신장치(1)의 메모리 장치(M1)에 미리 기록된 해독키를 나타냄과)같은 파라메타(X')를 얻어 상기 암호 메세지(M)를 해독하는 단계 ; 상기 파라메타(X')를 적어도 하나이상의 구역(X° 1) 및 한 구역(X'2)들에 형성하는 단계 ; 및 상기 구역 (X'2) 데이터 값이 상기 구역(X2)의 데이터 값(d)과 같음을 추론하기 위하여, 상기 구역(X'1)이, 상기 파라메타(X)의 소정조건을 만족하는 구역(X1)과 동일한 것을 확인하는 단계로 구성됨을 특징으로 한다.

본 발명의 장점은 정보가 얼마간 떨어져 기록될 수 있고, 특히 신용카드와 같은 휴대용 물체를 구성하는 수신장치에서 완벽한 비밀을 보장할 수 있다는 점이다.

이하 첨부도면에 의거 본 발명을 상세히 설명한다.

두 개의 전자장치(1,2)들이, 표준의 전기적인 또는 광학적인 전송 루우트(L)를 통해 국부적으로 도는 원격적으로 연결되어 있다.

수신장치(1)는 적어도 하나의 메모리 장치(M1)와, 처리회로(T1)와, 입/출력 인터페이스(I1)를 포함한다. 이러한 모든 회로들은 연결 버스(b1)통해 서로 연결된다.

전송장치(2)는 적어도 하나의 메모리 장치(M2)와,처리회로(T2)와, 키보드(CL)와 같은 하나의 입력장치와, 하나의 입/출력 인터페이스(I2)를 포함한다. 이러한 모든 회로들도 연결 버스(b2)를 통해 서로 연결된다. 상기 메모리 장치들(M1,M2)은 각각, 예를들어 적어도 2개 이상의 메모리 영역들(Z1,Z2)로 분리된다. 일단 이들이 기록되면, 상기 메모리 영역(Z1)에 기록된 데이터는 고정되어 외부로부터 판독 및 기록동작이 불가능하지만 메모리 영역(Z2)에 기록된 데이터는 외부로부터의 판독만은 가능하다. 이와는 반대로, 상기 메모리 영역들(Z1, Z2)에 기록된 모든 데이터는 상기 처리회로에 의해 자유롭게 처리 가능하다. 상기 메모리 장치들(M1,M2)은 또한 ,상기 처리회로에 의해 수행되는 과정중의 데이터를 중간 기억시키기 위한 작업영역(Z3)을 포함한다.

예를들어, 상기 수신장치(1)는 카드와 같은 휴대용 물체이며, 상기 전송장치(2)는, 상기 외부장치에 일시적으로 연결된 카드와 대화할 수 있는 외부장치이다. 상기 카드와 상기 장치 사이에 수립되는 대호가 보조회로(특정 응용에 따라 설치되지만 도시되지 않음)에 의하여 액세스 또는 서비스의 제공을 가능케 한다.

대화는 본래 데이터 교환에 관계되는 바, 여기서는 외부장치(2)가 카드(1)에 데이터(d)를 전송하는 가정하도록 하겠다.

제 1 의 보안 방법은 해독된 데이터가 전송된 데이터와 동일한 지를 식별할 수 있는 카드(1)에, 암호화된 데이터를 전송하는 방법, 즉, 명문의 데이터를 전송하지 않는 방법이다.

상기 데이터(d)는 외부장치(2)의 처리회로(T2)에 의해 계산된 데이터이거나 또는 외부장치(2)의 키보드(CL)의 데이터를 상기 처리회로(T2)로 미리 처리한 데이터이다.

상기 데이터(d)의 암호화는 상기 메모리 장치(M2)의 메모리 영역(Z1)내에 미리 기록된 프로그램(P2)과 상기 처리회로(T2)에 의해 행해진다. 이 프로그램(P2)은 흔히 있는 알고리즘을 암호화하는 함수(f2)를 이행하는 프로그램이다. 이러한 함수(f2)는 상기 메모리 장치(M2)의 메모리 영역(Z1)내에 미리 기록된 적어도 하나이상의 암호화 키이(S2)와 상기 데이터(d)와 결합된 파라메타(X)를 고려한다.

특히 상기 파라메타(X)는, 다수의 구역(X1,X2,...,Xn)들로 구성되는바, 이 구역들 중의 적어도 하나는 소정식을 만족하며, 이 구역들중의 적어도 하나는 2진 데이터(d) 또는 값을 나타낸다.

파라메타(X)는 예로써 다음과 같은 3개의 구역들(X1, X2, X3)로 형성될 수 있다.

- X1 = X2 = ad(d)

- X3 = V

여기서, ad(d)는 데이터(d)가 기록되는 카드(1)내의 메모리 소자의 어드레스이며, V는 데이터(d)값이다.

따라서, 암호화된 메시지(M)가 식 "M=f(X,S2)"로써 얻어진다.

이 메세지(M)은 전송 루우트(L)를 통해 카드(1)에 전송된다. 상기 카드(1)의 처리회로(T1)는, 수신된 메세지(M)에 대하여, 메모리 장치(M1)의 메모리 영역(Z1) 내에 미리 기록된 프로그램(P1)을 수행한다. 이 프로그램(P1)은 역 함수(f1)실행 프로그램이거나 또는 외부장치(2)에 의한 암호 작성 시점에서 사용된, 흔히 있는 알고리즘을 해독하는 프로그램이다. 이 프로그램(P1)은 메모리 장치(M1)의 메모리 영역(Z1)내에 미리 기록된 해독 키이(S1) 수단에 의해 상기 메시지를 다음과 같이

해독한다.

f1(M,S1)=X'

상기 파라메타(X)에서와 같이, 상술한 바와같이 하여 얻어진 파라메타(X')는 다수의 구역 (X'1,X'2,...,X'n)들로 형성되고, 상기 파라메타(X)의 구역에 의해 만족된 식이나 조건은 상기 파라메타(X')의 대응하는 구역에 의해 또한 만족되어져야 한다. 전술한 예를 고려하면, 상기 파라메타(X')는 3개의 구역들(X'1,X'2,X'3)로 형성된다.

본 발명에 따르면, 만약 상기 구역들(X'1,X'2)이 상기 구역들(X'1,X'2)과 동일한 식을 만족하면, 즉, 이러한 구역들의 데이터가 데이터(d)의 어드레스(da)와 동일하면, 메모리카드는 상기 구역(X'3)은 외부장치(2)에 의해 전송된 확실한 데이터(d) 값이라고 인식한다.

처리회로(T1)를 통해 상기 카드(1)는, 상기 카드(1)의 메모리 장치(M1)의 메모리 영역(Z2 또는 Z3)의 어드레스(ad)에 데이터를 기록한다.

이와 반대의 경우로써, 메모리 카드가 상기 파라메터(X')의 구역(X'3)의 데이터 값(V)이 전송된 데이터(d)값과 같지 않다고 인식하는 경우를 고려한다. 이러한 경우에, 상기 카드는 다음 사항중의 하나가 발생되었음을 인지하기 때문에, 수신된 메시지(M)를 고려하지 않는다.

- 상기 메시지(M)의 전송시 에러

- 상기 전송 과정중 메시지(M)의 변형

- 만약 암호 키이(S2)가, 유효한 카드(1)의 해독 키이(S1)과 대응하지 않으면, 상기 메시지(M)가 공인 되지 않은 장치에 의해 전송됨

데이터(d)의 전송의 보안성을 강화하기 위하여, 무작위로 선정된 수(E)를 고려하여 암호 프로그램(P2)을 만들 수 있다. 따라서, 동일한 데이터(d)가 다르게 암호화 됨으로써, 사취인이 초기 메시지(M)를 다시 사용하는 것을 방지할 수 있다.

상기 무작위로 선정된 수(E)는 카드 그 자체에 의해 공급된다. 특히 상기 수는 메모리 영역(Z2)이나 제어 영역내에서 샘플화되며, 상기 수중의 적어도 한 비트는 카드(1)의 사용후 변경된다. 따라서, 상기 무작위로 선정된 수는, 메모리 영역(Z1)내에서, 상기 변경된 최하위 비트를 포함하는 워드를 형성한다. 상기수(E)는 암호화 동작에 앞서 당연히 외부장치(2)에 전송된다.

한 병형예로서, 상기 무작위로 선정된 수(E)가, 메모리 장치내의 기록이 행해질 어드레스(ad)에서의 초기 내용으로 이루어질 수도 있다. 상기 메모리 장치내에 데이터의 기록은 워드 단위로서 이뤄지기 때문에, 다수 워드의 데이터(d)의 기록에서는, 데이터(d)의 기록이 완료될 때가지, 본 발명의 방법에 따라 연속적으로 수정되며, 각 어드레스(ad)의 초기내용으로 이루어진 각각 다른, 무작위로 선정된 수(E)를 가진 워드들의 전송이 필요하게 된다.

본 발명은, 외부장치(2)가 카드(1)에 의해 전송된 데이터를 확인할 때, 상술한 순서와 역순으로도 적용할 수도 있다.

상술한 암호 프로그램(P2)과 해독 프로그램(P1)은 동일할 수도 있는데, 이것은 키이(S1)와 카이(S2)가 동일하다는 것을 의미한다. 보안성을 고려하여, 이러한 키이들은 비밀 상태가 유지되어야 하며, 이러한 이유로써 이들은 외부로부터 도달할 수 없는 메모리 영역(Z1)내에 미리 기록되어야 한다.

다른 병형예로써, 상술한 알고리즘은 공공 키이를 가진 알고리즘을 고려할 수도 있다.

(57) 청구의 범위

청구항 1

표준 전송 루우트를 통해 상호 연결되며, 적어도 하나이상의 메모리 장치와 처리회로를 포함하는 전송장치(2)와 수신장치(1) 사이에 데이터 전송을 확실히 식별하기 위한 방법에 있어서, 전송장치(2)에서, 처리회로(T2)에 의해 수행된 프로그램(P2)에 의한 흔히 있는 알고리즘 암호함수(f2)의 실행에 의해, 식 "M=f2(S2,S)"(여기서,S2는 상기 전송장치(2)의 메모리장치(M2)내에 미리 기록된 알고리즘의 암호키이며, X는 데이터(d)의 값(V)을 나타내는 한 구역(X2) 및 소정 조건을 만족하는 적어도 하나이상의 구역(X1)으로 형성된 파라메타를 나타냄)와 같은 암호 메시지(M)를 형성하는 단계 ; 상기메세지(M)를 수신장치(1)에 전송하고, 상기 알고리즘의 해독함수(f1)의 실행에 의해 "X'=f1(M,S1)"(여기서, S1은 상기 수신장치(1)의 메모리 장치(M1)에 미리 기록된 해독키를 나타냄)과 같은 파라메타(X')를 얻어 상기 암호 메시지(M)를 해독하는 단계 ; 상기 파라메타(X')를 적어도 하나이상의 구역X'1)및 한 구역X'2)들에 형성하는 단계 ; 및 상기 구역(X'2)의 데이터 값이 상기 구역(X2)의 데이터의 값(d)과 같음을 추론하기 위하여,상기 구역(X'1)이, 상기 파라메타(X)의 소정 조건을 만족하는 구역(X1)과 동일한 것을 확인하는 단계로 구성됨을 특징으로 하는 전송로에 의해 원격적 또는 국부적으로 연결된 송,수신장치 사이의 데이터 전송을 확실히 식별하는 방법.

청구항 2

제 1 항에 있어서, 상기 방법은 상기 함수(f1,f2)가 무작위로 선정된 수(E)를 고려하는 단계를 포함함을 특징으로 하는 전송로에 의해 원격적으로 또는 국부적으로 연결된 송,수신장치 사이의 데이터 전송을 확실히 식별하는 방법.

청구항 3

제 2 항에 있어서, 상기 방법은 수신장치(1)나 또는 전송장치(2)가 휴대용 물체일 때 상기 휴대용

장치에 의해 처리된 상기 무작위로 선정된 수(E)를 모니터링 메모리 영역(Z2)으로 입력시켜 휴대용 물체가 사용될때마다 그 내용을 변경시키는 단계를 포함함을 특징으로 하는 전송로에 의해 원격적 또는 국부적으로 연결된 송,수신장치 사이의 데이터 전송을 확실히 식별하는 방법.

청구항 4

전술한 항들중의 어느 하나에 있어서, 상기 방법은 상기 데이터(d)가 기록되어야 하는 메모리 어드레스(ad)에서 개시하며, 상기 파라메타(X)의 구역(X1)이 만족해야 하는 소정 조건을 한정하는 단계를 포함함을 특징으로 하는 전송로에 의해 원격적 또는 국부적으로 연결된 송,수신장치사이의 데이터 전송을 확실히 식별하는 방법.

도면

도면1