

Privacy Weaknesses in Biometric Sketches

Koen Simoens*, Pim Tuyls^{†*} and Bart Preneel*

*Dept. Electrical Engineering-ESAT / COSIC, Katholieke Universiteit Leuven – IBBT, Belgium
koen.simoens@esat.kuleuven.be, bart.preneel@esat.kuleuven.be

[†]Intrinsic-ID, The Netherlands
pim.tuyls@intrinsic-id.com

Abstract

The increasing use of biometrics has given rise to new privacy concerns. Biometric encryption systems have been proposed in order to alleviate such concerns: rather than comparing the biometric data directly, a key is derived from these data and subsequently knowledge of this key is proved. One specific application of biometric encryption is the use of biometric sketches: in this case biometric template data are protected with biometric encryption. We address the question whether one can undermine a user’s privacy given access to biometrically encrypted documents, and more in particular, we examine if an attacker can determine whether two documents were encrypted using the same biometric. This is a particular concern for biometric sketches that are deployed in multiple locations: in one scenario the same biometric sketch is deployed everywhere; in a second scenario the same biometric data is protected with two different biometric sketches. We present attacks on template protection schemes that can be described as fuzzy sketches based on error-correcting codes. We demonstrate how to link and reverse protected templates produced by code-offset and bit-permutation sketches.

1. Introduction

In the past decade, there has been an increasing interest in the use of biometrics as keys to encrypt private data. Biometric encryption has similar advantages and disadvantages as traditional biometric recognition for user authentication and identification: conveniently, a user always carries his biometric with him, hence he cannot forget or lose his encryption keys; however, at the same time the encryption system must cope with changing keys because biometrics are inherently “noisy”. Early work ([1], [2], [3], [4]) has focussed on the problem of hiding data encrypted under biometrics and, more specifically, on the extraction of stable, uniform bitstrings that can be used as encryption keys.

So far, however, too little attention has been paid to biometric privacy. Our work addresses the question whether one can undermine a user’s privacy given access to biometrically encrypted documents. More in particular, we examine if, given two biometrically encrypted files, an attacker can determine whether they were encrypted using the same biometric. This question is interesting in practice because biometrics are considered to be unique and can be used as an identifier to link a user’s data from different applications for profiling or to trace his whereabouts. Moreover, biometric encryption is becoming an important component in biometric authentication systems. Instead of comparing a new measurement of the user’s biometric with a reference measurement, called the template, that was stored during a registration process, the user now authenticates himself by proving knowledge of the biometric key. The system only has to store some biometrically encrypted value, which we call the protected template, as a (public) reference to the biometric key. In this way, biometric encryption is becoming an important means to protect biometric templates and the user’s privacy.

In this paper we present attacks on biometric encryption systems that are used for biometric template protection and we will further refer to these systems as template protection schemes. These schemes can be modeled as fuzzy sketches as defined in the fuzzy extractor framework [4]. The fuzzy sketch model provides a strong security property. A fuzzy sketch allows errors in its input, at the cost of a reduction in entropy, i.e., the sketch leaks information about the biometric. However, it guarantees that this reduction is limited; even if an adversary is able to recover L bits about the original biometric measurement, the biometric is still hard to predict.

We define new and stronger attack models that take into consideration realistic ways in which biometric systems could be deployed. First, it is conceivable that different organizations may decide to use the same template protection scheme. In this case, the user’s biometric is measured and stored several times. Since each measurement is slightly different, and since a fuzzy sketch involves probabilistic choices, a new concern is that the various protected templates, when analyzed together, might leak extra informa-

This work was sponsored in part by the EU project TURBINE, which is funded by the European Community’s Seventh Framework Programme (FP7/2007-2013) under grant agreement nb. ICT-2007-216339.

tion about the user’s biometric. We therefore introduce a model in which an adversary is able to acquire different sketches (computed using the same algorithm) of the same biometric. We demonstrate that protected templates can still be compared to determine whether they come from the same biometric. However, this does not necessarily imply that the biometric (or biometrically encrypted) data is compromised. In a second model, we consider the situation in which the adversary is given fuzzy sketches of the same biometric, but this time, each sketch is computed using a different scheme. We show that in some cases protected templates can be completely reversed.

1.1. Biometrics and Privacy

Privacy risks in biometric systems have been expressed repeatedly in the literature, e.g., by Davida et al. [5] and by Prabhakar et al. [6]. First of all, biometric data are personal and might reveal sensitive information, such as ethnic origin, kinship, gender, or diseases a human being is suffering from. For example, it was suggested that there is a correlation between schizophrenia and specific fingerprint patterns [7]. Also, a large fraction of persons with Down syndrome has a ring of iris speckles, called Brushfield spots [8]. Although often challenged and sometimes very speculative, this kind of results indicates a potential exposure of sensitive information in current biometric systems. Some of this information is already discarded when samples are processed and templates are generated, however, it is often not clear how much information still resides in the templates.

A second privacy issue follows from a property which is desired for verification and identification, namely, uniqueness. A biometric sample, or a template derived from it, uniquely identifies a person within a certain set, with some error margin, and thus allows re-identification (or de-anonymization), i.e., one can determine whether a person is registered in a particular application or not. It also enables profiling by using the biometric data as an index to collect data from different applications or databases.

A third concern, often presented as a security issue instead of a privacy problem, is the risk of impersonation. Although many biometric characteristics are considered public, access to biometric templates should be controlled to prevent that an adversary reconstructs, from a template, a fake sample that would pass a verification test. We partially address this issue and focus mainly on the issue of using biometric data as unique identifier.

1.2. Biometric Template Protection

When a biometric property is measured, e.g., by taking an image of a finger or face, characteristic features are extracted from the captured data and quantized. In each measurement these features are slightly different. Because these features

have a particular distribution, biometrics, i.e., a feature or a combination of features (called the template), are modeled as random variables. If a template protection mechanism works on the features after quantization, biometrics are considered as discrete variables, otherwise as continuous variables.

Because two biometric measurements are never exactly the same, traditional cryptographic techniques that hide private data, e.g., password hashing or encryption, cannot be applied. The difference between two measurements of the same characteristic is considered as noise. Biometric template protection schemes are designed to eliminate this noise, while preserving the privacy of the input. They aim to fulfill two requirements in their attempt to deal with the problems mentioned above. Firstly, they transform the template¹ in a way that is hard to invert, hence an adversary cannot extract sensitive information or construct a fake sample from it. Secondly, they also aim to diversify the transformation to prevent recognition of different protected templates, originating from the same characteristic of the same person. We call these two properties irreversibility and indistinguishability. Other properties are often desired as well, e.g., collision-resistance to prevent impersonation, but we only consider the first two. As we do not know how much sensitive information is propagated in biometric templates we cannot make any claims about how well template protection schemes hide this residual information. Therefore, irreversibility will refer to the difficulty of determining (any information on) the original input.

The protection of biometric or noisy data has been formalized by Linnartz and Tuyls [3] who considered biometrics as continuous variables and by Dodis et al. [4] who treat them as discrete variables in their definitions for fuzzy extractors and fuzzy sketches. Unfortunately, it was shown by Smith [11] that due to the noisy nature of its input, a fuzzy sketch (or extractor) must always leak some information about its input (see also [12]). This was also shown in [3] for the continuous case. It is this information leakage and the privacy risks explained above that motivate us to reconsider biometric sketches that are used multiple times.

1.3. Scope and Attack Model

The security of fuzzy sketches or fuzzy extractors that are applied more than once on the same noisy input has been studied by Boyen in his work on reusable fuzzy extractors [13] where notions of security against outsider and insider chosen perturbation attacks were defined. Our security notions model a much weaker adversary, yet we show that

1. Some schemes can be applied directly to existing templates, e.g., fuzzy commitment on iriscodes [9], whereas others are applied on a sample directly, e.g., cancellable biometrics on fingerprints [10], or somewhere in between, e.g., fuzzy vault on minutiae [2]. We abstract from the input and use the term sample to indicate some biometric input, unless confusion may occur.

some sketches based on linear codes, such as the fuzzy commitment scheme of Juels and Wattenberg [1], cannot be securely reused when considering biometric privacy.

Our attack model assumes an adversary who has obtained a set of sketches, e.g., a set of protected biometric templates from different databases or tokens, that are possibly related. Related sketches are defined as sketches that originate from the same noisy input, e.g., the same characteristic of the same person. Two samples of the same input, e.g., fingerprints of the same finger, may be so different that they appear to be unrelated. Because the quality of the data captured during enrolment is relatively high we limit our definition of related sketches to sketches that were generated from samples that are similar enough to be recognized by the schemes we are analyzing. The objective of the adversary is to identify related sketches and to derive more information from two or more related sketches than a single sketch would theoretically disclose.

The problem of identifying related sketches is an instantiation of the key-privacy problem as presented by Bellare et al. [14]. Loosely put, the attack model in [14] assumes an adversary who wants to know which key from a set of public keys was used to create a given ciphertext. This property provides anonymity to the user for whom the ciphertext is intended. In the context of biometrics, the sketches are the ciphertexts and the biometric data are the underlying (private) keys. Because biometrics are noisy the sketches have to leak information about their input. It is the objective of this paper to formally analyze how the information that is leaked from multiple sketches can be combined and exploited by an attacker.

1.4. Contributions and Organization

In this paper we achieve the following results. We define notions of security against distinguishability and reversibility attacks on biometric sketches. Indistinguishability attacks refer to an adversary who tries to use the (protected) template as a unique identifier to link, potentially sensitive, information from different applications. E.g. an employer who registers its employees' fingerprints can try to use these to retrieve information from an (external) anonymized database. Reversibility attacks refer to an adversary who acquires multiple sketches from the same biometric. For example, if a person's biometric is registered with two companies that are acquired by a third company where the person's biometric is also registered, then the third company suddenly has access to three protected templates of the same biometric. Our notions model a weak adversary, yet they provide the minimal privacy requirements to justify reusing biometric template protection schemes in multiple applications or to justify storing templates in a central database.

We analyze two types of fuzzy sketches that are based on code-offsets (linear shifts) and bit-permutations, respectively. In the first case we demonstrate how an adversary can exploit the linearity of the underlying error-correcting code to compare two sketches. In the second case we exploit the probabilistic nature of the fuzzy sketch to classify related and unrelated sketches. We conclude that the code-offset sketch and the bit-permutation sketch are not secure under our notions of indistinguishability and irreversibility. For example, given a database of about one million templates that are protected with the code-offset schemes proposed in [15] or [16], an adversary can distinguish a related template from the rest with probability very close to 1. A similar result is given for a bit-permutation sketch. We also show that code-offset sketches can easily be reversed to the original sample from which they were derived, if two different codes are used on the same sample. For bit-permutation sketches this even holds for sketches using the same code.

Furthermore, bounds are determined on the leakage of information that can be used to distinguish templates in the code-offset construction and we give a necessary condition for perfect indistinguishability that holds for any fuzzy sketch: any sketch that leaks more information than needed to handle the errors in its input, cannot be perfectly indistinguishable.

Section 2 summarizes some aspects of coding theory and fuzzy sketches. In Section 3 we define our notions of sketch indistinguishability and sketch irreversibility. The notions are then applied on the code-offset construction in Sections 4.1 and 5.1 and on the bit-permutation sketch in Sections 4.2 and 5.2. Bounds on the sketch indistinguishability of the code-offset construction are given in Section 4.1, which, together with the indistinguishability results of the bit-permutation sketch in Section 4.2, lead to a condition for perfect indistinguishability in Section 4.3. An improved code-offset sketch is presented in Appendix A.

2. Preliminaries

We introduce some notation on error-correcting codes and reiterate the definition of a fuzzy sketch, along with two constructions that will be analyzed in Sections 4 and 5.

2.1. Error-Correcting Codes

A linear error-correcting code C over \mathbb{F}_q is denoted as an $[n, k, d]_{\mathbb{F}_q}$ -code (or $[n, k, d]$ -code if $q = 2$), which is a k -dimensional linear subspace of the vector space \mathbb{F}_q^n . It has minimum distance $d \geq 2t + 1$, and can correct up to t errors. The distance function for linear codes is the Hamming distance, denoted as $d(\cdot, \cdot)$, and we use $\|\cdot\|$ as notation for the Hamming weight. The distance to a code C

is defined as $\mathbf{d}(w, C) = \min_{c \in C} \|w - c\|$. If C is non-linear, C is an $(n, K, d)_{\mathbb{F}_q}$ -code, with K the number of codewords.

Let G be the generator matrix of a linear code C . For any linear code C an $(n-k) \times n$ parity check matrix H is defined that projects any vector $v \in \mathbb{F}_q^n$ on the space orthogonal to the code, i.e., the null space of G . This projection is called the syndrome and is denoted by $\text{syn}(v)$. A word $w \in \mathbb{F}_q^n$ is an element of C iff $\text{syn}(w) = 0$, i.e., $Hw = 0$. When a codeword c is transmitted over a noisy channel, the received word w contains errors, i.e., $w = c + e$. Because of the linearity of C the syndrome of the received word equals the syndrome of the error, $\text{syn}(w) = \text{syn}(e)$, which is used to determine the error vector e and perform decoding.

Let $A_q(n, d)$ be the maximum number of codewords in an arbitrary $(n, K, d)_{\mathbb{F}_q}$ -code. An important bound² on $A_q(n, d)$ is the Singleton bound, which indicates a trade-off between the size of the code and its error-correcting capacity: $A_q(n, d) \leq q^{n-d+1}$. The notation $B_q(n, d)$ is used for linear codes and $B_q(n, d) \leq A_q(n, d)$. Let $R = n^{-1} \log_q K$ be the rate of a code and $\delta = dn^{-1}$ the relative minimum distance. A function for the largest possible rate of infinitely long codes over \mathbb{F}_q is $\alpha_q(\delta) = \limsup_{n \rightarrow \infty} n^{-1} \log_q A_q(n, \delta n)$. The asymptotic Singleton bound gives us $\alpha_q(\delta) \leq 1 - \delta$ if $0 \leq \delta \leq 1$. It further holds that $\alpha_q(\delta) = 0$ for $1 - q^{-1} \leq \delta \leq 1$.

2.2. Fuzzy Sketches

Dodis et al. [4] defined the concept of a secure sketch, which is a formalization of schemes that allow reconstruction of discrete noisy inputs with the help of public helper data, called the sketch, but remain minimally privacy-invasive. We briefly recall the definition of a sketch, closely following Boyen's notation [13].

All logarithms in this definition and the remainder of the text are base 2, unless explicitly indicated otherwise. The min-entropy of a variable W is defined as $H_\infty(W) = -\log \max_w \Pr[W = w]$ and the average min-entropy of W given P is $\bar{H}_\infty(W|P) = -\log \mathbb{E}_{p \leftarrow P} [\max_w \Pr[W = w | P = p]]$.

Definition 1. An (\mathcal{M}, m, m', t) -secure fuzzy sketch is a pair of randomized procedures $\langle \text{Fsk}, \text{Rec} \rangle$ where

- **Fsk** is a sketching function that outputs a sketch $P \in \{0, 1\}^*$ on input $w \in \mathcal{M}$, where \mathcal{M} is a metric space with distance function \mathbf{d} , and
- **Rec** is a recovery function that, given a word $w' \in \mathcal{M}$ and any sketch $P = \text{Fsk}(w)$, outputs the original input w if $\mathbf{d}(w, w') \leq t$.

For any random variable W over \mathcal{M} with $H_\infty(W) \geq m$, the probability that an adversary who observes P guesses W is at most $2^{-m'}$, with $m' \leq \bar{H}_\infty(W|P)$.

2. See [17, Ch. 2] for an in-depth discussion on coding bounds.

The quantity $L = m - m'$ is called the entropy loss and indicates the amount of information that a sketch leaks about the input. It was shown in [11] and [12] that this entropy loss is unavoidable.

2.3. Permutation-Based Sketches.

A general technique was given in [4] to build sketches from transitive isometric permutations and error-correcting codes. The idea is the following; a randomly chosen permutation maps an input w onto a codeword c and other inputs w' that are close to w in the vicinity of c . Let $c \in_R C$ denote "a uniformly random element of".

Definition 2. A permutation-based sketch is a fuzzy sketch $\langle \text{Fsk}, \text{Rec} \rangle$ where

- **Fsk** outputs the specification of a transitive isometric permutation π_P in \mathcal{M} such that $\pi_P[w] = c \in_R C$, with C an (\mathcal{M}, K, t) -code, and
- **Rec** outputs $(\pi_P^{-1} \circ \text{Dec} \circ \pi_P)[w']$ on input w' and sketch P , with **Dec** the decoding procedure of C that maps $\pi_P^{-1}[w']$ to c if $\mathbf{d}(w, w') \leq t$.

A family of permutations $\mathcal{P} = \{\pi_p : \mathcal{M} \rightarrow \mathcal{M}\}$ is a transitive group if for any two elements $a, b \in \mathcal{M}$ there exists a permutation $\pi \in \mathcal{P}$ such that $\pi[a] = b$. A permutation is isometric if for any two elements $a, b \in \mathcal{M}$ it holds that $\mathbf{d}(a, b) = \mathbf{d}(\pi[a], \pi[b])$. The entropy-loss of a permutation-based sketch is $L = \log |\Pi| - \log \Gamma - \log K$ where Γ is defined as the minimum number of possible permutations that map w onto c , i.e., $\min_{w, c} |\{\pi \mid \pi[w] = c\}| \geq \Gamma$.

2.4. Code-Offset Construction

An example of a family of transitive, isometric permutations in Hamming spaces is the set of all shifts $\pi_x(y) = y - x$. A construction based on this permutation was presented by Juels and Wattenberg as the fuzzy commitment scheme [1]. We present it here as a fuzzy sketch. Let $c \in_R C$. The code-offset sketch is defined as:

- **Fsk** : $w \mapsto v = w - c$
- **Rec** : $w', v \mapsto \text{Dec}(w' - v) + v$

In the fuzzy commitment scheme **Fsk** outputs $\langle v : w - c, h(c) \rangle$, with h a one-way function, and **Rec** outputs $c' = \text{Dec}(w' - v)$ and verifies that $h(c') = h(c)$. The entropy loss of an $[n, k, d]_{\mathbb{F}_q}$ -code is $L = (n - k) \log q$.

2.5. Bit-Permutations

A bit-permutation is represented by a permutation matrix, which is obtained by permuting the rows of the $n \times n$ identity matrix I . A permutation matrix A_P has full rank and it holds that $A_P^{-1} = A_P^T$. Unfortunately, bit-permutations are not transitive and at first sight not suitable to construct

a permutation-based sketch. However, we can make them transitive in spaces over \mathbb{F}_2 by assuming that all inputs are balanced words, i.e., words that have an equal number of zeros and ones. This assumption introduces a (reasonable) constraint on the biometric model.

Let $\mathcal{M} = \{w \mid w \in \{0, 1\}^n, \|w\| = \frac{n}{2}\}$. Let $C \subset \mathcal{M}$ denote a balanced code, i.e., an $(n, K, \frac{n}{2})$ -code, and A_P a permutation matrix. The bit-permutation sketch is defined as:

- **Fsk** : $w \mapsto A_P \in_R \{A_P \mid wA_P \in C\}$
- **Rec** : $w', A_P \mapsto \text{Dec}(w'A_P)A_P^{-1}$

Similarly, the use of constant-weight codes, i.e., codes where all codewords have constant weight s , was suggested in [4] to construct a sketch for the set difference metric in small universes. The entropy loss of this sketch is $\log n! - \log s!(n-s)! - \log K$ or $\log \binom{n}{s} - \log K$, with $\binom{n}{s}$ the number of words of length n and weight s .

A first order Reed-Muller code $RM(1, m)$ is a $[2^m, m + 1, 2^{m-1}]$ -code with codewords that have constant weight 2^{m-1} , except for the words 0 and 1, which have weight 0 and 2^m respectively.

3. Security Notions

Before we analyze fuzzy sketches we need to formalize the properties that are required from a biometric template protection scheme and the scenarios in which they are used. Therefore, we define the minimal notions under which such a scheme must be secure.

3.1. Sketch Indistinguishability

The problem of using biometric data as identifier to link information from different applications suggests a notion of sketch indistinguishability. In cryptosystems, the notion of ciphertext indistinguishability means, informally, that no adversary has a significant advantage over random guessing to determine from a given ciphertext which element of a two-element message space was encrypted. This is the property that is traditionally required from cryptosystems.

Bellare et al. [14] considered a new problem that relates to the privacy of the keys (or key owners) and introduced a new notion called indistinguishability of keys. The notion is modeled as a game in which an adversary chooses a message and two public keys. He then receives the encryption of that message under one of the two keys and he has to guess which key was used. Additionally, the adversary can have access to decryption oracles for the two keys. In the context of biometrics the sketching function is a randomized procedure, like a probabilistic encryption function, that outputs sketches corresponding to specific biometric data, which can be considered as keys. However, the biometric data are considered entirely private. Therefore, the adversary does not have to

indicate from which biometric a sketch originates, but he has to determine whether the sketches originate from the same biometric or not.

We define security notions for sketch indistinguishability through two games in which the adversary is modeled as a very weak adversary. He does not get to choose the biometric sources, nor does he get to perform additional queries on the sketching function or the recovery function. Yet, we will demonstrate that some constructions are insecure, even for this weak adversary.

3.1.1. Indistinguishability Game. In a first scenario we assume that an adversary holds a protected template, a sketch, for which he knows the person who corresponds to it. The adversary holds a second template, e.g., retrieved from a token, and wants to know if it corresponds to the same person.

Formally, let $t \geq 0$ be the error-tolerance of a biometric system and let $\Delta|_t = \{\delta : \mathcal{M} \rightarrow \mathcal{M} \mid \mathbf{d}(m, \delta(m)) \leq t\}$ be the set of perturbation functions that represents the possible differences between two related samples. Consider the following game between a challenger and the adversary.

- 1) The challenger selects a random variable $W \in \mathcal{M}$ and samples W to obtain $w \in \mathcal{M}$, e.g., a fingerprint. The challenger produces a sketch $P = \text{Fsk}(w)$ and gives P to the adversary.
- 2) The challenger flips a fair coin $b \in \{0, 1\}$. If $b = 1$, the challenger selects $\delta \in_R \Delta|_t$ and computes $w' = \delta(w)$, e.g., a similar fingerprint. If $b = 0$, the challenger samples W to obtain w' , e.g., a random fingerprint. A sketch $P' = \text{Fsk}(w')$ is generated from w' and given to the adversary.
- 3) The adversary outputs a single bit $\hat{b} \in \{0, 1\}$ and wins if $\hat{b} = b$.

We call the adversary in the above game an **Fsk-IND** adversary and we define his advantage in the game as

$$\text{Adv}_{\text{ind}} = 2 \left| \Pr[\hat{b} = b] - \frac{1}{2} \right| = 2 \left| \Pr[\hat{b} \neq b] - \frac{1}{2} \right|.$$

The advantage and all other advantages in this section are scaled to lie between 0 and 1.

Definition 3. An (\mathcal{M}, m, m', t) -secure fuzzy sketch $\langle \text{Fsk}, \text{Rec} \rangle$ is ϵ -indistinguishable in $\Delta|_t$ if for any Fsk-IND adversary it holds that $\text{Adv}_{\text{ind}} \leq \epsilon$ and perfectly indistinguishable if $\text{Adv}_{\text{ind}} = 0$.

For a biometric sketch to be reusable it should be ϵ -indistinguishable with ϵ negligibly small. The game easily extends to a model where the adversary receives two or more related sketches in the first step.

3.1.2. N-Indistinguishability Game. We now model the situation where biometric data are stored in a central database. An adversary has obtained a database of protected templates

and wants to find the template, in the database, that is related to the one that he is holding. This specific situation models a profiling attack where the adversary tries to lookup records in a database by using a biometric template from another application as a key. The new game is based on the indistinguishability game and consists of the following steps.

- 1) The challenger performs step 1 of the indistinguishability game and gives the produced sketch $P = \text{Fsk}(w)$ to the adversary.
- 2) The challenger chooses an integer $k \in_R \{1, \dots, N\}$ and produces a sequence of N sketches $[P_1, \dots, P_N]$. The k -th sketch P_k is generated from $w_k = \delta(w)$, $\delta \in_R \Delta|_t$. The other sketches are generated from random samples of W . The challenger gives the sketches $[P_1, \dots, P_N]$ to the adversary.
- 3) The adversary outputs an integer $\hat{k} \in \{1, \dots, N\}$ and wins if $\hat{k} = k$.

We call the adversary in the modified indistinguishability game an **Fsk-IND-N** adversary and we define his advantage in the game as

$$\begin{aligned} \text{Adv}_{\text{ind-N}} &= \frac{N}{N-1} \left| \Pr[\hat{k} = k] - \frac{1}{N} \right| \\ &= \frac{N}{N-1} \left| \Pr[\hat{k} \neq k] - \frac{N-1}{N} \right|. \end{aligned}$$

This advantage cannot be derived directly from the advantage of an **Fsk-IND** adversary because it depends on the attack strategy and on the size of the database N , e.g., see Section 4.2.2.

Definition 4. An (\mathcal{M}, m, m', t) -secure fuzzy sketch (Fsk, Rec) is (N, ϵ) -indistinguishable in $\Delta|_t$ if for any **Fsk-IND-N** adversary it holds that $\text{Adv}_{\text{ind-N}} \leq \epsilon$.

To justify the storage of biometric data in a central database the templates should be protected with an (N, ϵ) -indistinguishable sketch, where N is the number of stored templates and ϵ is negligibly small. This implies that it is practically impossible to find a person's records in a database by using a biometric template as a key.

3.2. Sketch Irreversibility

Next to indistinguishability, the second and most important property of a biometric template protection scheme is that it irreversibly transforms biometric data, i.e., into a protected template from which the original data cannot be recovered but that still can be used for verification or identification. The irreversibility of fuzzy sketches has been studied by Boyen [13] in the setting where the same fuzzy sketch is applied multiple times on the same noisy input. To prevent distinguishability of the biometric input, which is not taken into account in [13], one could argue

to use different sketches for different applications. E.g., different error-correcting codes could be used in different applications in the hope that information that is leaked from the applications cannot be compared. We now consider irreversibility in this situation.

3.2.1. Irreversibility Game. An adversary has multiple sketches that were generated from the same noisy input, but with different sketching functions and his goal is to recover the original input.

Formally, let $\Delta|_t$ be the set of perturbation functions as defined in the indistinguishability game and let $\Phi = \{\langle \text{Fsk}_i, \text{Rec}_i \rangle\}$ be a family of $(\mathcal{M}, m, m'_i, t_i)$ -secure fuzzy sketches. Consider the following game between a challenger and the adversary.

- 1) The challenger selects a random variable $W \in \mathcal{M}$ and samples W to obtain $w \in \mathcal{M}$. The challenger then selects a sketch $(\text{Fsk}_1, \text{Rec}_1) \in_R \Phi$, produces a sketch $P = \text{Fsk}_1(w)$ and gives P to the adversary.
- 2) The challenger selects $\delta \in_R \Delta|_t$, for $t = \min\{t_i\}$, and a sketch $(\text{Fsk}_2, \text{Rec}_2) \in_R \Phi \setminus \{\langle \text{Fsk}_1, \text{Rec}_1 \rangle\}$. The challenger generates a sketch $P' = \text{Fsk}_2(w')$ from $w' = \delta(w)$ and gives P' to the adversary.
- 3) The adversary outputs a word $\hat{w} \in \mathcal{M}$ and wins if $\hat{w} = w$.

Guessing w' is equivalent to guessing w since w can always be recovered from w' and P .

We call the adversary in the above game an **Fsk-FOW** (fuzzy sketch family one-wayness) adversary and we define his advantage in the game as

$$\text{Adv}_{\text{fow}} = \frac{2^{\min(m'_1, m'_2)}}{2^{\min(m'_1, m'_2)} - 1} \left| \Pr[\hat{w} = w] - \frac{1}{2^{\min(m'_1, m'_2)}} \right|.$$

Because the sketches can only be reversed completely if they leak enough information, the adversary's advantage is bound by

$$\text{Adv}_{\text{fow}} \leq \frac{2^{\min(m'_1, m'_2) - \max(m'_1 + m'_2 - m, 0)} - 1}{2^{\min(m'_1, m'_2)} - 1}.$$

Definition 5. A family Φ of $(\mathcal{M}, m, m'_i, t_i)$ -secure fuzzy sketches $\{\langle \text{Fsk}_i, \text{Rec}_i \rangle\}$ is ϵ -irreversible in $\Delta|_t$, $t = \min\{t_i\}$, if for any **Fsk-FOW** adversary it holds that $\text{Adv}_{\text{fow}} \leq \epsilon$ and perfectly irreversible if $\text{Adv}_{\text{fow}} = 0$.

From this notion we can define a notion of irreversibility for a single sketch, which is similar to, but much weaker than Boyen's outsider security notion [13]. The adversary plays the irreversibility game with the difference that $\text{Fsk}_2 = \text{Fsk}_1$. The adversary is called an **Fsk-OW** adversary and his advantage in the single-sketch irreversibility game is

$$\text{Adv}_{\text{ow}} = \frac{2^{m'}}{2^{m'} - 1} \left| \Pr[\hat{w} = w] - \frac{1}{2^{m'}} \right|.$$

Definition 6. An (\mathcal{M}, m, m', t) -secure fuzzy sketch (Fsk, Rec) is ϵ -irreversible in $\Delta|_t$ if for any Fsk-OW adversary it holds that $\text{Adv}_{\text{ow}} \leq \epsilon$ and perfectly irreversible if $\text{Adv}_{\text{ow}} = 0$.

4. Distinguishability

In this section we apply the notions of sketch indistinguishability on the code-offset sketch and the bit-permutation sketch. These sketches permute or translate the underlying code to be able to perform error-correction around the original input. The permutation is specific to the input and is partially or indirectly leaked through the sketch. If enough information is leaked we expect to be able to compare the “permutations” of two sketches and to determine if they are related or not.

We demonstrate for both constructions that the adversary has a non-negligible advantage in the indistinguishability game and the N-indistinguishability game. These advantages are then expressed in terms of a generalized heuristic and a necessary condition for perfect indistinguishability is derived from a lower bound on Adv_{ind} that holds for any sketch that has uniform input.

4.1. Code-Offset Sketches

We present an attack strategy for the indistinguishability and the N-indistinguishability game where the sketches are produced by a (linear) code-offset sketch. Bounds on the adversary’s advantage are derived from bounds in coding theory and it is shown that this advantage is non-negligible.

4.1.1. Indistinguishability Game. The adversary plays the indistinguishability game and receives two sketches $P_1 = \langle v_1 : w_1 - c_1, h(c_1) \rangle$ and $P_2 = \langle v_2 : w_2 - c_2, h(c_2) \rangle$ generated by the code-offset construction with the same $[n, k, d]_{\mathbb{F}_q}$ -code C . The adversary’s goal is to guess the coin flip b that determined whether w_1 and w_2 are related or not.

The adversary will try to compare the two samples w_1 and w_2 implicitly, by subtracting the offsets v_1 and v_2 and decoding the difference $v = v_1 - v_2$. Because of the linearity of the code $\text{syn}(v) = \text{syn}(w_1 - w_2)$ and the decodability of v depends on the decodability of $w_1 - w_2$. If the sketches are related, i.e., if $d(w_1, w_2) \leq t$, then v is decodable. If they are not related then v can be either decodable or not decodable. If v is not decodable then $d(w_1, w_2) > t$ and the two sketches are not related. However, if $|d(w_1, C) - d(w_2, C)| \leq t$ then the two samples w_1 and w_2 produce a decodable difference, i.e., $d(v, C) \leq t$.

If an Fsk-IND adversary takes the decodability of v as a heuristic for guessing the coin flip b in the indistinguishability game then the adversary will always guess correctly if $b = 1$ or if $b = 0$ and v is not decodable. The probability

of making an incorrect guess is

$$\Pr[\hat{b} \neq b] = \Pr[d(v, C) \leq t | b = 0] \frac{1}{2}$$

and the adversary’s advantage is

$$\text{Adv}_{\text{ind}} = 1 - \Pr[d(v, C) \leq t | b = 0].$$

For a uniform W , the probability that v is decodable, given that w_1 and w_2 are not related, equals the probability that a random word $w \in_R \mathbb{F}_q^n$ is decodable. Let $V_q(n, r) = \sum_{i=0}^r \binom{n}{i} (q-1)^i$ be the number of vectors in a sphere with radius r in \mathbb{F}_q^n . The decodability probability of w is

$$\Pr[d(w, C) \leq t] = \frac{q^k V_q(n, t)}{q^n} \leq 1$$

and the adversary’s advantage is

$$\text{Adv}_{\text{ind}} = 1 - q^{-(n-k-\log_q V_q(n, t))}.$$

In practice, the advantage will be slightly worse because biometrics have a false acceptance rate and thus they are not truly uniform. However, if the false acceptance rate is too high, the biometric modality is not usable.

We define the following quantity as a quality measure for the indistinguishability of a code-offset sketch based on a particular code.

Definition 7. The distinguishing information leakage Λ of an $[n, k, d]_{\mathbb{F}_q}$ -code in the code-offset construction is given by

$$\Lambda = n - k - \log_q V_q(n, t)$$

hence,

$$\text{Adv}_{\text{ind}} = 1 - q^{-\Lambda}.$$

We conclude that the adversary’s advantage grows rapidly with the increasing distinguishing information leakage of the code that was used to generate the code-offset sketches in the indistinguishability game. The distinguishing information leakage, and thus also the advantage, is 0 for perfect codes, since $q^k V_q(n, t) = q^n$.

For $q = 2$ we have

$$\text{Adv}_{\text{ind}} \approx 1 - 2^{-(L - nh_2(\frac{t}{n}))}$$

with L the entropy loss of the sketch and h_2 the binary entropy function (see Equation (2) below).

The term $n - k$ in the distinguishing information leakage, i.e., the entropy loss of the sketch, indicates the number of bits that is leaked about the input. These bits are available to the adversary in the form of parity checks in the syndrome of the offset. Because of the linearity of the code it is easy to compare the syndromes of different offsets and thus the original inputs.

4.1.2. Adversary Advantage Bounds. A good code-offset sketch uses a code that has a small distinguishing information leakage such that the advantage of an Fsk-IND adversary is negligible. We are interested in the smallest distinguishing information leakage for which there exists an $[n, k, d]_{\mathbb{F}_q}$ -code and we denote this quantity with $\Lambda_q(n, d)$. This problem relates directly to the main problem in coding theory, i.e., given the length of the code and the desired minimum distance, what is the best dimension (or rate) that can be achieved. By definition

$$\begin{aligned}\Lambda_q(n, d) &= n - \log_q B_q(n, d) - \log_q V_q\left(n, \left\lfloor \frac{d-1}{2} \right\rfloor\right) \\ &\geq n - \log_q A_q(n, d) - \log_q V_q\left(n, \left\lfloor \frac{d-1}{2} \right\rfloor\right).\end{aligned}$$

To be able to deal with the quantity $\log_q V_q(n, \lfloor \frac{d-1}{2} \rfloor)$ we introduce the following asymptotic definition, which will allow us to approximate the advantage of an Fsk-IND adversary and to determine bounds on this advantage by using asymptotic bounds on $\alpha_q(\delta)$.

Definition 8. *The smallest relative distinguishing information leakage of infinitely long (linear) codes with relative minimum distance δ in the code-offset construction is defined as*

$$\lambda_q(\delta) = \liminf_{n \rightarrow \infty} n^{-1} \Lambda_q(n, \delta n)$$

and

$$\text{Adv}_{\text{ind}} \approx 1 - q^{-n \lambda_q(\delta)}. \quad (1)$$

Let H_q denote the q -ary entropy function such that for $0 < x \leq 1 - q^{-1}$ it holds that

$$H_q(x) = x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x) \quad (2)$$

and $H_q(0) = 0$. This function allows us to express $\lambda_q(\delta)$ in a form that is easier to work with.

Lemma 1. *For $0 \leq \delta \leq 1 - q^{-1}$*

$$\lambda_q(\delta) \geq 1 - \alpha_q(\delta) - H_q\left(\frac{\delta}{2}\right).$$

Proof: Let $\tau = tn^{-1}$ be the relative error-correcting capacity. It holds that $\lim_{n \rightarrow \infty} n^{-1} \log_q V_q(n, \lfloor \tau n \rfloor) = H_q(\tau) = H_q(\frac{\delta}{2})$ and by definition $\lambda_q(\delta) \geq 1 - \alpha_q(\delta) - H_q(\frac{\delta}{2})$. \square

We now apply bounds from coding theory to define upper and lower bounds on $\lambda_q(\delta)$, which will reveal what the best is we can hope for regarding the indistinguishability of linear code-offset sketches.

Two upper bounds on $\alpha_q(\delta)$ were defined by McEliece et al. [18], which we will refer to as the MMRW bounds,

following the notation in [17]. Let $0 \leq \delta \leq 1 - q^{-1}$. The first MRRW bound gives us

$$\alpha_q(\delta) \leq H_q\left(\frac{q-1-(q-2)\delta-2\sqrt{(q-1)\delta(1-\delta)}}{q}\right).$$

The second MMRW bound is better than the first but only valid for $q = 2$. Let $g(x) = H_2\left(\frac{1-\sqrt{1-x}}{2}\right)$ then

$$\alpha_2(\delta) \leq \min_{0 \leq u \leq 1-2\delta} 1 + g(u^2) - g(u^2 + 2\delta u + 2\delta).$$

Lemma 2. *Let $0 \leq \delta \leq 1 - q^{-1}$ then*

$$\lambda_q(\delta) \geq 1 - \text{MMRW} - H_q\left(\frac{\delta}{2}\right).$$

Proof: The result follows from Lemma 1 and the MMRW bounds. \square

A lower bound on $B_q(n, d)$ was given by Gilbert [19], [17] and yields an upper bound on $\lambda_q(\delta)$.

Lemma 3. *Let $0 \leq \delta \leq 1 - q^{-1}$ then*

$$\lambda_q(\delta) \leq H_q(\delta) - H_q\left(\frac{\delta}{2}\right)$$

Proof: The Gilbert bound states that an $[n, k, d]_{\mathbb{F}_q}$ -code exists if $V_q(n, d-1) \leq q^{n-k}$. In other words, $B_q(n, d) \leq \frac{q^n}{V_q(n, d-1)}$ or

$$\Lambda_q(n, d) \leq \log_q V_q(n, d-1) - \log_q V_q\left(n, \left\lfloor \frac{d-1}{2} \right\rfloor\right).$$

The result follows from Definition 8. \square

Given the bounds on $\lambda_q(\delta)$ we bind the adversary's advantage.

Proposition 4. *For $0 \leq \delta \leq 1 - q^{-1}$*

$$\begin{aligned}\text{Adv}_{\text{ind}} &\geq 1 - q^{-n[1 - \text{MMRW} - H_q(\frac{\delta}{2})]} \\ \text{Adv}_{\text{ind}} &\leq 1 - q^{-n[H_q(\delta) - H_q(\frac{\delta}{2})]}.\end{aligned}$$

Proof: The proof follows from Definition 8 and Lemmas 2 and 3. \square

Figure 1 shows the bounds on $\lambda_2(\delta)$. Figure 2 shows the bounds on the advantage of an Fsk-IND adversary observing sketches produced by a binary linear code of length $n = 100$. The bounds are computed from Proposition 4. For $d = 7$ the advantage is 0.54. This means that if the maximum allowed distance between two related samples is 3 bits, which is very small (see examples in Section 4.1.4), then the adversary will, on average, win the indistinguishability game 3 out of 4 times. We conclude that an Fsk-IND adversary has a non-negligible advantage when observing code-offset sketches produced with linear codes. This means that an adversary can easily identify protected templates originating from the

same person. The bounds can be improved by applying list decoding (see Appendix A), but the advantage remains substantial (see Figure 2).

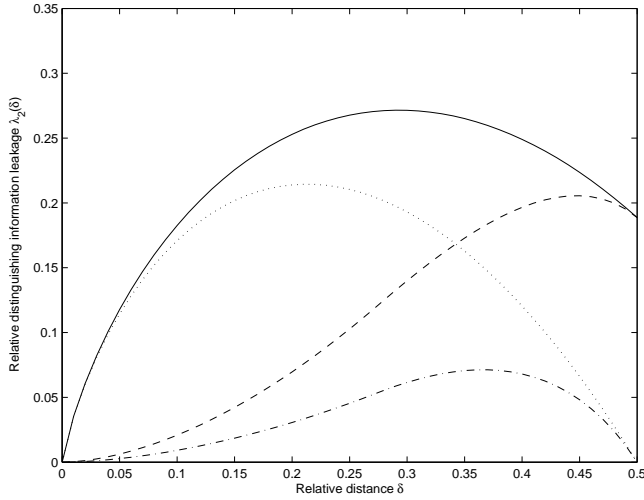


Figure 1. Upper (—) and lower bound (---) on the relative distinguishing information leakage $\lambda_q(\delta)$ of a binary linear code in the code-offset construction in terms of the relative distance δ and upper (···) and lower (- · - ·) bound for the construction based on list decoding (see Appendix A).

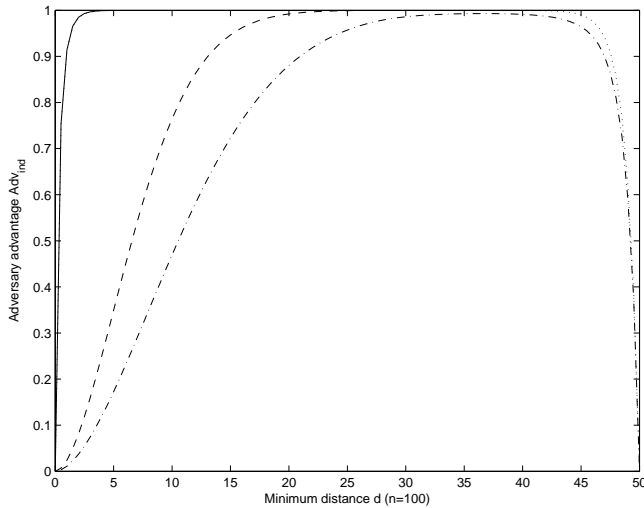


Figure 2. Upper (—) and lower bound (---) on the advantage of an Fsk-IND adversary for a binary linear code of length $n = 100$ derived from the bounds on $\lambda_q(\delta)$ (see Figure 1) and upper (···) and lower (- · - ·) bounds for the improved bounds on $\lambda_q(\delta)$ based on list decoding (Appendix A).

4.1.3. N-Indistinguishability Game. In the N-indistinguishability game the adversary obtains N sketches, $[P_1, \dots, P_N]$, of which the k -th sketch (P_k) is related to the sketch he is already holding. The adversary's goal is to guess the value k .

A simple strategy is to play the indistinguishability game on each sketch P_j , $j = \{1, \dots, N\}$, and to select all the sketches that appear to be related based on the decodability of the code-offset difference. The k -th sketch is related and will always be selected. Of the $N - 1$ remaining sketches, $q^{-\Lambda}(N - 1)$ sketches produce a decodable offset difference and will also be selected. From this selection the adversary chooses one sketch and outputs its index j as his guess in the N-indistinguishability game. The probability of making a correct guess is

$$\Pr[\hat{k} = k] = \frac{1}{q^{-\Lambda}(N - 1) + 1}$$

and the advantage of an Fsk-IND-N adversary using this strategy is

$$\text{Adv}_{\text{ind-N}} = \frac{1 - q^{-\Lambda}}{1 - q^{-\Lambda} + q^{-\Lambda}N}.$$

From the term $q^{-\Lambda}N$ it can be seen that increasing the size of the database hardly reduces the adversary's advantage, unless the order of magnitude of the size is q^Λ . Again, the adversary advantage increases rapidly with an increasing Λ . For $\Lambda = 0$ all sketches in the database will be selected and the advantage is 0, when using this strategy.

4.1.4. Examples. Tuyls et al. [15] applied the fuzzy commitment scheme on a uniform bit-string extracted from fingerprints. The suggested codes were two binary BCH codes with parameters $[511, 76, 171]$ and $[511, 40, 191]$. The first code produces offsets that leak $\Lambda = 511 - 76 - \log_2 V_2(511, 85) \approx 107$ distinguishing bits. For the second code $\Lambda \approx 121$ bits. The advantage of an Fsk-IND adversary for the two codes respectively is

$$\text{Adv}_{\text{ind}} \approx 1 - 2^{-107} \quad \text{and} \quad \text{Adv}_{\text{ind}} \approx 1 - 2^{-121}.$$

Let $N = 2^{20} \approx 10^6$ be the number of templates in the database, then the advantage of an Fsk-IND-N adversary for the code with the smallest Λ is

$$\text{Adv}_{\text{ind-N}} \approx \frac{1 - 2^{-107}}{1 - 2^{-107} + 2^{-87}} \approx 1 - 2^{-87}.$$

An advantage close to 1 is very good for the adversary and allows him to easily find related templates in large databases.

Bringer et al. [16] applied a product code of first order Reed-Muller codes, $\mathcal{RM}(1, 6) \times \mathcal{RM}(1, 5)$, to construct code offsets for 2048-bit iriscodes. The resulting code is a $[2048, 42, 512]$ -code and $\Lambda \approx 900$ distinguishing bits. The advantages are

$$\text{Adv}_{\text{ind}} \approx 1 - 2^{-900} \quad \text{and} \quad \text{Adv}_{\text{ind-N}} \approx 1 - 2^{-880}.$$

4.2. Bit-Permutations Sketches

We present an attack strategy to distinguish sketches that are produced by a bit-permutation sketch in the model where related sketches are generated from the same sample. The strategy can be extended to deal with sketches generated from similar, but non-equal samples, however, the complexity increases exponentially with the dimension of the underlying code.

4.2.1. Indistinguishability Game. The adversary plays the indistinguishability game and receives two sketches $P_1 = \langle A_1, h(c_1) \rangle$ and $P_2 = \langle A_2, h(c_2) \rangle$, where A_1 and A_2 are permutation matrices such that $w_1 A_1 = c_1$ and $w_2 A_2 = c_2$. Both c_1 and c_2 are codewords of the same $[n, k, d]$ -code C with generator matrix G . Again, the adversary's goal is to guess the coin flip b in the indistinguishability game.

Let $V_1 = \{v = xGA_1^T \mid x \in \mathbb{F}_2^k\}$ and $V_2 = \{v = xGA_2^T \mid x \in \mathbb{F}_2^k\}$ be subspaces of \mathbb{F}_2^n . It follows that $w_1 \in V_1$ and $w_2 \in V_2$. The adversary will try to determine if the two sketches are related by looking at the intersection of V_1 and V_2 . If the two sketches are related, in this model $w_1 = w_2 = w$, then V_1 and V_2 must have at least w in their intersection. The dimension of V_1 and V_2 is k and the dimension of their union can be found by comparing their bases GA_1^T and GA_2^T , hence the dimension of the intersection is

$$\begin{aligned} \dim(V_1 \cap V_2) &= \dim V_1 + \dim V_2 - \dim(V_1 \cup V_2) \\ &= 2k - \text{Rank} \begin{bmatrix} GA_1^T \\ GA_2^T \end{bmatrix}. \end{aligned} \quad (3)$$

Let D denote the dimension of the intersection of V_1 and V_2 . An Fsk-IND adversary will take the value of D as a heuristic for guessing the coin flip b in the indistinguishability game. He computes the conditional distribution on b given D as

$$\Pr[b \mid D] = \frac{\Pr[D \mid b] \frac{1}{2}}{\Pr[D \mid b=1] \frac{1}{2} + \Pr[D \mid b=0] \frac{1}{2}} \quad (4)$$

and outputs the value of b (1 or 0) with highest conditional probability as his guess.

The conditional distribution on D given b depends on the structure of the code. If this distribution cannot be derived analytically, it can be estimated from simulations, e.g., using Monte Carlo methods. The probability of making a correct guess is

$$\Pr[\hat{b} = b] = \sum_{i=0}^k \Pr[D = i] \max_b \Pr[b \mid D = i]$$

and the adversary's advantage is

$$\begin{aligned} \text{Adv}_{\text{ind}} &= 2 \left(\sum_i \Pr[D = i] \max_b \Pr[b \mid D = i] - \frac{1}{2} \right) \\ &= 2 \sum_i \Pr[D = i] \left(\max_b \Pr[b \mid D = i] - \frac{1}{2} \right) \\ &\stackrel{\text{(Equation 4)}}{=} 2 \sum_i \left(\frac{\max_b \Pr[D = i \mid b]}{2} - \frac{\Pr[D = i]}{2} \right) \\ &= \sum_i \left| \frac{\Pr[D = i \mid b=1] - \Pr[D = i \mid b=0]}{2} \right|. \end{aligned}$$

In the model where $w_1 \neq w_2$ but $d(w_1, w_2) \leq t$ the adversary will count the number of points in V_2 that are at most distance t from a point in V_1 and use this a heuristic instead of D . This is equivalent to verifying 2^k times that a point is decodable in V_1 .

4.2.2. N-Indistinguishability Game. Analogously to the N-indistinguishability game for code-offset sketches, the adversary will apply the attack strategy of the indistinguishability game for bit-permutations sketches on each of the N sketches $[P_1, \dots, P_N]$ to make a selection of potentially related sketches. From this selection the adversary will choose one and output its index as a guess for k .

The adversary uses again D as a heuristic and selects the sketch P_j if $\Pr[j = k \mid D] > \frac{1}{2}$. In the attack strategy for the code-offset construction the adversary always selects P_k . However, the strategy for the bit-permutation sketch allows only a probabilistic guess and there is no guarantee that P_k will be selected. Furthermore, to have an advantage over random guessing in this game, the adversary needs probabilities $\Pr[j = k \mid D] > \frac{1}{2}$. Otherwise, the adversary will not select any sketch as being potentially related. This allows us to determine bounds on N for which an Fsk-IND-N adversary still selects sketches.

The distribution

$$\Pr[j = k \mid D] = \frac{\Pr[D \mid j = k] \Pr[j = k]}{\Pr[D]}$$

is computed from the conditional distributions $\Pr[D \mid j = k]$ and $\Pr[D \mid j \neq k]$, which are the same as the conditional distributions $\Pr[D \mid b = 1]$ and $\Pr[D \mid b = 0]$, respectively, from the indistinguishability game. In this game $\Pr[j = k] = \frac{1}{N}$ and $\Pr[j \neq k] = \frac{N-1}{N}$. It follows that

$$\Pr[j = k \mid D] = \frac{\Pr[D \mid j = k]}{\Pr[D \mid j = k] + \Pr[D \mid j \neq k](N-1)}$$

and $\Pr[j = k \mid D] > \frac{1}{2}$ if

$$N < \frac{\Pr[D \mid j = k] + \Pr[D \mid j \neq k]}{\Pr[D \mid j \neq k]}.$$

Let $\mathcal{I} = \{i \mid \Pr[j = k \mid D = i] > \frac{1}{2}\}$. The probability that the related sketch is among the selected sketches is $\sum_{i \in \mathcal{I}} \Pr[D = i \mid j = k]$. The number of sketches that is selected as possibly related is $N \sum_{i \in \mathcal{I}} \Pr[D = i]$. The probability of correctly guessing k is

$$\Pr[\hat{k} = k] = \frac{1}{N \sum_{\mathcal{I}} \Pr[D]} \cdot \sum_{\mathcal{I}} \Pr[D \mid j = k]$$

and the advantage of an Fsk-IND-N adversary using this strategy is

$$\begin{aligned} \text{Adv}_{\text{ind-N}} &= \frac{1}{N-1} \left(\frac{\sum_{\mathcal{I}} \Pr[D \mid j = k]}{\sum_{\mathcal{I}} \Pr[D]} - 1 \right) \\ &= \frac{\sum_{\mathcal{I}} (\Pr[D \mid j = k] - \Pr[D \mid j \neq k])}{\sum_{\mathcal{I}} (\Pr[D \mid j = k] + (N-1) \Pr[D \mid j \neq k])}. \end{aligned}$$

4.2.3. Example. Let C be a first-order Reed-Muller code of length $n = 128$ without the codewords 0 and 1, i.e., $C = RM(1, 7) \setminus \{(0, \dots, 0), (1, \dots, 1)\}$. The code contains $2^8 - 2$ codewords of weight $n/2$. Table 1 gives the probabilities $\Pr[D \mid b]$ for $i = \{0, \dots, 8\}$. Note that D is never 0 because the intersection will always contain 0 and 1, which we expunged from the full $RM(1, 7)$ code. Appendix B explains how to compute the intersection probabilities for this particular sketch.

Table 1. Conditional probabilities on the size of the intersection $V_1 \cap V_2$ and bounds on N for a bit-permutation sketch based on $RM(1, 7)$.

i	$\Pr[D \mid b_0]$	$\Pr[D \mid b_1]$	$N <$
0	0	0	/
1	$1 - 2^{-57}$	0	1
2	2^{-57}	$1 - 2^{-57}$	2^{57}
3	2^{-132}	2^{-57}	2^{75}
4	2^{-222}	2^{-132}	2^{90}
5	2^{-324}	2^{-222}	2^{101}
6	2^{-432}	2^{-324}	2^{109}
7	2^{-546}	2^{-432}	2^{113}
8	2^{-662}	2^{-546}	2^{116}

The advantage of an Fsk-IND adversary is

$$\text{Adv}_{\text{ind}} \approx 1 - 2^{-57}.$$

The bounds for which an Fsk-IND-N adversary still selects sketches are also given in Table 1. If we take $N = 2^{20}$ then $\mathcal{I} = \{2, 3, \dots, 8\}$ and

$$\text{Adv}_{\text{ind-N}} \approx \frac{1 - 2^{-57}}{1 + 2^{-37}} \approx 1 - 2^{-37}.$$

4.3. Perfect Indistinguishability

It was proved by Smith [11] that a fuzzy sketch must always leak information about its input: “If a sketch Fsk corrects t errors and E is a uniform distribution over $\{v \mid \|v\| \leq t\}$ then for any distribution W we have $I(W; \text{Fsk}(W)) \geq H(W \mid W \oplus E)$. If W is uniform over $\{0, 1\}^n$ then $I(W; \text{Fsk}(W)) \geq H(E) \approx nh_2(\frac{t}{n})$.” We will use this observation on the information leakage of a sketch and generalize the results from the previous sections to derive a lower bound on Adv_{ind} and thus a necessary condition for fuzzy sketches to be perfectly indistinguishable.

4.3.1. Generalized Heuristic. First we describe adversary advantages in terms of a generalized heuristic H with range \mathbb{H} , which is a generalization of the attack strategy for bit-permutation sketches. Let $H : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \mathbb{H}$ be a deterministic function that takes as input two sketches, produced with the same sketching function Fsk, and that outputs an element of \mathbb{H} . Without loss of generality we assume \mathbb{H} to be discrete. We denote the conditional distribution on \mathbb{H} given that the input sketches are related as $f_{H|r_1}$ and as $f_{H|r_0}$ if the sketches are unrelated. The advantages of an Fsk-IND adversary and an Fsk-IND-N adversary are

$$\text{Adv}_{\text{ind}} = \frac{1}{2} \sum_{\mathbb{H}} |f_{H|r_1} - f_{H|r_0}| \quad (5)$$

$$\text{Adv}_{\text{ind-N}} = \sum_{\mathcal{H}} \frac{f_{H|r_1} - f_{H|r_0}}{f_{H|r_1} - (N-1)f_{H|r_0}} \quad (6)$$

where $\mathcal{H} = \{h \mid \Pr[r_1 \mid H = h] > \frac{1}{2}\}$.

If the heuristic is a binary function, i.e., $\mathbb{H} = \{h_0, h_1\}$, and if $\Pr[r_1 \mid h_1] > \frac{1}{2}$ then the advantages are

$$\text{Adv}_{\text{ind}} = \Pr[h_1 \mid r_1] - \Pr[h_1 \mid r_0] \quad (7)$$

$$\text{Adv}_{\text{ind-N}} = \frac{\Pr[h_1 \mid r_1] - \Pr[h_1 \mid r_0]}{\Pr[h_1 \mid r_1] + (N-1)\Pr[h_1 \mid r_0]}. \quad (8)$$

An example of such a binary heuristic is the decodability heuristic in the code-offset construction. Note that if a binary heuristic selects on one value (h_1) it will not select on the other value (h_0). If $\Pr[r_1 \mid h_1] > \frac{1}{2}$, i.e.,

$$(N-1)\Pr[h_1 \mid r_0] < \Pr[h_1 \mid r_1],$$

then for $N \geq 2$ it holds that $\Pr[r_1 \mid h_0] < \frac{1}{2}$ because

$$(N-1)\Pr[h_0 \mid r_0] > \Pr[h_0 \mid r_1].$$

4.3.2. Recovery Range Overlap. An example of a binary heuristic for sketches is a function that verifies whether the range of the recovery function REC for a given sketch overlaps with that of another sketch. This is equivalent to verifying the decodability of the subtracted code offsets in Section 4.1.

For a given sketch generated from w we denote the recovery range by $R_w = \text{Range}(\text{Rec}(\cdot, \text{Fsk}(w)))$ and the extended recovery range as R_w^E , i.e., all points in R_w and the points that are at most distance t from those points. The distinguishability of sketches $P_a = \text{Fsk}(a)$ and $P_b = \text{Fsk}(b)$ depends on their recovery ranges R_a and R_b . If the sketches are related then there is at least one point in the intersection $R_a^E \cap R_b$. If the intersection is empty then the sketches are not related. See Figure 3 for a visual representation of the recovery ranges of two unrelated sketches.

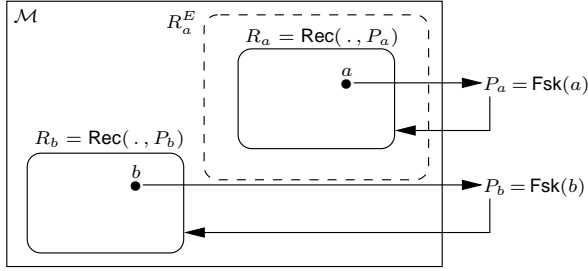


Figure 3. Extended recovery range R_a^E and recovery range R_b of unrelated sketches $P_a = \text{Fsk}(a)$ and $P_b = \text{Fsk}(b)$, respectively.

It is reasonable to assume that the adversary knows the recovery function and that he is able to determine whether R_b overlaps with R_a^E or not. The probability of having overlap depends on the structure of the recovery ranges, but a necessary condition is that at least one point in R_b lies in R_a^E . Let h_1 denote that the (extended) recovery ranges of two given sketches overlap, then

$$\Pr[h_1 | r_1] = 1 \quad \text{and} \quad \Pr[h_1 | r_0] \leq \frac{\#R_a^E}{\#\mathcal{M}}. \quad (9)$$

It is clear that 0-indistinguishability can only be achieved if two (extended) recovery ranges always overlap completely, irrespective of the sketches being related or not. In the code-offset sketch and the bit-permutation sketch this means that the underlying code must be perfect. Unfortunately, there are only few perfect codes and they have small error-correcting capacity [20], except for repetition codes, but these have dimension 1.

Given the attack based on the overlap heuristic we derive the following lower bounds on the advantages of an Fsk-IND and an Fsk-IND-N adversary.

Proposition 5. *Let Rec be the recovery function of an (\mathcal{M}, m, m', t) -secure fuzzy sketch (Fsk, Rec) . Let $R_w = \text{Range}(\text{Rec}(\cdot, \text{Fsk}(w)))$ and $R_w^E = \{x | \exists y \in R_w : d(x, y) \leq t\}$. If an adversary is able to verify if an arbitrary recovery range $R_{w'}$ overlaps with R_w^E then*

$$\text{Adv}_{\text{ind}} \geq 1 - \frac{\#R_w^E}{\#\mathcal{M}}$$

$$\text{Adv}_{\text{ind-N}} \geq \frac{\left(1 - \frac{\#R_w^E}{\#\mathcal{M}}\right)}{1 + (N-1) \left(1 - \frac{\#R_w^E}{\#\mathcal{M}}\right)}.$$

Proof: Using the attack strategy with the overlap heuristic, the result follows immediately from Equations (7), (8) and (9). \square

We can now define these bounds in terms of the information that is leaked by a sketch to determine a necessary condition for perfect indistinguishability that holds for any type of fuzzy sketch.

Corollary 6. *Let Fsk be the sketching function of an (\mathcal{M}, m, m', t) -secure fuzzy sketch (Fsk, Rec) that is ϵ -indistinguishable in $\Delta|_t$. Let input $W \in \mathcal{M}$ be uniformly distributed and E a uniform distribution over $\mathcal{E} = \{v \in \mathcal{M} | \|v\| \leq t\}$. If all points in R_W have pairwise distance greater than t then*

$$\text{Adv}_{\text{ind}} \geq 1 - 2^{-[I(W; \text{Fsk}(W)) - H(E)]} \quad (10)$$

and

$$\epsilon = 0 \quad \Rightarrow \quad I(W; \text{Fsk}(W)) = H(E). \quad (11)$$

Proof: If all points in R_w have pairwise distance greater than t then $\#R_w^E = \#R_w \cdot \#\mathcal{E}$. Because W and E are uniform $\#\mathcal{M} = 2^{H(W)}$, $\#R_w = 2^{H(W | \text{Fsk}(W))}$ and $\#\mathcal{E} = 2^{H(E)}$. From Proposition 5 it follows that

$$\text{Adv}_{\text{ind}} \geq 1 - \frac{2^{H(W | \text{Fsk}(W))} 2^{H(E)}}{2^{H(W)}}.$$

Since $I(X; Y) = H(X) - H(X|Y)$, this gives us the lower bound on Adv_{ind} .

If $\epsilon = 0$, $\text{Adv}_{\text{ind}} \leq 0$ or $1 - \frac{\#R_w^E}{\#\mathcal{M}} \leq 0$. Because $\frac{\#R_w^E}{\#\mathcal{M}} \leq 1$ it holds that $\#R_w \# \mathcal{E} = \#\mathcal{M}$ or

$$I(W; \text{Fsk}(W)) = H(E). \quad \square$$

We conclude that if a sketch leaks more information about its input than needed to correct the errors, then this extra leakage can be used to distinguish related sketches from unrelated sketches.

5. Reversibility

The previous section dealt with the problem of identifying related sketches. In this section we reconsider the desired irreversibility property of biometric sketches. We apply the notions of sketch irreversibility on the code-offset sketch and the bit-permutation sketch and we demonstrate how an adversary can combine the information that is leaked from two related sketches to learn more about the original input than he would learn from a single sketch.

5.1. Related Code-Offset Sketches

We consider sketches that are produced by different sketching functions from a family of code-offset sketches based on linear codes and we derive a necessary condition for this family to be perfectly irreversible.

5.1.1. Irreversibility Game. The adversary plays the irreversibility game and receives sketches $P_1 = \langle v_1 : w_1 - c_1, h(c_1) \rangle$ and $P_2 = \langle v_2 : w_2 - c_2, h(c_2) \rangle$ where c_1 and c_2 are randomly chosen from $[n_1, k_1, d_1]$ -code C_1 and $[n_2, k_2, d_2]$ -code C_2 , respectively. The adversary's goal in this game is to guess w_1 (or equivalently w_2). We assume that both codes have length $n = n_1 = n_2$.

Let $G_{1,2}$ denote the $k_1 + k_2 \times n$ matrix $\begin{bmatrix} G_1 \\ G_2 \end{bmatrix}$. If $w_1 = w_2 = w$, then the adversary will try to solve the linear system of equations

$$[x_1 \mid -x_2] G_{1,2} = v_2 - v_1 = c_1 - c_2.$$

From x_1 the adversary can compute c_1 and thus w_1 . The system has a unique solution if the sketches leak enough information, i.e., $k_1 + k_2 \leq n$ and if $\text{Rank } G_{1,2} = k_1 + k_2$. If $k_1 + k_2 > n$ or $G_{1,2}$ does not have full rank then the system is underdetermined.

The probability of reversing the sketches to w is

$$\Pr[\hat{w} = w] = \frac{1}{2^{k_1+k_2} - \text{Rank } G_{1,2}}$$

and the adversary's advantage is

$$\text{Adv}_{\text{fow}} = \frac{1}{2^{\min(m'_1, m'_2)} - 1} \cdot \left(\frac{2^{\min(m'_1, m'_2)}}{2^{k_1+k_2} - \text{Rank } G_{1,2}} - 1 \right).$$

If $w_1 \neq w_2$ but $\mathbf{d}(w_1, w_2) \leq t = \min(t_1, t_2)$, then the system of equations has no solution. However, an adversary can iterate over all possible error patterns e and check if the system

$$[x_1 \mid -x_2] G_{1,2} = v_2 - v_1 - e$$

is solvable by verifying that

$$\text{Rank} \begin{bmatrix} G_{1,2} \\ v_2 - v_1 - e \end{bmatrix} = \text{Rank } G_{1,2}.$$

Unfortunately, the number of error patterns to check becomes large if t is large, since $\#\{e \mid \|e\| \leq t\} \approx 2^{nh_2(\frac{t}{n})}$.

5.1.2. Perfect Irreversibility. If W is uniform, then $m'_1 = k_1$ and $m'_2 = k_2$, and if $w_1 = w_2$

$$\text{Adv}_{\text{fow}} = \frac{2^{\text{Rank } G_{1,2} - \max(k_1, k_2)} - 1}{2^{\min(k_1, k_2)} - 1}. \quad (12)$$

This leads us to the following necessary condition for perfect irreversibility of a family of code-offset sketches based on linear codes.

Proposition 7. Let Φ be a family of code-offset sketches $\{\langle \text{Fsk}_i, \text{Rec}_i \rangle\}$ having associated $[n, k_i, d_i]$ -code C_i and corresponding generator matrix G_i . Let Φ be ϵ -irreversible in $\Delta|_0$ on uniform input. For any pair of sketching functions $\langle \text{Fsk}_i, \text{Fsk}_j \in \Phi : i \neq j \rangle$ it holds that

$$\epsilon = 0 \Rightarrow \text{Rank} \begin{bmatrix} G_i \\ G_j \end{bmatrix} = \max(k_i, k_j).$$

Proof: Given the attack strategy above, the result follows from Equation (12). \square

This implies that for any pair of codes, corresponding to two sketches from a family of sketches that is perfectly irreversible, one of the codes must be a subcode of the other.

5.1.3. Example. Let C_1 be $RM(4, 10)$, a $[1024, 386, 64]$ Reed–Muller code, and C_2 a $[1023, 453, 127]$ BCH-code. Because the BCH-code is shorter, we assume that the first bit from the sample is punctured, which is equivalent to extending the generator matrix of the BCH-code by prepending it with a column of zeroes. Let \hat{G}_{BCH} be this extended generator matrix, then we have that

$$\text{Rank} \begin{bmatrix} \hat{G}_{BCH} \\ G_{RM} \end{bmatrix} = k_1 + k_2 = 839.$$

Following Equation (12) the adversary's advantage is 1 and any two offset sketches produced with these codes can be completely reversed.

5.2. Related Bit-Permutation Sketches

The adversary plays the irreversibility game for a single bit-permutation sketch. He receives two sketches $P_1 = \langle A_1, h(c_1) \rangle$ and $P_2 = \langle A_2, h(c_2) \rangle$, as in the indistinguishability game in Section 4.2, with the additional constraint that the sketches are related. Again, we limit the scope to the model in which related sketches are generated from the same sample w . The adversary's goal is to guess w .

The attack strategy is straightforward and follows from the results in Section 4.2. The adversary will look at the intersection of V_1 and V_2 and will randomly choose an element from that intersection as a guess for w . The probability of guessing correctly is

$$\Pr[\hat{w} = w] = \sum_{i=1}^k \frac{1}{2^i - 2} \cdot \Pr[D = i]$$

Note that $\Pr[D = i] = \Pr[D = i \mid b = 1]$. The adversary's advantage is

$$\text{Adv}_{\text{ow}} = \frac{2^{m'} - 1}{2^{m'} - 1} \left(\sum_{i=1}^k \frac{1}{2^i - 2} \cdot \Pr[D = i] - \frac{1}{2^{m'}} \right).$$

If W is uniform, then $2^{m'} = 2^k - 2$ and

$$\text{Adv}_{\text{ow}} = \frac{2^k - 2}{2^k - 3} \sum_{i=1}^{k-1} \left(\frac{1}{2^i - 2} - \frac{1}{2^k - 2} \right) \Pr[D = i].$$

In the example of Section 4.2.3 the advantage of an Fsk-OW adversary using this strategy is

$$\text{Adv}_{\text{ow}} \approx \frac{14}{13} \left(\frac{1}{2} - \frac{1}{2^{59}} - \frac{1}{14} \right) \approx 0.46.$$

6. Conclusion and Future Work

We have studied the two main properties, indistinguishability and irreversibility, of biometric template protection schemes in the model where the schemes are applied multiple times on the same noisy input. For these properties, security notions were defined that model a weak adversary and we have demonstrated that several constructions based on linear error-correcting codes are not secure under these notions. We have determined necessary conditions for perfect indistinguishability and perfect irreversibility from bounds on the adversary's advantages. A natural question is whether we can transpose our results to schemes that work with continuous sources, where quantization is used as error-correction, and models in which we take into account non-uniform error patterns.

Acknowledgement. The authors wish to thank Fr derik Vercauteren for the useful discussions on the distinguishability of permutation-based sketches. They also thank Brent Waters and abhi shelat for their feedback when preparing this paper and the anonymous reviewers for their valuable comments.

References

- [1] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *CCS '99: Proceedings of the 6th ACM conference on Computer and Communications Security*. New York, NY, USA: ACM Press, 1999, pp. 28–36.
- [2] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proceedings of IEEE International Symposium on Information Theory, Lausanne, Switzerland*, A. Lapidoth and E. Teletar, Eds. IEEE Press, 2002, p. 408.
- [3] J.-P. M. G. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in *AVBPA*, ser. Lecture Notes in Computer Science, J. Kittler and M. S. Nixon, Eds., vol. 2688. Springer, 2003, pp. 393–402.
- [4] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Advances in Cryptology - EUROCRYPT 2004*, ser. Lecture Notes in Computer Science, C. Cachin and J. Camenisch, Eds., vol. 3027. Springer, 2004, pp. 523–540, full version available at <http://eprint.iacr.org/2003/235.pdf>.
- [5] G. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through off-line biometric identification," *Proceedings of the IEEE Symposium on Security and Privacy - S&P '98*, pp. 148–157, May 1998.
- [6] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security and Privacy*, vol. 1, no. 2, pp. 33–42, March-April 2003.
- [7] R. Yousefi-Nooraie and S. Mortaz-Hedjri, "Dermatoglyphic asymmetry and hair whorl patterns in schizophrenic and bipolar patients," *Psychiatry Research*, vol. 157, no. 1–3, pp. 247–250, 15 January 2008.
- [8] R. B. Saenz, "Primary care of infants and young children with Down syndrome," *American Family Physician*, vol. 59, no. 2, pp. 381–390, 15 January 1999.
- [9] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.
- [10] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561–572, 2007.
- [11] A. D. Smith, "Maintaining secrecy when information leakage is unavoidable," Ph.D. dissertation, Massachusetts Institute of Technology, August 2004.
- [12] Y. Dodis and A. Smith, "Correcting errors without leaking partial information," in *STOC '05: Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*. New York, NY, USA: ACM, 2005, pp. 654–663.
- [13] X. Boyen, "Reusable cryptographic fuzzy extractors," in *CCS '04: Proceedings of the 11th ACM conference on Computer and Communications Security*. New York, NY, USA: ACM, 2004, pp. 82–91, full version available at <http://www.cs.stanford.edu/xb/ccs04/>.
- [14] M. Bellare, A. Boldyreva, A. Desai, and D. Pointcheval, "Key-privacy in public-key encryption," in *ASIACRYPT*, ser. Lecture Notes in Computer Science, C. Boyd, Ed., vol. 2248. Springer, 2001, pp. 566–582.
- [15] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaer, G. J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis, "Practical biometric authentication with template protection," in *AVBPA*, ser. Lecture Notes in Computer Science, T. Kanade, A. K. Jain, and N. K. Ratha, Eds., vol. 3546. Springer, 2005, pp. 436–446.
- [16] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Z emor, "Optimal iris fuzzy sketches," *Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007. First IEEE International Conference on*, pp. 1–6, 27–29 September 2007.
- [17] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.
- [18] R. J. McEliece, E. R. Rodemich, H. Rumsey, and L. R. Welch, "New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities," *IEEE Transactions on Information Theory*, vol. 23, no. 2, pp. 157–166, March 1977.
- [19] E. Gilbert, "A comparison of signaling alphabets," *Bell System Technical Journal*, vol. XXXI, no. 3, p. 504, May 1952.

- [20] A. Tietavainen, “On the nonexistence of perfect codes over finite fields,” *SIAM Journal on Applied Mathematics*, vol. 24, no. 1, pp. 88–96, 1973.
- [21] M. Sudan, “List decoding: algorithms and applications,” *SIGACT News*, vol. 31, no. 1, pp. 16–27, March 2000.
- [22] V. Guruswami, *List Decoding of Error-Correcting Codes: Winning Thesis of the 2002 ACM Doctoral Dissertation*, ser. Lecture Notes in Computer Science. Springer-Verlag Berlin Heidelberg, 2005, vol. 3282.

Appendix A. List Sketch

We can improve the indistinguishability of code-offset sketches by applying list decoding. For an introduction to the problem of list decoding see [21]. Unique decoding can correct up to $t = \frac{d-1}{2}$ errors where d is the minimum distance of the code. Given a word that was received after transmitting a codeword over a noisy channel, a list decoding algorithm outputs a list of codewords that are at most distance e from the received word and decoding is considered successful if the original word is in the list. For biometric authentication based on sketches, this only works if a verification value is available against which the codewords on the list can be tested, e.g., the hash of the codeword.

List decoding allows decoding beyond half the minimum distance of a code. Obviously, the size of the list increases with e . Guruswami [22] determined the following bound on the list decoding radius e . If

$$e < e_J(n, d, q) = \left(1 - \frac{1}{q}\right) \left(1 - \sqrt{1 - \frac{q}{q-1} \cdot \frac{d}{n}}\right) n$$

then there are at most

$$\min \left\{ n(q-1), \frac{nd}{nd - 2e\left(n - \frac{qe}{2(q-1)}\right)} \right\}$$

points in a sphere of radius e in \mathbb{F}_q^n with pairwise distances at least d . Alternatively, if

$$e \leq e_J(n, d, q, L) = n \left(1 - \frac{1}{q}\right) \left(1 - \sqrt{1 - \frac{q}{q-1} \frac{L-1}{L} \frac{d}{n}}\right)$$

then the size of the list is at most L . For (non-linear) binary codes this means that if $e \leq \frac{n}{2} \left(1 - \sqrt{1 - 2\frac{d}{n}}\right)$ then the number of codewords returned by a list decoding algorithms is at most $2n$. Efficient constructions on list decoding algorithms for several types of codes were given in [22].

We can improve our bounds on the distinguishing information leakage of a code (see Section 4.1) by using a code that has a minimum distance $d < 2e + 1$ with e the desired noise-tolerance of the sketch. The noise-tolerance stays the

same, $e = t$, but we can have more codewords (and a larger recovery range R_w , see Section 4.3), thus the entropy loss $n - k$ decreases, while $V_q(n, e)$ and the extensions around the elements of R_w remain the same.

Definition 9. An $(\mathcal{M}, m, m', t, l)$ -secure list fuzzy sketch is an (\mathcal{M}, m, m', t) -secure fuzzy sketch where $\text{Rec}(w', \text{Fsk}(w))$ outputs a list $L \subset \mathcal{M}$ such that $\#L \leq l$ and if $\mathbf{d}(w, w') \leq t$ then $w \in L$.

For binary codes the normalized bound of the list decoding radius of a binary code with relative distance δ is $J(\delta) = \frac{1 - \sqrt{1 - 2\delta}}{2}$. Because the bound is tight we can replace the term $H_2\left(\frac{\delta}{2}\right)$ in the bounds on the relative distinguishing information leakage of a binary code-offset sketch in Proposition 4 with $H_2(J(\delta))$. The improved bounds on the distinguishing information leakage and the advantage of an Fsk-IND adversary are shown in Figures 1 and 2. Unfortunately, the adversary still has a significant advantage.

Appendix B. Intersection Probabilities

In this section we show how to compute the intersection probabilities as defined in Section 4.2.3 by means of the following example. Let C be a first-order Reed-Muller code of length $n = 8$ without the codewords 0 and 1, i.e., $C = \text{RM}(1, 3) \setminus \{0, 1\}$.

The probability that a k -dimensional subspace $V_1 = \langle b_0, \dots, b_{k-1} \rangle$ of an n -dimensional (binary) vector space overlaps entirely with another k -dimensional subspace V_2 is

$$\Pr[V_1 = V_2] = \prod_{i=0}^{k-1} \frac{2^k - 2^i}{2^n - 2^i}.$$

This can be found by verifying that b_0 lies in V_2 , then by looking if b_1 is in V_2 given that b_0 is in V_2 , etc. Since basis vectors are linearly independent, the choices of the i -th basis vector are reduced with 2^i . In our example the subspaces are generated by a permuted generator matrix of C , which limits our choice for the i -th basis vector.

The generator matrices of first-order Reed-Muller $\text{RM}(1, m)$ codes can be defined recursively as

$$G_i = \left[\begin{array}{c|c} 0 \dots 0 & 1 \dots 1 \\ \hline G_{i-1} & G_{i-1} \end{array} \right] \quad \text{and} \quad G_1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

The generator matrix of our code $\text{RM}(1, 3)$ is

$$G_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Let $b_0 = [11111111]$, then $\Pr[b_0 \in V_2] = 1$. Let $b_1 = [00001111]$. There are $\binom{8}{4} = 70$ equiprobable permutations of b_1 and $2^4 - 2^1 = 14$ vectors left in V_1 .

Hence $\Pr[b_1 \in V_2 | b_0 \in V_2] = \frac{14}{70} = \frac{1}{5}$. Given the permutation of b_1 we have to look at the possible permutations of $b_2 = [00110011]$, which are the permutations that change b_2 but not the permutation of b_1 , i.e., all permutations that work on the ones in the permutation of b_1 but not on the zeros and vice versa. Thus, $\Pr[b_2 \in V_2 | \{b_0, b_1\} \in V_2] = \frac{2^4 - 2^2}{\binom{4}{2}^2} = \frac{1}{3}$.

Analogously, we have for $b_3 = [01010101]$ that $\Pr[b_3 \in V_2 | \{b_0, b_1, b_2\} \in V_2] = \frac{2^4 - 2^3}{\binom{4}{2}^2} = \frac{1}{2}$.

The probability that the i -th basis vector of V_1 is in V_2 given that the first till the $(i - 1)$ -th basis vector are in V_2 is, for $i \geq 1$,

$$\Pr[b_i \in V_2 | \{b_0, \dots, b_{i-1}\} \in V_2] = \frac{2^k - 2^i}{\binom{n/2^{i-1}}{n/2^i}}.$$

Let's denote this probability as $\Pr[b_i \rightarrow V_2]$. For unrelated sketches we define $\Pr[b_0 \rightarrow V_2] = 1$. For related sketches however, we define $\Pr[b_0 \rightarrow V_2] = 1$ and $\Pr[b_1 \rightarrow V_2] = 1$.

The probability that all b_i are in V_2 is

$$\Pr[V_1 = V_2] = \prod_{i=0}^{k-1} \Pr[b_i \rightarrow V_2].$$

To compute the probability that the dimension of the intersection is $k - 1$ we have to add the probabilities that any of the basis vectors is not in V_2 , or

$$\sum_{i=0}^{k-1} (1 - \Pr[b_i \rightarrow V_2]) \prod_{j=0, j \neq i}^{k-1} \Pr[b_j \rightarrow V_2].$$

For $D = k - 2$ we need to consider the probabilities that any combination of two basis vectors of V_1 is not in V_2 , etc.

In our example we have, for $i = \{0, \dots, 4\}$,

$$\Pr[D | b] = \begin{cases} 0 & 0 & 10/30 & 15/30 & 5/30 & b = 1 \\ 0 & 8/30 & 14/30 & 7/30 & 1/30 & b = 0 \end{cases}.$$