Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.6, Dec. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.6.1319

함수암호를 이용한 인증정보 Template 보호 기술*

박 동 희,† 박 영 호‡
세종사이버대학교

Authentication Template Protection Using Function Encryption*

Dong Hee Park,† Young-Ho Park‡
Sejong Cyber University

요 약

최근 생체정보, 위치정보 등이 다양한 디바이스 인증에 활용되고 있다. 그러나 이러한 인증정보 템플릿들은 평문 형태로 안전한 저장공간(Trust Zone)에 저장 되거나 또는 인증서버에 암호문으로 저장된 인증정보를 인증요청시 복호화하여 평문형태에서 인증에 사용된다. 따라서 해킹에 의한 인증정보의 유출시 치명적인 프라이버시 문제가 발생할 수 있다. 본 논문에서는 함수암호를 이용하여 암호화된 상태에서 인증정보의 노출 없이 안전하게 인증할 수 있는 방법을 제안한다.

ABSTRACT

Recently, biometrics and location information are being used for authentication in many devices. However, these information are stored as plaintext in safe device or, stored as ciphertext in authentication server it is used for authentication in plaintext by decrypting. Therefore, the leakage of authentication information as well as hacking can cause fatal privacy problems. In this paper, we propose a technique that can be authenticated without exposing authentication information to ciphertext using function encryption.

Keywords: Function encryption, Biometric authentication, Authentication template protection

I. 서 론

오늘날 클라우드 환경과 스마트 기기의 보급으로 다양한 온라인 서비스가 활성화 되면서 기기의 생체정보 또는 위치정보를 사용한 인증이 많아지고 있다. 그 중 스마트폰 등 다양한 디바이스에서 생체정보를 활용하여 안전하고 편리한 생체인증 방법이 주목 받고 있다.[1]

생체정보는 지문, 얼굴, 장문, 손 모양, 홍채, 정맥 등의 생물학적 특징과 서명, 음성, 키보드 입력, 걸음걸이 등의 행동학적 특징으로 구성되어 있다. 이러한 사용자의 생체정보를 이용하여 사용자의 편리함과 안전성을 유지하며 사용자의 자각을 최소화하는 차세대 인증연구가 활발하게 이루어지고 있다. 하지만 생체정보로부터 추출된 인증정보 템플릿을 암호화되지 않은 상태로 저장할 경우 정보의 유출로 인해 야기되는 피해는 지식기반인증과 소유기반인증을 사용할 때보다 더 크다고 할 수 있다. 이는 사용자의 생체정보가 변경되지 않기에 지식기반인증 또는 소유기반인증처럼 삭제하고 재발급하기 어렵다는 것에 근거한다.[2]

따라서 생체정보를 이용한 인증은 생체정보를 안전하게 보호할 수 있는 안전한 저장소(Trust Zone)가 갖추어진 스마트폰과 같은 디바이스에서 제한적으로 사용되어야 한다. 하지만 4차 산업혁명

Received(11. 12. 2019), Accepted(12. 06. 2019)
* 본 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2017-0-00380,차세대 인증 기술 개발)"
† 주저자, pdhwe@naver.com
‡ 교신저자, youngho@sjcu.ac.kr(Corresponding author)

시대에는 다양한 응용분야에서 생체정보나 위치정보 등 인증정보를 활용하여 온라인상에서 안전하게 인증할 수 있는 환경이 요구되고 있다. 이러한 온라인상의 생체정보를 활용한 인증은 일반적으로 인증서버에 인증정보템플릿을 암호화하여 저장하고, 인증요청 시 인증정보를 복호화하여 평문상태에서 인증을 시도한다. 따라서 인증서버는 인증정보를 평문상태에서 알 수 있으며 인증서버의 해킹 또는 관리자의 부주의로 인한 유출 문제가 대두된다. 따라서 안전한 하드웨어를 사용할 수 없는 온라인 인증환경에서도 인증정보를 암호화하여 복호화하지 않은 상태에서 인증할 수 있는 인증기법과 인증정보 템플릿을 안전하게 보호할 수 있는 기법이 필요하다.

본 논문에서는 함수암호를 이용하여 암호화된 상태에서 인증정보의 노출 없이 안전하게 인증할 수 있는 방법을 제안한다.

2장에서는 생체정보를 인증하기 위한 Fuzzy 인증과 Distance measure 방식에 대하여 소개하고 3장에서 안전성을 보장할 DDH기반의 함수암호를 소개한다. 4장에서는 함수암호를 이용한 안전한 인증 Template 보호 방법을 제안한다. 5장에서는 결론을 맺는다.

II. 생체 인증 정보

2.1 Fuzzy 인증

생체정보를 이용한 인증은 Noise가 존재하며 인가자를 비인가자로 판단하는 본인거부 에러(FRR)와 비인가자를 인가자로 판단하는 오인식 에러(FAR)가 발생한다. 따라서 등록된 생체정보와 인증 받을 정보 간의 차이가 발생한다. Fuzzy 인증기법은 Distance measure를 사용하여 Template 정보와 인증 대상 정보와의 유사도 분석결과를 도출한다. 이때 유사도 결과는 일치, 대략 일치, 대략 불일치, 불일치 등으로 표현되며 생체정보의 특성에 따라 적

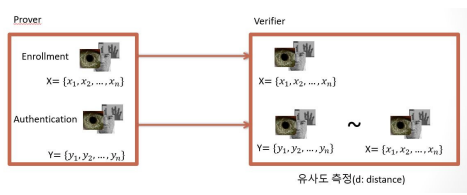

Fig. 1. Fuzzy Authentication

당한 거리함수를 이용하여 판단한다.[3]

2.2 Distance measure

거리함수는 크게 유클리디언 거리함수와 비유클리디언 거리함수로 구분된다. 유클리디언 거리함수에는 대표적으로 L_2 norm distance, L_∞ norm distance 그리고 L_1 norm distance가 있다. 비유클리디언 거리함수는 집합론에 근거한 Jaccard distance, Cosine 함수에 근거한 Cosine distance가 있다. Hamming distance는 서로 다른 비트의 개수를 출력하는 방식이다.[4]

2.2.1 Hamming distance를 이용한 유사도 비교

지문, 홍채, 얼굴인식 등 생체정보를 이용한 유사도 기법으로 Hamming distance(HD)를 많이 사용한다. Sudha Gupta는 HD를 이용하여 홍채 인식 방법을 제안하였다.[5] Ujwalla Gawande와 Anushree Spare등은 HD를 이용하여 지문정보와 홍채정보를 결합한 생체정보를 인식하는 방법을 제안하였다.[6] 이러한 HD는 데이터 X, Y의 불일치하는 비트 개수의 합으로 볼 수 있다. 따라서 n 비트의 데이터 $X=(x_1,...,x_n)$, $Y=(y_1,...,y_n)$를 비교할 때, Hamming distance는 다음과 같이 정의 될 수 있다.[7]

$$HD(X,Y)=\frac{1}{n}\sum_{j-1}^{n}X_j\bigoplus Y_j$$

2.2.2 Euclidean distance를 이용한 유사도 비교

유클리드 거리(Euclidean distance)는 다양한 이미지 인식을 위해 채택되어 매우 유용하게 사용된다.[8] 홍채와 지문 같은 생체정보는 등록된 이미지 벡터와 인증 요청된 이미지 벡터를 비교함으로써 인증 처리한다. 인증처리 방법은 두 벡터의 유클리드 거리를 계산하고, 계산된 거리를 임계값과 비교하여 인증한다. 이때 유클리드 거리가 임계값보다 작거나 같으면 인증알고리즘은 '일치' 그렇지 않으면 '불일치'를 반환한다.

l길이의 벡터 $X=(x_1,x_2,\cdots,x_l)$, $Y=(y_1,y_2,\cdots,y_l)$그리고 임계값을 τ라 하면 두 벡터

사이의 유클리드 거리 $d(X,Y)$는 다음과 같이 표현할 수 있다.

$$d(X,Y)=\sqrt{\sum_{i=1}^{l}(x_i-y_i)^2}$$

위 유클리드 거리 $d(X,Y)$를 내적으로 표현하면 다음과 같다.

$$d(X,Y)=\sqrt{<X-Y,X-Y>}$$

따라서 $d(X,Y)<\tau$ 의 경우 '일치'를 반환하고 그렇지 않으면 불일치를 반환한다.

III. DDH 가정에 근거한 함수암호

3.1 함수암호

공개키 암호는 평문을 공개키를 이용하여 암호화하고 개인키로 암호문을 복호화하여 평문을 얻는다. 하지만 함수암호는 평문을 공개키로 암호화하고 주어진 함수와 관련된 비밀키를 사용하여 암호문을 평문으로 복호화하지 않고 함수값 만을 얻을 수 있다. 따라서 함수암호를 이용하면 인증정보를 암호화한 상태에서 인증을 수행할 수 있는 가능성을 제시하고 있다. 함수암호는 일반적으로 다음 4가지 알고리즘으로 구성되어 있다.[9]

- $Setup(1^\lambda)$: 보안상수 1^λ 를 입력으로 하여 마스터 공개키 mpk와 마스터 비밀키 msk를 생성한다.
- $Keygen(msk,X)$: msk와 X를 이용하여 함수 f 에 근거한 비밀키 $sk(f)$를 생성한다.
- $Encrypt(mpk,Y)$: mpk를 이용하여 입력값 Y를 암호문 Ct로 암호화 한다.
- $Decrypt(sk(f),Ct)$: Ct로부터 비밀키 $sk(f)$를 이용하여 $f(Y)$를 얻는다.

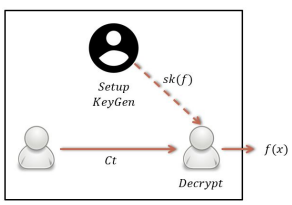

Fig. 2. Function Encryption Algorithm

3.2 DDH 가정에 근거한 내적함수

Decisional Diffie-Hellman(DDH)은 군 G는 위수가 소수 p인 생성원 g로 생성된 순환군이라 하면 (g^a,g^b,g^{ab})이 주어 졌을 때 (g^a,g^b,g^c)를 계산적으로 구분할 수 없다는 것을 가정한다. Abdalla가 제안한 다음과 같은 함수암호는 DDH 가정에 근거한 설계로 선택적 평문공격에 안전하다고 증명되었다.[10]

- $Setup(1^\lambda,1^l): \boldsymbol{s}=(s_1,s_2,\cdots,s_l)\leftarrow Z_p^l$
  $mpk=(h_1,...,h_l),\ h_i=g^{s_i},\ msk=\boldsymbol{s}$
- $Keygen(msk,X): X=(x_1,x_2,\cdots,x_l)$
  $sk(f)=<\boldsymbol{s},X>$
- $Encrypt(mpk,Y):\ k\leftarrow Z_p$
  $Y=(y_1,y_2,\cdots,y_l)$
  $ct_0=g^k,\ ct_i=h_i^k g^{y_i}$
  $Ct=[ct_0,(ct_i)_{i\in[l]}]$
- $Decrypt(sk_f,Ct): \prod_{i\in[l]} ct_i^{x_i}/ct_0^{sk_f}$
  $=\prod_{i\in[l]}(g^{s_i k+y_i})^{x_i}/g^{k(\sum_{i\in[l]}x_i s_i)}$
  $=g^{\sum_{i\in[l]}x_i s_i k+\sum_{i\in[l]}y_i x_i-k\sum_{i\in[l]}x_i s_i}$
  $=g^{\sum_{i\in[l]}y_i x_i}=g^{<X,Y>}$

Fig. 3. Abdalla function encryption scheme[10]

IV. 함수암호를 이용한 적용한 인증기법 설계

본 장에서는 Abdalla의 함수암호기법을 이용한 인증기법을 제안한다. 제안하는 인증기법은 사전단계, 등록단계, 인증단계로 구성된 3가지 단계로 나누어져 있다. 4.1에서는 난수를 안전하게 저장할 수 없는 디바이스의 경우에 적합한 인증 프로토콜을 제안하며 4.2에서는 난수를 안전하게 저장할 수 있는 디바이스에 적합한 인증 프로토콜을 제안한다.

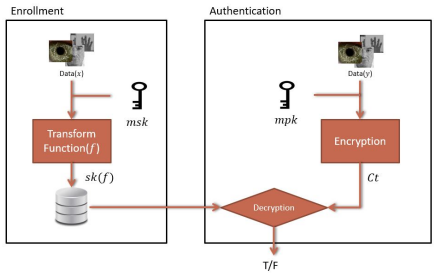

Fig. 4. Suggested protocol

4.1 제안 인증기법

본 소절에서는 난수를 안전하게 저장할 수 없는 디바이스에 적합한 인증 프로토콜을 제안한다.

4.1.1 사전단계

제안 인증 시스템에 사용될 파라미터와 군 G, 소수 p, 생성원 g를 설정한다. 또한 시스템의 마스터 공개키 mpk와 마스터 비밀키 msk를 생성한다.

- 1^{λ}: 보안 상수
- l : 암호문의 벡터의 길이
- $GroupGen(1^{\lambda}) : (G, p, g) : G = < g > = \{g^1, ..., g^p\}$
- $Setup(1^{\lambda}, 1^{l}) : msk = \boldsymbol{s} = (s_1, ..., s_l) \in Z_p^l,$
  $mpk = (h_1, ..., h_l), h_i = g^{s_i}$

4.1.2 등록단계

인증정보 X를 등록 요청 할 사용자 A는 다음 과정을 실행한다.

■ 사용자 A(User A): 인증정보 X를 추출한 후 난수 r을 선택하고 rX, X_A를 생성한다. (ID_A, rX, g^r, X_A)를 안전한 채널을 통해 서버에 송신하여 등록을 요청한다. ID_A는 사용자의 신분정보를 나타낸다.

$$1)\ X = (x_1, x_2, ..., x_l) \in Z_p^l$$
$$2)\ r \leftarrow Z_p$$
$$3)\ rX = r(x_1, x_2, ..., x_l) \bmod p$$
$$4)\ X_A = g^{r < X, X >}$$

■ 서버(Sever): (ID_A, rX, g^r, X_A)를 수신한 서버는 다음 $Keygen$ 알고리즘을 통해 sk_f를 생성한다.

$$KeyGen(msk, f) \rightarrow sk_f = < msk, rX > = r < \boldsymbol{s}, X > \pmod p = r \sum s_i x_i \pmod p$$

또한 사용자 ID_A의 인증요청 시 검증의 효율성을 위하여 본 제안기법에서는 검증테이블(Authentication Table)을 사용한다. 검증테이블에는 인증여부를 결정하기 위한 임계값 τ을 정하고 두 벡터 X, Y의 유클리드거리 함수 $d(X, Y)$값이 $0 \le d(X, Y)^2 \le \tau$ 을 만족하는 모든 경우에 대해 Table 2와 같은 효율적인 검증테이블(Authentication Table)을 만든다.

Table 1. Authentication Table

$d(X, Y)$	$H(ID_A \| g^{r[d(X,Y)]^2})$
0	$H(ID_A \| g^0)$
1	$H(ID_A \| g^r)$
2	$H(ID_A \| g^{4r})$
…	…
τ	$H(ID_A \| g^{\tau^2 r})$

검증테이블은 저장공간의 효율성을 위해서 $ID_A \| g^{r[d(X,Y)]^2}$ 값에 해시 H를 적용하여 $H(ID_A \| g^{r[d(X,Y)]^2})$ 만든 후 Table에 저장한다.

4.1.3 인증단계

(1) 요청단계

인증 요청할 사용자는 자신의 ID인 ID_A를 서버에 송신한 후 서버는 난수 t를 생성하여 ID_A에 해당되는 g^r을 이용하여 g^{rt}를 계산하고 사용자에게 송신한다. g^{rt}를 수신한 사용자는 다음 과정을 실행한다.

■ 사용자 A(User A): 인증정보 Y를 추출 한 후 난수 k을 선택하고 Ct 그리고 Y_A를 생성한다. (ID_A, Ct, Y_A) 를 서버에 송신하여 인증을 요청한다.

- $Encrypt(mpk, Y) \rightarrow Ct = (ct_0, (ct_i)_{i \in [l]})$
  1) $Y = (y_1, y_2, ..., y_l) \in Z_p^l$
  2) $k \leftarrow Z_p,\ ct_0 = g^k,\ ct_i = h_i^k g^{y_i}, i \in [l]$
  3) $Y_A = g^{rt < Y, Y >}$

■ 서버(Sever) : $(ID_A,\ Ct,\ Y_A)$를 수신한 서버는 $Y'_A = Y_A^{1/t} = g^{r < Y, Y >}$ 을 계산한 후 ID_A의 정보 $rX = (rx_1, \cdots, rx_l)$ 를 사용하여 다음 $Decrypt$ 알고리즘을 통해 $g^{r < X-Y, X-Y >}$를 생성한다.

- $$Decrypt(sk_f, Ct) \rightarrow X_A \left[\prod_{i=1}^{l} (ct_i^{rx_i} / ct_0^{sk_f}) \right]^{-2} Y'_A$$
$$= X_A (g^r)^{-2 < X, Y >} Y'_A$$
$$= g^{r < X, X >} g^{-2r < X, Y >} g^{r < Y, Y >}$$
$$= g^{r[< X, X > -2 < X, Y > + < Y, Y >]}$$
$$= g^{r < X-Y, X-Y >}$$

(2) 검증단계

요청단계에서 얻은 $Decrypt(sk_f, Ct) = g^{r < X-Y, X-Y >}$값은 Euclidean Distance $d(X, Y)$으로 표현하면 $Decrypt(sk_f, Ct) = g^{r < X-Y, X-Y >} = g^{r[d(X,Y)]^2}$ 으로 정리할 수 있다. 따라서 요청단계에서 얻은 $Decrypt(sk_f, Ct)$ 값을 사용하여 $H(ID_A \| g^{r < X-Y, X-Y >})$ 을 구하고 ID_A의 검증테이블과 비교하여 검증한다. 해당 검증테이블에 저장된 값과 일치하면 '일치' 판정을 하고 저장된 값과 일치하지 않으면 '불일치' 판정을 한다.

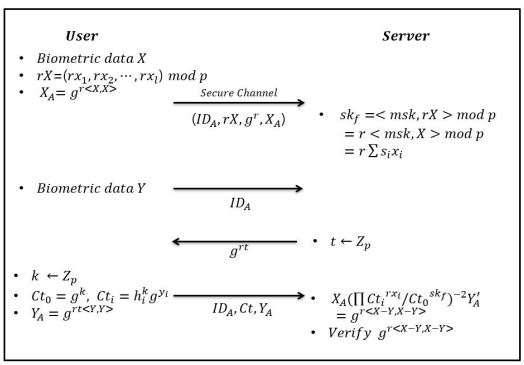

Fig. 5. Registration & Authentication protocol

4.2 변형된 제안 인증기법

난수 r을 안전하게 저장할 수 있는 Trust Zone을 가지고 있는 디바이스의 경우에 적합한 인증 프로토콜을 제안한다. 난수 r을 안전하게 저장할 수 있으므로 4.1.3 의 g^{rt}를 수신하는 단계를 제외하여 간단하게 설계할 수 있다.

4.2.1 사전단계 및 등록단계

4.1에서 제안한 스킴의 사전단계 및 등록단계와 동일하다.

4.2.2 인증단계

(1) 요청단계

생체정보 Y를 인증 요청할 사용자는 다음 과정을 실행한다.

■ 사용자 A(User A) : 인증정보 Y를 추출 한 후 난수 k을 선택하고 Ct 그리고 Y_A를 생성한다. $(ID_A,\ Ct,\ Y_A)$ 를 서버에 송신하여 인증을 요청한다.

- $Encrypt(mpk, Y) \rightarrow Ct = (ct_0, (ct_i)_{i \in [l]})$
  1) $Y = (y_1, y_2, ..., y_l) \in Z_p^l$
  2) $k \leftarrow Z_p, ct_0 = g^k,\ ct_i = h_i^k g^{y_i}, i \in [l]$
  3) $Y_A = g^{r < Y, Y >}$

■ 서버(Sever) : $(ID_A,\ Ct,\ Y_A)$를 수신한 서버는 다음과 같이 $Decrypt$ 알고리즘을 통해 $g^{r < X-Y, X-Y >}$을 생성한다.

- $$Decrypt(sk_f, Ct) \rightarrow X_A \left[\prod_{i=1}^{l} (Ct_i^{rx_i} / Ct_0^{sk_f}) \right]^{-2} Y_A$$
$$= X_A (g^r)^{-2 < X, Y >} Y_A$$
$$= g^{r < X, X >} g^{-2r < X, Y >} g^{r < Y, Y >}$$
$$= g^{r[< X, X > -2 < X, Y > + < Y, Y >]}$$
$$= g^{r < X-Y, X-Y >}$$

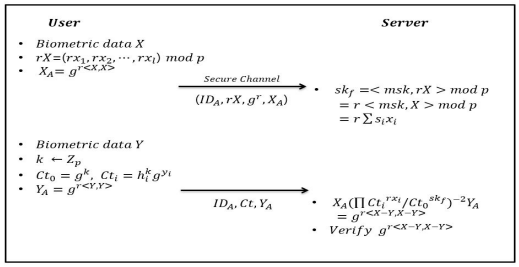

Fig. 6. Modified protocol

(2) 검증단계

4.1에서 제안한 스킴의 인증 검증단계와 동일하다.

V. 제안된 프로토콜의 안전성 및 효율성

5.1 프로토콜의 안전성

본 논문에서 제안된 인증기법은 Abdalla의 함수 암호를 사용함으로서 안전성을 보장하며 Discrete Logarithm Problem(DLP)와 Diffie-Hellman Problem(DHP)의 어려움에 기반을 두고 있다. 제안된 프로토콜은 아래와 같은 공격에 대하여 안전하다.

- 반복공격(Replay Attack) : 공격자가 사용했던 정보 $Y_A = g^{rt<Y,Y>}$를 다시 사용하면 인증요청단계에서 난수 t가 변경되어 검증과정을 통과할 수 없다.
- 위장공격(Impersonation Attack) : 공격자가 사용자 A로 위장하여 속이려 한다고 가정하자. 먼저 공격자가 Y를 변조하지 않았을 경우 검증과정을 통과하기 위해서는 $g^{<Y,Y>}$를 얻어야 한다. g^{rt}, $g^{rt<Y,Y>}$를 알고 있는 상황에서 $g^{<Y,Y>}$를 얻는 것은 DHP와 DLP에 의하여 어렵다. 공격자가 Y를 변조하였을 경우 $g^{rt<Y,Y>}$를 얻어야 한다. 만일 정당한 사용자의 생체정보 Y대신 $Z(\neq Y)$로 하여 $g^{rt<Z,Z>}$ 얻을 경우 인증 검증단계에서 $H(ID_A \| g^{r<X-Z,X-Z>})$가 검증테이블을 만족하기 어렵다. 그러므로 본 프로토콜은 위장공격을 방어할 수 있다.
- 비밀키 노출 : 제안된 프로토콜은 인증서버에서 비밀키 sk_f가 노출 된다고 하여도 사용자의 인증정보는 유출되지 않는다는 특성을 가지고 있다. 만일 $sk_f = r\sum s_i x_i \,(\mathrm{mod} p)$을 노출되었다 하더라도 r값과 $X=(x_1, x_2, ..., x_l)$을 알기 어렵다. 또한 등록단계에서 수신한 rX, $g^{r<X,X>}$으로부터 r은 사용자가 만들어낸 난수이다. 따라서 서버는 사용자의 인증정보 X를 알 수 없으므로 악의적인 인증 서버 관리자로부터 안전하다. 단, 제안 프로토콜에서는 X의 원소 $x_1, x_2, ..., x_l$는 균일한 난수분포에서 사용자마다 생성된다고 가정한다.

5.2 프로토콜의 효율성

본 프로토콜에서 주된 계산량은 G에서의 지수승 연산에 의존하며 multi-exponentiation연산이 사용된다. Straus의 Multi-exponentiation 알고리즘[11]을 이용하여 효율적으로 연산할 수 있으며 고정된 값에 대한 지수승에 대해서는 조금 더 효율적으로 연산할 수 있다. 따라서 지수승 연산을 exponentiation(exp), fixed-exponentiation ($fexp$), multi-exponentiation($mexp$), fixed multi-exponentiation($fmexp$)으로 구분하여 인증요청단계의 효율성을 분석하였다. 사전 등록단계와 검증단계는 상대적으로 효율적이므로 분석을 생략한다.

Table 2에서는 인증요청단계에서 $User$와 $Server$의 지수승 연산 횟수를 나타내었다.

Table 2. efficiency

	연산	지수승 횟수
$User$	$ct_0 = g^k$	$fexp$: 1
	$ct_i = (g^{s_i})^k \; g^{y_i}$	$fmexp$: l
	$Y_A = g^{rt<Y,Y>}$	exp : 1
$Server$	$(g^r)^t$	$fexp$: 1
	$Y_A' = (g^{rt<Y,Y>})^{1/t}$	exp : 1
	$X_A \left[\prod_{i=1}^{l} (ct_i^{rx_i} / ct_0^{sk_f})\right]^{-2} Y'_A$	$mexp$: $l+1$

VI. 결 론

본 논문은 함수암호를 이용하여 노이즈가 있는 인증정보의 Template 보호 기술을 제안하였다. 내적을 위해 설계된 Abdalla의 함수 암호를 적용하였으며 인증정보를 암호화한 후, 유클리드 거리 함수를 통하여 유사도를 비교하는 인증 방법을 제시하였다. 기존 인증기법과 달리 함수암호를 이용하여 인증정보를 암호화된 상태에서 복호화 하지 않고 인증을 수행할 수 있는 기법을 제안하였으며 제안된 기법은 Trust Zone과 같은 안전한 공간이 없는 디바이스에서도 안전하게 인증정보를 보호하여 온라인상에서도 생체인증과 위치인증 등 인증서비스를 수행할 수 있도록 한다.

본 제안기법은 기존 RSA, ECC 등 기존 공개키

기반 암호의 도메인 파라미터를 그대로 적용할 수 있으며 기존 암호가 탑재된 환경에서 효율적으로 적용 가능하다. 하지만 인증정보의 벡터값 l이 커지면 연산 효율성이 떨어질 수 있다.

따라서 상대적으로 작은 템플릿정보를 갖는 생체인증에 효율적이며 생체정보 이외에도 위도, 고도, 경도로 이루어진 GPS위치정보 인증에 활용할 수 있다. 위치정보에 제안한 기법을 활용하면 접근하려는 목표 위치와 인접함을 증명할 때 미사일과 같은 군사무기 사용에 있어서 위치정보의 노출 없이 효율적으로 활용할 수 있다.

References

[1] HeeJin Park, Younho Lee "Survey on Privacy-preserving Techniques for Biometric Authentication", Journal of KIIT. vol. 16, no. 4, pp. 109-122, Apr. 2018

[2] Lifeng Lai, Siu-Wai Ho and H. Vicent Poor, "Privacy-Security Trade-Offs in Biometric Security Systems-Part Ⅱ:Multiple Use Case," IEEE Transactions on information forensics and security, vol. 6, no. 1, pp. 140-151, Mar. 2011

[3] Fuchun Guo, Willy Susilo anc Yi Mu, " Distance-Based Encryption: How to Embed Fuzziness in Biometric-Based Encryption" IEEE Transactions on information forensics and security, vol. 11, no. 2, pp. 247-257, Feb. 2016

[4] Kim S, Lewi K, Mandal A, Montgomery H, Roy A, Wu D.J. (2018) Function-Hiding Inner Product Encryption Is Practical. In: Catalano D, De Prisco R. (eds) Security and Cryptography for Networks. SCN 2018. Lecture Notes in Computer Science, vol 11035. Springer, Cham

[5] Sudha Gupta, Viral Doshi, Abhinav Jain and Sreeram Iyer, "Iris Recognition System using Biometric Template Matching Technology", International Journal of Computer Applications, vol. 1, no. 2 , pp. 21-30, Feb. 2010

[6] Ujwalla Gawande, Anushree Spare, Apurva Jain, Sachita Bhriegu, Shruti Sharma,"Fingerprint-Iris Fusion Based Multimodal Biometric System Using Single Hamming Distance Matcher", International Journal of Engineering Inventions, vol 2, no. 4, pp. 54-61 , Feb. 2013

[7] John G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15, no. 11, Nov. 1993

[8] Fuchun Guo, Willy Susilo anc Yi Mu, "POSTER:Euclidean Distance Based Encryption: How to Embed Fuzziness in Biometric Based Encryption", Proc. ACM Conference of Computer Communication and Security, pp. 1430-1432, 2014

[9] Boneh D., Sahai A., Waters B. (2011) Functional Encryption: Definitions and Challenges. In: Ishai Y. (eds) Theory of Cryptography. TCC 2011. Lecture Notes in Computer Science, vol 6597. Springer, Berlin, Heidelberg

[10] Abdalla M, Bourse F, De Caro A, Pointcheval D. (2015) Simple Functional Encryption Schemes for Inner Products. In: Katz J. (eds) Public-Key Cryptography, PKC 2015. Lecture Notes in Computer Science, vol 9020. Springer, Berlin, Heidelberg

[11] Möller B. (2001) Algorithms for Multi-exponentiation. In: Vaudenay S., Youssef A.M. (eds) Selected Areas in Cryptography. SAC 2001. Lecture Notes in Computer Science, vol 2259. Springer, Berlin, Heidelberg

〈저 자 소 개〉

박 동 희 (Dong Hee Park) 학생회원
2010년 2월: 서울과학기술대학교 전기정보공학과 공학사
2018년 3월~현재: 세종사이버대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호, 공개키 암호시스템, 차세대인증, 생체인증

박 영 호 (Young-Ho Park) 종신회원
1990년 2월: 고려대학교 수학과 이학사
1993년 2월: 고려대학교 수학과 이학석사
1997년 2월: 고려대학교 수학과 이학박사
2002년 2월~현재: 세종사이버대학교 정보보호학과 교수
〈관심분야〉 공개키 암호, 암호 프로토콜, 부채널 공격, 암호안전성평가, 차세대인증