(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년10월22일
(11) 등록번호 10-0864903
(24) 등록일자 2008년10월16일

(51) Int. Cl.
H04L 9/32 (2006.01)
(21) 출원번호 10-2003-7011877
(22) 출원일자 2003년09월09일
심사청구일자 2007년03월09일
번역문제출일자 2003년09월09일
(65) 공개번호 10-2003-0084983
(43) 공개일자 2003년11월01일
(86) 국제출원번호 PCT/FR2002/000884
국제출원일자 2002년03월12일
(87) 국제공개번호 WO 2002/73876
국제공개일자 2002년09월19일
(30) 우선권주장
01/03313 2001년03월12일 프랑스(FR)
(56) 선행기술조사문헌
G. D. Crescenzo 외 2명, Improved Setup Assumptions for 3-Round Resettable Zero Knowledge, ASIACRYTP 2004, pp.530-544 (2004.11.)
Jaramillo, C. I. 외 3명, An Implementation of a zero-knowledge protocol for a secure networklogin procedure, Southeastcon 89, pp.197-201 (1989.04.09.)
(73) 특허권자
프랑스 텔레콤
프랑스, 에프-75015 파리, 프라스 달러레, 6
텔레디퓨지옹 드 프랑스
프랑스, 에프-75732 파리, 스터 15, 뤼 도라두-쉬르-그란느, 10
(72) 발명자
길로우루이
프랑스,에프-35230부르베르,루드리스,16
(74) 대리인
특허법인 씨엔에스 · 로고스

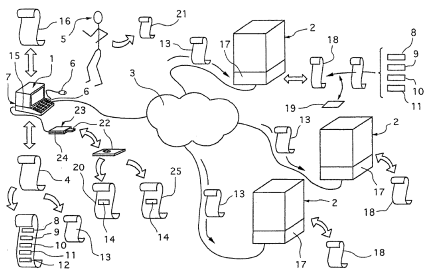
전체 청구항 수 : 총 13 항 심사관 : 양종필

(54) 일시적 모듈을 사용한 암호 인증

(57) 요 약

본 발명은 제1 컴퓨터 장치(1)가 제2 컴퓨터 장치(2)에 의해 인증될 수 있게 하는 방법 및 시스템의 기술 분야에 관한 것이다. 본 발명에 따른 방법은 세션 지속시간에 대한 긴 사용시간에 대해 서명키(14)에 대한 접근을 제공하는 개인 식별자(21)를 제공함으로써, 로그-온 진행 소프트웨어의 작동을 사용자가 시작하는 단계를 포함한다. 상기 로그-온 진행 소프트웨어는, 세션 식별 데이터 Id, 공개 일시 모듈 n(9), 공개 지수 v, 적어도 한쌍의 일시 공개 값 G(11), 다음과 같은 일반 방정식을 통해 생성되는 일시 개인 값 Q(12): $G \equiv Q^{v} \pmod{n}$ 또는 $G \times Q^{v} \equiv 1 \pmod{n}$, 및 상기 개인 서명키(14), Id(8) 및 n(9)을 이용하여 일시 인증서(13)를 생성한다. 공개 일시 모듈 n(9)은 개인 서명키(14)에 비해 크기가 감소된다. 본 발명에 따른 방법은 사용자가 증거 소프트웨어의 작동을 시작하는 단계 및 제어 소프트웨어의 작동을 시작하는 단계를 포함한다.

대 표 도



특허청구의 범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

제1 컴퓨터 장치와 제2 컴퓨터 장치 간의 제한된 지속 시간의 통신 세션(session) 동안, 상기 제1 컴퓨터 장치가 적어도 하나의 상기 제2 컴퓨터 장치에 의해 인증되도록 하는 방법에 있어서,

로그-온(log-on) 소프트웨어 프로그램(4)을 실행시키고, 사용자(5)의 신원을 확인하고 상기 사용자(5)가 개인 서명키(14)에 접근하는 것을 가능하도록 하는 개인 식별자(21)를 도입함으로써 상기 제1 컴퓨터 장치(1)에 로그-온 하는 단계;

상기 로그-온 소프트웨어 프로그램(4)이,

세션 식별자 데이터 Id,

각각의 키 쌍(Q_i,G_i)이 $G_i \times Q_i^v \equiv 1 \bmod n$ 또는 $G_i \equiv Q_i^v \bmod n$ 의 식을 만족하고, m은 1보다 크거나 같은 정수이고, i는 1과 m 사이의 정수이며, v는 공개 지수이고, n은 f개의 소인수 $p_1,p_2,\ldots,p_f$의 곱과 같은 공개 정수이고, 상기 소인수 중 적어도 두 개의 소인수는 서로 다르고, f는 1 보다 큰 정수이고, 상기 세션의 지속 시간의 기간 동안 컴퓨터에 의해 인수분해될 수 없도록 상기 공개 모듈 n은 상기 개인 서명키(14)에 비해 작은 하나 이상의 개인 값 $Q_1,Q_2,\ldots,Q_m$ 및 각각의 공개 값 $G_1,G_2,\ldots,G_m$의 세트, 및

상기 개인 서명키로 적어도 상기 세션 식별자 데이터 Id와 상기 공개 모듈 n을 서명함으로써 인증서(13)를 생성하는 단계;

상기 로그-온 소프트웨어 프로그램(4)의 실행을 중지하는 단계;

적어도 상기 제1 컴퓨터 장치(1)의 상기 제2 컴퓨터 장치 각각에 대한 제1 연결 기간 동안,

영-지식(zero-knowledge) 인증 프로토콜(protocol)의 증명자(prover)로서 행동하는 증명 소프트웨어 프로그램(16)의 실행을 시작하는 단계;

상기 제2 컴퓨터 장치(2)로 상기 인증서(13)를 전송하는 단계;

상기 제2 컴퓨터 장치(2)가 상기 영-지식 인증 프로토콜에서 검증자로서 행동하는 검증 소프트웨어 프로그램(18)의 실행을 시작하는 단계;

상기 검증 소프트웨어 프로그램(18)이, 상기 개인 서명키(14)와 연관된 공개키로서 상기 인증서(13)를 개봉하고, 해당 인증서(13)로부터 상기 세션 식별자 데이터 Id와 상기 공개 모듈 n을 추출하는 단계; 그리고

상기 증명 소프트웨어 프로그램(16)과 상기 검증 소프트웨어 프로그램(18)이 상기 영-지식 인증 프로토콜을 완료하는 단계로 이루어지는 제1 컴퓨터 장치가 적어도 하나의 제2 컴퓨터 장치에 의해 인증되도록 하는 방법.

청구항 22

제21항에 있어서,

상기 제1 컴퓨터 장치(1)는 상기 개인 서명키(14)의 암호문(20)을 포함하고, 상기 방법에서, 상기 로그-온 소프트웨어 프로그램(4)은 상기 개인 식별자(21)를 사용하여 상기 암호문(20)을 해독하는 단계를 더 포함하는 것을 특징으로 하는 제1 컴퓨터 장치가 적어도 하나의 제2 컴퓨터 장치에 의해 인증되도록 하는 방법.

청구항 23

제21항에 있어서,

상기 개인 서명키(14)의 암호문(20)은 상기 사용자(5)가 소유하는 메모리카드(22)에 포함되고, 상기 방법은,

상기 제1 컴퓨터 장치(1)와 연관된 메모리카드 리더(23)에 상기 메모리카드(22)를 삽입하는 단계; 그리고

상기 로그-온 소프트웨어 프로그램(4)이 상기 개인 식별자(21)를 사용하여 상기 암호문(20)을 해독하는 단계를 더 포함하는 것을 특징으로 하는 제1 컴퓨터 장치가 적어도 하나의 제2 컴퓨터 장치에 의해 인증되도록 하는 방법.

청구항 24

제21항에 있어서,

상기 개인 서명키(14)는 상기 사용자(5)가 소유하는 메모리카드(22) 내에 서명 알고리즘(algorithm)(25)과 함께 위치하고, 상기 방법은,

상기 제1 컴퓨터 장치(1)와 연관된 메모리카드 리더(23)에 상기 메모리카드(22)를 삽입하는 단계; 그리고

상기 로그-온 소프트웨어 프로그램(4)이 상기 개인 서명키(14)를 사용하여 상기 서명 알고리즘(25)을 실행함으로써 상기 인증서(13)를 생성하는 단계를 더 포함하는 것을 특징으로 하는 제1 컴퓨터 장치가 적어도 하나의 제2 컴퓨터 장치에 의해 인증되도록 하는 방법.

청구항 25

제21항 내지 제24항 중 어느 하나의 항에 있어서,

상기 영-지식 인증 프로토콜은 GQ0 타입인 것을 특징으로 하는 제1 컴퓨터 장치가 적어도 하나의 제2 컴퓨터 장치에 의해 인증되도록 하는 방법.

청구항 26

제21항 내지 제24항 중 어느 하나의 항에 있어서,

상기 영-지식 인증 프로토콜은 GQ1 타입의 인증 프로토콜이고, P_j가 j=1,2,...,f에서 모듈러스 n의 소인수일 때 상기 공개 지수 v는 모든 수 (p_j -1)와 서로소이고, i=1,2,...,m 일 때 각각의 공개 값 G_i는 RSA 표준 서명 포맷 Red를 각각의 메시지 m_i에 적용함으로써 얻어지고, i=1,2,...,m이고 j=1,2,...,f 일 때 상기 개인 값 Q_i는 (sv-1)이 모든 수(p_j-1)의 곱과 같도록 하는 공개 지수 s에 대해 $Q_i \equiv G_i^s \bmod n$의 식을 만족하는 것을 특징으로 하는 제1 컴퓨터 장치가 적어도 하나의 제2 컴퓨터 장치에 의해 인증되도록 하는 방법.

청구항 27

제21항 내지 제24항 중 어느 하나의 항에 있어서,

상기 영-지식 인증 프로토콜은 GQ2 타입 인증 프로토콜이고, k가 1보다 큰 정수 값을 갖는 보안 파라미터(security parameter)일 때 v는 $v=2^k$식을 만족하고, 각각의 공개 값 G_i(i=1,2,...,m)는 g_i(i=1,2,...,m)가 1보다 큰 정수 값을 갖는 기수(base number)일 때 $G_i \equiv g_i^2 \bmod n$의 식을 만족하고, i=1,2,...,m이고 j=1,2,...,f 일 때 상기 개인 값 Q_i는 (sv-1)이 모든 수(p_j-1)의 곱과 같도록 하는 공개 지수 s에 대해 $Q_i \equiv G_i^s \bmod n$의 식을 만족하는 것을 특징으로 하는 제1 컴퓨터 장치가 적어도 하나의 제2 컴퓨터 장치에 의해 인증되도록 하는 방법.

청구항 28

제1 컴퓨터 장치(1)와 적어도 하나의 제2 컴퓨터 장치(2)를 포함하는 시스템에 있어서, 상기 컴퓨터 장치들은 통신 네트워크(3)에 연결되고, 상기 시스템은 상기 제1 컴퓨터 장치(1)와 상기 제2 컴퓨터 장치(2) 간의 제한된 지속 시간의 통신 세션 동안, 상기 제1 컴퓨터 장치가 적어도 하나의 상기 제2 컴퓨터 장치에 의해 인증되도록 하는 시스템으로서,

상기 제1 컴퓨터 장치(1)는,

상기 제1 컴퓨터 장치(1)를 로그-온 할 때 제어 유닛(6)을 실행함으로써, 그리고 개인 식별자(21)가 사용자(5)의 신원을 검사하도록 하고 상기 사용자(5)의 개인 서명키(14)의 접근을 가능하도록 하는 개인 식별자(21)들을 상기 제어 유닛(6)을 통해 도입함으로써 상기 사용자(5)에 의해 실행될 로그-온 프로그램(4)을 기록하는 제 1 메모리;

상기 로그-온 소프트웨어 프로그램(4)에 의해 제어되는 제1 계산 수단(7)으로서,

세션 식별자 데이터 Id,

각각의 키 쌍(Q_i,G_i)이 $G_i \times Q_i^v \equiv 1 \bmod n$ 또는 $G_i \equiv Q_i^v \bmod n$ 의 식을 만족하고, m은 1보다 크거나 같은 정수이고, i는 1과 m 사이의 정수이며, v는 공개 지수이고, n은 f개의 소인수 $p_1,p_2,\ldots,p_f$의 곱과 같은 공개 정수이고, 상기 소인수 중 적어도 두 개의 소인수는 서로 다르고, f는 1 보다 큰 정수이고, 상기 세션의 지속 시간의 기간 동안 컴퓨터에 의해 인수분해될 수 없도록 상기 공개 모듈 n은 상기 개인 서명키(14)에 비해 작은 하나 이상의 개인 값 $Q_1,Q_2,\ldots,Q_m$ 및 각각의 공개 값 $G_1,G_2,\ldots,G_m$의 세트, 및

상기 개인 서명키(14)로 적어도 상기 세션 식별자 데이터 Id와 상기 공개 모듈 n을 서명함으로써 인증서(13)를 생성하는 수단을 갖는 제1 계산 수단(7);

상기 로그-온 소프트웨어 프로그램(4)의 실행을 중지하는 수단을 갖는 중지수단(15);

상기 제1 계산 수단(7)을 제어하기 위한, 그리고 적어도 상기 제1 컴퓨터 장치(1)의 상기 제2 컴퓨터 장치 각각에 대한 제1 연결 기간 동안 영-지식 인증 프로토콜의 증명자로서 상기 제어 유닛(6)을 실행시킴으로써 상기 사용자(5)에 의해 실행될 때 동작하도록 하기 위한 명령어들을 갖는 증명 소프트웨어 프로그램(16)을 기록하는 제 2 메모리; 및

상기 인증서(13)를 상기 제2 컴퓨터 장치(2)로 전송하기 위한 수단을 포함하는 제1 컴퓨터 장치(1)이고; 그리고

상기 제2 컴퓨터 장치(2)는,

상기 영-지식 인증 프로토콜에서 검증자로서 행동하기 위해, 제2 계산 수단(17)을 제어하기 위한, 상기 개인 서명키(14)와 관련된 공개키로서 상기 인증서(13)를 개봉하기 위한, 그리고 해당 인증서(13)로부터 상기 세션 식별자 데이터 Id와 상기 공개 모듈 n을 추출하기 위한 명령어를 갖는 검증 소프트웨어 프로그램(18)을 기록하는 메모리; 및

상기 검증 소프트웨어 프로그램(18)의 실행의 시작을 위한 시작 수단을 포함하는 제2 컴퓨터 장치(2)인 것을 특징으로 하는 시스템.

청구항 29

제28항에 있어서,

상기 제1 컴퓨터 장치(1)는 상기 개인 서명키(14)의 암호문(20)을 더 포함하고, 그리고

상기 로그-온 소프트웨어 프로그램(4)은 상기 개인 식별자(21)를 사용하여 상기 암호문(20)을 해독하기 위한 명령어를 더 포함하는 것을 특징으로 하는 시스템.

청구항 30

제28항에 있어서,

상기 사용자(5)가 소유하고 상기 개인 서명키(14)의 암호문(20)을 포함하는 메모리카드(22); 및

상기 메모리카드(22)를 판독하기 위한 상기 제1 컴퓨터 장치(1)와 관련된 메모리카드 리더기(23)를 더 포함하고,

상기 로그-온 소프트웨어 프로그램(4)은 상기 개인 식별자(21)를 사용함으로써 상기 암호문(20)을 해독하기 위한 명령어를 갖는 것을 특징으로 하는 시스템.

청구항 31

제28항에 있어서,

상기 사용자(5)가 소유하고 서명 알고리즘과 함께 상기 개인 서명키(14)를 포함하는 메모리카드(22); 및

상기 메모리카드(22)를 판독하기 위한 상기 제1 컴퓨터 장치(1)와 관련된 메모리카드 리더기(23)를 더 포함하고;

상기 로그-온 소프트웨어 프로그램(4)은 상기 개인 서명키(14)로 상기 서명 알고리즘(25)을 실행함으로써 상기 인증서(13)를 생성하기 위한 명령어들을 갖는 것을 특징으로 하는 시스템.

청구항 32

제21항에 있어서,

상기 검증 소프트웨어 프로그램(18)이, 상기 개인 서명키(14)와 연관된 공개키로서 상기 인증서(13)를 개봉하고, 해당 인증서(13)로부터 상기 세션 식별자 데이터 Id와 상기 공개 모듈 n을 추출하는 단계에서,

상기 검증 소프트웨어 프로그램(18)이 상기 인증서(13)로부터 상기 공개 지수 v 또는 상기 공개 값 $G_1,G_2,\ldots,G_m$를 더 추출하는 것을 특징으로 하는 방법.

청구항 33

제28항에 있어서,

상기 검증 소프트웨어 프로그램(18)은 상기 인증서(13)로부터 상기 공개 지수 v 또는 상기 공개 값 $G_1,G_2,\ldots,G_m$를 더 추출하기 위한 명령어를 갖는 것을 특징으로 하는 시스템.

명 세 서

기 술 분 야

<1> 본 발명은 개인 컴퓨터와 같은 제1 컴퓨터 장치가 서버와 같은 적어도 하나의 제2 컴퓨터 장치에 의해 인증될 수 있게 하는 방법 및 시스템의 기술 분야에 관한 것이다.

배 경 기 술

<2> 본 발명에서 사용되는 영 지식 GQ 인증 메커니즘은 유럽특허 EP 0 311 470 B1호, PCT 출원 WO 00/46946호(2000년 8월 10일 공개), PCT 출원 WO 00/45550호(2000년 8월 3일 공개) 및 PCT 출원 WO 00/46947호(2000년 8월 10일 공개)에 게시되어 있다. 상기 문헌들은 참고로 인용될 것이다.

발명의 상세한 설명

<3> **방법**

<4> 본 발명은 개인 컴퓨터와 같은 제1 컴퓨터 장치가 서버와 같은 적어도 하나의 제2 컴퓨터 장치에 의해 인증될 수 있게 하는 방법에 관한 것이다. 상기 컴퓨터 장치들은 통신 네트워크에 연결되어 있다.

<5> 본 발명에 따른 방법은 다음의 두 단계를 포함한다: 상기 제1 컴퓨터 장치 상에서 세션을 초기화하기 위해 특정

사용자가 로그-온 하는 단계 및 상기 세션을 지속하는 단계.

<6> *Ⅰ. 특정 사용자에 의해 상기 제1 컴퓨터 장치로 로그-온 하는 단계*

<7> 상기 로그-온 하는 단계에서, 본 발명에 따른 방법은, 특정 사용자가 상기 제1 컴퓨터 장치 상에서 개인 식별자, 특히 패스워드 및/또는 지문을 제공하여 로그-온 소프트웨어의 실행을 시작함으로써 예를 들어 수 시간의 제한된 지속시간의 세션을 위해 로그-온하는 단계를 포함한다. 상기 개인 식별자는 상기 특정 사용자의 신원을 확인하고 상기 특정 사용자의 개인 서명키(signature key)를 호출하게 한다.

<8> 상기 로그-온 소프트웨어는 특히 상기 특정 사용자를 인식하기 위한 데이터 및/또는 상기 제1 컴퓨터 장치를 식별하기 위한 데이터 및/또는 날짜 및/또는 시간 및/또는 상기 세션 지속시간으로부터 세션 식별자 데이터 Id를 생성한다.

<9> 또한, 상기 로그-온 소프트웨어는 공개 일시 모듈(public ephemeral module) n, 공개 지수(public exponent) v 및 적어도 한쌍의 일시 공개 값 G를 생성하고, 하기 식 1의 형태의 일반 방정식에 의해 관련된 일시 개인 값 Q를 생성한다.

수학식 1

<10> $G \equiv Q^{v} \pmod{n}$ 또는 $G \times Q^{v} \equiv 1 \pmod{n}$

<11> 또한, 상기 로그-온 소프트웨어는 상기 특정 사용자의 개인 서명키, 상기 세션 식별자 데이터 Id, 상기 공개 일시 모듈 n 및 경우에 따라 상기 공개 지수 v 또는 일시 공개 값 G를 이용하여 서명 시 고유 일시 인증서(unique ephemeral certificate)를 생성한다.

<12> *Ⅱ. 세션을 지속하는 단계*

<13> 상기 로그-온하는 단계 이후 또는 세션의 지속 시간 동안 상기 로그-온 소프트웨어의 동작은 중지된다.

<14> 세션이 지속되는 동안, 각각의 상기 제2 컴퓨터 장치에 상기 제1 컴퓨터 장치의 제1 연결이 적어도 지속되는 동안, 본 발명의 방법은, 상기 특정 사용자가 증명 소프트웨어 프로그램(proof software program)의 실행을 시작하는 단계를 포함한다. 상기 증명 소프트웨어 프로그램은 통신 네트워크를 통해 상기 제2 컴퓨터 장치로 상기 일시 인증서를 배포한다. 상기 증명 소프트웨어는 영 지식(zero-knowledge) 인증 메커니즘, 특히 GQ 타입의 실행에 이용되는 증명을 생성한다.

<15> 영 지식 GQ 인증 메커니즘은 유럽특허 EP 0 311 470 B1호, PCT 출원 WO 00/46946호(2000년 8월 10일 공개), PCT 출원 WO 00/45550호(2000년 8월 3일 공개) 및 PCT 출원 WO 00/46947호(2000년 8월 10일 공개)에 게시되어 있다. 상기 문헌들은 참고로 인용될 것이다.

<16> 본 발명에서, GQ 인증 프로토콜에서 이해되는 바에 따르면 상기 증명 소프트웨어는 증명자(prover)의 역할을 한다.

<17> 세션이 지속되는 동안, 본 발명에 따른 방법은 상기 제2 컴퓨터 장치가 상기 개인 서명키에 관련된 공개키를 이용하여 상기 일시 인증서를 개봉하는 검증(verification) 소프트웨어 프로그램의 실행을 시작하는 단계 및 상기 일시 인증서로부터 상기 세션 식별자 데이터 Id 및 상기 공개 일시 모듈 n, 또한 경우에 따라 상기 공개 지수 v 또는 상기 일시 공개 값 G를 추출하는 단계를 더 포함한다.

<18> 상기 GQ 인증 프로토콜에서 이해되는 바에 따르면 상기 증명 소프트웨어는 검증자(verifier)의 역할을 한다.

<19> 바람직하게는, 본 발명에 따른 방법의 일실시형태에서, 상기 특정 사용자의 개인 서명키는 상기 제1 컴퓨터 장치 내에 포함된 암호문 내에 위치한다. 이러한 실시형태에서, 본 발명에 따른 방법은 상기 로그-온 소프트웨어가 상기 특정 사용자의 개인 식별자를 실행할 때 상기 암호문을 해독하는 단계를 더 포함한다.

<20> 바람직하게는, 본 발명에 따른 방법의 다른 실시형태에서, 상기 특정 사용자의 개인 서명키는 상기 특정 사용자에 의해 사용되는 메모리 카드에 포함된 암호문 내에 위치한다. 이러한 실시형태에서, 본 발명에 따른 방법은, 상기 특정 사용자가 상기 제1 컴퓨터 장치에 연결된 메모리 카드 리더(reader)에 상기 메모리 카드를 삽입하는 단계를 더 포함한다. 이러한 실시형태에서, 본 발명에 따른 방법은 상기 로그-온 소프트웨어가 상기 특정 사용자의 개인 식별자를 실행함으로써 상기 암호문을 해독하는 단계를 더 포함한다.

<21> 바람직하게는, 본 발명에 따른 방법의 또 다른 실시형태에서, 상기 특정 사용자의 개인 서명키는 상기 특정 사용자에 의해 사용되는 메모리 카드 내의 서명 알고리듬으로 정의된다. 이러한 실시형태에서, 본 발명에 따른 방법은 상기 특정 사용자가 상기 제1 컴퓨터 장치와 연결된 메모리 카드 리더에 메모리 카드를 삽입하는 단계를 더 포함한다. 이러한 실시형태에서, 본 발명에 따른 방법은 상기 로그-온 소프트웨어 프로그램이 상기 개인 서명키를 실행하는 상기 서명 알고리듬을 실행할 때 상기 일시 인증서를 생성하는 단계를 더 포함한다.

<22> *제1 실시형태 : GQ0 타입 인증 프로토콜의 경우*

<23> 바람직하게는, 본 발명의 제1 실시형태에 따른 방법은 GQ0 타입 인증 프로토콜의 경우에 수행된다. 이 경우에 상기 공개 일시 모듈 n, 상기 공개 지수 v, 적어도 한쌍의 일시 공개 값 G 및 일시 개인 값 Q의 생성을 위해, 본 발명의 제1 실시형태에 따른 방법은 다음 단계를 더 포함한다:

<24> - 상기 공개 지수 v의 값을 설정하는 단계,

<25> - 상기 공개 일시 모듈 n을 무작위로 선택하는 단계,

<26> - m개의 일시 개인 값 Q_1 내지 Q_m을 선택하는 단계,

<27> - 상기 일반 방정식 중의 하나를 획득하여 상기 일시 공개 값 G를 계산하는 단계.

<28> 상기 일시 인증서는 세션 식별자 데이터 Id에 대한 상기 공개 일시 모듈 n, 공개 지수 v 및 일시 공개 값 G와 관련된다.

<29> 바람직하게는, 본 발명의 제1 실시형태에서 상기 GQ0 타입 인증 프로토콜은 상기 공개 일시 모듈 n 및 상기 m개의 일시 개인 값 Q_1 내지 Q_m을 실행하는 증명 메커니즘을 포함한다.

<30> *제2 실시형태 : GQ1 타입 인증 프로토콜의 경우*

<31> 바람직하게는, 본 발명의 제2 실시형태에 따른 방법은 GQ1 타입 인증 프로토콜의 경우에 수행된다. 이 경우에 상기 공개 일시 모듈 n, 상기 공개 지수 v, 적어도 한쌍의 일시 공개 값 G 및 일시 개인 값 Q의 생성을 위해, 본 발명의 제2 실시형태에 따른 방법은 다음 단계를 더 포함한다:

<32> - 상기 공개 지수 v의 값을 설정하는 단계,

<33> - v가 각각의 일시소인수-1을 갖는 소수가 되도록 적어도 두 개의 일시 소인수를 곱함으로써 상기 일시 모듈 n을 생성하는 단계,

<34> - 메시지 m_i에 대해 RSA 서명 표준 포맷 메커니즘의 적용을 통해 일시 공개 값 G를 생성하는 단계($G=Red(m_i)$),

<35> - s.v-1이 각각의 일시소인수-1의 배수가 되도록 개인 지수 s를 결정하는 단계,

<36> - 특히 상기 일시 공개 값 G를 상기 개인 지수 s만큼 제곱하여 모듈로 n함으로써 상기 일시 개인 값 Q_i를 생성하는 단계 및/또는 m개의 일시 개인값 Q_i의 m×f개의 일시 개인 콤포넌트 $Q_{i,j}$를 생성하는 단계.

<37> 상기 일시 인증서는 세션 식별자 데이터 Id에 대한 상기 공개 일시 모듈 n 및 공개 지수 v와 관련된다. 즉, 본 발명의 제2 실시형태의 경우에, 메시지 m_i는 어떠한 특별 보호를 필요로 하지 않는다.

<38> 바람직하게는, 본 발명의 제2 실시형태에서 상기 GQ1 타입 인증 프로토콜은 다음을 실행하는 증명 메커니즘을 포함한다:

<39> ● 상기 공개 일시 모듈 n 또는 상기 m개의 일시 개인 값 Q_1 내지 Q_m,

<40> ● 또는 상기 일시 모듈 $n=p_1\times...\times p_f$의 f개의 일시 소인수 p_1 내지 p_f, m×f개의 일시 개인 컴포넌트 $Q_{1,1}$ 내지 $Q_{f,m}$ 및 일시 차이니즈 나머지(Chinese remainder)의 f-1개의 파라미터.

<41> *제3 실시형태 : GQ2 타입 인증 프로토콜의 경우*

<42> 바람직하게는, 본 발명의 제3 실시형태에 따른 방법은 GQ2 타입 인증 프로토콜의 경우에 수행된다. 이 경우에 상기 공개 일시 모듈 n, 상기 공개 지수 v, m($m\geq 1$)쌍의 일시 공개 값 G 및 일시 개인 값 Q의 생성을 위해, 본

발명의 제3 실시형태에 따른 방법은 다음 단계를 더 포함한다:

<43> - $v=2^k$ 형태의 상기 공개 지수 v의 계산을 가능하게 하는 파라미터 k의 값을 설정하는 단계,

<44> - f개의 일시 소인수의 곱인 공개 일시 모듈 $n(n=p_1\times p_2\times\ldots\times p_f,\ f\geq 2)$을 생성하는 단계,

<45> - 바람직하게는 작은, 특히 100보다 작은 값이며, $G_i=g_i^2$ 형태의 m개의 일시 공개 값 G_i를 정의하는 m개의 일시 베이스 값 g_i를 선택하는 단계,

<46> - 특히 상기 일시 공개 값 G를 상기 개인 지수 s만큼 제곱하여 모듈로 n함으로써 상기 일시 개인 값 Q_i를 생성하는 단계 및/또는 m개의 일시 개인값 Q_i의 m×f개의 일시 개인 콤포넌트 $Q_{i,j}$를 생성하는 단계.

<47> 상기 일시 인증서는 세션 식별자 데이터 Id에 대한 상기 공개 일시 모듈 n과 관련된다. 즉, 상기 숫자 k 및 상기 m개의 베이스 값 g_i는 어떠한 특별 보호를 필요로 하지 않는다.

<48> 바람직하게는, 본 발명에 따른 방법의 제3 실시형태에서 상기 GQ2 타입 인증 프로토콜은 다음을 실행하는 증명 메커니즘을 포함한다:

<49> ● 상기 일시 모듈 n 및 상기 m개의 일시 개인 값 Q_1 내지 Q_m

<50> ● 또는 상기 일시 모듈 $n=p_1\times\ldots\times p_f$의 f개의 일시 소인수 p_1 내지 p_f, m×f개의 일시 개인 컴포넌트 $Q_{1,1}$ 내지 $Q_{f,m}$ 및 일시 차이니즈 나머지의 f-1개의 파라미터.

<51> RSA 타입 로그-온 프로토콜과 관련된 차이니즈 나머지 방법을 사용하는 GQ 타입 인증 프로토콜에서 작은 크기의 일시 공개 값 G 및 일시 개인 값를 실행하는 것은 다음을 가능하게 한다:

<52> ● 작업부하 및 그와 유사하게, 접근하기를 원하는 서버에 의한 사용자의 개인 컴퓨터의 각각의 인증 단계 동안 사용자의 대기 시간을, RSA 타입 프로토콜을 실행하는 경우와 비교할 때 1/100의 비율로 감소시키며,

<53> ● 짧은 시간동안 세션이 지속될 때 작은 크기의 임시 공개 값 G 및 임시 개인 값의 실행에 의해 인증 방법의 보안을 저하시키지 않고서 결과를 얻는다.

<54> 즉,

<55> ● 첫째, 우회(circumvention)에 대한 비슷한 계산 용량에 대해, 상기 GQ 프로토콜은 RSA 프로토콜보다 높은 보안을 제공한다.

<56> ● 둘째, 일시 인증서를 생성하는데 사용되는 RSA 타입, 긴 지속시간, 큰 크기의 개인 서명키가 세션이 지속되는 동안 접근이 용이하지 않다.

<57> ● 마지막으로, 작은 크기의 공개 값 G 및 개인 값의 특징은, 부정한 사람에게 GQ 프로토콜로부터 신뢰성 있는 데이터를 복구하는데 소모되는 시간을 허용하지 않는다.

<58> 본 발명에 따른 방법은 세션이 지속되는 동안 특정 개인 컴퓨터를 사용하는 사용자를 식별하고 여러 서버로부터 상기 개인 컴퓨터를 인증하는데 사용될 수 있다. 상기 사용자가 여러개의 패스워드를 기억할 필요가 없다. 상기 사용자뿐만 아니라 서버의 관리자도 그들의 개인용 컴퓨터 또는 서버에서 큰 계산 자원을 가질 필요가 없다.

<59> **<u>시스템</u>**

<60> 본 발명은 PC와 같은 제1 컴퓨터 장치가 서버와 같은 적어도 하나의 제2 컴퓨터 장치에 의해 인증될 수 있게 하는 시스템에 관한 것이다. 상기 컴퓨터 장치들은 통신 네트워크에 연결되어 있다.

<61> 본 발명에 따른 시스템은 다음의 두 단계를 수행하는 구성요소들 포함한다: 상기 제1 컴퓨터 장치 상에서 세션을 초기화하기 위해 특정 사용자가 로그-온 하는 단계 및 상기 세션을 지속하는 단계.

<62> *Ⅰ. 특정 사용자에 의해 상기 제1 컴퓨터 장치로 로그-온 하는 단계*

<63> 로그-온 단계를 수행하기 위해 상기 제1 컴퓨터 장치는 상기 제1 컴퓨터 상에 설치된 로그-온 소프트웨어 프로그램을 포함한다. 제한된 지속시간의 세션을 위한 상기 제1 컴퓨터 장치로 로그-온할 때, 제어 유닛, 특히 상기 제1 컴퓨터 장치의 키보드의 조작에 의해, 상기 제어 유닛을 통해 개인 식별자 특히 패스워드 및/또는 지문을 제공함으로써 상기 로그-온 소프트웨어 프로그램의 실행이 특정 사용자에 의해 시작된다. 상기 개인 식별자는 상기 특정 사용자의 신원을 확인하고 상기 특정 사용자의 개인 서명키를 호출하게 한다. 상기 제1 컴퓨터 장치는, 특히 상기 특정 사용자를 인식하기 위한 데이터 및/또는 상기 제1 컴퓨터 장치를 식별하기 위한 데이터 및/또는 날짜 및/또는 시간 및/또는 상기 세션 지속시간으로부터 세션 식별자 데이터 Id를 생성하기 위해, 상기 로그-온 소프트웨어에 의해 제어되는 제1 계산 수단을 더 포함한다. 또한, 상기 로그-온 소프트웨어에 의해 제어되는 상기 제1 계산 수단은 공개 일시 모듈 n, 공개 지수 v 및 적어도 한쌍의 일시 공개 값 G를 생성하고, 하기 식 2의 형태의 일반 방정식에 의해 관련된 일시 개인 값 Q를 생성한다.

수학식 2

<64> $G \equiv Q^{v} \pmod{n}$ 또는 $G \times Q^{v} \equiv 1 \pmod{n}$

<65> 또한, 상기 로그-온 소프트웨어에 의해 제어되는 상기 제1 계산 수단은 상기 특정 사용자의 개인 서명키, 상기 세션 식별자 데이터 Id, 상기 공개 일시 모듈 n 및 경우에 따라 상기 공개 지수 v 또는 일시 공개 값 G를 이용하여 서명 시 고유 일시 인증서를 생성한다.

<66> *Ⅱ. 세션을 지속하는 단계*

<67> 상기 로그-온하는 단계 이후 또는 세션의 지속 시간 동안 상기 제1 컴퓨터 장치는 로그-온 소프트웨어의 동작을 중지시키는 중지수단을 더 포함한다.

<68> 상기 제1 컴퓨터 장치는 상기 제1 컴퓨터 장치 상에 설치된 증명 소프트웨어 프로그램을 더 포함한다. 상기 세션이 지속되는 동안, 각각의 상기 제2 컴퓨터 장치에 상기 제1 컴퓨터 장치의 제1 연결이 적어도 지속되는 동안, 컨트롤 유닛, 특히 상기 제1 컴퓨터 장치의 키보드의 조작을 통해, 상기 특정 사용자에 의해 상기 증명 소프트웨어의 실행이 시작된다.

<69> 상기 제1 컴퓨터 장치는, 통신 네트워크를 통해 상기 제2 컴퓨터 장치로 상기 일시 인증서를 배포하고 영지식 인증 메커니즘, 특히 GQ 타입의 실행에 이용되는 증명을 생성하기 위해, 상기 증명 소프트웨어에 의해 제어되는 제1 계산 수단을 더 포함한다. GQ 인증 프로토콜에서 이해되는 바에 따르면 상기 증명 소프트웨어는 증명자의 역할을 한다. 상기 제2 컴퓨터 장치는, 상기 제2 컴퓨터 장치 상에 설치된 검증 소프트웨어 프로그램 및 상기 검증 소프트웨어 프로그램의 실행을 시작하는 시작 수단을 더 포함한다. 상기 제2 컴퓨터 장치는, 상기 개인 서명키에 관련된 공개키를 이용하여 상기 일시 인증서를 개봉하고, 상기 일시 인증서로부터 상기 세션 식별자 데이터 Id 및 상기 공개 일시 모듈 n, 또한 경우에 따라 상기 공개 지수 v 또는 상기 일시 공개 값 G를 추출하기 위해, 상기 검증 소프트웨어 프로그램에 의해 제어되는 제2 계산 수단을 더 포함한다. 상기 증명 소프트웨어 프로그램은 GQ 프로토콜의 검증자의 역할을 한다.

<70> 바람직하게는, 본 발명에 따른 시스템의 일실시형태에서, 상기 특정 사용자의 개인 서명키는 상기 제1 컴퓨터 장치 내에 포함된 암호문 내에 위치한다. 이러한 실시형태에서, 상기 제1 컴퓨터 장치는 상기 특정 사용자의 개인 식별자를 실행할 시 상기 암호문을 해독하기 위해 상기 로그-온 소프트웨어에 의해 제어되는 제1 계산 수단을 더 포함한다.

<71> 바람직하게는, 본 발명에 따른 시스템의 다른 실시형태에서, 상기 특정 사용자의 개인 서명키는 상기 특정 사용자에 의해 사용되는 메모리 카드에 포함된 암호문 내에 위치한다. 이러한 실시형태에서, 본 발명에 따른 시스템은, 상기 제1 컴퓨터 장치에 연결된 메모리 카드 리더를 더 포함하며, 상기 특정 사용자는 상기 메모리 카드를 상기 메모리 카드 리더에 삽입한다. 상기 메모리 카드 리더는 상기 메모리 카드와 제1 컴퓨터 장치 간의 데이터 전송을 위한 수단을 포함한다. 이 경우, 상기 제1 컴퓨터 장치는 상기 특정 사용자의 개인 식별자를 실행할 시 상기 암호문을 해독하기 위해 상기 로그-온 소프트웨어 프로그램에 의해 제어되는 제1 계산 수단을 더 포함한다.

<72> 바람직하게는, 본 발명에 따른 시스템의 또 다른 실시형태에서, 상기 특정 사용자의 개인 서명키는 상기 특정 사용자에 의해 사용되는 메모리 카드 내의 서명 알고리듬으로 정의된다. 이러한 실시형태에서, 본 발명에 따른 시스템은, 상기 제1 컴퓨터 장치에 연결된 메모리 카드 리더를 더 포함하며, 상기 특정 사용자는 상기 메모리 카드를 상기 메모리 카드 리더에 삽입한다. 상기 메모리 카드 리더는 상기 메모리 카드와 제1 컴퓨터 장치 간의

데이터 전송을 위한 수단을 포함한다. 상기 제1 컴퓨터 장치는 상기 개인 서명키를 실행하는 상기 서명 알고리듬을 실행할 때 상기 일시 인증서를 생성하기 위해 상기 로그-온 소프트웨어 프로그램에 의해 제어되는 제1 계산 수단을 더 포함한다.

<73> *제1 실시형태 : GQ0 타입 인증 프로토콜의 경우*

<74> 바람직하게는, 본 발명의 제1 실시형태에 따른 시스템은 GQ0 타입 인증 프로토콜의 경우에 수행된다. 이 경우에 상기 공개 일시 모듈 n, 상기 공개 지수 v, 적어도 한쌍의 일시 공개 값 G 및 일시 개인 값 Q의 생성을 위해, 상기 로그-온 소프트웨어 프로그램에 의해 제어되는 상기 제1 계산 수단은 다음의 수단을 더 포함한다:

<75> - 상기 공개 지수 v의 값을 설정하기 위한 수단,

<76> - 상기 공개 일시 모듈 n을 무작위로 선택하기 위한 수단,

<77> - m개의 일시 개인 값 Q_1 내지 Q_m을 무작위로 선택하기 위한 수단,

<78> - 상기 일반 방정식 중의 하나를 획득하여 상기 일시 공개 값 G를 계산하기 위한 수단,

<79> 상기 일시 인증서는 세션 식별자 데이터 Id에 대한 상기 공개 일시 모듈 n, 공개 지수 v 및 일시 공개 값 G와 관련된다.

<80> 바람직하게는, 본 발명의 제1 실시형태에서 상기 GQ0 타입 인증 프로토콜은 상기 공개 일시 모듈 n 및 상기 m개의 일시 개인 값 Q_1 내지 Q_m을 실행하는 증명 메커니즘을 포함한다.

<81> *제2 실시형태 : GQ1 타입 인증 프로토콜의 경우*

<82> 바람직하게는, 본 발명의 제2 실시형태에 따른 시스템은 GQ1 타입 인증 프로토콜의 경우에 수행된다. 이 경우에 상기 공개 일시 모듈 n, 상기 공개 지수 v, 적어도 한쌍의 일시 공개 값 G 및 일시 개인 값 Q의 생성을 위하여, 상기 로그-온 소프트웨어 프로그램에 의해 제어되는 상기 제1 계산 수단은 다음의 수단을 더 포함한다:

<83> - 상기 공개 지수 v의 값을 설정하기 위한 수단,

<84> - v가 각각의 일시소인수-1을 갖는 소수가 되도록 적어도 두 개의 일시소인수를 곱함으로써 상기 일시 모듈 n을 생성하기 위한 수단,

<85> - 메시지 m_i에 대해 RSA 서명 표준 형식의 포맷 메커니즘의 적용을 통해 일시 공개 값 G를 생성하기 위한 수단 ($G=Red(m_i)$),

<86> - s.v-1이 각각의 일시소인수-1의 배수가 되도록 개인 지수 s를 결정하기 위한 수단,

<87> - 특히 상기 일시 공개 값 G를 상기 개인 지수 s만큼 제곱하여 모듈로 n함으로써 상기 일시 개인 값 Q_i를 생성하는 단계 및/또는 m개의 일시 개인값 Q_i의 m×f개의 일시 개인 콤포넌트 $Q_{i,j}$를 생성하기 위한 수단.

<88> 상기 일시 인증서는 세션 식별자 데이터 Id에 대한 상기 공개 일시 모듈 n 및 공개 지수 v와 관련된다. 즉, 메시지 m_i는 어떠한 특별 보호를 필요로 하지 않는다.

<89> 바람직하게는, 본 발명의 제2 실시형태에서 상기 GQ1 타입 인증 프로토콜은 다음을 실행하는 증명 메커니즘을 포함한다:

<90> ● 상기 공개 일시 모듈 n 및 상기 m개의 일시 개인 값 Q_1 내지 Q_m,

<91> ● 또는 상기 일시 모듈 $n=p_1\times\ldots\times p_f$의 f개의 일시 소인수 p_1 내지 p_f, m×f개의 일시 개인 컴포넌트 $Q_{1,1}$ 내지 $Q_{f,m}$ 및 일시 차이니즈 나머지(Chinese remainder)의 f-1개의 파라미터.

<92> *제3 실시형태 : GQ2 타입 인증 프로토콜의 경우*

<93> 바람직하게는, 본 발명의 제3 실시형태에 따른 시스템은 GQ2 타입 인증 프로토콜의 경우에 수행된다. 이 경우, 공개 일시 모듈 n, 공개 지수 v, 적어도 한 쌍의 일시 공개 값 G 및 일시 개인 값 Q를 생성하기 위해, 상기 로그-온 소프트웨어 프로그램에 의해 제어되는 상기 제1 계산 수단은 다음의 수단을 더 포함한다:

<94> - $v=2^k$ 형태의 상기 공개 지수 v의 계산을 가능하게 하는 파라미터 k의 값을 설정하기 위한 수단,

<95> - f개의 일시 소인수의 곱인 공개 일시 모듈 $n(n=p_1\times p_2\times\ldots\times p_f,\ f\geq 2)$을 생성하기 위한 수단,

<96> - 바람직하게는 작은, 특히 100보다 작은 값이며, $G_i=g_i^2$ 형태의 m개의 일시 공개 값 G_i를 정의하는 m개의 일시 베이스 값 g_i를 선택하기 위한 수단,

<97> - 특히 상기 일시 공개 값 G를 개인 지수 s만큼 제곱하여 모듈로 n함으로써 상기 일시 개인 값 Q_i를 생성하는 수단 및/또는 m개의 일시 개인값 Q_i의 m×f개의 일시 개인 콤포넌트 $Q_{i,j}$를 생성하기 위한 수단.

<98> 상기 일시 인증서는 세션 식별자 데이터 Id에 대한 상기 공개 일시 모듈 n과 관련된다. 즉, 상기 숫자 k 및 상기 m개의 베이스 값 g_i는 어떠한 특별 보호를 필요로 하지 않는다.

<99> 바람직하게는, 본 발명에 따른 시스템의 제3 실시형태에서 상기 GQ2 타입 인증 프로토콜은 다음을 실행하는 증명 메커니즘을 포함한다:

<100> ● 상기 일시 모듈 n 및 상기 m개의 일시 개인 값 Q_1 내지 Q_m

<101> ● 또는 상기 일시 모듈 $n=p_1\times\ldots\times p_f$의 f개의 일시 소인수 p_1 내지 p_f, m×f개의 일시 개인 컴포넌트 $Q_{1,1}$ 내지 $Q_{f,m}$ 및 일시 차이니즈 나머지의 f-1개의 파라미터.

<102> 본 발명의 다른 특징 및 효과는 첨부된 도면 및 본 발명을 한정하지 않는 예시에 의해 이하의 실시예에 대한 설명을 통해 나타날 것이다.

실 시 예

<104> 본 발명은 상기한 바와 같은 서비스 및 그 다양한 개발을 완성한다. 본 발명에 따른 소프트웨어 브릭(brick)은 가상 사설망에 있어서 접근 제어 문제에 대한 새로운 해결책을 제공한다. 상기 모델 및 분석에서 나타난 바와 같이, 상기 작업부하(workloads)는 종래 알려진 방법을 이용한 경우와 비교할 때 100 이상의 비율에 의하여 두 개의 규모로 감소된다. 게다가 상기 작업부하는 균형을 이루게 된다. 즉 증명(proof)을 하는데 요구되는 부하는 검증(verification)을 하기 위한 부하에 가까우며, 따라서 사용자들 사이에 간단한 방법으로 상호 인증을 획득할 수 있도록 한다.

<105> 상기 사용자의 관점에서, 본원 발명은 두 단계로 요약될 수 있다.

<106> (1) 각각의 로그-온 과정에 있어서, 상기 개인 컴퓨터는 다음과 같이 (재)시작하여야 한다:

<107> - GQ 형 영지식 프로토콜을 수반하여 운영하는데 필요한 숫자 및 일시적 모듈의 생성하는 과정,

<108> - 상기 일시적 모듈을 세션 식별 데이터와 연관시키기 위하여 상기 사용자의 개인키, 특히 RSA 개인키를 이용한 일시적인 인증서의 생성 또는 유발하는 과정.

<109> (2) 상기 세션 동안에, 상기 사설망(private network)을 통하여 자원에 각각 접근함에 있어서,

<110> - 일시적 인증 및 GQ 형 영지식 프로토콜에 있어서 상기 일시적 모듈의 분해 지식을 이용하는 과정;

<111> 우선, 다음에 대한 설명이 이루어져야 한다:

<112> - 세션

<113> - 가상 사설망에서 접근 제어에 의하여 발생하는 문제들

<114> - 사용자의 키 쌍(the user's pair of keys) 및

<115> - 대수적 모듈을 제조함에 있어서의 문제점.

<116> 이와 같이 요구되는 설명들은 상기 RSA 와 GQ 영지식 기술을 상기 대응하는 작업부하를 평가하는 것과 비교하여

상기 인증 구조의 분류법(taxonomy)에 의하여 보충된다.

<117> 이와 같은 설명은 이하에서 본 발명을 더욱 상세히 설명할 수 있도록 할 것이다.

<118> **- 세션-** 세션이란 컴퓨터 장치, 예를 들어 개인용 컴퓨터, 개인 오거나이저(organizer), 이동 전화 또는 가입자 텔레비젼 복호기(decoder) 상에서 제한된 시간 동안에 사용자에 의하여 이루어지는 제어를 말한다. 세션은 다음과 같은 다양한 종류의 데이터에 의하여 식별된다:

<119> - 상기 컴퓨터 장치의 식별을 위한 데이터와

<120> - 사용자 식별 데이터와

<121> - 로그-온 날자 및 시간과

<122> - 상기 세션 동안에 계획된 최대 지속시간.

<123> 하나의 컴퓨터 장치가 다수의 사용자를 갖거나 또는 셀프-서비스(self-service)와 같은 토대로 사용하지 못할 이유는 없다; 그러나, 시간상으로 주어진 시점에서는, 상기 컴퓨터 장치는 한 명의 사용자에 의한 배타적인 지배하에 있게 된다: 각각의 컴퓨터 장치 상에서, 상기 세션은 서로 서로 겹침이 없이 차례 차례 잇따라서 일어난다.

<124> 상기 컴퓨터 장치는 다음과 같은 이유 때문에 세션을 종료한다:

<125> - 사용자쪽의 상기 세션을 종료하기 위한 명백한 행동.

<126> - 사용자쪽의 행동이 없음을 감지.

<127> - 상기 세션을 위하여 계획된 최대 지속 시간을 초과.

<128> - 세션을 개방(open)하려는 사용자의 명백한 행동.

<129> **- 가상 사설망에서 접근 제어에 의하여 발생하는 문제들-** 회사망 내에서는 지속적으로 증가하는 양의 접근 제어가 있으며, 이는 문제를 일으키게 된다. 몇 가지 예를 들면 다음과 같다:

<130> - 전문화된 서버가 에이전트(agent)로부터 사용 중지를 요구받은 경우에는, 상기 서버는 각각의 사용자를 확인하여야 하며, 이러한 동작은 일반적으로 개별 패스워드를 이용한 특별한 절차에 의하여 이루어진다. 현재 이러한 종류의 서비스는 통일화가 되지 않은 상태에서 특별한 토대의 진보된 절차를 이용하여 상당히 증가하고 있다. 이러한 서비스들의 높은 증가율은 사용자에게는 실제로 골치거리이다.

<131> - 방랑하는(nomad) 사용자는 전화호(telephone call)를 수신하는 포털 서버(portal server)를 이용하여 회사망에 접근한다: 이러한 식별은 개별 패스워드 및 의사-임의 시간(pseudo-random of time)를 제공하는 SecurId™ 카드와 같은 하드웨어 장치를 이용한 특별 절차에 따라서 이루어진다. 상기 카드는 RSA 시큐러티(RSA Security)사에 의하여 개발되고 상업적으로 배포된 것이다. 명백한 보안상의 이유로, 상기 카드는 다수의 서버 또는 자원 사이에는 공유될 수 없다. 게다가, 이러한 카드의 사용은 전화호가 있는 경우에 사용자에게 상당한 스트레스가 된다.

<132> - 최종적으로, 상기 컴퓨터 장치는 역시 패스워드를 구비하는 초기화 절차에 의하여 다양한 정도로 보호된다; 이러한 절차 중 가장 좋은 절차는 종종 제조자들에 의하여 직접 개발되어진 것이며, 예를 들면 도시바(Toshiba) 개인 컴퓨터를 패스워드로 작동시키는데 사용되는 절차가 있다. 만약 패스워드를 잊었다면, 이러한 패스워드에 의해 보호되는 하드 디스크는 상기 하드 디스크에 저장된 정보를 접근할 수 있는 다른 방법을 갖고 있는 상기 제조자에게 문의함으로써 복구될 수 있다.

<133> 이러한 모든 접근 기술들은 진보되고 있으며 서로에게 유익한 영향을 미친다.

<134> - 공개키 기반구조(infrastructure)는 상기 각각의 사설망 사용자에게 한벌의 개인키 및 공개키가 제공되도록 설정되고 있다.

<135> - 회사의 디렉토리(directory)는 각각의 사용자에게 부여된 권한을 이용하여 상기 공개키를 관리한다.

<136> - 컴퓨터를 동작시킬 때 보안 기능을 제공할 수 있도록 스마트카드가 출시되고 있다. 이러한 카드는 다른 종류의 절차 및 그에 따른 패스워드를 처리할 수 있다. 또한 이러한 카드는 상기 사용자의 개인키 및 상기 개인키의 사용 알고리즘을 한정할 수 있다.

<137> - 패스워드 기술에 대한 보충적인 기술로서 사용자 식별을 위한 생체인식기술(biometrics)이 개발되어지고 있다.

<138> 일련의 관찰이 있어야 한다.

<139> - 위에서 언급한 서비스들의 일부에서는 다음과는 구분되지 않는다.

<140> ·사용자의 식별, 즉 사용자의 패스워드 및/또는 생체인식기술 특성을 테스트하는 동작, 그에 따른 비암호화동작, 및

<141> ·컴퓨터장치의 암호화 인증, 즉 인간의 두뇌가 그 키(key)를 기록 또는 그 알고리즘을 실행할 수 없도록 하는 동작.

<142> - 위에서 언급된 서비스는 특별한 것이다; 상기 패스워드를 풀(pool)로 만드는 것은 불가능하다. 이들을 공개키 하부구조로 통합시킬 수는 없다. 공개키에 기반한 백그라운드(background) 인증을 하는 공통 서비스(common service)가 요구된다.

<143> - 위에서 언급한 서비스는 그 역할이 결정되는 방식으로 추구된다; 상기 개인용 컴퓨터는 상기 서버가 검증하는 증명(proof)을 설정한다. 많은 경우에 있어서, 상기 개인용 컴퓨터는 상기 서버 또는 자원의 인증을 보증할 수 있도록 하는 것이 좋다. 증명 및 검증된 작업부하의 균형을 제시하면서, 상기 공개키의 디렉토리 또는 하부구조에 위치한 개인용 컴퓨터 사이에 상호 인증 기능을 얻을 수 있는 서비스가 필요하다.

<144> - 상기 세션 동안에 상기 개인용 컴퓨터에 존재하는 어떠한 개인키라도 트로이 목마(Trojan horse)에 의하여 가로챔을 당할 위험이 있다; 일시적 개인키의 침해 결과는 매우 제한된다.

<145> - 마지막으로, 비록 상기 사용자가 상기 개인키를 제한하는 칩 카드(chip card)를 갖고 그 공개키가 공개키의 하부구조에 있는 동안에 알고리즘을 사용할지라도, 백그라운드 인증 때문에 상기 사용자의 개인키가 상기 개인용 컴퓨터에서 자유롭게 실행되는 소프트웨어 프로그램에 접근할 수 있도록 하는 것은 좋지 않다. 상기 사용자는 이러한 개인키의 사용에 대하여 배타적인 제어능력을 갖고 있어야만 한다. 상기 칩 카드에 한정되는 경우에도, 상기 세션 동안에 상기 개인용 컴퓨터에 의하여 자유롭게 사용되는 어떤 개인키라도 상기 사용자의 제어능력을 넘어서 그 사용용도로부터 벗어날 수 있는 위험이 있다.

<146> 하나의 관찰이 있어야 한다: 효과적이고 확실한 공캐키 구조(scheme)가 부족하다. 본 발명은 패스워드 및 절차의 곱셈을 확실히 피할 수 있도록 한다: 상기 사용자에게 배타적으로 지역적인 사용을 할 수 있는 독특한 패스워드가 부착된다. 본 발명은 영지식 GQ 기술, 특히 ZK GQ2 기술을 이용하여 상기 사용자의 키 쌍(예를 들면 RSA 키 쌍)을 보완하는 방법을 제안한다. 본 발명은 상기 공개키 하부구조 및 개인키와 알고리즘을 한정하는 스마트 카드의 구현을 보완한다.

<147> **- 사용자의 키 쌍-** 상기 메모리에서는, 각각의 사용자는 공개키 및 개인키(예를 들면 RSA 키 쌍)의 키 쌍을 갖는다.

<148> 상기 사용자 공개키는:

<149> - 자신의 디렉토리를 가지고서 동작 및 관리하는 상기 각각의 컴퓨터 장치를 가지고서 상기 사용자가 접근해야 하는 자원 및 서버에 알려지거나;

<150> - 상기 사용자가 접근해야 하는 자원 및 서버에서 이용 가능한 공개키 하부구조로 통합되어, 전문화된 디렉토리에 의하여 관리된다.

<151> 상기 사용자의 개인키는 디지털 서명을 계산하는데 이용되며 다음과 같이 위치할 수 있다:

<152> - 상기 개인용 컴퓨터에 존재하는 암호문내에 위치하거나, 상기 개인키를 상기 개인용 컴퓨터와 통신하는 저가의 대중용(down-market) 스마트카드에 위치할 수 있다; 상기 컴퓨터는 상기 사용자의 패스워드를 이용하여 상기 암호문을 해독한다; 이와 같은 방법으로 상기 사용자의 패스워드를 획득하고, 그 다음에는 상기 서명 알고리즘을 실행하며, 이후 해독 및 사용된 개인키를 그 메모리로부터 삭제한다,

<153> - 또는 상기 사용자의 패스워드가 제시되는지 여부에 따라 실행되는 서명 알고리즘에 한정되는, 고가의 스마트 카드에 위치할 수 있다.

<154> **- 상기 모듈의 인수분해 및 크기의 문제-** 다양한 인증 구조들이 다음과 같은 인수분해의 문제를 이용한다: "-공

개 모듈 n은 적어도 두 개의 큰 암호 소수(prime number)의 생산물이다, 즉: $p_1 \leq ... p_f$ (f>1), 이들 중 적어도 두 개는 서로 다르며, p1<pf이고, 따라서: $n=p_1 \times ... p_f$"이다. 상기 사용자의 키 쌍은 몇 년 동안은 유지되어야 한다; 이것을 장기 키(long-term key)라고 칭한다. 만약 상기 사용자의 키 쌍이 상기 RSA 형이라면, 상기 키 쌍은 인수분해가 몇 년 동안 남아있어야 하는 공개 모듈을 포함한다. 장기 모듈(long-term module) 동안에 다음의 결과에 대한 참조가 이루어 질 수 있다. 현재 상기 512 비트의 수를 1년 이내에 인수분해할 수 있으나, 이경우 상당한 자원이 필요하다. 인수분해 방법에서는 160 비트까지의 인수를 찾는다. 상기 모듈의 크기는 512비트보다 커야 한다(예를 들면 4년 동안 768비트 및 8년 동안 1024 또는 1536 비트). 안전성의 한계가 요구된다. 오늘날 각각의 장기 RSA 모듈은 두 요소의 생산물이다; 그러나, 3개 요소 또는 더 많은 요소를 이용하는 것이 쉬울 수 있으나, 이는 현재 RSA 적용의 관행이 아니다.

<155> 한 쌍의 일시적 키는 몇 시간 동안, 즉 최소한 일 근로일(one working day) 동안 지속되어야 한다; 이것을 단기 키(short-term key)라고 칭한다. 본 발명은 인수분해가 몇시간 동안 비밀로 유지되어야 하는 공개 모듈에 기반한 일시적 키 쌍을 고려한다. 상기 단기 모듈 동안에, 420-비트 및 세 개의 140-비트의 소수가 현재 적당하다; 또한 640-비트 크기 및 160-비트 인수를 구상하는 것이 가능하다. 상기 단기 모듈의 크기를 개발하는 것은 인수분해 수행 능력의 개발을 고려함에 있어서 조절되어야 하는 매개변수(parameter)이다; 이는 매일 변할 수 있는 매개변수이며 시스템 설계시 고려하여야 한다.

<156> 요약하면, 일시적 모듈은 장기 모듈보다 두 배 또는 네 배 짧을 수 있다.

<157> 공개 모듈은 항상 공개 지수(exponent)와 함께 사용된다. 상기 공개 지수의 특성은 고려하는 구조(scheme)에 따라 다르다.

<158> - 상기 RSA 구조는 공개 지수로서 홀수(odd number)를 사용하고, 일반적으로는 소수(prime) 특히 v=3 및 $v=2^{16}+1$을 사용한다.

<159> - 상기 ZK GQ1 구조는 상기 RSA 서명, 특히 $v=2^{16}+1$에 의존한다. 여기서 요구되는 것은 RSA 서명에 대한 지식을 누설하지 않으면서도 이를 증명하는 것이다.

<160> - 상기 라빈 서명(Rabin signature)은 공개 지수 2(v=2)를 사용한다.

<161> - 상기 ZK GQ2 구조는 공개 지수로서 2보다 큰 2의 지수(즉, $V=2^k$, k>1)를 사용한다. 여기서 요구되는 것은 누설하지 않으면서도 상기 모듈 분해(decomposition)의 지식을 증명하는 것이다.

<162> **-인증 구조의 분류 및 작업부하의 평가-** 인증 구조는 상기 두 개의 엔티티(entity)를 작동시킨다. 하나의 엔티티는 정보와 관련된 증명을 생성한다. 다른 엔티티는 정보와 관련된 상기 증명을 검증한다. 한마디로, 상기 검증을 수행하는 엔티티는 상기 증명자(prover)가 실제로 같은 정보를 말하고 있는지 여부를 검증한다. 이는 완전성을 위협하는 침해자에 의해 야기되는 위험을 피하기 위한 순서이다. 상기 정당한 증명자의 동작과 위조행위를 하려는 침해자의 동작은 서로 구분 되어야 한다. 상기 침해자는 위조 행위를 통하여 상기 증명자의 모든 비밀에 대한 아무런 사전 지식을 갖지 않고서 상기 검증자(verifier)를 교란하려고 한다. 명백히 상기 증명자는 적어도 그 개인키를 보호하고 이를 비밀로 유지해야 한다.

<163> **정적 인증-** 상호작용이 없는 인증 구조에서는, 상기 증명자는 식별 데이터를 상기 검증자에 보낸다; 이와 관련된 증명은 이러한 데이터의 디지털 서명이다. 상기 증명자는 공개 검증키를 상기 디지털 서명에 적용한다. 통신 인터페이스는 상기와 같은 데이터 및 각각의 인증에 있어서 통과되는 상기 동일한 서명을 감지한다. 그리면 이러한 인증을 정적(static)이라고 한다.

<164> 정적 인증이 상기 카드의 시각적 관찰을 강화함에 있어서 국부적으로 유용한 반면에, 종종 인터넷과 같은 네트워크를 통한 먼 거리에서는 유용하지 못하다.

<165> **RSA를 이용한 정적인증의 예-** 다음의 구조는 1984년부터 프랑스 은행 카드(French bank card)에 사용되고 있다; 또한 이는 유로페이(Europay), 마스터카드(Mastercard) 및 비자(Visa)와 같은 신용 카드 운용자들에 의하여 1996년 공개되어진 국제 사양에도 들어 있고, EMV '96이라 불려진다. ISO/CEI 9796 및 14888 표준 시리즈는 예시적인 디지털 서명 구조(특히 상기 RSA 형)를 제공한다.

<166> - 상기 카드-발급 엔티티는 RSA 키 쌍을 갖는다.

<167> ○ 개인 서명키는 상기 카드 발급 엔티티의 비밀이다. 상기 개인 서명키는 개인 서명 지수 s 및 공개 모듈 n을 갖는다.

<168> ○ 각각의 지불 단말(payment terminal)은 상기 공개 입증키를 인지한다. 상기 지불 단말은 공개 입증 지수 v 및 공개 모듈 n을 포함한다.

<169> - 일대일맞춤(customization)(이 용어는 이하에서 카드의 발급에 관한 것으로 사용됨) 동안에, 각각의 카드는 식별 데이터 및 상기 데이터의 RSA 서명을 수신한다. 상기 사용되는 RSA 서명 표준은 상기 식별 데이터, 즉 Id에 의하여 대표되는 바이트의 문자열을 다수의 정수 고리(ring) 모듈로n으로 변환하며, J=Red(Id)를 제공하는 형태 메카니즘인 Red()를 갖는다. 이러한 데이터의 RSA 서명은 정수 고리수 S 모듈로n 이다; 이러한 S라는 숫자는 상기 개인 서명키를 J라는 수에 적용함으로써 획득되며, $S \equiv J^{S} \pmod{n}$를 제공한다.

<170> - 각각의 지불 동작 동안에, 상기 단말은 상기 카드 식별 데이터 Id 및 상기 공개 입증키를 이용하여 입증되는 그 서명 S에 대한 지식을 얻는다. 이러한 인증은 상기 Red(Id) 숫자가 $S^{v} \pmod{n}$의 숫자와 일치하는지 여부에 따라 성공하거나 실패한다.

<171> ⇒그리고나서 증명은 상기 RSA 순열(permutation)에 따른다.

<172> 상기 검증자는 상기 공개 검증키를 상기 서명에 적용한다. 즉, 상기 검증자는 상기 숫자 S를 v제곱 모듈로n까지 증가시킨다. 이러한 동작을 수행하기 위하여 상기 검증자는 상기 지수 v를 이진수 모드로 기록하고 최상위비트(the most significant bit)에 이어지는 비트로부터 최하위비트(the least significant bit)까지 연속적인 비트들을 검사한다. S와 동일한 변수로부터, 각각의 비트에서, 상기 검증자는 상기 변수를 스퀘어 모듈로n(square module n)까지 증가시킨다. 그리고나서, 만약 상기 비트가 1과 동일하면, 상기 입증기는 상기 변수를 S 모듈로n으로 곱한다. 모든 비트가 고려된 때는, 상기 변수의 값이 찾고자 하는 결과인 $S^{v} \pmod{n}$이다.

<173> 따라서 상기 검증자의 작업부하는 공개 입증 지수 v에 의존한다. 스퀘어 모듈로는 승산 모듈로의 약 3/4를 대표한다는 점을 주목해야 한다.

<174> 즉, $XM_n \approx 0.75\ MM_n$

<175> - v=3(즉 이진수 모드로는 11)에 대하여, 상기 검증자는 스퀘어 모듈로n을 실행하고 이어서 승산 모듈로n이 뒤따른다.

<176> 즉, $1\ XM_n + 1\ MM_n \approx 1.75\ MM_n$

<177> - $V=2^{16}+1$(즉 이진수 모드로는 1 0000 0000 0000 0001)에 대하여, 상기 검증자는 16스퀘어 모듈로n을 실행하고 이어서 승산 모듈로n이 뒤따른다.

<178> - 즉, $16\ XM_n + 1\ MM_n \approx 13\ MM_n$

<179> **동적 인증-** 상호작용을 하는 인증 구조에서는, 상기 증명자와 상기 검증자 사이에 대화가 설정된다; 각각의 엔티티는 교대로 전송기 및 수신기가 되는데, 이는 실시간 증명, 즉 반복될 수 없는 증명을 획득하기 위한 것이다. 다음의 두 개의 예에 있어서, 상기 검증자는 임으로 얻어지는 요구를 발급하게 되며, 따라서 예측불가능하다; 상기 요구의 특성은 그럼에도 불구하고 더블릿(doublet) 인증과 트리플릿(triplet) 인증 사이에 상당히 다르다는 것을 알게 될 것이다.

<180> **동적 더블릿 인증-** 2개의 전송으로, 상기 검증자는 임의로 생성된 요구를 발급한다: 그리고나서, 상기 증명자는 응답을 발생한다: 최종적으로, 상기 검증자는 상기 응답이 상기 요구에 진실로 적당하다는 것을 확인한다. 각각의 요구는 고유한 것이어야 한다. 이는 만약 상기 발생 가능한 요구가 상당히 많은 수를 갖는 경우에는 통계적으로 보장되는 것이다.

<181> 상기 증명자가 상기 메시지를 인지하는 것을 보장하기 위하여, 상기 응답은 상기 요구 및 인증될 메시지에 의존하여야 한다; 그리고나서 상기 검증자는 상기 응답이 진실로 상기 요구 및 상기 메시지에 적당하다는 것을 확인한다.

<182> 관찰이 있어야 한다.

<183> - 상기 증명은 디지털 서명이 될 수 있다. 그러나, 상기 디지털 서명에 대하여 요구되는 제한이 이러한 프로토콜(protocol)에 있어서는 충분한 반면에, 그 역을 성립하지 않는다. 이러한 프로토콜은 다음의 ZK 더블릿 인증에서 설명하는 바와 같이 상기 디지털 서명보다 훨씬 적을 제한은 갖는다.

<184> **RSA를 이용한 동적 인증 예-** 각각의 증명은 RSA 및 더블릿(doublet)의 두 숫자를 갖는다: 상기 두 숫자는 Red(요구, 메시지) 및 그 응답으로 전송된 숫자이다. 그리고 상기 증명의 집합(set)은 상기 RSA 순열의 부분 집합(subset)이다. 상기 증명자는 상기 검증자가 검증하여야 하는 RSA 서명을 계산한다.

<185> - 상기 모듈로n을 분해하지 않고서, 즉 상기 소인수(prime factor)를 사용하지 않고서, 상기 증명자는 숫자를 s 제곱의 모듈로 n으로 증가시킨다, 즉 평균적으로 한 번 걸러서 승산 모듈로n으로 분할되는, $\log_2 n$ 스퀘어 모듈로n을 실행한다.

<186> 즉, $(\log_2 n)XM_n+0.5(\log_2 n)MM_n \approx 5/4\ \log_2 nMM_n$ 이다.

<187> - 상기 소인수 및 상기 차이니즈 나머지를 사용함에 있어서, 상기 증명자는 다음을 실행한다;

<188> ○ 우선 상기 정수 고리 요소의 모듈로n의 숫자를 상기 고리를 형성하는 각각의 갈로이스(Galois) 필드(field)의 숫자인 f 요소로 분해한다.

<189> ○ 이후에 각각의 필드에서, 승산 모듈로 p에 의하여 평균적으로 한 벌 걸러 분할되는 $\log_2 p$ 스퀘어 모듈로p 내부의 서명 요소를 실행한다;

<190> 즉, $f(\log_2 p)XM_p+f/2(\log_2 p)MM_p \approx 1.25\log_2 nMM_p$ 이다.

<191> 실제 상기 인자(factor)들은 대략 같은 크기를 갖는다. 따라서, 각각의 p는 n보다 f배 짧으며, $p^f \approx n$, 즉 $f\log_2 p \approx \log_2 n$이다.

<192> ○ 그리고, 최종적으로 각각의 갈로이스 필드 내부의 하나인, f 요소들로부터 정수 고리 모듈로n의 내부에서 서명을 설정하기 위한 차이니즈 나머지 동작을 실행한다.

<193> 상기 모듈의 길이를 f로 승산하는 것은 상기 승산 모듈로의 부하를 f^2 으로 승산하는 것과 같다, 즉 $MM_p \approx MM_n/f^2$ 이다. 이와 같은 규칙은 상기 부하를 다음과 같이 평가되도록 한다.

<194> 즉, $분해_f + (5/4\log_2 nMM_n)/f^2 + CRT_f$ 이다.

<195> **동적 트리플릿 인증-** 3개의 전송으로, 제로-지식 인증이 수행된다. 즉, 비밀을 아는 것외에는 아무것도 누설함이 없이 인증이 수행되는 것을 말한다; 상기 증명자는 임의값을 설정하는 것으로부터 시작하여, 이후에는 계산 및 서약(commitment)을 발급하며, 그리고나서 상기 검증자는 임의로 생산되는 요구를 발급한다; 그러면 상기 증명자는 상기 임의값의 함수로서 응답과, 비밀과, 요구를 보낸다; 최종적으로는, 상기 검증자는 상기 응답 및 요구로부터 서약을 재설정한다; 만약 두개의 서약이 동일하고 영(zero)이 아니라면 상기 인증은 성공한 것이다.

<196> 상기 대화과정은 서로 독립적이므로, 각각의 요구는 다시 발생할 수 있다; 이는 오직 예측 불가능한 것이다; 결과적으로, 발생 가능한 요구의 수는 2개로 감소될 수 있다.

<197> 2개의 관찰이 만들어져야 한다.

<198> - 3개의 영지식 전송으로, 상기 상기 증명자가 상기 메시지를 인지하는 것을 보장할 수 있다; 상기 서약을 전송하는 대신에, 상기 증명자는 상기 서약 및 상기 인증될 메시지의 해쉬 코드(hash code)를 계산하며 전송한다; 상기 검증자는 상기 응답 및 요구로부터 서약을 재설정한다; 만약 두 개의 해쉬 코드들이 영이 아닌 재설정 서약에 대하여 서로 동일하다면 상기 인증은 성공이다. 그러나, 상기 트리플렛(triplet)은 항상 상기 프로토콜의 핵심에 있다.

<199> - 상기 검증자는 상기 검사에 대한 주도권을 갖으며, 이는 "요구 서명(challenge commitment)"을 발급함으로써 실행하게 되고, 이는 상기 두개의 임의값, 즉 증명을 하는 증명자의 임의값과 검증을 하는 검증자의 임의값을

끌어내도록 한다. 그러나, 상기 트리플렛(triplet)은 항상 상기 프로토콜의 핵심에 있다.

<200> **ZK GQ1을 이용한 동적 트리플릿 인증예-** $v=2^{16}+1$을 이용하여 RSA 서명의 지식을 증명하기 위하여, 상기 증명자는 ZK GQ1 트리플렛을 계산한다.

<201> - 상기 모듈n의 분해를 이용하지 않고서, 즉 소인수를 사용하지 않고서 상기 증명자는 다음을 계산한다.

<202> ○ 우선 16 스퀘어 모듈로n에서 서약 $r^{v}(\text{mod } n)$을 계산하고, 이후에 승산 모듈로n을 계산한다,

<203> ○ 그리고나서, 평균 8 승산 모듈로n상에서 15스퀘어 모듈로n에서 응답 $r\times Q^{d}(\text{mod } n)$을 계산하며, 이후 승산 모듈로n을 계산한다.

<204> 즉, $31XM_n+10MM_n \approx 33.25MM_n$ 이다.

<205> - 상기 소인수 및 상기 차이니즈 나머지를 이용하여, 상기 증명자는 다음을 계산한다.

<206> ○ 16 스퀘어 모듈로p와 하나의 승산 모듈로p에서, 각각의 인자마다 하나의 서약 요소 $r_j\times Q_j^{d}(\text{mod } p_j)$를 계산하고, 이후에 서약 모듈로n을 설정하기 위하여 차이니지 나머지 동작을 계산한다,

<207> ○ 평균 8 승산 모듈로p 및 승산 모듈로p 상에서, 15 스퀘어 모듈로p에서, 각각의 인자마다 하나의 응답 요소 $r_j\times Q_j^{d}(\text{mod } p_j)$를 계산하고, 이후에 응답 모듈로 n을 설정하기 위하여 차이니즈 나머지 동작을 계산한다.

<208> 즉, $(31\ XM_n + 10\ MM_n \approx 33.25\ MM_n)/f + 2CRT_f$ 이다.

<209> - 상기 검증자는 평균 8 승산 모듈로n 상에서, 16 스퀘어 모듈로n에서 서약 $G^{d}\times D^{v}(\text{mod } n)$을 재설정하고, 이후에 승산 모듈로n을 설정한다.

<210> 즉, $16\ XM_n + 9\ MM_n \approx 21\ MM_n$ 이다.

<211> 각각의 증명은 3개의 숫자를 포함한다: 서약(commitment), 요구(challenge) 그리고 응답(response). 상기 서약 및 응답은 두개의 n 보다 크로 영이 아닌 수 R 및 D 이다. 상기 요구는 d 이고 0 부터 v-1 사이의 값을 갖는다. 이들이 함께 ZK GQ1 트리플렛을 형성한다. ZK GQ1 트리플렛의 집합은 정수 고리 모듈로n의 v 순열의 집합체(family)를 구성한다. 상기 영(zero) 요구는 상기 RSA 순열에 대응한다.

<212> **ZK GQ2를 이용한 동적 트리플릿 인증예-** 상기 모듈로n의 분해에 대한 지식을 증명하기 위해, 상기 증명자는 ZK GQ2 트리플렛을 계산한다.

<213> - 상기 모듈로n의 분해를 이용하지 않고서, 즉 상기 소인수를 이용하지 않고서, 상기 증명자는 k 스퀘어 모듈로n에서 서약을 계산한다. 상기 증명자는 평균 (k-1의 m 배)/2 승산 모듈로2상에서, k-2 스퀘어 모듈로n에서의 응답을 계산하고, 이후에 승산 모듈로 n을 계산한다.

<214> 즉, $kXM_n + (k-2)XM_n + m(k-2)/2MM_n + MM_n \approx (m+3)(k-1)/2MM_n$ 이다.

<215> - 상기 소인수 및 상기 차이니즈 나머지를 이용하여, 상기 증명자는 다음을 계산하다.

<216> ○ k 스퀘어 모듈로 p에서, 각각의 인자마다 하나의 서약 요소를 계산하고, 이후에 서약 모듈로n을 설정하기 위한 차이니즈 나머지 동작을 계산한다.

<217> ○ 평균 (k-1의 m배)/2 승산 모듈로 p 상에서 k-2 스퀘어 모듈로 p 인자 마다 하나의 응답 요소를 계산하고, 이후에 승산 모듈로 p를 계산하며, 그리고 나서 응답 모듈로n을 설정하기 위하여 차이니지 나머지 동작을 계산하다.

<218> 즉, $((m+3)(k-1)/2MM_n)/f+CRT_f$ 이다.

<219> - 상기 검증자는 인증서(certificate)를 개방한다. 그리고나서 상기 검증자는 k 스퀘어 모듈로 n에서 서약을 재설정한다. 실제로, 베이스 값(base number)를 이용한 상기 승산 또는 제산(divisions)은 무시할 수 있다.

<220> 즉, 인증서 + kXM_n ≈ 인증서 + $0.75kMM_n$ 이다.

<221> 각각의 증명은 3개의 숫자를 포함한다: 서약, 요구 그리고 응답. 상기 서약 및 상기 응답은 영보다 큰 두 개의 영이 아닌 수 R과 D이다. 상기 요구 d 는 k-1에 m을 곱한 만큼의 비트로 구성되는 숫자이다. 이들은 ZK GQ2 트리플렛을 형성한다.

<222> **ZK GQ2 420 비트를 이용한 RSA 1024 비트의 비교-** RSA 키 쌍의 실제적인 예에서는 두개의 인자를 갖는 1024-비트 모듈을 사용한다. RSA는 현재 두개의 인자 보다 많은 인자를 갖도록 사용되지는 않고 있으나, 이렇게 해야만 할 이유가 있는 것은 아니다. 다음은 작업부하이다.

<223> - RSA 서명의 생성은 다음을 대표한다.

<224> ○ CRT가 없는 1280 MM_{1024}

<225> ○ CRT(f=2)인 경우의 324 MM_{1024}

<226> - RSA 서명의 입증은 다음을 대표한다.

<227> ○ v=3 인 경우의 1.75 MM_{1024}

<228> ○ $v=2^{16}+1$ 인 경우의 13 MM_{1024}

<229> 한 쌍의 ZK GQ2 키의 실제적인 예는 두 개의 베이스 값 및 k=9를 갖는 3개의 140-비트 인자의 420-비트 모듈을 이용한다.

<230> - 트리플릿 ZK GQ2의 생성은 다음을 대표한다.

<231> ○ CRT를 갖는 $11.25MM_{420}$, 즉 $1.89MM_{1024}$.

<232> - 트리플릿 ZK GQ2의 입증은 다음을 대표한다.

<233> ○ CRT를 갖는 $6.75MM_{420}$, 즉 $1.14MM_{1024}$.

<234> - 1024-비트 인증서의 개방은 다음을 대표한다.

<235> ○ 스퀘어(라빈 서명)에 대한 $0.75MM_{1024}$.

<236> ○ 큐브(cube)(RSA 서명)에 대한 $1.75MM_{1024}$.

<237> 이와 같은 설명들은 사용자 RSA 개인키를 구현함에 따른 작업부하와 상기 ZK GQ2 기술에서의 일시적 모듈을 구현함에 따른 작업부하 사이의 두 개 규모(magnitude)의 이득(gain)을 보여준다. 이와 같은 실행상의 차이는 기술적인 균열을 나타낸다. 본 발명에 따르면 종래의 시스템과 비교하여 사용자에게 경제적인 만족과 향상된 보안성을 제공한다.

<238> **제로-지식 인증의 다른 방법-** "더 많은 것을 할 수 있는 자는 더 적게 할 수 있다." 영지식 기술은 더블릿 동적 인증 및 메시지 서명까지도 가능하게 한다.

<239> **ZK GQ 더블릿 동적 인증의 예-** 상기 검증자는 수십 비트, 예를 들면 32 엔트로피 비트(entropy bits)를 포함하는 요구를 발급한다.

<240> 상기 증명자는 이후에 하나 또는 그 이상의 ZK GQ 트리플렛과 상기 검증자의 요구 및 인증할 메시지를 계산한다. 여기서 ZK 요구는 상기 해쉬 코드 또는 상기 서약으로부터 오는 것이다. 모든 ZK 요구의 엔트로피는 상기 검증자의 요구에 대한 엔트로피와 같거나 더 크며, 예를 들면 32비트의 검증자 요구에 대한 48비트의 ZK 요구와 같다. 상기 증명은 상기 ZK GQ 트리플렛 또는 복수의 트리플렛 또는 이러한 복수의 트리플렛들의 적절한 부집합을 포함한다.

<241> - 즉, 상기 요구가 있은 후의 상기 서약 및 상기 응답은 용이하게 재설정되며,

<242> - 또는 더욱 유리하게는, 상기 서약이 있은 후의 상기 요구 및 상기 응답은 용이하게 재설정된다.

<243> ZK GQ1 증명의 실제적인 예는 $v=2^{16}+1$을 갖는 3개의 트리플렛 또는 더욱 유리하게는, $2^{48}-65$를 갖는 단일 트리플렛이다. ZK GQ2를 이용한 다른 실제적인 예에서는 두개의 베이스 값를 갖는 세개의 인자 모듈을 이용한다: 상기 증명은 k=9에 대한 세개의 트리플렛 및 k=25에 대한 오직 하나의 트리플렛을 포함한다.

<244> **ZK GQ 서명의 예-** 상기 증명자는 이후에 하나 또는 그 이상의 ZK GQ 트리플렛과 상기 검증자의 요구 및 인증할 메시지를 계산한다. 여기서 ZK 요구는 상기 해쉬 코드 또는 상기 서약으로부터 오는 것이다. 상기 ZK 요구의 크기는 예를 들어 64비트 또는 80 비트와 같이 충분히 커야 한다. 상기 증명은 상기 ZK GQ 트리플렛 도는 복수의 트리플렛 또는 이러한 복수의 트리플렛의 적절한 부집합을 포함한다.

<245> - 즉, 상기 요구가 있은 후의 상기 서약 및 상기 응답은 용이하게 재설정되며,

<246> - 또는 더욱 유리하게는, 상기 서약이 있은 후의 상기 요구 및 상기 응답은 용이하게 재설정된다.

<247> ZK GQ1 증명의 실제적인 예는 $v=2^{16}+1$을 갖는 3개의 트리플렛 또는 더욱 유리하게는, $2^{64}-257$을 갖는 단일 트리플렛이다. ZK GQ2를 이용한 다른 실제적인 예에서는 두개의 베이스 값를 갖는 세개의 인자 모듈을 이용한다: 상기 증명은 k=9에 대한 세개의 트리플렛 및 k=25에 대한 오직 하나의 트리플렛을 포함한다.

<248> **- 각각의 로그-온 동작에서,** 상기 컴퓨터 장치는 다음의 특성(상기 동작의 순서는 중요하지 않다)을 갖는 초기화 소프트웨어 프로그램을 실행한다.

<249> - 상기 세션이 초기화되는 동안에 식별 데이터를 생성하며, 이 데이터는 Id로 표시된다.

<250> - 공개 일시 모듈n을 생성하고, 공개 지수 v는 2 및 최소한 한 쌍의 GQ 수보다 크며, 예를 들면 $m \geq 1$과 같다. 각각의 쌍은 공개 숫자 G 와 일반 등식 GQ와 관련되 개인 숫자 Q를 포함한다.

<251> 정등식(direct equation): $G \equiv Q^{v} \pmod{n}$,

<252> 또는 역등식(inverse equation): $G \times Q^{v} \equiv \pmod{n}$ 이다.

<253> - 상기 세션 동안에 상기 일시 모듈과 상기 세션 식별 데이터를 연관시킬 목적으로 상기 사용자의 개인키의 제어하에서 상기 서명을 생성 또는 생성 유발하기 위하여, 고유한 국부 절차, 예를 들면 생체인식기술 등에 의하여 구현가능한 상기 사용자의 고유한 패스워드를 이용하여 상기 사용자를 식별한다. 이와 같은 서명은 일시적인 인증서이다.

<254> 상기 사용된 GQ0, GQ1 또는 GQ2와 같은 GQ 방법에 따라서, 상기 일시적 모듈과, 상기 지수 및 상기 공개 숫자뿐만 아니라 상기 인증서의 구조를 생성함에 있어서 특별한 제한이 적용된다.

<255> **첫 번째 방법(GQ0)에서는,** 공개 지수v는 고정되며 공개 모듈n 및 m 공개 숫자 Q_i는 임의로 선택된다. 이러한 경우에, 상기 일시적 개인키는 상기 모듈로n 및 상기 m 개인 숫자(Q_1 부터 Q_m)에 의해 대표되어야 한다; 상기 일시적 인증서는 상기 세션 식별 데이터를 상기 공개 숫자n,v,G_1,...G_m과 관련시킨다.

<256> **두 번째 방법(GQ1)에서는,** 상기 증명자는 RSA 서명에 대한 지식을 노출시키지 않고서 증명하여야 하며, 상기 검증자는 RSA 서명에 대한 지식이 없이 이 RSA를 검증하여야 한다. 그리고 나서 모든 메시지를 숫자로 표시되도록 변환하여 RSA 서명 표준을 포맷 메카니즘(format mechanism)과 함께 이용하여야 한다; 일반적으로 이러한 메카니즘은 해쉬 함수(hash function)를 이용한다. 모든 RSA 입증키는 공개 지수v 및 공개 모듈 n을 갖으며, 이는 v가 p_1-1 및 p_2-1을 갖는 인수가 되도록 두개의 크고, 구별되는 비밀 소인수 p_1 및 p_2 의 생성물이다. 이와 같은 경우에, 각각의 공개 숫자 G_i는 상기 서명 표준의 포맷 메카니즘의 적용함으로써 얻어진다; 즉: G_i = Red(메시지$_i$)이다; 상기 모듈 n 및 상기 m 개인 숫자(Q_1 부터 Q_m)까지에 의한 대표에 부가하여, 상기 일시적 개인키는 다시 f 소인수(p_1 부터 p_f), m×f 개인 요소($Q_{1,1}$ 부터 $Q_{f,m}$) 및 상기 차이니지 나머지인 f-1 변수에 의하여 유리하게 대표될 수 있다; 상기 일시적 인증서는 상기 세션 식별 데이터를 상기 두 개의 수 n 및 v에 관련시킨다; 실제로, 메시지$_1$부터 메시지$_m$는 어떠한 특별 보호도 필요하지 않다.

<257> **세 번째 방법(GQ2)에서는,** 상기 증명자는 상기 모듈 분해의 지식을 노출시키지 않고서 보여주며, 상기 검증자는 사전 지식이 없이 상기 모듈의 분해를 입증한다. 상기 모듈n은 최소한 두 개의 큰 소인수의 생성물이고, 상기 소인수 중 최소한 두 개는 서로 구별되며, 예를 들면 $f \geq 2$, $p_1 \leq p_2 \ldots \leq p_f$, $p_1 \leq p_f$ 이며 $n = p_1 \times p_2 \ldots \times p_f$; 상기

공개 지수v는 2 보다 2가 큰 거듭제곱이며, 예를 들면 $v=2^k$ ($k\geq 2$)이다; $m\geq 1$ 인 공개 숫자는 모두 작은 스퀘어(small square), 즉 $G^i=g_i^2$ 이다. 상기 g_1 부터 g_m 까지의 숫자는 베이스 값이다. 이러한 경우에 있어서, 상기 모듈로 n 및 상기 m 개인 숫자(Q_1 부터 Q_m)에 부가하여, 상기 일시적 개인키는 다시 f 소인수(p_1 부터 p_f), $m\times f$ 개인 요소($Q_{1,1}$ 부터 $Q_{f,m}$) 및 상기 차이니지 나머지인 f-1 변수에 의하여 유리하게 대표될 수 있다; 상기 일시적 인증서는 상기 세션을 상기 숫자 n에 관련시킨다; 실제로, 상기 매우 작은 숫자 k 및 g_1부터 g_m은 어떠한 특별 보호도 필요하지 않다.

<258> **- 상기 세션 동안에,** 상기 컴퓨터 장치는 자원에 접근할 수 있도록 하는 장치(예를 들어 접근 포탈) 또는 자원을 구성하는 장치(예를 들어 프린터 또는 저장 서버)와 대화한다.

<259> - 상기 컴퓨터 장치는 다음의 특성을 갖는 증명 소프트웨어 프로그램을 실행한다.

<260> ○ 상기 증명 소프트웨어 프로그램은 상기 사용자의 개인키를 모른다.

<261> ○ 상기 증명 소프트웨어 프로그램은 상기 사용자의 공개키(여기서 상기 공개키는 공개키의 디렉토리 내부에 있다)를 알고 있는 자 모두에 대하여 Id 및 n을 설정하는 것을 가능하도록 하는 일시적 인증서를 분배한다.

<262> ○ 상기 증명 소프트웨어 프로그램은 증명을 구성하는 ZK GQ 트리플렛을 설립하기 위하여 ZK GQ의 역할을 수행한다.

<263> - 각각의 자원은 다음의 특성을 갖는 입증 소프트웨어 프로그램을 실행한다.

<264> ○ 상기 입증 소프트웨어 프로그램은 상기 사용자의 공개키를 인지하고 있거나 혼자서 확실한 방법으로 상기 키를 획득할 수 있다. 상기 입증 소프트웨어 프로그램은 이것을 상기 인증서를 "개방(open)"하는데 사용하며, 이와 같이 하여 상기 세션 식별 데이터와 일시적 모듈 및 필요한 경우에는 지수 및 공개 숫자를 설정한다.

<265> ○ 상기 입증 소프트웨어 프로그램은 증명을 입증하기 위하여 ZK GQ의 역할을 수행한다.

<266> 공개키의 지식을 얻기 위한 디렉토리에 접근하기 위한 수단이 있다면, 입증 소프트웨어 프로그램을 갖는 컴퓨터 장치는 상기 디렉토리 내부에서 어떠한 사용자에 의하더라도 로그-온된 세션을 절대적으로 인증할 수 있다는 것을 관찰하여야 한다.

<267> 본 발명에 따른 시스템은 제1 컴퓨터 장치(1)가 하나 이상의 제2 컴퓨터 장치(2)에 의해 인증 받도록 한다. 본질적으로 알려진 방법으로, 통신 네트워크(3)를 통해 사용자(5)가 그의 제1 컴퓨터 장치(1)를 제2 컴퓨터 장치(2)에 연결시킨다.

<268> 로그-온 단계

<269> 이하, 인증된 접근을 하는 사용자(5)가 상기 제1 컴퓨터 장치(1)에 로그-온하는 단계에 대해 설명할 것이다. 약 1일의 제한된 지속시간동안 지속되도록 세션이 설계된다. 상기 제1 컴퓨터 장치(1)는 로그-온 소프트웨어 프로그램(4)을 갖는다. 상기 사용자 또는 자격을 갖는 임의의 사람에 의해 로그-온 되기 이전에, 상기 로그-온 소프트웨어 프로그램(4)은 상기 제1 컴퓨터 장치(1)에 설치된다. 상기 사용자(5)는 제어 유닛(6)의 키를 조작하나 상기 로그-온 소프트웨어 프로그램(4)에 해당하는 아이콘을 마우스로 클릭하여 상기 로그-온 소프트웨어 프로그램(4)의 동작을 시작한다. 상기 사용자는 제어 유닛(6)를 이용하여 개인 식별자(21), 특히 패스워드를 상기 제1 컴퓨터 장치(1)로 제공한다. 패스워드의 사용은 지문에 의해 대체될 수 있다. 본질적으로 알려진 방법으로, 상기 개인 식별자(21)는 상기 로그-온 소프트웨어 프로그램(4)이 상기 특정 사용자(5)의 신원을 검증하고 상기 특정 사용자의 개인 서명키(14)를 호출하게 한다. 도 1에 언급되지 않은 다른 실시형태의 경우에, 상기 사용자(5)의 개인 서명키(14)는 상기 특정 사용자(5)가 소유하는 메모리카드(22) 내에 포함된 암호문(20) 내에 위치한다. 메모리카드(22)의 리더(23)가 상기 제1 컴퓨터 장치(1)에 연결된다. 세션을 시작할 때, 상기 사용자(5)는 그의 메모리카드(22)를 상기 리더(23)에 삽입한다. 상기 리더(23)는 상기 메모리카드(22)와 상기 제1 컴퓨터 장치(1)의 제1 계산 수단(7) 사이의 데이터 전송을 위한 데이터 전송수단(24)을 갖는다. 상기 로그-온 소프트웨어 프로그램의 제어를 통해, 상기 제1 계산 수단(7)은 본질적으로 알려진 방법으로 상기 특정 사용자(5)의 개인 식별자(21)를 실행함으로써 상기 암호문(20)을 해독한다.

<270> 다른 실시형태에서, 상기 사용자(5)의 개인 서명키(14)는 상기 제1 컴퓨터 장치(1)의 메모리 영역에 포함된 암호문(20) 내에 위치한다. 이러한 실시형태에서, 상기 로그-온 소프트웨어 프로그램(4)에 의해 제어되는 제1 계

산 수단(7)은 상기 사용자(5)의 개인 식별자(21)를 실행하여 상기 암호문(20)을 해독한다.

<271> 또 다른 실시형태에서, 상기 사용자(5)의 개인 서명키(14)는 상기 특정 사용자(5)에 의해 사용되는 메모리카드(22) 내에 서명 알고리즘(25)으로 정의된다. 이러한 실시형태에서, 상기 사용자는 상기 제1 컴퓨터 장치(1)에 연결된 메모리카드(22)의 리더(23)로 상기 메모리카드(22)를 삽입한다. 상기 리더(23)는 상기 메모리카드(22)와 상기 제1 컴퓨터 장치(1) 사이에 데이터를 전송하는 전송 수단(24)을 갖는다. 상기 로그-온 소프트웨어 프로그램(4)에 의해 제어되는 제1 컴퓨터 장치(1)의 제1 계산 수단(7)은, 상기 개인 서명키(14)를 실행하고 상기 서명 알고리즘(25)을 수행함으로써 이하에 설명되는 일시 인증서(13)를 생성한다.

<272> 이하, 로그-온 단계에 대해 계속 설명할 것이다. 상기 로그-온 소프트웨어 수단(4)에 의해 제어되는 상기 제1 컴퓨터 장치(1)의 제1 계산 수단(7)은 사용자 식별자 데이터(5), 제1 컴퓨터 장치(1) 식별자 데이터, 날짜, 시간 및 세션의 지속시간으로부터 세션 식별자 데이터 Id(8)를 생성한다. 또한, 상기 제1 계산 수단(7)은 공개 일시 모듈 n(9), 공개 지수 v(10), 적어도 한쌍의 일시 공개 값 G(11) 및 일시 개인 값 Q(12)를 생성한다. 파라미터 n, v, G 및 Q는 다음과 같은 형태의 일반 방정식에 의해 상호 관련된다.

<273> $G \equiv Q^{v} \pmod{n}$ 또는 $G \times Q^{v} \equiv 1 \pmod{n}$.

<274> 또한, 상기 제1 계산 수단(7)은, 세션 식별자 데이터 Id(8) 및 상기 공개 일시 모듈 n(9)을 서명할 때 사용자(5)의 상기 개인 서명키(14)를 이용하여 고유 일시 인증서(13)를 생성한다. 또한, 필요하다면, 상기 인증서는, 상기 공개 지수 v(10) 또는 일시 공개 값 G(11)의 서명을 포함할 수 있다.

<275> 상기 "고유 인증서"라는 용어는, 사용자(5)의 식별자 데이터, 제1 컴퓨터 장치(1)의 식별자 데이터, 로그-온 날짜 및 시간, 세션에 대해 계획된 최대 지속시간에 의해 식별되는 세션이 진행되는 동안 사실상 어떠한 다른 인증서도 생성하지 않을 것이라는 사실을 말한다. 그러나, 동일한 세션이 진행되는 동안, 서명 작동을 수행하기 위해 사용자는 그의 개인 서명키를 사용할 것이라는 점을 제외하는 것은 아니다. 고려되는 세션이 진행되는 동안 다른 인증서의 발급을 방지하기 위한 목적으로, 제1 컴퓨터 장치(1)는, 로그-온 단계 이후 세션이 진행되는 동안, 로그-온 소프트웨어 프로그램(4)의 작동을 중지시키는 중지수단(15)을 갖는다.

<276> 세션이 진행되는 단계

<277> 이하, 세션이 진행되는 동안 이루어지는 인증 작동에 대해 설명할 것이다. 하나의 제2 컴퓨터 장치(2)에 제1 컴퓨터 장치(1)의 제1 연결이 적어도 지속되는 동안, 사용자(5)는 상기 제1 컴퓨터 장치(1)에 설치된 증명 소프트웨어 프로그램(16)의 작동을 시작한다. 상기 사용자(5) 또는 자격을 가진 임의의 사람에 의해 수행되는 로그-온 작동 이전에 상기 증명 소프트웨어 프로그램(16)이 상기 제1 컴퓨터 장치(1)에 설치된다. 상기 사용자(5)는 제어 유닛(6)의 키를 조작하거나 상기 증명 소프트웨어 프로그램(16)에 해당하는 아이콘을 마우스로 클릭하여 상기 증명 소프트웨어 프로그램(16)의 동작을 시작한다. 상기 증명 소프트웨어 프로그램(16)에 의해 제어되는 제1 계산 수단(7)은, 통신 네트워크(3)를 통해 제2 컴퓨터 장치(2)로 상기 일시 인증서(13)를 전송한다. 상기 증명 소프트웨어 프로그램(16)에 의해 제어되는 제1 계산 수단(7)은, 상기 제1 계산 수단(7) GQ 기법에 따라 본질적으로 알려진 방법으로 증명을 생성한다. 상기 증명은 영지식 GQ 타입 인증 메커니즘의 실행에 사용되기 위한 것이다. 상기 증명 소프트웨어 프로그램(16)은 GQ 프로토콜에 따라 증명자의 역할을 한다.

<278> 검증 소프트웨어 프로그램(18)은 제2 컴퓨터 장치(2)에 설치된다. 상기 서버는 본질적으로 알려진 방법에 따라 개인 컴퓨터에 연결된 컴퓨터의 설정이 진행되는 동안 작동되는 시작 수단을 갖는다. 상기 시작 수단은 상기 검증 소프트웨어 프로그램(18)의 작동을 시작한다.

<279> 상기 검증 소프트웨어 프로그램(18)의 제어에 의해, 제2 계산 수단(17)은, 상기 개인 서명키(14)에 관련된 공개키(19)를 이용하여 일시 인증서(13)를 개봉한다. 상기 검증 소프트웨어 프로그램(18)의 제어를 통해, 상기 제2 계산 수단(17)은, 상기 일시 인증서(13)로부터 세션 식별자 데이터 Id(8), 상기 일시 모듈 n(9)과 경우에 따라 상기 공개 지수 v(10) 및 상기 일시 공개 값 G(11)를 추출한다. 상기 증명 소프트웨어 프로그램(16)은 GQ 프로토콜에 따라 검증자의 역할을 한다.

<280> 이하, 인증 프로토콜이 GQ0 타입인 본 발명에 따른 시스템의 제1 실시형태를 보다 상세하게 설명한다. 이러한 실시형태의 경우, 제1 계산 수단(7)은, 로그-온 소프트웨어 프로그램(4)의 제어를 통해, 공개 일시 모듈 n(9), 공개 지수 v(10), 적어도 한쌍의 일시 공개 값 G(11) 및 일시 개인 값 Q(12)를 이하에 설명되는 방법으로 생성한다. 상기 제1 계산 수단(7)은 상기 공개 지수 v(10)를 설정하기 위한 수단, 무작위로 상기 공개 일시 모듈 n(9)을 선택하는 수단, 무작위로 상기 일시 개인 값 Q(12)를 선택하는 수단, 상기 일반 방정식 중 하나를 적용

하여 상기 일시 공개 값 G(11)를 계산하는 수단을 더 포함한다. 이러한 실시형태의 경우, 일시 인증서(13)는 세션 식별자 데이터 Id에 대한 공개 일시 모듈 n(9), 공개 지수 v(10), 일시 공개 값 G(11)에 관련된다. 이러한 실시형태의 경우, GQ0 타입 인증 프로토콜은 상기 공개 일시 모듈 n(9) 및 상기 m개의 일시 개인 값 Q_1 내지 Q_m을 실행하는 증명 메커니즘을 포함한다.

<281> 이하, 인증 프로토콜이 GQ1 타입인 본 발명에 따른 시스템의 제2 실시형태를 보다 상세하게 설명한다. 이러한 실시형태의 경우, 로그-온 소프트웨어 프로그램(4)에 의해 제어되는 제1 계산 수단(7)은, 공개 일시 모듈 n(9), 공개 지수 v(10), 적어도 한쌍의 일시 공개 값 G(11) 및 일시 개인 값 Q(12)를 이하에 설명되는 방법으로 생성한다. 상기 제1 계산 수단(7)은 상기 공개 지수 v(10)의 값을 설정하기 위한 수단, v가 각각의 일시 소인수-1을 갖는 소수가 되도록 적어도 두 개의 일시 소인수를 곱하여 상기 일시 모듈 n(9)을 생성하기 위한 수단, 메시지 m_i에 대해 RSA 서명 표준 포맷 메커니즘의 적용을 통해 일시 공개 값 G(11)를 생성하기 위한 수단($G=Red(m_i)$), s.v-1이 각각의 일시소인수-1의 배수가 되도록 개인 지수 s를 결정하기 위한 수단, 특히 상기 일시 공개 값 G(11)를 상기 개인 지수 s만큼 제곱하여 모듈로 n함으로써 상기 일시 개인 값 Q_i(12)를 생성하는 수단 및/또는 m개의 일시 개인값 Q_i(12)의 m×f개의 일시 개인 콤포넌트 $Q_{i,j}$를 생성하기 위한 수단을 포함한다. 따라서, 본 발명에 따른 시스템의 제3 실시형태는 일시 개인 값 Q_i(12)를 직접 사용할 필요가 없다고 보이나, 상기 일시 개인 콤포넌트 $Q_{i,j}$를 사용한다. 상기 일시 인증서(13)는 세션 식별 데이터 Id에 대한 공개 일시 모듈 n(9) 및 공개 지수 v(10)에 관련된다. 즉 이러한 실시형태의 경우, GQ1 타입 인증 프로토콜은 상기 공개 일시 모듈 n(9) 및 상기 m개의 일시 개인 값 Q_1 내지 Q_m(12)또는 상기 일시 모듈 $n=p_1\times\ldots\times p_f$의 f개의 소인수 p_1 내지 p_f(26), m×f개의 일시 개인 컴포넌트 $Q_{1,1}$ 내지 $Q_{f,m}$ (27)및 일시 차이니즈 나머지(Chinese remainder)의 f-1개의 파라미터(28)을 포함한다.

<282> 이하, 인증 프로토콜이 GQ2 타입일 때, 본 발명에 따른 시스템의 제3 실시형태에 대해 보다 상세하게 설명할 것이다. 이러한 실시형태의 경우, 상기 로그-온 소프트웨어 프로그램(4)에 의해 제어되는 상기 제1 계산 수단(7)은, 공개 일시 모듈 n(9), 공개 지수 v(10), 적어도 한 쌍의 일시 공개 값 G(11) 및 일시 개인 값 Q(12)를 이하에 설명되는 방법으로 생성한다. 상기 제1 계산 수단(7)은 $v=2^k$ 형태의 상기 공개 지수 v(10)의 계산을 가능하게 하는 파라미터 k의 값을 설정하기 위한 수단, f개의 일시 소인수의 곱인 공개 일시 모듈 $n(n=p_1\times p_2\times\ldots\times p_f,\ f\geq 2)$을 생성하기 위한 수단, 특히 100보다 작은 값이며, $G_i=g_i^2$ 형태의 m개의 일시 공개 값 G_i(11)를 정의할 수 있는 m개의 일시 베이스 값 g_i를 선택하기 위한 수단, 특히 상기 일시 공개 값 G(11)를 n을 법으로 하는 개인 지수 s만큼 제곱하여 모듈로 n함으로써 상기 일시 개인 값 Q_i(12)를 생성하는 수단 및/또는 m개의 일시 개인값 Q_i(12)의 m×f개의 일시 개인 콤포넌트 $Q_{i,j}$(12)를 생성하기 위한 수단을 포함한다. 이러한 실시형태의 경우, 상기 일시 인증서(13)는 세션 식별자 데이터 Id에 대한 상기 공개 일시 모듈 n(9)과 관련된다. 즉, 상기 숫자 k 및 상기 m개의 베이스 값 g_i는 어떠한 특별 보호를 필요로 하지 않는다. 이러한 실시형태에서, 상기 GQ2 타입 인증 프로토콜은 상기 일시 모듈 n(9) 및 상기 m개의 일시 개인 값 Q_1 내지 Q_m(12) 또는 상기 일시 모듈 $n=p_1\times\ldots\times p_f$의 f개의 일시 소인수 p_1 내지 p_f(26), m×f개의 일시 개인 컴포넌트 $Q_{1,1}$ 내지 $Q_{f,m}$(27)및 일시 차이니즈 나머지의 f-1개의 파라미터(28)을 실행하는 증명 메커니즘을 포함한다.

<283> RSA 타입 로그-온 프로토콜과 관련된 차이니즈 나머지 방법을 사용하는 GQ 타입 인증 프로토콜에서, 작은 크기의 일시 공개 값 G(11) 및 일시 개인 값 Q(12)를 실행하는 것은 본 발명에 의해 제기되는 문제를 해결하고 본 발명의 목적을 달성하게 한다. 즉, 상술한 기술적 특징의 조합은 작업부하를 감소시키며, 그와 유사하게 접근하기를 원하는 서버에 의한 사용자의 개인 컴퓨터의 각각의 인증 단계 동안 사용자의 대기 시간을 감소시킨다. 상기 작업부하는, 종래에 알려진 프로토콜, 특히 RSA 타입 프로토콜을 실행하는 경우와 비교할 때 1/100의 비율로 감소된다. 짧은 세션 지속시간 동안 작은 크기의 일시공개 값 G(11) 및 일시 개인 값의 실행에 의해 얻어지는 작업부하의 감소는 다음과 같은 이유로 인해 인증의 보안을 감소시키지 않는다:

<284> ● 첫째, 비슷한 우회(circumvention) 용량에 대해, 상기 GQ 프로토콜은 RSA 프로토콜보다 높은 보안을 제공한다.

<285> ● 둘째, 일시 인증서를 생성하는데 사용되는 RSA 타입, 큰 크기, 긴 지속시간의 개인 서명키가 세션이 지속되

는 동안 접근이 용이하지 않다.

<286> ● 마지막으로, 작은 크기의 공개 값 G 및 개인 값의 일시적인 특징은, 부정한 사람에게 GQ 프로토콜의 신뢰성 있는 데이터를 복구하는데 소모되는 시간을 허용하지 않는다.

산업상 이용 가능성

<287> 본 발명에 따른 방법은,

<288> ● 상기 사용자가 여러개의 패스워드를 기억할 필요가 없으며,

<289> ● 상기 사용자 및 서버의 관리자도 그들의 개인용 컴퓨터 또는 서버에서 사용되는 실질적인 계산 자원을 가질 필요 없이,

<290> 세션이 지속되는 동안 관련된 특정 개인 컴퓨터를 사용하는 사용자를 식별하고 여러 서버로부터 상기 개인 컴퓨터를 인증하는데 사용될 수 있다.

도면의 간단한 설명

<103> 도 1은 본 발명에 따른 시스템의 제2 실시형태의 개략 구성도이다.

도면

도면1