I. J. Computer Network and Information Security, **2013, 4, 8-16**
Published Online April 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.04.02

Statistical Hiding Fuzzy Commitment Scheme for Securing Biometric Templates

Alawi A. Al-Saggaf[1], Haridas Acharya[2]
[1]King Fahd University of Petroleum and Minerals, Dhahran-31261, Saudi Arabia.
[1]Ph.D. candidate in computer studies at Symbiosis International University
[2]Allan Institute of Management Sciences, University of Pune, Pune-411001, India.
alawi@kfupm.edu.sa[1], haridas.undri@gmail.com[2]

Abstract **—** By considering the security flaws in cryptographic hash functions, any commitment scheme designed straight through hash function usage in general terms is insecure. In this paper, we develop a general fuzzy commitment scheme called an *ordinary fuzzy commitment scheme* (OFCS), in which many fuzzy commitment schemes with variety complexity assumptions is constructed. The scheme is provably statistical hiding (the advisory gets almost no statistically advantages about the secret message). The efficiency of our scheme offers different security assurance, and the trusted third party is not involved in the exchange of commitment.

The characteristic of our scheme makes it useful for biometrics systems. If the biometrics template is compromised, then there is no way to use it directly again even in secure biometrics systems. This paper combines biometrics and OFCS to achieve biometric protection scheme using smart cards with renewability of protected biometrics template property.

Index Terms **—** Cryptography, commitment schemes, fuzzy commitment scheme, error correcting codes, biometrics, and template security

I. INTRODUCTION

In cryptography, commitment schemes are commonly two-phased; (commit and open) cryptographic protocol, ensures secure communication between two parties, with complete disillusionment of information for mistrusted parties. The sender, A, and the receiver, B. At the end of the commit phase, the sender, A, is committed to a specific value, in which the scheme satisfies the following constraints: (1) The receiver, B, learns nothing about a committed value before the open phase (this is known as the *hiding* property), (2) The sender, A, is bound to at most one value (this is known as the *binding* property). In the open phase, the sender, A, sends extra information to the receiver, B, which allows him to determine the committed value. Commitment schemes are conventionally opened using identical information. However, there are several security applications noisy inputs could not be avoided such as biometric systems. Therefore, it is important to protect the biometrics information whenever replaced password/key in authentication systems. A solution to facilitate the use of approximate information in cryptographic systems is achieved by combining techniques from the areas of cryptography and error correcting codes.

In 1997, Crépeau [1] introduced a bit-commitment scheme based on error correcting codes. The scheme is apply a binary symmetric channel (BSC) to a binary codeword from the set of error correcting codes. In [2,3], a cryptographic primitive is proposed to enhance the biometric template protection. The scheme is a synthesis of techniques from the areas of error correcting codes and cryptography. The drawbacks of the scheme are leads to leakage of information about the user's biometric data [4] and the error tolerance of the scheme is small (the authors assumption that only up to 10% bit of the iris code can be corrected). In fact up to 30% bits of the iris code could be difference between different presentations of the same iris [5].

In [6], Juels and Wattenberg proposed theoretical basis for biometrics protection schemes that they referred to as "fuzzy commitment scheme" (FCS). The Juels and Wattenberg's scheme can be seen as a generalized and improved of [2]. In the last decade, the FCS became a popular technique for designing biometrics secrecy systems [7]. However, the fuzzy commitment scheme (FCS) is solely based on cryptographic hash function SHA1. By considering the security flaws in cryptographic hash functions such as MD5 and SHA1 families, and any commitment scheme designed through hash function has been proved to be false solution [16]. Furthermore, Commitment schemes based on noisy channels has been discussed briefly in [35, 36]

In [8], Juels and Sudan derived a fuzzy vault scheme from the fuzzy commitment scheme which is based on the hardness of polynomial reconstruction. Several concepts of cryptographic primitives based on error correcting codes have been introduced, referred to as "fuzzy extractors" and "fuzzy sketches" [9-15].

Motivated by above examples that shows the importance of securing biometrics systems, and the question how to improve Juels and Wattenberg's scheme in a secure way, this paper proposes general fuzzy commitment scheme called an *ordinary fuzzy commitment scheme* (OFCS), in which the security of the Juels and Wattenberg's scheme is resolved and many fuzzy commitment schemes with variety complexity assumptions constructed. Our scheme is provably secure against all power computation adversary receiver and computation bounded adversary sender. The efficiency of our scheme offers different security assurance, then the systems usage become non-trivial. Mathematical analysis and proves are provided in detail to show that our scheme is secure and efficient.

Moreover, we exploit our OFCS scheme to enhance the security of biometric authentication systems. If the biometrics template is compromised, then there is no way to use it directly again even in secure biometrics systems. This paper combines biometrics and OFCS to achieve biometric protection scheme using smart cards with renewability of protected biometric templates property.

The rest of the paper is organized as follows: In section 2 we give background theory in error correcting codes and biometrics. Section 3 reviews Juels and Wattenberg fuzzy commitment scheme and describe its security flaw. The proposed *ordinary fuzzy commitment scheme* and corresponding security analysis is presented in Section 4 and 5, respectively. In Section 6, we present several constructions of *ordinary fuzzy commitment scheme*. In section 7 we discuss an application to biometric identification systems. Finally, we draw our conclusions in Section 8.

II. BACKGROUND THEORY

A. Error correcting codes

Error correcting codes are used for detecting and correcting errors when data transmitted from one place to another over a noisy channel. They naturally find applications where fuzziness' may creep in [2,3,6,8], especially because like noise fuzziness is a noise like effect which needs to be carefully accounted for. Following definitions and terminology would be fundamental to our discussions.

Definition 1 (code set C): Let C be a proper subset of $\{0,1\}^n$, with 2^k elements. Then we refer to elements of C as *codewords* of length n and, 2^k the size of the code. We denote the code set as $C(n,k)$.

Definition 2 (Hamming distance): Given a code set $C(n,k)$ as defined above, The Hamming distance between any two codewords c_i and c_j of the code set C is given by:

$$H_{dist}(c_i,c_j)=\frac{1}{n}\sum_{r=1}^{n}|c_i^r-c_j^r| \qquad (1)$$

Definition 3: Let $M=\{0,1\}^k$ be a message space. The function $g:M\rightarrow C$ which we call an error correction encoded function, represents a one-to-one mapping of messages to codewords. (conversely, g^{-1} is the inverse of g which used to retrieve the transmitted message from the reconstructed codeword).

Definition 4: The maximum number of errors that can be corrected in the corrupted codeword is called error correction threshold of the error correcting code C, and denoted by t_{sh}.

Definition 5: (Error correction decoded function): An error correction decoded function $f:\{0,1\}^n\rightarrow C\cup\perp$, for a code set C is defined as: For any $c'\in\{0,1\}^n$,

$$f(c')=\begin{cases}c & \text{If } H_{dist}(c',c)\le t_{sh}\\ \perp & \text{otherwise}\end{cases} \qquad (2)$$

where $\perp$ is denoted that an invalid codeword.

Definition 6 (Statistical distance): Let X and Y be two random variables over the same sample space, and let D_1 and D_2 be their associated discrete probability distributions. Then, we defined and denoted the statistical distance between D_1 and D_2 as follows:

$$S_{dist}(D_1;D_2)=\sum_{a\in\psi}\left|\text{Prob}[\mathrm{X}=a]-\text{Prob}[\mathrm{Y}=a]\right| \qquad (3)$$

B. Biometrics

A biometric system is defined as the automated measurements of physiological or behavioral characteristics (e.g. fingerprints, facial geometry, iris patterns, retinal patterns, hand geometry, voice prints, or, DNA) to determine, verify, or identify of a human being [17,18]**.** A Biometric authentication system performs automated authentication of users depending on their physical and behavioral characteristics. Such an authentication system consists of several basic modules:

Biometric Sensor Module: The biometric sensor requires users to present their biometrics in the form of an image and therefore the analog to digital conversion. The output of the biometric sensor is the raw biometric data. The sensor is used at the enrollment of a user and every time a user needs to be authenticated.

Feature Extraction Module: The raw data are processed and analyzed. The result of the feature extraction (template) should be the most distinctive features for every user. Feature extraction is performed during the enrollment process as well as during an authentication.

Matching Module: The biometric matching module is requires that the user present their biometric for reading, template generating process is also applied here, and compared with the stored template. Then match score is generated. Matching is performed whenever a user needs to be authenticated.

Decision Module: The process of determining or authenticate the identity of the user.

The two basic processes of a biometric authentication system are the "enrollment" process and the "authentication" process. In the enrollment process of a biometric authentication system, all users are registered with the system, and biometric references data x_{ref} is stored in the database of the system. On the other hand, the authentication process denotes the process of identity verification or determination. In this process the authentication system performs a comparison between the presented biometrics x_{test} and the stored references of the previous enrollment phase according to some metric distance.

III. RELATED WORK

A. Review of Juels and Wattenberg's scheme

In 1999, Juels and Wattenberg combined well known techniques from the areas of error correcting codes and cryptography to achieve a new type of cryptographic primitives referred to as fuzzy commitment scheme (FCS).

The fuzzy commitment scheme consists of a function F, used to commit to a codeword $c \in C(n,k)$ and a witness $x \in \{0,1\}^n$, where both c and x are n-bits string. The difference vector $\delta \in \{0,1\}^n$, where $\delta = x - c$, and the hash value $h(c)$ are stored as commitment $F(c,x) = (h(c),\delta)$. To open the commitment $F(c,x) = (h(c),\delta)$ using witness x', the receiver computes the codeword $f(c')$ and verifies $h(f(c')) \overset{?}{=} h(c)$. If it holds, the commitment $F(c,x) = (h(c),\delta)$ has been successful opened. Otherwise x' is an incorrect witness.

The idea of "*fuzziness of* x" that each x' is sufficient "close" to the original x, according to an appropriate distance metric, such as Hamming distance, but not necessary identical. The difference vector δ used to translate x' in the direction of x, facilitating to reconstruct the codeword $f(c')$ [6].

B. Security flaw of Juels and Wattenberg's scheme

The Juels and Wattenberg scheme is a simple commitment construction based solely on cryptographic hash function "the sender commit to a secret message c $h(c)$". Obviously, the amount of information about the codeword and the witness is hidden in the hash value $h(c)$. However, such strategy is *not* secure enough [16], because the cryptographic hash functions such as MD5 and SHA families are proven theoretically and practically *vulnerable* to collision and second preimage attacks (RFC 4270). Furthermore, several researchers have noticed serious security flaws and vulnerabilities in most widely used MD and SHA families [19-27]. Moreover, in response to a SHA-1 vulnerability announced in Feb. 2005, NIST (National Institute of Standard and Technology) was apparently not confident in the strength of SHA-1 [28].

Therefore, the Juels and Wattenberg's scheme *not* satisfy the hiding and binding properties of commitment schemes and hence the systems using it are *not* secure.

IV. THE PROPOSED ORDINARY FUZZY COMMITMENT SCHEME

An *ordinary Fuzzy Commitment Scheme* is three-phase (Setup, Commit and Open phases) represents by the tuple $\{\mathrm{M, X, Y, K, ECCS, FPCK_F, P}, E(e_i,t_i)\}$ where:

M : A set of all possible resources (message space) states, not necessarily binary?

X : A set of witnesses states.

Y : A set of all possible fuzzy commitments.

K : A set of indices k encoded by unary ($1^{\mathbf{k}}$), which we call it the security parameter.

ECCS : Error Correcting code System $\{C,g,f\}$, where $C(n,k)$ is a code set, g is a error correction encoded function and f is an error correction decoded function.

$\mathrm{FPCK_F}$: A family of fuzzy public commitment keys (fuzzy PCK). For each $k \in \mathrm{K}$, there fuzzy PCK, $\mathrm{F}:g(\mathrm{M}) \times \mathrm{X} \to \mathrm{Y}$, which is denoted and defined as:

$$\mathrm{F}(g(m),x) = (\varepsilon,\delta),$$

where $\delta = x - c$, is called the difference vector and the $\varepsilon = F_k(c,x)$ is a conventional commitment scheme computed using the public commitment key $F_k : C \times \mathrm{X} \to \mathrm{E}$.

P : A set of individuals, generally with three elements **A** as a committing party, **B** as the party to which a commitment made and **Ted** as the trusted party.

$E(e_i,t_i)$ **:** A set of events occurring at times t_i and carried out by the algorithms e_i for $i = 1,2,3$.

The scheme is illustrated in Fig. 1. Initially, the environment is setup according to Algorithm 1 labeled by *Setup* (event e_1) occurs at time t_1 .The **Ted** selects security parameter $k \in \mathrm{K}$ and generates the parameters of the fuzzy PCK, F.

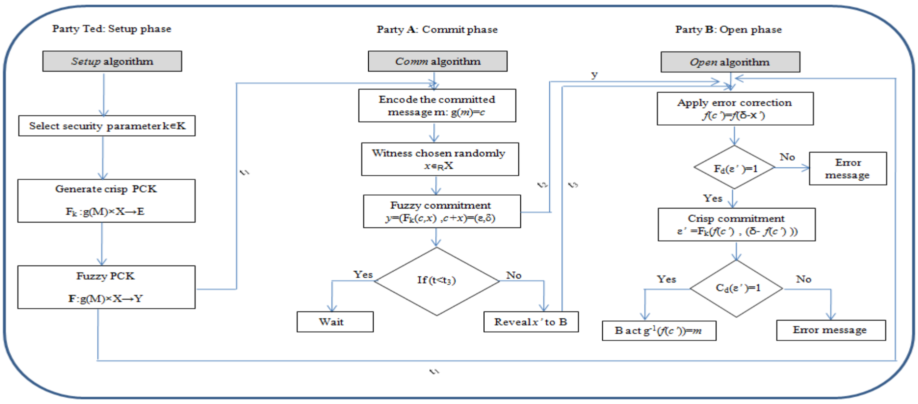

Figure 1: The proposed ordinary fuzzy commitment scheme

Algorithm 1: Setup phase of the OFCS scheme. This procedure is run by the trusted third party Ted.

Input: Security parameter k encoded by unary 1^k.

$Setup(1^k) \rightarrow param(\mathrm{F})$

Output: A parameters of the fuzzy public commitment key - $param(\mathrm{F})$.

Then the fuzzy PCK $\mathrm{F}: g(\mathrm{M}) \times \mathrm{X} \rightarrow \mathrm{Y}$ of OFCS scheme defines as $\mathrm{F}(g(m), x) = (F_k(c,x), x-c) = (\varepsilon, \delta)$

The trusted third party **Ted** publishes the fuzzy public commitment key $\mathrm{F}: g(\mathrm{M}) \times \mathrm{X} \rightarrow \mathrm{Y}$ to both the sender **A** and the receiver **B** (after that the **Ted** becomes inactive).

During the commit phase, the sender commit to his secret message $m \in \mathrm{M}$ using Algorithm 2 labeled by $Comm$ (event e_2) occurs at time t_2.

Algorithm 2: Commit phase of the OFCS scheme. This procedure is run by the sender **A**.

Input: A secret message $m \in \mathrm{M}$ and the fuzzy public commitment key F.

- Compute $c = g(m)$.
- Choose a random witness $x \in_R \mathrm{X}$.
- Compute the commitment $\varepsilon = F_k(m, x)$.
- Compute the difference vector $\delta = x - c$.

Output: A fuzzy commitment $y = (\varepsilon, \delta)$.

The sender **A** sends the fuzzy commitment y to the receiver **B** at time t_2. When the time reaches $t > t_2$ ((t_3)), the sender reveals the opening key $op_{key} = x'$ to the receiver. Then the receiver make use of the opening key to execute the open phase according to Algorithm 3 labeled by $Open$ (event e_3) occurs at time t_3.

Algorithm 3: Open phase of the OFCS scheme. This procedure is run by the sender **B**.

Input: A commitment y, fuzzy public commitment key F and the opening key $op_{key} = x'$.

- Compute $f(c') = f(x' - \delta)$.
- Fuzzy decision making; verify $\mathrm{F}_d(f(c')) = 1$. If true,
- Compute the crisp commitment $\varepsilon' = F_k(f(c'), (\delta - f(c')))$.
- Crisp decision making; verify $C_d(\varepsilon') = 1$. If true,

Output: The committed message is accepted as $m = m' = g^{-1}(f(c'))$. Otherwise an error message, invalid opening key is revealed.

V. SECURITY ANALYSIS

In the design of any commitment scheme, hiding and binding properties are the most important security aspects to be considered. In this Section we investigate the security of the proposed *ordinary fuzzy commitment scheme* with respect to all power computation receiver (hiding property) and computationally bounded sender (binding property). To simplify our analysis, It should be noted that the definitions of message space is $\mathrm{M} = \{0,1\}^k$, the witness set $\mathrm{X} = \{0,1\}^n$ and code set $C \subset \{0,1\}^n$. These sets are independent random variables over the same sample space $\{0,1\}^n$. Furthermore, these sets are finite and all their associated probabilities distributions are discrete. Also we will assume that the operation "+" is exclusive OR and denoted by "$\oplus$".

A. Hiding Property

The hiding property characterizes the resistance of the scheme against attempts carried out by an adversary receiver **B*** to determine the codeword *c* or the witness *x*, from the fuzzy commitment $y = (\varepsilon, \delta)$. We assume that the adversary receiver **B*** knows F_k and has an access to the fuzzy commitment pair $y = (\varepsilon, \delta)$. Then an adversary may be compromises the committed codeword from either the difference vector δ or the conventional commitment $\varepsilon = F_k(c, x)$.

Lemma 1: Suppose that X and Y are two independent random variables over the same sample space ψ. Let Z be a random variable obtained by exclusive "OR" of X and Y. Then, the three random variables X, Y, and Z are pair-wise independent.

Proof: Let X and Y are two independent random variables over the same sample space ψ. So we have,

$$\mathrm{Prob}[X=u, Y=v] = \mathrm{Prob}[X=u]\mathrm{Prob}[Y=$$

$$\leq \frac{1}{|X||Y|} \tag{4}$$

Now, let $Z = w$, such that $w = u \oplus v$, and thus $v = w \oplus u$. Since the variables $X = u$ and $Y = w \oplus u$ are independent random variables, therefore X and Z. Similarly, Y and Z are independent.

Theorem 1: Suppose that X (witness space) and C (error correcting code set) are two independent random variables over the same sample space $\{0,1\}^n$, and let $Z = \{\delta = x \oplus c : x \in X, c \in C\}$ be a random variable obtained by "exclusive OR" of elements of X and C. Then, the probability that an adversary receiver **B*** is able to compute either c or x from the difference vector is no more than 2^{-k}, where k is the size of the error correcting code C.

Proof: Assume that X and C be two independent random variables over the same sample space $\{0,1\}^n$, clearly $|C| = 2^k$ and $k < n$, thus

$$\mathrm{Prob}[X = x, C = c] = \mathrm{Prob}[X = x]\mathrm{Prob}[C = c] \leq \frac{1}{2^n} \cdot \frac{1}{2^k} \tag{5}$$

Let $Z = \{\delta = c \oplus x : c \in C, c \in X\}$ be an event obtained by "exclusive OR" elements of X and C. Thus Z, **X**, and **C** are pair-wise independent random variables (Lemma1). Hence we have

$$\mathrm{Prob}[X = x \mid Z = \delta] = \mathrm{Prob}[X = x] \leq \frac{1}{2^n} \quad , \tag{6}$$

and

$$\mathrm{Prob}[C = c \mid Z = \delta] = \mathrm{Prob}[C = c] \leq \frac{1}{2^k} \tag{7}$$

Therefore

$$\mathrm{Prob}[X = x \mid Z = \delta \text{ or } C = c \mid Z = \delta]$$
$$= \mathrm{Max}\{\mathrm{Prob}[X = x], \mathrm{Prob}[C = c]\} \leq 2^{-k}$$

(Max: means minimum of two numbers).

Definition 7: [Statistically hiding measure]

The OFCS scheme is λ-hiding if for any two codewords, $c_1 = g(m_1)$ and $c_2 = g(m_2)$, such that $H_{dist}(c_1, c_2) > t_{sh}$ are secured using the same F_k. The distributions $D(c_1)$ and $D(c_2)$ given by:

$$D(c_1) = \mathrm{Prob}[F_k(c_1, x) = \varepsilon, \text{ for some } x \in X]$$
$$= \sum_{x \in X} \mathrm{Prob}[x] \cdot \mathrm{Prob}[\varepsilon \mid x] \tag{8}$$

and

$$D(c_2) = \mathrm{Prob}[F_k(c_2, x) = \varepsilon, \text{ for some } x \in X]$$
$$= \sum_{x \in X} \mathrm{Prob}[x] \cdot \mathrm{Prob}[\varepsilon \mid x] \quad ,$$

(9) are two probability distribution over the same sample space.

Then,

$$S_{dist}(D(c_1), D(c_2)) = \lambda \tag{10}$$

Eq (10) states that an adversary able to distinguish between what sender committed to, only to extend of measurable difference given by λ. To provide a measure of the hiding property, $\lambda = 0$ -hiding represents the perfect OFCS hiding and the weakest OFCS hiding is given by $\lambda = 1$-hiding. In the following theorem bound derivation for statistically-hiding property.

Theorem 2 [Hiding-Measurement] For any $k \in K$, let $F : C \times X \rightarrow Y$ be a fuzzy public commitment key. Then, an ordinary fuzzy commitment scheme based on F is λ-hiding and the value of λ is always computed as: For $c_1 = g(m_1)$ and $c_2 = g(m_2)$ in C

$$S_{dist}(D(c_1), D(c_2)) = 2^{-2n} \sum_{\varepsilon \in E} |\rho_{\varepsilon, c_1} - \rho_{\varepsilon, c_2}| = \lambda \tag{11}$$

***Proof*:**

For given $c = g(m) \in C$, let $D(c)$ be a probability distribution on the code set C, defined as $D(c) = \mathrm{Prob}[C = c : F_k(c, x) = \varepsilon]$.

For any $\varepsilon \in E$, let $\rho_{\varepsilon,c}$ be the size of pre-image set $\Omega_\varepsilon(c) = \{x : F_k(c, x) = \varepsilon\}$.

For fixing $\varepsilon_0 \in \mathbf{E}$, $D(c_0)$ is defined by:

$$D(c_0) = \mathrm{Prob}[C = c_0 : F_k(c_0, x) = \varepsilon_0, \text{ for some } x \in X]$$
$$= \sum_{x \in X} \mathrm{Prob}[x] \cdot \mathrm{Prob}[F_k(c_0, x) = \varepsilon_0 \mid x] \tag{12}$$

Then for some value $x_0 \in X$,

$$\mathrm{Prob}[F_k(c_0, x_0) = \varepsilon_0 \mid x_0] = \mathrm{Prob}[x_0 : F_k(c_0, x_0) = \varepsilon_0]$$

$$= \begin{cases} 2^{-n} & \text{if } x_0 \in \Omega_{\varepsilon_0}(c_0) \\ 0 & \text{Otherwise} \end{cases} \tag{13}$$

Hence

$$D(c_0) = \mathrm{Prob}[F_k(c_0, x) = \varepsilon_0, \text{ for some } x \in X]$$
$$= \sum_{x \in X} \mathrm{Prob}[x] \cdot \mathrm{Prob}[F_k(c_0, x) = \varepsilon_0 \mid x] \tag{14}$$
$$= 2^{-n} \sum_{x \in \Omega_{\varepsilon_0}(c_0)} 2^{-n} = 2^{-2n} \rho_{\varepsilon_0, c_0}$$

Assume that the receiver can find two codewords c_1 and c_2 in C, such that $H_{dist}(c_1, c_2) > t_{sh}$ and $F_k(c_1, x_1) = F_k(c_2, x_2) = \varepsilon$ for some $x_1, x_2 \in \mathbf{X}$. Thus,

$$S_{dist}(D(c_1),D(c_2))=\sum_{\varepsilon\in\mathrm{E}}|\,\mathrm{Prob}[F_k(c_1,x)=\varepsilon]-\mathrm{Prob}[F_k(c_2,x)=\varepsilon]\,|$$
$$=\sum_{\varepsilon\in\mathrm{E}}|\sum_{x\in\mathrm{X}}\mathrm{Prob}[x]\square\mathrm{Prob}[F_k(c_1,x)=\varepsilon]-\sum_{x\in\mathrm{X}}\mathrm{Prob}[x]\square\mathrm{Prob}[F_k(c_2,x)=\varepsilon]\,|$$
$$\le\sum_{\varepsilon\in\mathrm{E}}|\,2^{-2n}\sum_{x\in\Omega_\varepsilon(c_1)}1-\sum_{x\in\Omega_\varepsilon(c_2)}1\,|$$
$$=2^{-2n}\sum_{\varepsilon\in\mathrm{E}}|\,\rho_{\varepsilon,c_1}-\rho_{\varepsilon,c_2}\,|=\lambda$$

B. Binding Property

The binding property of our OFCS scheme characterizes the resistance against attempts carried out by an adversary receiver **A*** to determine the codeword c' such that $H_{dist}(c,c')>t_{sh}$ and $F_k(c,x)=F_k(c',x')=\varepsilon$, for some $x'\in\mathrm{X}$.

Definition 8 [Computationally-binding measure] The OFCS scheme is η-binding if for any distinct codeword $c'\ne c\in C$ such that $H_{dist}(c,c')>t_{sh}$ and $F_k(c,x)=F_k(c',x')=\varepsilon$, for some $x,x'\in\mathrm{X}$, with knowledge of public commitment key F_k and the fuzzy commitment ε. Then:

$$\mathrm{Prob}[c',H_{dist}(c',c)>t_{sh}:F_k(c',x')=\varepsilon,\ x'\in\mathrm{X}]\le 2^{-2n}\rho_{\varepsilon,c'}=\eta \qquad (15)$$

Theorem 3 [Binding -Measurement] Let $\mathrm{F}:\mathrm{C}\times\mathrm{X}\to\mathrm{Y}$ be the fuzzy PCK. Then, an ordinary fuzzy commitment scheme based on the fuzzy PCK is η–binding and the value of η is always be computed as follows:

$$\mathrm{Prob}[c',H_{dist}(c',c)>t_{sh}:F_k(c',x')=\varepsilon,\ x'\in\mathrm{X}]\le 2^{-2n}\rho_{\varepsilon,c'}=\eta$$

Proof:

Assume that $c=g(m)\in C$, $x\in\mathrm{X}$, and $F_k(c,x)=\varepsilon$ be the commitment in the fuzzy commitment y. Let $\rho_{\varepsilon,c}$ be the size of pre-image set $\Omega_\varepsilon(c)=\{x:F_k(c,x)=\varepsilon\}$.

Our task is to find the probability that an adversary sender A* finds an opening key $x'\in\mathrm{X}$, with $H_{dist}(x,x')=H_{dist}(c,c')>t_{sh}$ such that the equality $F_k(c,x)=F_k(c',x')=\varepsilon$, holds.

Fix a codeword $c'\in C$ and Using Eq.(13) and (14)

$$\mathrm{Prob}[c':F_k(c',x')=F_k(c,x)=\varepsilon,\ x'\in\mathrm{X}]$$
$$=\sum_{x'\in\mathrm{X}}\mathrm{Prob}[x']\square\mathrm{Prob}[F(c',x')=\varepsilon\,|\,x']$$
$$\le 2^{-2n}\rho_{\varepsilon,c'}=\eta$$

VI. Constructions of Ordinary Fuzzy Commitment Schemes

This section introduces several constructions of an ordinary fuzzy commitment schemes. We distinguish between number-theoretic constructions [29, 32-34] applying the hardness of factoring for instance, existence of collision-free hash functions –based constructions and complexity-based construction using general cryptographic assumptions like the existence of Pseudo-random generator.

A. Factoring –Based Construction

The factoring-based ordinary fuzzy commitment scheme is based on Halevi's conventional commitment [29]. To set up the factoring–based OFCS scheme the trusted third party **Ted** runs a $Setup(1^k)$ which will generate a composite number $n=p\square q$ as a parameter of the fuzzy public commitment key, where p and q are two prime numbers chosen randomly, such that $p=3\ (\mathrm{mod}\,8)$ and $q=7\ (\mathrm{mod}\,8)$. Halevi used the Goldwasser-Micali-Rivest (GMR) claw-free permutation pairs [18], $P_{N,c}$, and then the parameter n is given to both the sender and the receiver

To commit to the message $m\in\mathrm{M}$ the sender chooses a random witness $x\in_R\mathrm{X}$, computes the crisp commitment $\varepsilon=F_k(c,x)=P_{N,c}\left(x^2\right)\ (\mathrm{mod}\,n)$ and the difference vector $\delta=x-c$, where $c=g(m)$ is the encoded message, then the crisp commitment and the difference vector together sends to the receiver as fuzzy commitment termed $\mathrm{F}(m,x)=(\varepsilon,\delta)$.

During the open phase, the sender sends the receiver the opening key $op_{key}=x'$ in which sufficient "close" to the original $op_{key}=x$, according to appropriate distance metric,, but not necessary identical, should be able to reconstruct the codeword $f(c')=f\left(x'-\delta\right)=f\left((x'-x)-c\right)$ from the difference vector δ and translate x' into the direction of x, $x''=\delta-f(c')$. After that the receiver computes the crisp commitment $\varepsilon'=F_k\left(f(c'),x''\right)$ and matches against the stored crisp commitment ε, $\varepsilon'\overset{?}{=}\varepsilon$. If it fails, the receiver does not accept $op_{key}=x'$ as an opening key. Otherwise the receiver accept and retrieve the secret message $m=m'=g^{-1}\left(f(c')\right)$..

B. Collision-Free Hash Function –Based Construction with universal Hash

The collision-free hash function-based ordinary fuzzy commitment scheme is based on Halevi and Micali's conventional commitment [16]. To set up the collision-free hash function –based OFCS scheme the trusted third party Ted runs a $Setup(1^k)$ which will generate a collision-free hash function $h:\{0,1\}^*\to\{0,1\}^k$, and then the collision-free hash function will given to both the sender and the receiver.

To commit to the message $m \in \text{M}=\{0,1\}^k$ the sender chooses a random witness $x \in_R \text{X}=\{0,1\}^n$, computes the conventional commitment $\varepsilon = F_k(c,x) = (h(c),u)$, where $u:\{0,1\}^n \to \{0,1\}^k$ be a universal hash function chosen randomly such that $u(c)=x$,and the difference vector $\delta = x - c$, where $c = g(m)$ is the encoded message, then the commitment and the difference vector together sends to the receiver as fuzzy commitment termed $\text{F}(m,x)=(\varepsilon,\delta)$.

During the open phase, the sender sends the receiver the opening key $op_{key}=x'$ in which sufficient "close" to the original x, according to appropriate distance metric,, but not necessary identical, should be able to reconstruct the codeword $f(c') = f(x'-\delta) = f((x'-x)-c)$ from the difference vector δ and translate x' into the direction of x , $x''=\delta - f(c')$. After that the receiver checks $u(f(c'))\overset{?}{=}x''$. If it fails, the receiver does not accept the opening key. Otherwise, computes the conventional commitment $\varepsilon' = F_k(f(c'),x'')$ and matches against the stored conventional commitment ε , $\varepsilon'\overset{?}{=}\varepsilon$. If it fails, the receiver do not accept $op_{key}=x'$ as an opening key. Otherwise, the receiver accept and retrieve the secret message $m = m' = g^{-1}(f(c'))$.

C. Pseudo-Random Generator –Based Construction

The pseudo random generator-based ordinary fuzzy commitment scheme is based on Naor's conventional commitment [30]. To set up the pseudo random generator–based OFCS scheme the trusted third party **Ted** runs a $Setup(1^k)$ which will generate a pseudo random generator $\text{G}:\{0,1\}^n \to \{0,1\}^{2n}$ defined as $G(x)=B(1)B(2)....B(2n)$, where $B(i)$ is ith bit of $G(x)$ and a random vector $\vec{R}=(r_1,r_2,.....,r_{2n})$, Such that $H_{dist}(\vec{0},\vec{R})=n$, where $r_i \in \{0,1\}$ for $1 \le i \le 2n$. Then the parameters $(G,\vec{R})$ are given to both the sender and the receiver.

To commit to the message $m \in \text{M}=\{0,1\}^k$ the sender chooses a random witness $x \in_R \text{X}=\{0,1\}^n$, computes the conventional commitment $\varepsilon = F_k(c,x) = \begin{cases} B(i) & if\ r_i = 0 \\ B(i) \oplus c & if\ r_i = 1 \end{cases}$ and the difference vector $\delta = x - c$, where $c = g(m)$ is the encoded message, then the conventional commitment and the difference vector together sends to the receiver as fuzzy commitment termed $\text{F}(m,x)=(\varepsilon,\delta)$.

During the open phase, the sender sends the receiver the opening key $op_{key}=x'$ in which sufficient "close" to the original x, according to appropriate distance metric, but not necessary identical, should be able to reconstruct the codeword $f(c') = f(x'-\delta) = f((x'-x)-c)$ from the difference vector δ and translate X' into the direction of x , $x''=\delta - f(c')$. After that the receiver computes the conventional commitment $\varepsilon' = F_k(f(c'),x'')$ and matches against the stored conventional commitment ε , $\varepsilon'\overset{?}{=}\varepsilon$. If it fails, the receiver does not accept $op_{key}=x'$ as an opening key. Otherwise, the receiver accept and retrieve the secret message $m = m' = g^{-1}(f(c'))$.

VII. Fuzzy Biometrics Authentication with Renewable Template using smart card

The lacks of secrecy of biometrics (e.g., leaving fingerprint impressions on the surfaces we touch, face and eye images being captured by hidden cameras) are identified as the main problems of biometric systems [31]. Unlike replacing key or password in traditional authentication systems, once the biometric template is compromised, there is no way to use it directly again even in secure biometric authentication. In this section, we propose fuzzy biometric authentication with the renewability of protected biometric templates property to overcome this problem, in which the template is privacy protected and multiple fuzzy commitments of the templates can be derived from the same biometric template for the purpose of template renewability. If the biometric template is compromised, then the user needs to register again using the same biometric template with selection of different codeword.

A. Registration phase

When the user U needs to register with the system S , they perform the following steps:

1. U chooses a random codeword c from a code set $C(n,k)$.
2. U presents her/his personal biometric data B on the specific device which will generate a biometric template x , and provides the codeword c , and the identity ID to the system S via secure channel.
3. S computes the fuzzy commitment $\text{F}(c,x)=(\varepsilon,\delta)$ and the ciphertext $E(c)$ of the codeword (for the re-registration purpose).
4. S stores $(\varepsilon,E(c),ID)$ in the system database and loads (ε,δ,ID) in U 's smart card, and then sends it to U via secure channel.

B. Authentication phase

Whenever the user U wants to login to the system S , she/he must perform the following steps:

1. U inserts her/his smart card into the card reader and presents her/his personal biometric data B on the

specific device which will generate a biometric template x'.

2. The smart card computes the codeword $f(c') = f(x' - \delta)$ and $x'' = \delta + f(c')$, and then the commitment $\varepsilon' = F_k(f(c'), x'')$. The commitment ε' matches against the stored ε in the system database i.e. $\varepsilon' \overset{?}{=} \varepsilon$.
3. If the above mentioned verifications failed, the scheme will be terminated and as a result U will not pass this stage. Otherwise, if the above verification holds, the user is authenticated.

VIII. CONCLUSION

In this paper, we developed a general fuzzy commitment scheme called an *ordinary fuzzy commitment scheme* (OFCS), in which many fuzzy commitment schemes with variety complexity assumptions constructed and the security of Juels and Waterberg fuzzy commitment scheme is resolved. The proposed scheme is proved to be resistance to all power computation adversary receiver and computation bounded adversary sender. The efficiency of our scheme offers different security assurance and the trusted third party involved only in the setup phase.

The characteristic of our scheme makes it more effective and promising to design high secure biometrics protection scheme. This paper also proposed fuzzy biometric authentication scheme based on OFCS scheme with the renewability of protected biometric templates property, in which the template is privacy protected and multiple fuzzy commitments of the templates can be derived from the same biometric template for the purpose of template renewability.

ACKNOWLEDGMENT

We would like to thank King Fahd University of Petroleum and Minerals for providing facilities for this research.

REFERENCES

[1] C. Cr épeau, “Efficient cryptographic protocols based on noisy channels,” In Proceedings of the 16th annual international conference on Theory and application of cryptographic techniques, LNCS , Springer-Verlag Berlin, Heidelberg 1997; 1233, pp. 306-317.

[2] G. Davida, Y. Frankel, B. Matt, “On enabling secure applications through off-line biometric identification,” In Proc. IEEE Security and Privacy, Oakland, CA , USA, pp. 148 – 157, 1998. DOI: 10.1109/SECPRI.1998.674831.

[3] G. Davida, Y. Frankel, B. Matt, R. Peralta, “On the relation of error correction and cryptography to an offline biometric based identification scheme,” In Proc. Workshop Coding and Cryptography, pp. 129–138, 1999.

[4] U. Uludag, S. Pankanti, S. Prabhakar, “Jain A. Biometric Cryptosystems: Issues and Challenges,” In Proceedings of the IEEE, 92(6), 948 – 960, 2004. DOI: 10.1109/JPROC.2004.827372.

[5] J. Daugman, “High confidence visual recognition of persons by a test of statistical independence,” IEEE Trans. Pattern Anal. Machine Intell., 15, 1148–1161, 1993.

[6] A. Juels, M. Wattenberg, “A fuzzy commitment scheme,” In Proc. 6th ACM Conf. Computer and Communications Security, G. Tsudik, Ed., pp. 28–36, 1999.

[7] T. Ignatenko, “Information Leakage in Fuzzy Commitment Scheme,” IEEE Transaction on Info. Forensics and Security 5(2), 337-348, 2010.

[8] A. Juels, M. Sudan, “A fuzzy vault scheme,” In Proc. IEEE Int. Symp. Information Theory, A. Lapidoth and E. Teletar (Eds), p. 408, 2002.

[9] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data,” In Proc EUROCRYPTO’04, LNCS, 3027, 523-540, 2004.

[10] E. Verbitskiy, P. Tuyls, C. Obi, B. Schoenmakers, B. Ŝkorić, “Key extraction from general non-discrete signals,” IEEE Trans Info. Forensic and Security, 5(2), 269-279, 2010.

[11] F. Monrose, M. Reiter, Q. Li, S. Wetzel, “Cryptographic key generation from voice. In SP ’01 Proc. of the 2001 IEEE Symp. on Security and Privacy, Washington USA, pp. 202, 2001.

[12] F. Monrose, M. Reiter, Q. Li, S. Wetzel, “Using Voice to Generate Cryptographic Keys,” In Proc. of the Speech Recognition Workshop, pp. 237-242, 1998.

[13] F. Monrose, M. Reiter, S. Wetzel, “Password hardening based on keystroke dynamics,” In Proc. of 6th ACM Conf on Computer and Communications Security (CCCS), Washington USA, 73-82, 1999.

[14] L. Ballard, S. Kamara, F. Monrose, M. Reiter, “On the requirements of biometric key generators,” Technical Report TR-JHU-SPARBKMR- 090707. Submitted and available as JHU Department of Computer Science Technical Report, 2007.

[15] H. Feng, C. Wah, “Private key generation from on-line handwritten signatures,” Information Management Computer Security, 10(18), 159-164, 2002.

[16] S. Halevi, S. Micali, “Practical and Provably-Secure Commitment Schemes from Collision-Free Hashing,” Advances in Cryptology – CRYPTO ’96, Proc. of 16th Annual International Cryptology Conference, USA, pp. 201–215, 1996.

[17] A. Jain, P. Flynn, A. Ross, “Handbook of Biometrics,” Springer, 2008.

[18] A. Jain, K. Nandakumar A. Nagar, “Biometric template security,” EURASIP J Adv Signal Process, pp. 1-17 2008.

[19] B. Preneel, “The stat of cryptographic hash functions,” In Lectures on Data Security: Modern Cryptology in Theory and Practice, LNCS, Berlin: Springer, 1561, 158-192, 1999.

[20] B. Preneel, “The State of Hash Functions and the NIST SHA-3 Competition (Extend abstract),” Information Security and Cryptography, LNCS, 5487, 1-11, 2009.

[21] D. Boer, A. Bosselaers, “Collision for the Comparison function of MD-5,” In Helleseth, T.(ed), EUROCRYPT’93, LNCS, 765, 293-304, 1994.

[22] H. Dobbertin, “The Status of MD5 after recent attack,” CryptoBytes, 2(2),1-6, 1994.

[23] V. Klima, “Tunnels in Hash Functions: MD5 collisions within a minute,” IACR ePrint archive, 2006, http://eprint.iacr.org/2006/105.pdf.

[24] X. Wang, A. Yao, F. Yao, “Cryptanalysis of SHA-1 Hash Function,” Technical Report, National Institute of Standard and Technology (NIST), 2005, Available at http://csrc.nist.gov/groups/ST/hash/documents/Wang_SHA1-New-Result.pdf .

[25] X. Wang, L. Yin, H. Yu, “Finding Collisions in the full SHA-1,” In V. Shoup (ed) CRYPTO’05, LNCS, Springer, 3621, 17-36, 2005.

[26] X. Wang, H. Yu, “How to Break MD5 and other Hash Functions,” In Carmer, R. (ed) EUROCRYPT’05, LNCS, Springer, 3494, 19-35, 2005.

[27] E. Biham, R. Chen, A. Joux, P. Carribault, C. Lemuet, W. Jalby, “Collision of SHA-0 and reduced SHA-1,” In R. Cramer (ed), EUROCRYPTO’05, LNCS, Springer, 3494, 36-57, 2005.

[28] NIST (National Institute of Standards and Technology). (2007). SHA-3 Competition. http://csrc.nist.gov/groups/ST/hash/timeline.html.

[29] S. Halevi, “Efficient commitment with bounded sender and unbounded receiver,” In D. Coppersmith, editor, Proc. Crypto `95. Lecture Notes in Computer Science, volume 963, Pages 84-96, Springer-Verlag, 1995.

[30] M. Naor, “Bit Commitment Using Pseudo-Randomness,” In Gilles Brassard, editor, Advances in Cryptology - CRYPTO ’89, 9th Annual International Cryptology Conference, LNCS, Santa Barbara, California, USA, 435, 128–136, 1989.

[31] U. Uludag, “Secure Biometric Systems,” Ph.D. Thesis, Michigan State University, 2006.

[32] E. Fujisaki, T. Okamoto, “Statistical Zero-Knowledge Protocols to prove Modular Polynomial Relations, In Crypto’97, LNCS, Springer, 1294, pp. 16-30, 1997.

[33] E. Fujisaki, T. Okamoto, “Statistical Zero-Knowledge Protocols to Prove Modular Polynomial Relations,” IEICE Trans. Fund., E82-A, 1, 81–92, 1999.

[34] S. Halevi, “Efficient commitment with bounded sender and unbounded receiver,” In D. Coppersmith, editor, Proc. Crypto `95, Lecture Notes in Computer Science, Springer-Verlag, 963, pp. 84-96, 1995.

[35] A. Alsaggaf, H. Acharya, “A Fuzzy Commitment Scheme,” Advances in Computer Vision and Information Technology, Part_7, ch_13, pp. 1164-1169, Nov. 2007, I. K. International Pvt Ltd.

[36] A. Alsaggaf, “Crisp Commitment Scheme based on Noisy Channels,” In Proc. of IEEE 1st Saudi International Conference on Phonics, Electronic and Communication, pp. 1-4, April 2011, Riyadh, Saudi Arabia. DIO: 10.1109/SIECPC.2011.5876892.

Alawi Al-Saggaf, Born on 9th Sep. 1972. M.Sc. in Mathematics (1st honor) from University of Pune-India, and Ph.D. candidate in computer studies at Symbiosis International University -India. Currently working as a lecturer at KFUPM –Saudi Arabia.

In recent years, Biometric Protection Schemes have been actively researched. His main research interests include information security, cryptography and biometric protection systems.

Dr. Haridasa S. Acharya, Born on 19th Jan 1948. MSc(Mathematics, 1970) from University of Pune, and PhD (1975) from IIT Kanpur, is currently Professor at the Allana Inst of Management Sciences, Azam Campus , Pune. Was awarded Shiksha Rattan Puraskar for his contribution to education by the India International Friendship Society, New Delhi in the year 2008. He was a National Fellow of Biotechnology, (DST Govt if India) at IASRI New Delhi in the year 1990-91. Was principal investigator , and Co-Investigator in many scientific projects funded by UGC(New Delhi), ICAR(new Delhi). Has more than 30 reseach papers in the fields of Mathematics, Soil Science and Engineering, Computer applications. Has authored a Book and has edited three proceedings of National and Regional conferences. Has guided 4 PhD students in the field of Computer Science and Information technology .