



(51) 국제특허분류:

G06F 21/32 (2013.01)

H04L 9/30 (2006.01)

G06F 21/45 (2013.01)

(21) 국제출원번호:

PCT/KR2018/005012

(22) 국제출원일:

2018년 4월 30일 (30.04.2018)

(25) 출원언어:

한국어

(26) 공개언어:

한국어

(30) 우선권정보:

10-2017-0055803 2017년 4월 29일 (29.04.2017) KR

(71) 출원인: 서울대학교산학협력단 (SEOUL NATIONAL UNIVERSITY R&DB FOUNDATION) [KR/KR]; 08826 서울시 관악구 관악로 1, Seoul (KR).

(72) 발명자: 천정희 (CHEON, Junghee); 08826 서울시 관악구 관악로 1, Seoul (KR). 송용수 (SONG, Yongssoo); 08826 서울시 관악구 관악로 1, Seoul (KR).

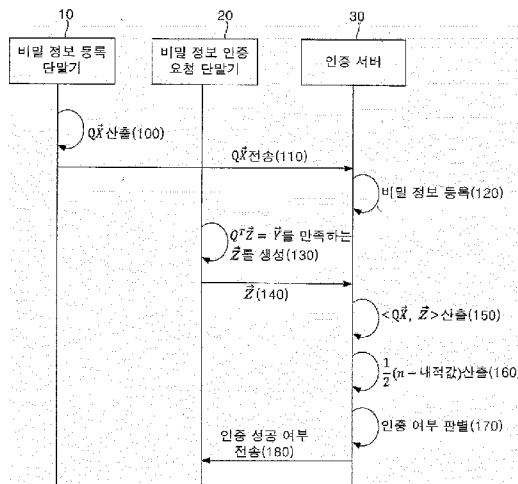
(74) 대리인: 백도현 (BACK, Doehyun); 07997 서울시 양천구 목동동로 293, 3103호, Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI

(54) Title: BIOMETRIC INFORMATION AUTHENTICATION METHOD FOR PROTECTING BIOMETRIC INFORMATION

(54) 발명의 명칭: 생체 정보를 보호하는 생체 정보 인증 방법



10 ... Confidential information registration terminal
20 ... Confidential information authentication request terminal
30 ... Authentication server
100 ... Calculate QX
110 ... Transmit QX
120 ... Register confidential information
130 ... Create Z which satisfies $Q^T Z = Y$
150 ... Calculate $\langle QX, Z \rangle$
160 ... Calculate $1/2(n - \text{inner product})$
170 ... Determine whether authenticated
180 ... Transmit whether authentication is succeeded

(57) Abstract: A confidential information authentication method according to the present invention comprises: a first step of allowing a confidential information authentication server to receive, from a confidential information registration terminal, the product of a first confidential information vector and a matrix (Q) and store the same; a second step of allowing the confidential information authentication server to receive, from a confidential information authentication request terminal, a third vector enabling the value, obtained by multiplying a transposed matrix (QT) of the matrix and the third vector, to become a second confidential vector, with respect to a second confidential information vector for which an authentication request was made; a third step of allowing the confidential information authentication server to calculate the product of the matrix and a first confidential vector and an inner product of the third vector; and a fourth step of allowing the confidential information authentication server to calculate $1/2(n - \text{inner product})$, determine the confidential information authentication to have succeeded if the value is less than or equal to a predetermined value, and determine the confidential information authentication to have failed in all other cases.

(57) 요약서: 본 발명에 의한 비밀 정보 인증 방법은, 비밀 정보 인증 서버가, 제1 비밀 정보 벡터와 행렬(Q)의 곱을 비밀 정보 등록 단말기로부터 수신하고 저장하는 제1 단계와; 비밀 정보 인증 서버가, 인증 요청된 제2 비밀 정보 벡터에 대해서, 행렬의 전치행렬(QT)과 제3 벡터를 곱한 값이 제2 비밀 벡터가 되는 제3 벡터를 비밀 정보 인증 요청 단말기로부터 수신하는 제2 단계와; 비밀 정보 인증 서버가, 행렬과 제1 비밀 벡터의 곱과 제3 벡터의 내적값(inner product)을 산출하는 제3 단계와; 비밀 정보 인증 서버가, $1/2(n - \text{내적값})$ 을 산출하고, 이 값이 소정의 값보다 작거나 같은 경우에 비밀 정보 인증에 성공한 것으로 판별하고, 그 이외의 경우에는 비밀 정보 인증 실패로 판별하는 제4 단계를 포함한다.

(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML,
MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

명세서

발명의 명칭: 생체 정보를 보호하는 생체 정보 인증 방법 기술분야

- [1] 본 발명은 비밀 정보 인증 방법에 대한 것으로서 특히 생체 정보의 인증 방법에 대한 것이다.

배경기술

- [2] 최근에 지문, 홍채 정보 등과 같은 인간마다 고유하게 가지고 있는 생체 정보를 이용하여 인증 방법이 널리 개발되고 있다. 생체 정보는 사람마다 고유하기 때문에 비밀번호를 외워야 하는 등의 번거로움이 없고, 유출의 우려도 없는 장점이 있다.
- [3] 그런데 생체 정보 인증은 기존의 인증 방법과 다른 특징을 가지고 있다. 첫째, 생체 정보 인식 과정에서 발생하는 노이즈에 의해서 인식을 위해 입력되는 생체 입력 정보가 조금씩 달라지는데 이처럼 노이즈가 있는 상태에서도 인증이 가능해야 한다. 둘째, 생체 정보가 노출되는 경우라고 해도, 비밀번호와 달리 생체 정보는 변경이 불가능하다. 따라서, 노출의 위험성을 원천적으로 차단해야 한다.
- [4] 이와 같은 생체 정보 인증의 특성을 고려하여 Fuzzy extractor나 Inner product encryption 등의 암호화 방식이 연구되고 있다. 그러나 종래의 암호화 방식에 따른 인증은 속도가 느리거나 암호문의 크기가 크다는 단점이 존재한다.

[5]

발명의 상세한 설명

기술적 과제

- [6] 본 발명은 전술한 종래 기술의 문제점을 해결하여, 암호문의 크기가 짧고 속도가 빠른 비밀 정보 특히 생체 정보 인증 방법을 제공하는 것을 목적으로 한다.

[7]

과제 해결 수단

- [8] 본 발명에 의한 비밀 정보 인증 방법은, 비밀 정보 등록 단말기와, 비밀 정보 인증 서버와, 비밀 정보 인증 요청 단말기를 포함하는 환경에서 비밀 정보 인증 서버가 수행되며, 비밀 정보 인증 서버가, 비밀 정보 벡터 $\vec{X} \in \{-1, 1\}^n$ 와

행렬 $Q \in \mathbb{Z}_q^{m \times n}$ 의 곱인 $Q\vec{X}$ 를 비밀 정보 등록 단말기로부터 수신하고

저장하는 제1 단계와; 비밀 정보 인증 서버가, 인증 요청된 비밀 정보 벡터

$\vec{Y} \in \{-1, 1\}^n$ 에 대해서, $Q^T \vec{Z} = \vec{Y}$ 의 관계를 만족하도록 생성된 벡터 $\vec{Z}$ 를

비밀 정보 인증 요청 단말기로부터 수신하는 제2 단계와; 비밀 정보 인증 서버가,

$Q\vec{X}$ 와 $\vec{Z}$ 의 내적값(inner product)을 산출하는 제3 단계와; 비밀 정보 인증 서버가,
 $\frac{1}{2}(n - \text{내적값})$ 을 산출하고, 이 값이 소정의 값보다 작거나 같은 경우에 비밀

정보 인증에 성공한 것으로 판별하고, 그 이외의 경우에는 비밀 정보 인증
 실패로 판별하는 제4 단계를 포함한다.

- [9] 본 발명의 다른 실시형태에 의하면, 본 발명에 의한 인증 방법은, 비밀 정보
 인증 서버가, 비밀 정보 벡터 $\vec{X} \in \{-1, 1\}^n$ 와 행렬 $Q \in \mathbb{Z}_q^{m \times n}$ 의 곱을 비밀

정보 등록 단말기로부터 수신하는 제1 단계와; 비밀 정보 인증 서버가, 인증
 요청된 비밀 정보 벡터 $\vec{Y} \in \{-1, 1\}^n$ 와 에러벡터($\vec{e} \leftarrow \mathbb{Z}_q^n$)에 대해서,

$Q^T \vec{Z} = \vec{Y} + \vec{e}$ 의 관계를 만족하도록 생성된 벡터 $\vec{Z}$ 를 비밀 정보 인증 요청

단말기로부터 수신하는 제2 단계와; 비밀 정보 인증 서버가, $Q\vec{X}$ 와 $\vec{Z}$ 의

내적값(inner product)을 산출하는 제3 단계와; 비밀 정보 인증 서버가,
 $\frac{1}{2}(n - \text{내적값})$ 을 산출하고, 이 값이 소정의 값보다 작거나 같은 경우에 비밀

정보 인증에 성공한 것으로 판별하고, 그 이외의 경우에는 비밀 정보 인증
 실패로 판별하는 제4 단계를 포함한다.

- [10] 제1 단계 수행 후 행렬 Q 는 비밀 정보 등록 단말기로부터 삭제될 수 있다.

- [11] $Q\vec{X}$ 및 $\vec{Z}$ 중 적어도 어느 하나는 공개키로 암호화되어 전송될 수 있다.

[12]

발명의 효과

- [13] 본 발명에 의하면, 비밀 정보가 암호화되어 인증 서버로 전송되므로 도중에
 누출되거나 인증 서버가 공격받더라도 비밀 정보는 누출되지 않는 효과가 있다.
 그리고 인증 요청을 받은 암호화된 비밀 정보와 등록되어 있는 암호화된 비밀
 정보를 복호화할 필요없이 인증 여부를 판별할 수 있기 때문에 비밀 정보가
 누설될 가능성을 원천적으로 차단할 수 있다. 또한, 비밀 정보는 길이가 m 인
 벡터로 되어 있는 암호문의 내적값으로 인증 여부를 판별하기 때문에 기존의
 방법에 비해 효율성도 고양된다.

[14]

도면의 간단한 설명

- [15] 도 1은 본 발명에 의한 비밀 정보 인증 방법의 흐름도.

발명의 실시를 위한 형태

- [16] 이하에서는 첨부 도면을 참조하여 본 발명에 대해서 자세하게 설명한다.

- [17] 본 명세서에서 수행되는 정보(데이터) 전송 과정은 필요에 따라서
 암호화/복호화가 적용될 수 있으며, 본 명세서 및 특허청구범위에서

정보(데이터) 전송 과정을 설명하는 표현은 별도로 언급되지 않더라도 모두 암호화/복호화하는 경우도 포함하는 것으로 해석되어야 한다. 본 명세서에서 "A로부터 B로 전송(전달)" 또는 "A가 B로부터 수신"과 같은 형태의 표현은 중간에 다른 매개체가 포함되어 전송(전달) 또는 수신되는 것도 포함하며, A로부터 B까지 직접 전송(전달) 또는 수신되는 것만을 표현하는 것은 아니다. 본 발명의 설명에 있어서 각 단계의 순서는 선행 단계가 논리적 및 시간적으로 반드시 후행 단계에 앞서서 수행되어야 하는 경우가 아니라면 각 단계의 순서는 비제한적으로 이해되어야 한다. 즉 위와 같은 예외적인 경우를 제외하고는 후행 단계로 설명된 과정이 선행 단계로 설명된 과정보다 앞서서 수행되더라도 발명의 본질에는 영향이 없으며 권리범위 역시 단계의 순서에 관계없이 정의되어야 한다. 그리고 본 명세서에서 "A 또는 B"은 A와 B 중 어느 하나를 선택적으로 가리키는 것 뿐만 아니라 A와 B 모두를 포함하는 것도 의미하는 것으로 정의된다. 또한, 본 명세서에서 "포함"이라는 용어는 포함하는 것으로 나열된 요소 이외에 추가로 다른 구성요소를 더 포함하는 것도 포괄하는 의미를 가진다.

- [18] 본 명세서에서는 본 발명의 설명에 필요한 필수적인 구성요소만을 설명하며, 본 발명의 본질과 관계가 없는 구성요소는 언급하지 아니한다. 그리고 언급되는 구성요소만을 포함하는 배타적인 의미로 해석되어서는 아니되며 다른 구성요소도 포함할 수 있는 비배타적인 의미로 해석되어야 한다.
- [19] 본 발명은 전자적 연산이 가능한 컴퓨터 등의 전자적 연산 장치에 의해서 수행되며, 후술하는 본 발명의 각 단계의 수학적 연산 및 산출은 해당 연산 또는 산출을 하기 위해 공지되어 있는 코딩 방법 및/또는 본 발명에 적합하게 고안된 코딩에 의해서 컴퓨터 연산으로 구현될 수 있다.
- [20] 그리고 본 명세서에서 "값"이라 함은 스칼라값 뿐만 아니라 벡터, 행렬도 포함하는 개념으로 정의된다.
- [21] 본 명세서에서는 본 발명이 생체 정보인 비밀 정보에 적용되는 실시예에 대해서 주로 설명하지만, 본 발명에 의한 암호화 방법 및 인증 방법은 통상적인 비밀 정보(예를 들어, 비밀 번호와 비밀키, 개인민감 정보 등)에도 적용할 수 있으며, 생체 정보에 적용되는 것으로 권리범위가 제한되어서는 아니된다.
- [22] 도 1에는 본 발명에 의한 비밀 정보 인증 방법이 수행되는 흐름도가 도시되어 있다. 본 발명에 의한 비밀 정보 인증 방법은, 비밀 정보 등록 단말기(10)와, 비밀 정보 인증 요청 단말기(20)와, 인증 서버(30)를 포함하는 환경에서 수행된다. 비밀 정보 등록 단말기(10)는, 최초에 사용자의 비밀 정보를 인증 서버(30)에 등록하기 위한 단말기이며, 비밀 정보 인증 요청 단말기(20)는 비밀 정보 등록 후 인식된 비밀 정보를 인증 서버(30)로 전송하여 비밀 정보를 인증받기 위한 단말기이다. 비밀 정보 등록 단말기(10)와 비밀 정보 인증 요청 단말기(20)는 서로 동일한 단말기일 수도 있고, 서로 다른 단말기일 수도 있다. 본 명세서에서는 서로 다른 단말기인 것으로 가정하고 설명하기로 한다. 등록되고

인증 요청되는 비밀 정보로는 예를 들어 지문 정보가 될 수 있다.

- [23] 등록하고자 하는 비밀 정보를 사용자가 비밀 정보 등록 단말기(10)에 입력하면 단말기는 비밀 정보 벡터를 $-1, 1$ 로 구성된 길이 n 인 벡터 $\vec{X} \in \{-1, 1\}^n$ 로

생성한다. 그리고 $m \times n$ 행렬 $Q \in \mathbb{Z}_q^{m \times n}$ 와 입력받은 비밀 정보 벡터 $\vec{X}$ 의 곱인

$Q\vec{X}$ 을 산출한다(100). 행렬 Q 는 비밀 정보 등록 단말기(10)에서 최초로 비밀 정보를 등록하는 과정을 거친 후에 단말기(10)에서 삭제할 수 있다. 행렬 Q 를 비밀 정보 등록 후에 삭제해 버리면 이후에 유출될 위험을 제거할 수 있다.

- [24] 산출된 $Q\vec{X}$ 는 인증 서버(30)로 전송된다(110). 행렬 Q 는 비밀 정보 등록 단말기(10)만 가지고 있는 값이기 때문에 인증 서버(30)로 전송되는 값은 일종의 비밀 정보 암호화 값이다. 인증 서버(30)는 전송받은 $Q\vec{X}$ 값을 비밀 정보의 암호화값으로 등록한다(120).

- [25] 비밀 정보가 등록된 후에, 비밀 정보 인증을 받고자 하는 사용자는 비밀 정보 인증 요청 단말기(20)에 자신의 비밀 정보를 판독시키거나 입력하여 비밀 정보 인증 요청 단말기(20)가 $-1, 1$ 로 구성된 길이 n 인 비밀 정보 벡터 $\vec{Y} \in \{-1, 1\}^n$ 를 생성한다.

- [26] 그리고 비밀 정보 인증 요청 단말기(20)는, 인증 요청된 비밀 정보 벡터 $\vec{Y} \in \{-1, 1\}^n$ 에 대해서, $Q^T \vec{Z} = \vec{Y}$ 의 관계를 만족하는 벡터 $\vec{Z}$ 를 생성한다(130). 벡터 $\vec{Z}$ 는 예를 들어, $(m-n)$ 개의 성분을 임의의 값으로 랜덤하게 선택한 후에, 나머지 n 개 성분을 위 관계를 만족하도록 계산하여 생성할 수 있다.

- [27] m 과 n 의 관계는 $m \gg n$ 인 것이 바람직하다. n 은 비밀 정보의 차원이고, m 에 의해서 보안성이 결정된다. m 과 n 의 차이인 $k(=m-n)$ 값이 중요한데 이는 후술하는 LWE 문제의 안전성을 담보한다. 소망하는 보안성의 정도와 다른 인수들에 따라서 차이는 있지만, 대략 k 값은 500 내지 1,000을 취하는 것이 일반적이다. 예를 들어 홍채 인식의 경우 n 을 2,000으로, m 은 2,500으로 설정하여 k 값을 500으로 할 수 있다. 물론, 본 발명은 그러한 구체적인 값에 보호범위가 제한되지 것으로 해석되지 않는다.

- [28] 산출된 $\vec{Z}$ 는 인증 서버로 전송된다(140).

- [29] 비밀 정보 등록시 사용한 비밀 정보 벡터 $\vec{X}$ 와, 비밀 정보 인증시 생성된 비밀 정보 벡터 $\vec{Y}$ 가 $\vec{X}, \vec{Y} \in \{-1, 1\}^n$ 이므로 $\vec{X}$ 와 $\vec{Y}$ 의 해밍 거리(hamming distance)

$d(\vec{X}, \vec{Y})$ 는 다음과 같이 $\vec{X}$ 와 $\vec{Y}$ 의 내적 계산을 통해서 산출이 가능하다.

[30] [수식1]

$$d(\vec{X}, \vec{Y}) = \frac{1}{2}(n - \langle \vec{X}, \vec{Y} \rangle)$$

[31] 두 벡터의 해밍 거리는 두 벡터의 같은 위치에 있는 원소를 비교했을 때 서로 다른 원소의 개수를 의미한다. 예를 들어, 벡터 1100과 벡터 1000의 해밍 거리는 1이고, 벡터 1111과 벡터 1100 사이의 해밍 거리는 2가 된다. 즉 비밀 정보를 벡터로 표현하면 해밍 거리가 작을수록 서로 비슷한 비밀 정보로 볼 수 있다.

[32] 인증 서버(30)는 등록해 놓은 암호화된 비밀 정보

$$Q\vec{X}$$

와 벡터

$$\vec{Z}$$

의 내적값을 산출한다(150). 이 내적값은 다음과 같은 관계를 만족한다.

[33] [수식2]

$$\langle Q\vec{X}, \vec{Z} \rangle = \langle \vec{X}, Q^T \vec{Z} \rangle = \langle \vec{X}, \vec{Y} \rangle$$

[34] 수학식 1에 의해서 비밀 정보 등록 정보 벡터

$$\vec{X}$$

와, 비밀 정보 인증시 생성된 비밀 정보 벡터

$$\vec{Y}$$

의 해밍 거리

$$d(\vec{X}, \vec{Y})$$

를

$$\frac{1}{2}(n - \text{내적값})$$

으로 산출한다(160). 이렇게 산출된 해밍 거리가 미리 정한 범위 이내라면 인증을 요청한 비밀 정보가 정당한 것으로 판별하고, 그렇지 않으면 인증 실패로 판별한다(170). 인증 성공 여부는 인증 서버(30)가 비밀 정보 인증 요청 단말기(20)로 전송한다(180).

[35] 생체 정보가 아닌 비밀정보는 노이즈가 개입할 여지가 없으므로 해밍 거리가 0이 되어야 인증에 성공한 것으로 판단한다.

[36] 노이즈가 없는 비밀 정보의 경우에는 해밍 거리가 0인 경우에만 인증에 성공하는 것으로 할 수 있다.

[37] 인증 서버(30)로 전달되는

$$Q\vec{X}$$

와

$\vec{Z}$

중 적어도 어느 하나를 인증 서버(30)의 공개키로 암호화하여 전송하면 보안성이 더 고양될 수 있다.

[38] 본 발명의 다른 실시예에 의하면

$$Q^T \vec{Z} = \vec{Y} + \vec{e}$$

(

$$\vec{e} \leftarrow \mathbb{Z}_q^n$$

)의 관계를 만족하도록 생성된 벡터

$\vec{Z}$

를 사용할 수도 있다. 벡터

$\vec{e}$

는

$$\mathbb{Z}_q^n$$

로부터 랜덤하게 선택되는 LWE 문제에 있어서의 크기가 작은 노이즈 벡터이다. 이 실시예에서는, 인증 서버(30)가

$$Q\vec{X}$$

와

$\vec{Z}$

의 내적값을 산출하고, 그 내적값으로부터 수학식 1에 의해 등록된 비밀 정보 벡터

$\vec{X}$

와 인증 요청을 받은 비밀 정보 벡터에 에러값이 더해진

$$\vec{Y} + \vec{e}$$

의 해밍 거리를 산출하여 수학식 1에 따라서 인증 여부를 판단한다.

[39] [수식3]

$$\langle \vec{X}, \vec{Y} + \vec{e} \rangle = \langle \vec{X}, \vec{Y} \rangle + \langle \vec{X}, \vec{e} \rangle$$

[40] 위 수학식 3의 관계에 따라서,

$$\langle \vec{X}, \vec{Y} + \vec{e} \rangle$$

는 작은 오차

$$\langle \vec{X}, \vec{e} \rangle$$

를 가지는

$$\langle \vec{X}, \vec{Y} \rangle$$

의 근사값으로 볼 수 있다. 따라서, 비밀 정보 인증에 사용할 수 있다.

[41] 이 실시예에 의하면, LWE 문제에 의해 에러가 포함되어 암호화되므로 비밀 정보 인증을 위해 전송되는 비밀 정보

$\vec{y}$

의 보안성을 더 높이는 효과가 있다.

[42] 본 발명에 의하면, 비밀 정보가 암호화되어 인증 서버로 전송되므로 도중에 노출되거나 인증 서버가 공격받더라도 비밀 정보는 누출되지 않는 효과가 있다. 그리고 전송한 바와 같은 행렬 Q 를 이용하여 암호화함으로써 인증 요청받은 암호화된 비밀 정보와 등록되어 있는 암호화된 비밀 정보를 복호화할 필요없이 인증 여부를 판별할 수 있기 때문에 비밀 정보가 누설될 가능성을 원천적으로 차단할 수 있다. 또한, 비밀 정보는 길이가 m 인 벡터로 되어 있는 암호문의 내적값으로 인증 여부를 판별하기 때문에 기존의 방법에 비해 효율성도 고양된다.

[43] 이상 첨부 도면을 참고하여 본 발명에 대해서 설명하였지만 본 발명의 권리범위는 후술하는 특허청구범위에 의해 결정되며 전송한 실시예 및/또는 도면에 제한되는 것으로 해석되어서는 아니된다. 그리고 특허청구범위에 기재된 발명의, 당업자에게 자명한 개량, 변경 및 수정도 본 발명의 권리범위에 포함된다는 점이 명백하게 이해되어야 한다.

[44]

청구범위

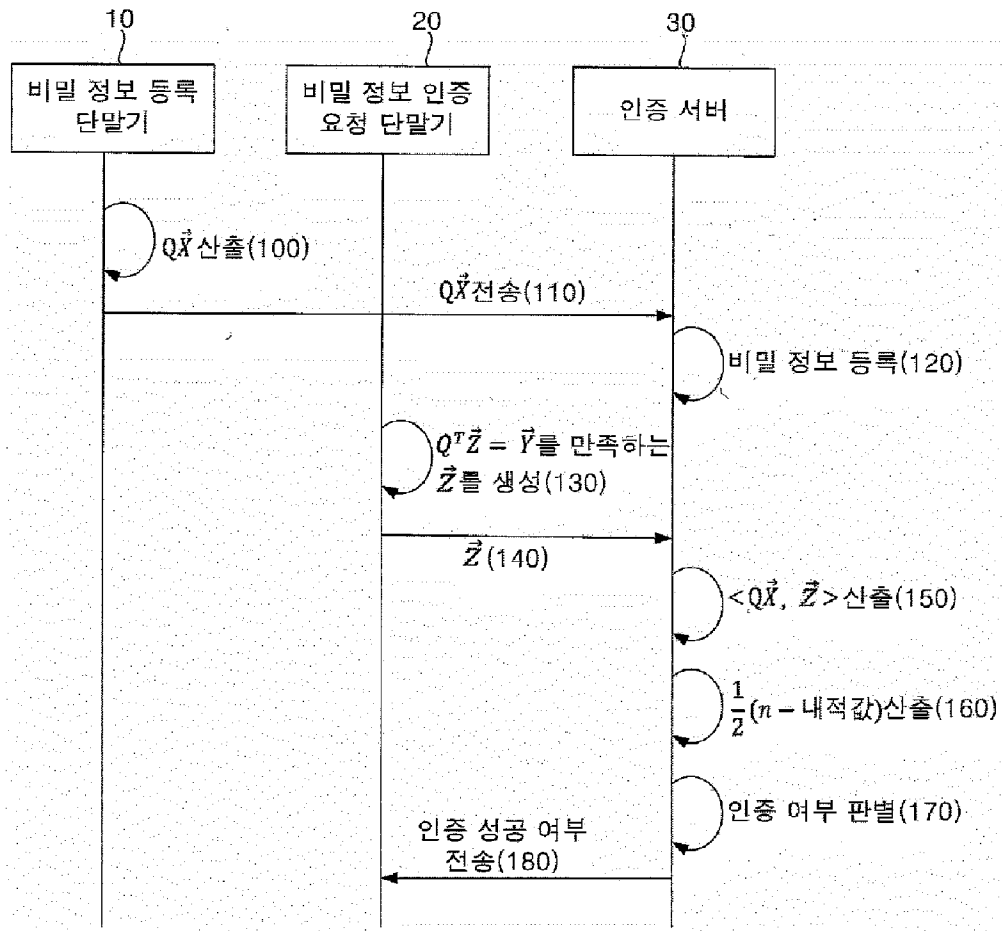
- [청구항 1] 비밀 정보 등록 단말기와, 비밀 정보 인증 서버와, 비밀 정보 인증 요청 단말기를 포함하는 환경에서 비밀 정보 인증 서버가 수행하는 비밀 정보 인증 방법에 있어서,
비밀 정보 인증 서버가, 비밀 정보 벡터 $\vec{X} \in \{-1, 1\}^n$ 와 행렬 $Q \in \mathbb{Z}_q^{m \times n}$ 의 곱인 $Q\vec{X}$ 를 비밀 정보 등록 단말기로부터 수신하고 저장하는 제1 단계와,
비밀 정보 인증 서버가, 인증 요청된 비밀 정보 벡터 $\vec{Y} \in \{-1, 1\}^n$ 에 대해서, $Q^T \vec{Z} = \vec{Y}$ 의 관계를 만족하도록 생성된 벡터 $\vec{Z}$ 를 비밀 정보 인증 요청 단말기로부터 수신하는 제2 단계와,
비밀 정보 인증 서버가, $Q\vec{X}$ 와 $\vec{Z}$ 의 내적값(inner product)을 산출하는 제3 단계와,
비밀 정보 인증 서버가, $\frac{1}{2}(n - \text{내적값})$ 을 산출하고, 이 값이 소정의 값보다 작거나 같은 경우에 비밀 정보 인증에 성공한 것으로 판별하고, 그 이외의 경우에는 비밀 정보 인증 실패로 판별하는 제4 단계를 포함하는, 비밀 정보 인증 방법.
- [청구항 2] 비밀 정보 등록 단말기와, 비밀 정보 인증 서버와, 비밀 정보 인증 요청 단말기를 포함하는 환경에서 비밀 정보 인증 서버가 수행하는 비밀 정보 인증 방법에 있어서,
비밀 정보 인증 서버가, 비밀 정보 벡터 $\vec{X} \in \{-1, 1\}^n$ 와 행렬 $Q \in \mathbb{Z}_q^{m \times n}$ 의 곱을 비밀 정보 등록 단말기로부터 수신하는 제1 단계와,
비밀 정보 인증 서버가, 인증 요청된 비밀 정보 벡터 $\vec{Y} \in \{-1, 1\}^n$ 와 에러벡터($\vec{e} \leftarrow \mathbb{Z}_q^n$)에 대해서, $Q^T \vec{Z} = \vec{Y} + \vec{e}$ 의 관계를 만족하도록 생성된 벡터 $\vec{Z}$ 를 비밀 정보 인증 요청 단말기로부터 수신하는 제2 단계와,
비밀 정보 인증 서버가, $Q\vec{X}$ 와 $\vec{Z}$ 의 내적값(inner product)을 산출하는 제3 단계와,
비밀 정보 인증 서버가, $\frac{1}{2}(n - \text{내적값})$ 을 산출하고, 이 값이 소정의 값보다 작거나 같은 경우에 비밀 정보 인증에 성공한 것으로 판별하고, 그

이외의 경우에는 비밀 정보 인증 실패로 판별하는 제4 단계를 포함하는,
비밀 정보 인증 방법.

[청구항 3] 청구항 1 또는 청구항 2에 있어서,
제1 단계 수행 후 행렬 Q 는 비밀 정보 등록 단말기로부터 삭제되는,
비밀 정보 인증 방법.

[청구항 4] 청구항 1 또는 청구항 2에 있어서,
 $Q\vec{X}$ 및 $\vec{Z}$ 중 적어도 어느 하나는 공개키로 암호화되어 전송되는,
비밀 정보 인증 방법.

[도1]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2018/005012

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/32(2013.01)i, G06F 21/45(2013.01)i, H04L 9/30(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/32; G06F 17/10; G06F 21/20; H04L 9/32; G06K 9/00; G06F 21/00; G06T 7/00; G06F 21/45; H04L 9/30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models: IPC as above

Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: biometric data, authentication, secret information, registered terminal, authentication server, vector, matrix, inner product, success, failure, distinction

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2009-0042143 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 29 April 2009 See paragraphs [0017]-[0042]; and claims 1-7.	1-4
A	KR 10-2010-0013486 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 10 February 2010 See paragraphs [0019]-[0091]; claim 1; and figures 1-3.	1-4
A	KR 10-0911594 B1 (KABUSHIKI KAISHA HITACHI SEISAKUSHO(D/B/A HITACHI, LTD.)) 07 August 2009 See paragraphs [0017]-[0061]; claim 1; and figures 1-4.	1-4
A	JP 2012-022507 A (NTT DATA CORP.) 02 February 2012 See paragraphs [0013]-[0025]; claim 1; and figures 1-2.	1-4
A	JP 2013-120580 A (HITACHI LTD.) 17 June 2013 See paragraphs [0013]-[0030]; claim 1; and figure 1.	1-4



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

09 AUGUST 2018 (09.08.2018)

Date of mailing of the international search report

10 AUGUST 2018 (10.08.2018)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 189 Sconsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2018/005012

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2009-0042143 A	29/04/2009	KR 10-1010218 B1 US 2009-0113209 A1 US 8239685 B2	21/01/2011 30/04/2009 07/08/2012
KR 10-2010-0013486 A	10/02/2010	KR 10-0986980 B1	11/10/2010
KR 10-0911594 B1	07/08/2009	CN 101159554 A CN 101159554 B EP 1912151 A1 JP 2008-092413 A JP 4996904 B2 KR 10-2008-0031622 A US 2008-0178008 A1 US 8443201 B2	09/04/2008 23/05/2012 16/04/2008 17/04/2008 08/08/2012 10/04/2008 24/07/2008 14/05/2013
JP 2012-022507 A	02/02/2012	JP 5439306 B2	12/03/2014
JP 2013-120580 A	17/06/2013	JP 5852870 B2 WO 2013-084617 A1	03/02/2016 13/06/2013

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/32(2013.01)i, G06F 21/45(2013.01)i, H04L 9/30(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 21/32; G06F 17/10; G06F 21/20; H04L 9/32; G06K 9/00; G06F 21/00; G06T 7/00; G06F 21/45; H04L 9/30

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 생체 정보, 인증, 비밀 정보, 등록 단말기, 인증 서버, 벡터, 행렬, 내적 값(inner product), 성공, 실패, 판별

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2009-0042143 A (한국전자통신연구원) 2009.04.29 단락 [0017]-[0042]; 및 청구항 1-7 참조.	1-4
A	KR 10-2010-0013486 A (한국전자통신연구원) 2010.02.10 단락 [0019]-[0091]; 청구항 1; 및 도면 1-3 참조.	1-4
A	KR 10-0911594 B1 (가부시키가이샤 히타치세이사쿠쇼) 2009.08.07 단락 [0017]-[0061]; 청구항 1; 및 도면 1-4 참조.	1-4
A	JP 2012-022507 A (NTT DATA CORP.) 2012.02.02 단락 [0013]-[0025]; 청구항 1; 및 도면 1-2 참조.	1-4
A	JP 2013-120580 A (HITACHI LTD.) 2013.06.17 단락 [0013]-[0030]; 청구항 1; 및 도면 1 참조.	1-4

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2018년 08월 09일 (09.08.2018)

국제조사보고서 발송일

2018년 08월 10일 (10.08.2018)

ISA/KR의 명칭 및 우편주소



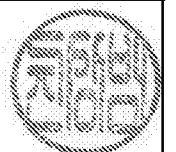
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-481-8578

심사관

진상범

전화번호 +82-42-481-8398



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2009-0042143 A	2009/04/29	KR 10-1010218 B1 US 2009-0113209 A1 US 8239685 B2	2011/01/21 2009/04/30 2012/08/07
KR 10-2010-0013486 A	2010/02/10	KR 10-0986980 B1	2010/10/11
KR 10-0911594 B1	2009/08/07	CN 101159554 A CN 101159554 B EP 1912151 A1 JP 2008-092413 A JP 4996904 B2 KR 10-2008-0031622 A US 2008-0178008 A1 US 8443201 B2	2008/04/09 2012/05/23 2008/04/16 2008/04/17 2012/08/08 2008/04/10 2008/07/24 2013/05/14
JP 2012-022507 A	2012/02/02	JP 5439306 B2	2014/03/12
JP 2013-120580 A	2013/06/17	JP 5852870 B2 WO 2013-084617 A1	2016/02/03 2013/06/13