*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.32, NO.5, Oct. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.5.779

# 효율적인 LWE 기반 재사용 가능한 퍼지 추출기*

김 주 언,[1†] 이 광 수,[2] 이 동 훈[3‡]
[1,3]고려대학교 (대학원생, 교수), [2]세종대학교 (교수)

# An Efficient LWE-Based Reusable Fuzzy Extractor*

Juon Kim,[1†] Kwangsu Lee,[2] Dong Hoon Lee[3‡]
[1,3]Korea University (Graduate student, Professor),
[2]Sejong University (Professor)

요 약

퍼지 추출기는 노이즈가 섞여 입력값이 항상 같지 않은 생체 데이터로 키를 생성하여 생체 정보 노출 없이 안전하게 인증을 수행하는 바이오-암호화 기술이다. 그러나 한 사용자가 생체 데이터를 여러 서버에 등록할 경우 퍼지 추출기의 인증 과정에서 키를 올바르게 추출하기 위해 공개되는 정보인 보조 데이터에 대한 다양한 공격으로 키가 노출될 수 있다. 따라서 여러 서버에 같은 사람의 생체 데이터를 등록해도 안전한 재사용 가능한 퍼지 추출기에 관한 연구가 많이 이루어지고 있으나, 현재까지 제시된 연구들은 키 길이가 늘어남에 따라 키를 복구하는 과정의 횟수가 점진적으로 증가하여 효율적이지 않고 보안성 높은 시스템에 적용하기 힘들다. 이에 본 논문에서는 키 길이가 늘어나도 인증 과정의 수행 횟수가 같거나 비슷한 LWE 기반의 효율적이고 재사용 가능한 퍼지 추출기를 설계하였고, 제안 기법이 Apon et al.[5]이 정의한 재사용의 안전성을 만족함을 보였다.

ABSTRACT

Fuzzy extractor is a biometric encryption that generates keys from biometric data where input values are not always the same due to the noisy data, and performs authentication securely without exposing biometric information. However, if a user registers biometric data on multiple servers, various attacks on helper data which is a public information used to extract keys during the authentication process of the fuzzy extractor can expose the keys. Therefore many studies have been conducted on reusable fuzzy extractors that are secure to register biometric data of the same person on multiple servers. But as the key length increases, the studies presented so far have gradually increased the number of key recovery processes, making it inefficient and difficult to utilize in security systems. In this paper, we design an efficient and reusable fuzzy extractor based on LWE with the same or similar number of times of the authentication process even if the key length is increased, and show that the proposed algorithm is reusably-secure defined by Apon et al.[5].

**Keywords:** Fuzzy extractor, Biometric authentication, Reusabley-secure, Reusability, Learning with errors

## I. 서 론

생체 데이터는 한 번 노출되면 값을 변경하기 어렵고, 생체 정보 특성상 노이즈가 존재하므로 생체 데이터 노출 없이 적절한 오차 범위 내에서 인증이 수행되어야 한다. 퍼지 추출기(Fuzzy extractor)

Received(08. 03. 2022), Modified(09. 16. 2022), Accepted(09. 16. 2022)
* 본 논문은 고려대 암호기술 특화연구센터 (UD210027XD)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행된 연구임.
* 본 논문은 2022년도 한국정보보호학회 하계학술대회에 발표한 우수논문을 개선 및 확장한 것임.
† 주저자, jjjuon@korea.ac.kr
‡ 교신저자, donghlee@korea.ac.kr(Corresponding author)

는 생체 인식 시스템에서 생체 정보로부터 키를 생성하여 안전하게 인증하는 바이오-암호화 기술로, 등록 과정과 인증 과정으로 구성되어 있다[1]. 등록 과정에서 생체 정보를 입력하여 암호화 키를 만들고 보조 데이터를 생성해 서버에 저장하면, 인증 과정에서 입력된 노이즈가 섞인 생체 정보와 저장된 보조 데이터를 이용해 키를 재생성하여 등록 과정에서 만든 키와 비교함으로써 사용자를 검증한다. 이때 보조 데이터는 키와 독립적인 공개된 값으로 생체 데이터나 키에 대한 어떠한 정보도 노출해서는 안 된다[2].

그러나 한 사용자가 생체 데이터를 여러 서버에 등록하면, 상관관계가 있는 입력값들에 대해 출력되는 보조 데이터로 인증에 필요한 키에 대한 정보가 노출될 수 있다[3]. 따라서 사용자가 동일한 생체 정보를 여러 곳에 등록해도 키가 노출될 수 있는 공격들로부터 안전한 퍼지 추출기가 필요하다. Boyen[3]은 상관관계가 있는 비밀 값, 즉 같은 사람의 생체 데이터를 여러 번 반복해서 등록해도 안전한 재사용 가능한 퍼지 추출기에 대해 처음으로 정의를 내렸으며, 최근 이에 관한 연구가 활발히 이루어지고 있다[4-7].

Canetti et al.은 노이즈가 있는 생체 데이터들의 상관관계에 대한 가정 없이 생체 데이터 분포의 엔트로피가 낮을 때도 안전하고 재사용 가능한 퍼지 추출기를 설계하였다[4]. 그러나 Canetti et al.이 제안한 기법은 랜덤 오라클 모델에 의존하며 노이즈로 인해 발생하는 오차의 하위 선형 부분만을 허용하는 단점이 있다. Wen et al.이 제안한 DDH 가정 기반 재사용 가능한 퍼지 추출기는 오차의 선형 부분을 모두 허용하나, 입력하는 생체 데이터 분포에 제한이 있다[6]. Apon et al.은 랜덤 오라클 모델에 의존하지 않고 생체 데이터의 조건과 상관없이 재사용 가능한 LWE 기반의 퍼지 추출기를 설계하였다[5]. 그러나 Apon et al.이 제안한 기법은 키가 $\{0,1\}^m$으로 키 길이($m$)가 늘어남에 따라 인증 과정의 수행 횟수가 점진적으로 증가하는 한계가 있다.

따라서 본 논문에서는 랜덤 오라클 모델에 의존하지 않고, 입력하는 생체 데이터 분포에 제한이 없으며, 키를 $\{0,1\}^m$에서 $Z_q$로 확장하여 키 길이가 늘어나도 인증 과정에서 키를 복구하기 위해 수행되는 알고리즘의 횟수가 같거나 비슷한 LWE 기반의 효율적이고 재사용 가능한 퍼지 추출 기법을 제시한다. Apon et al. 기법은 키의 길이가 $m$일 때 인증 과정을 $\lceil \log_2 m \rceil$번 수행해야 하지만, 제안 기법은 $\lceil \log_q m \rceil$번 수행하여 키를 복구할 수 있다. 설계한 기법은 LWE 기반 키 교환 시 한 비트 오류 여부를 알 수 있도록 하는 Peikert의 조정(reconciliation) 메커니즘을 활용하여 키를 복구하며, Apon et al.이 정의한 재사용의 안전성(reusably-secure)을 만족한다.

본 논문의 구성은 다음과 같다. 2장에서는 배경지식을 서술하고, 3장에서는 퍼지 추출기를 소개한다. 4장에서는 제안하는 효율적인 LWE 기반 재사용 가능한 퍼지 추출기를 제시하고, 5장에서는 제안한 모델의 안전성을 분석한다. 마지막으로 6장에서는 결론을 맺는다.

## II. 배경지식

### 2.1 Peikert의 조정 메커니즘

Peikert[11]는 조정 메커니즘(Rec)을 이용해 두 사용자가 키를 올바르게 합의하는 래티스 기반 키 교환 프로토콜을 설계하였다. Rec은 노이즈로 인해 한 비트 에러가 생길 수 있는 LWE 기반 키를 정확하게 복구하기 위해 모듈러 라운딩(modular rounding) 함수 $\lfloor \bullet \rceil_2 : Z_q \rightarrow Z_2$와 크로스 라운딩(cross rounding) 함수 $\langle \bullet \rangle_2 : Z_q \rightarrow Z_2$를 사용한다.

모듈러 라운딩 함수는 키 스트림을 생성하는 함수로, $Z_q$상에 있는 계수를 각각 그림 1의 (a)와 같이 0과 $\frac{q}{2}$ 중 더 가까운 지점의 범위 값(0 또는 1)으로 바꾸어 키를 만든다. 크로스 라운딩 함수는 노이즈로 인해 키에 에러가 생겼는지에 대한 정보를 주기 위해 추가적인 힌트를 만드는 함수로, $Z_q$상에 있는 계수를 각각 그림 1의 (b)와 같이 0, $\frac{q}{4}$, $\frac{q}{2}$, $\frac{3q}{4}$ 중 더 가까운 지점의 범위 값(0 또는 1)으로 바꾸어 공개한다.

예를 들어, 두 사용자 $A$와 $B$가 키를 합의하고자 하는데 노이즈로 인해 $A, B$가 공유하는 값을 각각 $\frac{q}{4}$, $\frac{q}{4}+1$로 도출했다고 하자. 모듈러 라운딩 함수의 결과 키로 $A$는 0을, $B$는 1을 갖게 되므로 둘은 올바르게 키를 합의하지 못한다. 이때, 크로스 라

운딩 함수로 출력된 공개 값이 각각 0, 1로 다르므로 $A,B$는 이를 통해 키에 한 비트 에러가 발생한 사실을 알 수 있으며 결과적으로 같은 키를 합의할 수 있다.

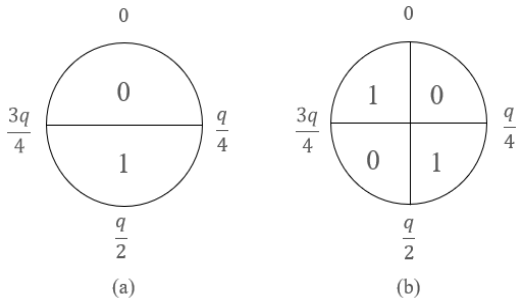


Fig. 1. (a) Modular rounding function (b) Cross rounding function

### 2.2 Learning With Errors

Regev[12]가 제안한 LWE(Learning With Errors)는 양자 컴퓨터로도 풀기 어려운 격자 기반 문제다. LWE 문제는 단순하고 유연하며 현재까지 이를 푸는 양자 알고리즘이 없어 다양한 공개키 암호 시스템에 응용된다[13-16]. LWE 분포에서 표본 추출된 결과가 출력될 때 LWE 문제는 Search LWE 문제와 Decision LWE 문제로 나뉘며 LWE 가정은 두 LWE 문제를 다항 시간 안에 풀 확률이 무시할 수 있을 만큼 매우 낮다(negligble)는 것을 의미한다. Goldwasser et al.[18]은 에러 분포의 엔트로피를 바탕으로 다항 시간 안에 LWE 가정이 성립하는 Decision LWE 문제의 안전성 파라미터를 정리 1과 같이 설정하였다.

**정의 1. [LWE 표본]** 임의의 $A \leftarrow Z_q^{m \times n}$, 비밀 벡터 $s \leftarrow Z_q^n$, 그리고 에러 분포 $\chi$(이산 가우시안 분포 $D_{Z,\alpha}$)에서 추출한 오류 $e \leftarrow \chi^m$를 이용해 출력한 $(A, b = < A, s > + e \pmod q)$를 $\mathrm{LWE}_{n,m,q,\chi}$ 표본이라고 한다.

**정의 2. [Search LWE]** $m$개의 LWE 표본 $(A, < A, s > + e \pmod q)$이 주어졌을 때, $s \leftarrow Z_q^n$를 찾는 문제를 Search LWE 문제라고 한다.

**정의 3. [Decision LWE]** $m$개의 표본이 주어졌을 때, 이것이 LWE 표본 $(a, < a, s > + e \pmod q)$인지 임의의 값 $(a,b)$인지 구분하는 문제를 Decision LWE 문제라고 한다.

**정리 1.** $k \geq \log q$이고 함수 $h : \{0,1\}^n \rightarrow \{0,1\}^*$를 역변환하는 것이 $2^{-k}$만큼 어려울 때, 즉 주어진 $h(s)$에서 $s$를 다항 시간 안에 찾을 확률이 $2^{-k}$보다 작을 때 다음과 같다. $l = \frac{k - w(\log n)}{\log q}$인 $\mathrm{LWE}_{l,m,q,D_{Z,\beta}}$가정에서 $m = \mathrm{poly}(n)$, $\alpha, \beta \in (0,q)$여서 $\beta/\alpha = \mathrm{negl}(n)$이면 $\{A, b = As + e, h(s)\}$와 임의의 $u \leftarrow Z_q^m$으로 구성된 $\{A, u, h(s)\}$를 구분하기 어렵다[18].

## III. 퍼지 추출기

### 3.1 퍼지 추출기 개요

Dodis et al.[8]이 정의한 퍼지 추출기는 생체 정보로 키를 생성하여 사용자를 인증하는 생체 인증 프리미티브로, (Gen, Rep) 알고리즘 쌍으로 구성된다. Gen(Generation) 알고리즘은 퍼지 추출기의 등록 과정으로 생체 정보$(w)$를 입력하여 키$(r)$와 보조 데이터$(p)$를 출력하고 출력된 보조 데이터는 서버에 저장한다. Rep(Reproduction) 알고리즘은 퍼지 추출기의 인증 과정으로 입력된 생체 정보$(w')$와 서버에 저장된 보조 데이터$(p)$를 이용하여 키$(r')$를 출력한다.

등록 과정에서 입력된 생체 정보 $w$와 인증 과정에서 입력된 생체 정보 $w'$의 차이가 임계치를 넘지 않고 충분히 비슷하면, Rep 알고리즘에서 키를 재생성하였을 때 Gen 알고리즘에서 생성한 키 $r$이 올바르게 복원되어 사용자는 인증을 통과한다. 그림 2는 등록, 인증 과정으로 구성된 퍼지 추출기로, (Gen, Rep) 알고리즘 쌍을 각각 수식으로 나타내면 $(p,r) \leftarrow Gen(w)$, $r' \leftarrow Rep(p,w')$이다.

**정확성(Correctness).** $w$와 $w'$을 벡터로 나타냈을 때 해밍 거리 $dist$가 임계치 $\delta$ 이하라면, 즉 $dist(w,w') \leq \delta$이면 $r'$은 $r$과 같다.

퍼지 추출기의 안전성은 Gen 알고리즘에서 출력되는 키 $r$을 임의의 값과 구분할 수 없는 것을 기반

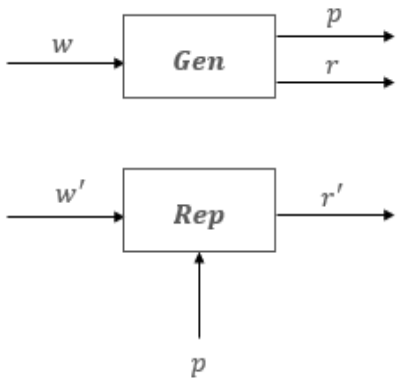


Fig. 2. Fuzzy extractor scheme

으로 한다[9]. 하나의 생체 데이터 $w_1$에서 추출한 키 $r_1$이 임의의 값과 구분 불가능하며 보조 데이터 $p_1$을 가지고 어떠한 정보도 얻을 수 없으면 안전하다. 그러나 노이즈가 섞인 상관관계가 있는 여러 개의 생체 데이터들 $w_1, w_2, ..., w_n$에서 추출한 키들 $r_1, r_2, ..., r_n$은 서로 상관관계가 있는 완전한 임의의 값이 아니며, 보조 데이터 $p_1, p_2, ..., p_n$를 이용해 키와 관련된 정보를 도출할 수 있는 공격이 가능하므로 동일한 생체 정보를 재사용하는 것은 안전하지 않다.

### 3.2 재사용 가능한 퍼지 추출기

재사용 가능한 퍼지 추출기는 사용자가 같은 생체 정보를 여러 번 등록했을 때 상관관계가 있는 생체 데이터들 $w_1, w_2, ..., w_n$에서 추출한 키들 $r_1, r_2, ..., r_n$이 완전한 임의의 값을 가지며 보조 데이터 $p_1, p_2, ..., p_n$가 모두 공개되어도 키에 관한 어떠한 정보도 얻을 수 없는 것이다. Apon et al.[5]은 Fuller et al.[10]이 제안한 재사용 불가능한 LWE 기반의 퍼지 추출기를 재사용이 가능하도록 새롭게 설계하였다. 행렬 $A$를 $Z_q^{n\times n}$에서 균일하고 랜덤하게 뽑았을 때, Apon et al.이 설계한 LWE 기반 재사용 가능한 퍼지 추출기(RFE)는 다음과 같이 3개의 알고리즘(그림 3~5)으로 이루어져 있다.

Gen(Generation) 알고리즘(그림 3)은 생체 정보로부터 키를 생성하여 사용자를 등록하는 과정으로, 랜덤으로 뽑은 비밀 값 $s$를 통해 $c$에서 생체 정보 $w$를 숨기고 $h$에서 LWE 문제에 기반하여 키 $r$을 숨긴다. Rep(Reproduction) 알고리즘(그림 4)

**Input:** $(A,w)$
**Output:** $(p,r)$

1. Sample $s\in Z_q^n$ uniformly.
2. Let $c=As+w$
3. Sample $r\in\{0,1\}^m$, $B\in Z_Q^{m\times n}$ uniformly.
4. Sample $e\leftarrow D_{Z,\alpha}^m$
5. Let $h=Bs+e+\frac{Q}{2}r$
6. Let $p=(c,B,h)$

Fig. 3. RFE Gen algorithm

**Input:** $(A,w',p)$
**Output:** $r'\in\{0,1\}^m$

1. Let $b=c-w'$
2. Compute $s'=Decode(A,b)$
3. For each coordinate $i\in[m]$,
   ① If the $i$-th coordinate of $h-Bs'$ is between $\frac{3Q}{8}$ and $\frac{5Q}{8}$, then the $i$-th coordinate of $r'$ is 1.
   ② Else if the $i$-th coordinate of $h-Bs'$ is less than $\frac{Q}{8}$ or greater than $\frac{7Q}{8}$, then the $i$-th coordinate of $r'$ is 0.
   ③ Else, output $\perp$.

Fig. 4. RFE Rep algorithm

**Input:** $(A,b)$
**Output:** $s'$

1. Select random $2n$ rows $i_1,...,i_{2n}\leftarrow[1,m]$.
2. Restrict $A,b$ to rows $i_1,...,i_{2n}$ and called $A_{i_1,...,i_{2n}}$, $b_{i_1,...,i_{2n}}$.
3. Find $n$ linearly independent rows of $A_{i_1,...,i_{2n}}$. If no such rows exist, output $\perp$.
4. Restrict $A_{i_1,...,i_{2n}}$, $b_{i_1,...,i_{2n}}$ to these $n$ rows and called $A'$, $b'$.
5. Compute $s'=(A')^{-1}b'$.
6. If $b-As'$ has more than $O(\log(n))$ nonzero coordinates, restart the algorithm.

Fig. 5. RFE Decode algorithm

은 키를 재생성하여 사용자를 인증하는 과정으로, 생체 정보 $w'$을 입력하여 Decode 알고리즘(그림 5)

으로 $s'$을 계산한다. 이때, $w'$과 $w$의 해밍 거리가 임계치보다 작아 충분히 비슷하면 $s'$을 이용해 키를 올바르게 복구할 수 있다. Decode(Decoding) 알고리즘은 $w$와 $w'$간에 노이즈로 인해 오차가 존재하는 벡터의 개수, 즉 해밍 거리가 $O(\log(n))$ 이하일 때 비밀 값 $s'$을 계산하는 과정이다.

## IV. 제안하는 효율적인 LWE 기반 재사용 가능한 퍼지 추출기

### 4.1 등록 과정

그림 6은 제안 모델의 Gen 알고리즘으로 $Z_q^{m\times n}$에서 균일하고 랜덤하게 뽑은 행렬 $A$와 생체 정보 $w$를 입력하였을 때, $w$에 대응되는 보조 데이터 $p$와 키 $r$을 생성함으로써 사용자를 등록한다. $c$는 $Z_q^n$에서 비밀 값 $s$를 뽑아 $A$와 곱한 후 생체 정보 $w$를 더한 것으로, $w$와 유사한 생체 데이터를 갖고 있지 않으면 $c$가 공개되어도 $s$를 올바르게 계산할 수 없다. $h$는 $Z_Q^{m\times n}$에서 균일하고 랜덤하게 뽑은 행렬 $B$와 비밀 값 $s$를 곱한 후 $2r$, $r\times \lfloor r \rceil_2$, 그리고 랜덤하게 뽑은 매우 작은 $e$를 더한 값으로 LWE 기반 형태이다.

**Input:** $(A,w)$
**Output:** $(p,r)$

1. Sample $s\in Z_q^n$ uniformly.
2. Let $c=As+w$
3. Sample $r\in Z_q^m$, $B\in Z_Q^{m\times n}$ uniformly.
4. Sample $e\leftarrow D_{Z,\alpha}^m$
5. Let $h=Bs+e+2r+r\times \lfloor r \rceil_2$
6. Let $h'=<r>_2$
7. Let $p=(c,B,h,h')$

Fig. 6. Proposed Gen algorithm

제안하는 모델은 인증 시 보조 데이터 $h$에서 $Bs$를 뺀 후 작은 값 $e$의 범위를 고려하여 키 $r$을 재생성한다. 따라서 $s$를 올바르게 계산한 정당한 사용자만 Peikert의 조정 메커니즘에 기반하여 $r$을 복구할 수 있다. $h-Bs$에서 $r$을 올바르게 복구하기 위해 제안 기법의 Gen 알고리즘에서는 $h$를 다음과 같은 세 조건을 만족하도록 설계하였다.

① 키를 모듈러 라운딩 함수에 입력한 결과인 $\lfloor r \rceil_2$을 포함한다.

② 키를 크로스 라운딩 함수에 입력하였을 때 출력되는 힌트 값인 $h'=<r>_2$을 이용해 $\lfloor r \rceil_2$가 0일 때와 1일 때를 구분할 수 있다.

③ $\lfloor r \rceil_2$가 0일 때와 1일 때의 $h-Bs$의 범위가 겹치는 부분에서는 $h'$ 값이 각각 다르다.

### 4.2 인증 과정

그림 7은 제안 모델의 Rep 알고리즘으로 주어진 행렬 $A$와 보조 데이터 $c,B,h,h'$, 그리고 인증 과정에서 입력된 생체 데이터 $w'$로 키 $r'$을 재생성함으로써 사용자를 인증한다. $h$에서 키를 복구하기 위해서는 먼저 $s$를 계산해야 하므로 그림 5의 Decode 알고리즘을 이용한다. $c$에서 $w'$을 뺀 값 $b(=As')$와 행렬 $A$를 Decode 알고리즘에 입력하면 $s'$이 출력되는데, 이때 $w'$이 $w$와 충분히 비슷하면 $s'$이 $s$와 거의 유사하여 $h-Bs'$을 계산하여 키를 올바르게 재생성할 수 있다.

$h-Bs'$은 $e+2r+r\times \lfloor r \rceil_2$로 $r$의 범위에 따라 표 1과 같이 두 경우(Case 1, Case 2)로 나뉜다. $r$이 $[0,\frac{q}{4}]$ 또는 $[\frac{3q}{4},q]$에 속할 때, $\lfloor r \rceil_2$은 0이므로 $h-Bs'$은 $2r+e$이며 해당 범위는 $[0+e,\frac{q}{2}+e]$ 또는 $[\frac{3q}{2}+e,2q+e]$이다. $r$이 $[\frac{q}{4},\frac{3q}{4}]$에 속할 때, $\lfloor r \rceil_2$은 1이므로 $h-Bs'$은 $3r+e$이며 해당 범위는 $[\frac{3q}{4}+e,\frac{9q}{4}+e]$이다. $e$는 매우 작은 수이므로 키를 복구할 때 $\frac{q}{2}$, $\frac{3q}{4}$, $\frac{3q}{2}$, $2q$, $\frac{9q}{4}$를 기준으로 한 비트

Table 1. 2 cases of $h-Bs'$

| | Range of $r$ | $h-Bs'$ | Range of $h-Bs'$ |
|---|---|---|---|
| **Case 1.** $\lfloor r \rceil_2=0$ | $[0,\frac{q}{4}]$, $[\frac{3q}{4},q]$ | $2r+e$ | $[0+e,\frac{q}{2}+e]$, $[\frac{3q}{2}+e,2q+e]$ |
| **Case 2.** $\lfloor r \rceil_2=1$ | $[\frac{q}{4},\frac{3q}{4}]$ | $3r+e$ | $[\frac{3q}{4}+e,\frac{9q}{4}+e]$ |

**Input:** $(A, w', p)$
**Output:** $r' \in Z^m$

1. Let $b = c - w'$
2. Compute $s' = Decode_t(A, b)$
3. For each coordinate $i \in [m]$,
   ① If the $i$-th coordinate of $h - Bs'$ is in $[0, \frac{q}{2}]$, and $h'$ is 0, then the $i$-th coordinate of $r'$ is $\left\lfloor \frac{h - Bs'}{2} + \frac{1}{2} \right\rfloor$.
   ② Else if the $i$-th coordinate of $h - Bs'$ is in $[\frac{q}{2}, \frac{3q}{4}]$, and $h'$ is 1, then the $i$-th coordinate of $r'$ is $\left\lfloor \frac{h - Bs'}{2} + \frac{1}{2} \right\rfloor$.
   ③ Else if the $i$-th coordinate of $h - Bs'$ is in $[\frac{q}{2}, \frac{3q}{4}]$, and $h'$ is 0, then the $i$-th coordinate of $r'$ is $\left\lfloor \frac{h - Bs'}{3} + \frac{1}{2} \right\rfloor$.
   ④ Else if the $i$-th coordinate of $h - Bs'$ is in $[\frac{3q}{4}, \frac{3q}{2}]$, and $h'$ is 0, then the $i$-th coordinate of $r'$ is $\left\lfloor \frac{h - Bs'}{2} + \frac{1}{2} \right\rfloor$.
   ⑤ Else if the $i$-th coordinate of $h - Bs'$ is in $[\frac{3q}{4}, \frac{3q}{2}]$, and $h'$ is 1, then the $i$-th coordinate of $r'$ is $\left\lfloor \frac{h - Bs'}{3} + \frac{1}{2} \right\rfloor$.
   ⑥ Else if the $i$-th coordinate of $h - Bs'$ is in $[\frac{3q}{2}, 2q]$, and $h'$ is 1, then the $i$-th coordinate of $r'$ is $\left\lfloor \frac{h - Bs'}{2} + \frac{1}{2} \right\rfloor$.
   ⑦ Else if the $i$-th coordinate of $h - Bs'$ is in $[\frac{3q}{2}, 2q]$, and $h'$ is 0, then the $i$-th coordinate of $r'$ is $\left\lfloor \frac{h - Bs'}{3} + \frac{1}{2} \right\rfloor$.
   ⑧ Else if the $i$-th coordinate of $h - Bs'$ is in $[2q, \frac{9q}{4}]$, and $h'$ is 0, then the $i$-th coordinate of $r'$ is $\left\lfloor \frac{h - Bs'}{3} + \frac{1}{2} \right\rfloor$.
   ⑨ Else, output $\perp$.

Fig. 7. Proposed Rep algorithm

오류가 생길 수 있다. 또한, $h - Bs'$가 $[\frac{3q}{2} + e, 2q + e]$ 범위에 있을 때는 두 경우가 겹치므로 이를 구분하기 위해 추가적인 정보가 필요하다. 따라서 키를 오류 없이 올바르게 복구하기 위해 $\frac{q}{2}$, $\frac{3q}{4}$, $\frac{3q}{2}$, $2q$, $\frac{9q}{4}$ 지점에서 공개된 힌트($h'$)를 활용한다.

표 2는 $h - Bs'$에서 $\lfloor r \rceil_2$이 달라지는 구간인 $\frac{q}{2}$, $\frac{3q}{4}$, $\frac{3q}{2}$, $2q$, $\frac{9q}{4}$을 기준점으로 보조 데이터 $h'$을 이용하여 키 $r'$을 재생성하는 방법으로, $h - Bs'$ 범위 $[0, \frac{9q}{4}]$의 각 기준점에서 $\lfloor r \rceil_2$이 0일 때와 1일 때 두 가지 경우의 수로 나누어 키를 복구한다. $\lfloor r \rceil_2$이 0인 경우 $h - Bs'$는 $2r + e$이고 $\lfloor r \rceil_2$이 1인 경우 $h - Bs'$는 $3r + e$이다. 이때 $e$는 매우 작은 값이며 양수인지 음수인지 알 수 없으므로, 키 $r$을 복구하기 위해 $\lfloor r \rceil_2$이 0인 경우 $h - Bs'$를 2로 나눈 후 반올림하고, $\lfloor r \rceil_2$이 1인 경우 $h - Bs'$를 3으로 나눈 후 반올림한다. 이를 수식으로 나타내면, $\lfloor r \rceil_2$이 0일 때 키는 $\left\lfloor \frac{h - Bs'}{2} + \frac{1}{2} \right\rfloor$이고 $\lfloor r \rceil_2$이 1일 때 키는 $\left\lfloor \frac{h - Bs'}{3} + \frac{1}{2} \right\rfloor$이다.

Table 2. Key reproduction method using reconciliation mechanism

| Range of $h - Bs'$ | $\lfloor r \rceil_2$ | Range of $r$ | $h'$ | $r'$ |
|---|---|---|---|---|
| $[0, \frac{q}{2}]$ | 0 | $[0, \frac{q}{4}]$ | 0 | $\left\lfloor \frac{h - Bs'}{2} + \frac{1}{2} \right\rfloor$ |
| $[\frac{q}{2}, \frac{3q}{4}]$ | 0 | $[\frac{q}{4}, \frac{3q}{8}]$ | 1 | $\left\lfloor \frac{h - Bs'}{2} + \frac{1}{2} \right\rfloor$ |
| | 1 | $[\frac{q}{6}, \frac{q}{4}]$ | 0 | $\left\lfloor \frac{h - Bs'}{3} + \frac{1}{2} \right\rfloor$ |
| $[\frac{3q}{4}, \frac{3q}{2}]$ | 0 | $[\frac{3q}{8}, \frac{3q}{4}]$ | 0 | $\left\lfloor \frac{h - Bs'}{2} + \frac{1}{2} \right\rfloor$ |
| | 1 | $[\frac{q}{4}, \frac{q}{2}]$ | 1 | $\left\lfloor \frac{h - Bs'}{3} + \frac{1}{2} \right\rfloor$ |
| $[\frac{3q}{2}, 2q]$ | 0 | $[\frac{3q}{4}, q]$ | 1 | $\left\lfloor \frac{h - Bs'}{2} + \frac{1}{2} \right\rfloor$ |
| | 1 | $[\frac{q}{2}, \frac{2q}{3}]$ | 0 | $\left\lfloor \frac{h - Bs'}{3} + \frac{1}{2} \right\rfloor$ |
| $[2q, \frac{9q}{4}]$ | 1 | $[\frac{2q}{3}, \frac{3q}{4}]$ | 0 | $\left\lfloor \frac{h - Bs'}{3} + \frac{1}{2} \right\rfloor$ |

표 2의 각 행에 대한 설명은 다음과 같다. 첫 번

째 행은 $h-Bs'$이 $[0,\frac{q}{2}]$ 범위에 있을 때로 Case 1의 $\lfloor r \rceil_2$이 0인 경우이다. 이때 $r$의 범위는 $h-Bs'$의 범위를 2로 나눈 $[0,\frac{q}{4}]$이므로 $h'$은 0이다.

두 번째 행은 $h-Bs'$이 $[\frac{q}{2},\frac{3q}{4}]$ 범위에 있을 때로, $r$이 $\frac{q}{2}$이면서 $e$가 양수인 $\lfloor r \rceil_2$이 0인 경우와 $r$이 $\frac{3q}{4}$이면서 $e$가 음수인 $\lfloor r \rceil_2$이 1인 경우로 나뉜다. $\lfloor r \rceil_2$이 0인 경우 $r$의 범위는 $h-Bs'$의 범위를 2로 나눈 $[\frac{q}{4},\frac{3q}{8}]$이므로 $h'$은 1이고, $\lfloor r \rceil_2$이 1인 경우 $r$의 범위는 $h-Bs'$의 범위를 3으로 나눈 $[\frac{q}{6},\frac{q}{4}]$이므로 $h'$은 0이다. 따라서 $h'$ 정보를 이용해 $h-Bs'$이 겹치는 $[\frac{q}{2},\frac{3q}{4}]$ 범위에서 키를 올바르게 복구할 수 있다.

세 번째 행은 $h-Bs'$이 $[\frac{3q}{4},\frac{3q}{2}]$ 범위에 있을 때로, $r$이 $\frac{3q}{2}$이면서 $e$가 음수인 $\lfloor r \rceil_2$이 0인 경우와 Case 2의 $\lfloor r \rceil_2$이 1인 경우로 나뉜다. $\lfloor r \rceil_2$이 0인 경우 $r$의 범위는 $h-Bs'$의 범위를 2로 나눈 $[\frac{3q}{8},\frac{3q}{4}]$이므로 $h'$은 0이고, $\lfloor r \rceil_2$이 1인 경우 $r$의 범위는 $h-Bs'$의 범위를 3으로 나눈 $[\frac{q}{4},\frac{q}{2}]$이므로 $h'$은 1이다. 따라서 $h'$ 정보를 이용해 $h-Bs'$이 $[\frac{3q}{4},\frac{3q}{2}]$인 범위에서 키를 올바르게 복구할 수 있다.

네 번째 행은 $h-Bs'$이 $[\frac{3q}{2},2q]$ 범위에 있을 때로, Case 1의 $\lfloor r \rceil_2$이 0인 경우와 Case 2의 $\lfloor r \rceil_2$이 1인 경우로 나뉜다. $\lfloor r \rceil_2$이 0인 경우 $r$의 범위는 $h-Bs'$의 범위를 2로 나눈 $[\frac{3q}{4},q]$이므로 $h'$은 1이고, $\lfloor r \rceil_2$이 1인 경우 $r$의 범위는 $h-Bs'$의 범위를 3으로 나눈 $[\frac{q}{2},\frac{2q}{3}]$이므로 $h'$은 0이다. 따라서 $h'$ 정보를 이용해 $h-Bs'$이 $[\frac{3q}{2},2q]$인 범위에서 키를 올바르게 복구할 수 있다.

다섯 번째 행은 $h-Bs'$이 $[2q,\frac{9q}{4}]$ 범위에 있을 때로 Case 2의 $\lfloor r \rceil_2$이 1인 경우이다. 이때 $r$의 범위는 $h-Bs'$의 범위를 3으로 나눈 $[\frac{2q}{3},\frac{3q}{4}]$이므로 $h'$은 0이다. 위의 8가지 경우를 바탕으로 제안 모델은 인증 시 $h-Bs'$의 범위와 $h'$을 이용해 $\lfloor r \rceil_2$이 0인지 1인지 판단한 후 $r'$을 생성한다.

### 4.3 효율성

제안하는 모델은 퍼지 추출기의 등록 과정에서 키 길이가 늘어나도 인증 시 키를 복구하기 위해 수행하는 과정의 횟수가 같거나 비슷한 효율적이고 재사용 가능한 퍼지 추출기이다. 설계한 기법은 Apon et al.[5]이 설계한 LWE 기반 재사용 가능한 퍼지 추출기를 개선하여 랜덤 오라클에 의존하지 않고 입력하는 생체 정보에 제한이 없으며 효율적이다. Apon et al. 기법의 키는 길이가 $m$일 때 $\{0,1\}^m$로 인증 과정을 $\lceil \log_2 m \rceil$번 반복해야 하지만, 제안 모델의 키는 $Z_q$로 인증 과정을 $\lceil \log_q m \rceil$번 수행해 키를 재생성할 수 있다. 또한, Apon et al. 기법은 키 길이가 $m$일 때 공격자가 전사적 공격으로 키를 계산하는 복잡도가 $2^m$이지만, 제안 모델은 $q^m$으로 보안성이 더 높다.

제안 모델의 효율성을 분석하기 위해 Intel Core i5-7500 CPU(RAM 16GB) 환경에서 기존 기법(Apon et al.[5])과 제안 기법을 C언어로 각각 구현하여 표 3과 같이 키의 길이에 따라 인증 과정을 한 번 수행하는데 걸리는 시간을 측정하였다. 기존 기법과 제안 기법의 올바른 비교를 위해 구현 시 두 기법의 조건은 동일하게 설정하였다. 행렬 $A$와 $B$는 행과 열의 수가 키의 길이로 같은 정방행렬로 하였으며 키와 행렬값의 범위인 $q$와 $Q$는 모듈러 라운딩 함수와 크로스 라운딩 함수의 분포를 균일하게 하는 4의 배수인 8로 설정하였다. 또한, 인증 과정에서의 생체 정보가 등록 과정에서의 생체 정보와 충분히 비슷하여 키를 올바르게 재생성하고 인증을 통과한다는 가정하에 실험을 진행하였다.

표 3과 4는 각각 퍼지 추출기에서 인증 과정의 알고리즘을 한 번 수행하기 위한 시간과 인증 과정의 알고리즘 총 수행 횟수를 키의 길이에 따라 기존 기법과 제안 기법으로 나누어 비교한 표다. 표 5는 표 3과 4의 값을 곱하여 인증을 수행하는데 걸리는 총 시간을 나타낸 표로 인증 과정을 한 번 수행하는데 걸리는 시간은 두 기법이 비슷하지만, 제안 기법은

키를 복구하기 위한 과정의 횟수가 적어 최종적으로 인증을 위해 걸리는 시간이 기존 기법보다 덜 소요된다.

Table 3. Comparison of original scheme and proposed scheme for the time required to perform the authentication process once according to the key length

| Key length | Original scheme | Proposed scheme |
|---|---|---|
| 4 | 0.003 sec | 0.003 sec |
| 8 | 0.184 sec | 0.171 sec |
| 9 | 2.104 sec | 2.122 sec |
| 10 | 17.432 sec | 16.674 sec |
| 11 | 217.190 sec | 212.326 sec |

Table 4. Comparison of original scheme and proposed scheme for the number of algorithms required to perform authentication according to the key length

| Key length | Original scheme | Proposed scheme |
|---|---|---|
| 4 | 2 | 1 |
| 8 | 3 | 1 |
| 9 | 4 | 2 |
| 10 | 4 | 2 |
| 11 | 4 | 2 |

Table 5. Comparison of original scheme and proposed scheme for the total time required to perform the authentication process according to the key length

| Key length | Original scheme | Proposed scheme |
|---|---|---|
| 4 | 0.006 sec | 0.003 sec |
| 8 | 0.552 sec | 0.171 sec |
| 9 | 8.416 sec | 4.244 sec |
| 10 | 69.728 sec | 33.348 sec |
| 11 | 868.76 sec | 424.652 sec |

## V. 안전성 분석

본 장에서는 제안 모델이 LWE 문제의 어려움에 기반하여 Apon et al.[5]이 정의한 재사용의 안전성을 만족함을 보인다. Apon et al.[5]은 안전성 모델에서 공격자에게 보조 데이터 $p$만 주어졌을 때의 약한 재사용 가능한 안전성과 공격자에게 보조 데이터 $p$와 추출한 키 $r$이 주어졌을 때의 강한 재사용 가능한 안전성을 각각 정의하였다. 정의 4는 [5]에서 정의한 강한 재사용 가능한 퍼지 추출기이며 그림 8은 정의 4의 안전성 모델이다.

**정의 4. [재사용 가능한 퍼지 추출기]** 공격자 $Adv$와 챌린저 $C$로 이루어진 안전성 모델에서 $Adv$가 공격에 성공할 확률이 $1/2+\epsilon$보다 작으면 분포 $\mathsf{W}$에서의 $(l,t,\epsilon)$-퍼지 추출기 $\Pi=(Gen,Rep)$은 $\epsilon$-재사용 가능하다.

1) $C$가 행렬 $A\in Z_q^{m\times n}$와 분포 $W\in\mathsf{W}$를 지정한다.

2) $C$가 $W$에서 표본 추출한 값 $w^*$와 행렬 $A$를 $Gen$ 알고리즘에 입력해 $p^*$과 $r^*$을 출력한 후 $Adv$에게 $p^*$을 준다.

3) $C$가 $b\leftarrow\{0,1\}$를 선택하여 만약 $b$가 0이면 $C$가 $Adv$에게 $r^*$을 주고, $b$가 1이면 $C$가 $Adv$에게 $u\leftarrow\{0,1\}^l$을 준다.

4) $Adv$는 해밍 가중치가 $t$ 이하인 $\delta_i\in\{0,1\}^m$으로 생성한 $w+\delta_i$을 $Gen$ 알고리즘에 질의하여 $Gen(w+\delta_i)$의 출력값인 $p_i$와 $r_i$를 얻는다.

5) $Adv$는 $b'$을 출력한다. 만약 $b=b'$이면 $Adv$는 공격에 성공한다.

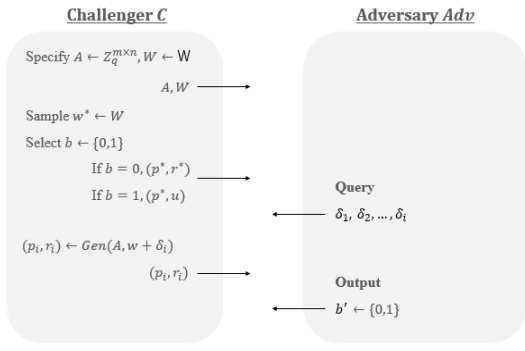


Fig. 8. Reusable fuzzy extractor security model

**정리 2.** 적절한 파라미터 $Q, \alpha \in \mathrm{superpoly}(n)$, $q, \beta \in \mathrm{poly}(n)$에 대해 $n \geq 3m$, $l = \frac{k-w(\log n)}{\log q}$인 $\mathrm{LWE}_{\mathrm{n,m,q,u}(-\beta,\beta)}$와 $\mathrm{LWE}_{\mathrm{l,m,q,D}_{Z,\alpha}}$가 어려우면, $\Pi = (Gen, Rep)$는 재사용의 안전성을 만족한다[5].

제안 모델은 정의 4의 강한 재사용 가능한 안전성 모델에서 Apon et al.이 정리한 재사용 안전함을 보인다. 재사용 가능한 퍼지 추출기는 키와 보조 데이터가 독립적이며 키를 임의의 값과 구분할 수 없으므로 공격자가 한 서버에 등록한 생체 정보 $w_i$로 추출된 키 $r_i$를 알아내도 다른 서버에 등록한 $w_j (i \neq j)$로 추출한 키 $r_j$는 안전하다. 표 6은 제안하는 기법의 안전성 분석을 위해 구성한 6개의 시나리오다. 시나리오 $i (i = 1,2,...,5)$와 $i+1$이 모두 구분 불가능하면, 즉 키 $r^*$과 임의의 값 0을 구분할 수 없으면 $h_i$가 $r_i$에 의존하지 않고 독립적이기 때문에 재사용해도 안전하다.

Table 6. 6 Scenarios for security analysis

| | |
|---|---|
| 1 | $c^* = As + w,\ c_i = As_i + w + \delta_i,$ $h^* = B^* s + e + 2r^* + r^* \times \lfloor r^* \rceil,$ $h_i = B_i s_i + e_i + 2r_i' + r_i' \times \lfloor r_i' \rceil$ |
| 2 | $c_i = A(s + \triangle_i) + w + \delta_i,$ $h_i = B_i(s + \triangle_i) + e_i + 2r_i' + r_i' \times \lfloor r_i' \rceil$ |
| 3 | $h_i = (C_i D_i + E_i)(s + \triangle_i) + e_i + 2r_i' + r_i' \times \lfloor r_i' \rceil$ |
| 4 | $h_i = (C_i D_i)(s + \triangle_i) + e_i + 2r_i' + r_i' \times \lfloor r_i' \rceil$ |
| 5 | $h_i = C_i u_i + e_i + 2r_i' + r_i' \times \lfloor r_i' \rceil$ $(u_i \leftarrow Z_q^n)$ |
| 6 | $r_i' = 000...0$ |

**정리 3.** 시나리오 1과 2는 분포가 동일하여 구분 불가능하다.

증명. 시나리오 2는 시나리오 1의 $s_i$를 $s$에서 아주 작은 오차 $\triangle_i$만큼 더한 값으로 대체했다. $c_i$는 래티스를 기반으로 하는 LWE 표본으로 주어진 분포 내에서 값을 조금 이동해도 준동형 사상이므로 이동하기 전과 분포가 동일하다. □

**정리 4.** 시나리오 2와 3은 Decision LWE 문제의 어려움에 기반하여 계산적으로 구분 불가능하다.

증명. 시나리오 3은 시나리오 2의 임의의 행렬 $B_i$를 $C_i D_i + E_i$로 대체했다. $C_i D_i + E_i$는 공개되는 임의의 두 행렬 $C_i \in Z_q^{m \times l}$, $D_i \in Z_q^{l \times n}$와 정규 분포 $(-\beta, \beta), \beta \in \mathrm{poly}(n)$상의 공개되지 않는 $m \times n$ 크기의 행렬 $E_i$로 구성된 LWE 표본 형태이다. 이때 $h_i$를 구성하는 $e_i$의 크기가 매우 작다면 $B_i$와 $C_i D_i + E_i$를 구분하는 것은 Decision LWE 문제로 계산적으로 어렵다. □

**정리 5.** 시나리오 3과 4는 통계적으로 구분 불가능하다.

증명. 시나리오 4는 시나리오 3의 $C_i D_i + E_i$를 $C_i D_i$로 대체했다. $h_i$를 구성하는 정규 분포의 표본 $e_i$가 $E_i(s + \triangle_i)$보다 크기 때문에 시나리오 3의 분포와 이를 미세하게 이동시킨 시나리오 4의 분포는 통계적으로 구분 불가능하다. □

**정리 6.** 시나리오 4와 5는 계산적으로 구분 불가능하다.

증명. 시나리오 5는 시나리오 4의 $D_i(s + \triangle_i)$를 $u_i$로 대체했다. 이는 $u_i \in Z_q^n$를 이용해 키 $s$를 재구성하는 것이 계산적으로 어려운 leftover hash lemma를 기반으로 한다[17][18]. LWE 형태의 $b^* = As + w$에서 $f_A(s)$의 역변환이 어려우므로 $D_i(s + \triangle_i)$와 $u_i$는 구분 불가능하다. □

**정리 7.** 시나리오 5와 6은 Decision LWE 문제의 어려움에 기반하여 계산적으로 구분 불가능하다.

증명. 시나리오 6은 시나리오 5의 $r_i'$를 0으로 된 문자열 000...0으로 두었다. 이에 따라 $u_i = u + \triangle_i$와 $c^*$의 $s$는 독립적이기 때문에 $h^*$와 임의의 $h_i$를 구분하는 것은 Decision LWE 문제로 계산적으로 어렵다. 임의의 $h_i$가 키 $r_i'$으로 이루어진 것인지 0으로 된 문자열인지와 관계없이 $h^*$와 구분 불가능하므로 $r^*$과 임의의 값 0을 구분할 수 없다. □

정리 3~7은 표 6의 6개의 시나리오가 각각 구분 불가능함을 나타내며 결과적으로 제안하는 퍼지 추출기의 기존 파라미터인 시나리오 1과 임의의 값인 시나리오 6이 구분 불가능함을 보인다. 따라서 제안하는 모델은 Apon et al.이 정의한 키와 임의의 값을 구분할 수 없고 키와 보조 데이터가 독립적인 재사용의 안전성을 만족한다.

## VI. 결 론

본 논문에서는 사용자가 여러 서버에 같은 생체 데이터를 등록해도 키나 생체 데이터의 노출로부터 안전하며, 키 길이가 증가해도 사용자를 검증하기 위한 과정의 알고리즘 수행 횟수가 같거나 비슷한 효율적이고 재사용 가능한 퍼지 추출기를 제안하였다. 제안 모델은 노이즈가 섞인 생체 데이터로 보조 데이터와 독립적인 키를 생성하며, LWE 문제를 기반으로 하여 Apon et al.이 정의한 재사용의 안전성을 만족함을 보였다. 본 연구는 긴 키 길이가 필요한 보안성 높은 시스템에 적용할 수 있으므로 향후 다양한 생체 인증 프로토콜에 활용 가능할 것으로 기대된다.

## References


[1] M. Zhang, B. Yang, W. Zhang, and T. Takagi, "Multibiometric Based Secure Encryption, Authentication Scheme with Fuzzy Extractor," *International Journal of Network Security,* vol. 12, no. 2, pp. 50-57, Mar. 2011.

[2] N. Li, F. Guo, Y. Mu, W. Susilo, and S. Nepal, "Fuzzy extractors for biometric identication," *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pp. 667-677, July 2017.

[3] X. Boyen, "Reusable cryptographic fuzzy extractors," *Proceedings of the 11th ACM conference on Computer and Communications Security,* pp. 82-91, Oct. 2004.

[4] R. Canetti, B. Fuller, O. Paneth, L. Reyzin, and A. Smith, "Reusable fuzzy extractors for low-entropy distributions," *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 117-146, 2016.

[5] D. Apon, C.Cho, K. Eldefrawy, and J. Katz "Efficient, reusable fuzzy extractors from LWE," *International Conference on Cyber Security Cryptography and Machine Learning*. Springer, Cham, pp. 1-18, June 2017.

[6] Y. Wen, S. Liu, and S. Han, "Reusable fuzzy extractor from the decisional Diffie-Hellman assumption," *Designs, Codes and Cryptography*, vol. 86, no. 11, pp. 2495-2512, Jan. 2018.

[7] Y. Wen and S. Liu, "Robustly reusable fuzzy extractor from standard assumptions," *International Conference on the Theory and Application of Cryptology and Information Security,* Springer, Cham, pp.459-489, June 2018.

[8] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *International conference on the theory and applications of cryptographic techniques,* Springer, Berlin, Heidelberg, pp. 523-540, May 2004.

[9] M. Blanton and M. Aliasgari, "On the (non-) reusability of fuzzy sketches and extractors and security in the computational setting," *Proceedings of the International Conference on Security and Cryptography*, pp. 68-77, July 2011.

[10] B. Fuller, X. Meng, and L. Reyzin, "Computational fuzzy extractors," *Information and computation*, vol. 275, 104602, Dec. 2020.

[11] C. Peikert, "Lattice cryptography for the internet," *International workshop*

*on post-quantum cryptography,* Springer, vol. 8772, pp. 197-219, 2014.

[12] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM (JACM)*, vol. 56, no. 6, pp. 1-40, Sept. 2009.

[13] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," *SIAM Journal on computing,* vol. 43, no. 2, pp. 831-871, 2014.

[14] Z. Brakerski and V. Vaikuntanathan, "Lattice-based FHE as secure as PKE," *Proceedings of the 5th conference on Innovations in theoretical computer science*, pp. 1-12, Jan. 2014.

[15] C. Gentry, C.Peikert, and V.Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pp. 197-206, May 2008.

[16] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (H) IBE in the standard model," *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, pp. 553-572, 2010.

[17] B. Barak, Y. Dodis, H. Krawczyk, O. Pereira, K. Pietrzak, F. X. Standaert, Y. Yu, "Leftover hash lemma, revisited," *Annual Cryptology Conference,* Springer, Berlin, Heidelberg, pp. 1-20, 2011.

[18] S. Goldwasser, YT. Kalai, C. Peikert, and V. Vaikuntanathan, "Robustness of the learning with errors assumption," *Proceedings of the Innovations in Computer Science,* pp. 230-240, 2010.

## 〈저 자 소 개〉

김 주 언 (Juon Kim) 학생회원
2022년 2월: 이화여자대학교 사이버보안학과 졸업
2022년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 암호 알고리즘, 생체인증 보안, 양자컴퓨터

이 광 수 (Kwangsu Lee) 종신회원
1998년 2월: 연세대학교 컴퓨터과학과 졸업
2000년 2월: 한국과학기술원 전산학과 석사
2011년 2월: 고려대학교 정보보호학과 박사
2016년 9월~2019년 8월: 세종대학교 정보보호학과 조교수
2019년 9월~현재: 세종대학교 정보보호학과 부교수
〈관심분야〉 암호 프로토콜, 공개키 암호

이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학사 졸업
1987년 12월: Oklahoma University 전산학과 석사 졸업
1992년 5월: Oklahoma University 전산학과 박사 졸업
1993년 3월~1997년 2월: 고려대학교 전산학과 조교수
1997년 3월~2001년 2월: 고려대학교 전산학과 부교수
2001년 3월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 암호 프로토콜, 암호이론, USN이론, 키 교환, 익명성 연구, PET 기술