ARITHMETIC METHODS
IN MATHEMATICAL PHYSICS AND BIOLOGY
BANACH CENTER PUBLICATIONS, VOLUME 109
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 2016

CURRENT CHALLENGES FOR BIOMETRIC SECURITY, WITH FOCUS ON FINGERPRINTS

PREDA MIHĂILESCU

Mathematical Institute, University of Goettingen
Bunsenstr. 3–5, D-37073 Goettingen, Germany
E-mail: preda@uni-math.gwdg.de

BENJAMIN TAMS

Institute for Mathematical Stochastics, University of Goettingen
Goldschmidtstr. 5–7, D-37077 Goettingen, Germany
E-mail: btams@math.uni-goettingen.de

Abstract. In this paper we discuss some imminent vulnerabilities of biometric systems, which have been potentially known for a longer time, yet they have not been sufficiently taken into account. In particular, we explain why comparing lower bounds of security of biometric systems with the state of the art lower bounds known from cryptography is a logical necessity and not a far reached goal: insufficient security in complex hybrid systems easily may compromise the stronger components in the complex.

1. Introduction. *Confidential* communication is a request with an old tradition, mostly within military applications. However, the advent of Internet has lead to a need for confidentiality in a very broad area of applications using electronic communication. While military application can be secured by method corresponding to the highest standards, in civil applications a combination of easiness of use with *sufficient* security is often wished for.

We shall argue here about the fact that the two aims may be in apparent contradiction, and an insufficient care in trying to fulfill them simultaneously can lead to compromising the system. However, this negative is not necessary and can be circumvented with more effort and investment.

We shall take the paradigm of secure communication in open networks in order to illustrate the hybrid systems we take into consideration. However, the same issues will be encountered in practically all scenarios in which biometry is used for identification in a secure context.

2010 *Mathematics Subject Classification*: Primary 92-01; Secondary 94A17.
The paper is in final form and no version of it will be published elsewhere.

It has been rightfully argued that there are various applications requiring less than cryptographic security and where the amount of entropy of biometry should be sufficient for the purpose of the application.[1] Such applications may be access control to areas requiring entry fees or identity control — such as private clubs, museums, zoos, swimming areas or other similar facilities where entry can be granted for a fixed time frame, allowing multiple entries. In such applications the security requirements are indeed lower and can be met by biometric identification, with the full advantage of easiness of use. However, one serious side effect which has to be discussed in its full set of consequences is related to the uniqueness of biometric traits. Certainly, in the situation described, an intruder might not have the material motivation for attempting a — possible, yet time and work consuming — attack of the biometric identification system. However, the intruder might wish to gain information from a low protection application, as the ones enumerated above, and then use it in areas of higher security levels. Such attacks are easily conceived and their possibility is certainly not a novelty. Nevertheless, they have been little discussed in all consequence in the literature; the fast spread of biometric application in higher security identification contexts induces more urgency for this discussion. After having mentioned this necessity of investigating the consequence of possible transfer of information gathered while breaking low security systems to other systems of higher security level, we shall restrict our focus in this paper to the topic of secure communication and authentication.

Two parties wish to communicate in such a way that no unauthorized (by them) third party may have *a slight chance* to reveal the content of the communication. Some side-requirements in such a setting are

- The request for *secure authentication.*
- The request for provable *signatures*, or, more generally, insurance of the impossibility to repudiate the origin of a message.

A common answer to these requirements was provided by cryptography. A fast method of encryption relays on the use of shared keys, known to both communicating peers, say Alice and Bob, as cryptographers often design them. In this case one speaks of secret key encryption, and the present time international standard for this purpose is AES and was designated after an international competition among a series of algorithms proposed by specialists both from academia and commercial companies specialized in security.

The secret key cryptography may still be used with success even in modern computer times, for protecting the message contents. At the advent of computer networks, the alternative of *public key cryptography* was invented independently by two groups of young American researchers involved in the incipient ARPA net of the 70-es and by an engineer working for the MI5, who was allowed to disclose his discovery in the year 2000. The common idea is to split the key of a peer, say A, for Alice, in two parts, a private part $S(A)$ and a public part $P(A) \subsetneq S(A)$, which is available to the world. Encryption does work both ways like in the secret case. Only, for writing to A, peers B will use the public key, creating messages that only can be decrypted using the private key $S(A)$. In addition, Alice will be now able to authenticate herself, by encrypting *any public message* — for instance "hellow world" — with her private key. Since nobody else should be able to

[1] We shall see that it is indeed the low entropy in biometric traits which causes security issues.

find the private key of Alice, upon description with the public key, Bob or anyone, can be convinced of the fact that it was indeed Alice that generated the encryption — in this situation, the encryption with the private key replaces something like a hand-written signature; it is therefore also called *digital signature*. The same procedure is used to obtain non-repudiation of the origin of a message. These facilities are essential for private secure electronic communication.

Therefore public key cryptography has found its exponential spread at the time of the opening of the world wide web to the large public, in the mid-90-es. While public key cryptography is found in more and more applications, several new, important problems arise.

1. The *reliability* of public keys obtained in the public domain.
2. The multitude of secret key protections required.
3. The very reliability of hardware used in transactions that require personal authentication.
4. User friendliness.

When it comes to implementing public key cryptography, a new challenge arises: certainly, the secret keys used are both too large and deprived of semantic signification to be possibly memorized by the user. Instead, the user will know some password, which enables the computer or smart card to use her key bundle. It is at this point that biometry enters the game: The contexts in which passwords are required are so numerous that a user can often not recall all passwords it has in usage; hence the idea to replace identification through passwords by biometric identification. The change of focus is sometimes described as switching from *identification by what you know or have* to identification *by what you are*. What you have or know can be represented by passwords or some physical devices carrying identification information. "Who you are" refers to some biometric trait of the individual, such as fingerprints, retina patterns, palm characteristics, facial identity, and many more.

The purpose of this paper is to discuss the challenges of modern IT security induced by the proliferation of password usage and the advent of biometry. An important application of biometry, which is more and more spread is the governmental use, like biometric ID's, biometric control at customs and several more, similar applications. These applications are clearly very important, and while being slightly different from the secure communication paradigm that we discuss, the important issues that we find in the latter apply also to governmental applications.

2. Trends and challenges in information security. In the last three decades, *cryptology* has become a major field of research, together with its Janus-faced duality: *cryptography*, for the design of algorithms and protection principles and *cryptanalysis* for investigation of possible attacks against these algorithms. The core algorithms, *also called 'primitives'*, are divided into:

A. Secret key Algorithms
B. Public Key Algorithms
C. One way functions, hashes
D. Key management.

We have discussed briefly the first two. One way functions or hashes have the paradoxical property of being highly non-injective maps, since they map the realm of all possible messages to fixed-length blocks, of, say, 192 bits. Such a hash would be a map $\chi : \mathbb{N} \to \mathbb{Z}/(192 \cdot \mathbb{Z})$. However, the size of the image set is large enough to ensure that it is not computationally feasible to find even one single *collision*, i.e. $x \neq y$ with $\chi(x) = \chi(y)$. Little to say about a *match*, which would require to find, for a given hash of an unknown value, say $h = \chi(x)$ a value $y \in \mathbb{N}$ with $\chi(y) = h$. The collision problem is easier, since it only requires two random hashes to match; in the second case one hash value is already fixed. One way functions must fulfill certain properties related to the conditions discussed. If they do, they are used for two purposes: saving passwords in a protected way, without use of encryption — just substitute a password by its hash value, so the stored data will reveal no information about the initial password. The second application of hashes is in connection with *digital signatures*: Messages to bind to a digital signature are sometimes very large, so one prefers to replace them by their unique hash value and place a digital signature on this hash value.

Key management is less of a cryptographic primitive and more of a set of requirements for the privacy and reliability of keys and passwords used in secure communication. Key management draws on standards of key authentication, as well as hardware tokens such as chip cards or other devices, carrying sensitive keys, etc. It is the task of key management to provide not only for secure key storage — either on encrypted memory or chip cards or similar devices — but also for *trust diffusion*. By this we mean that two peers, Alice and Bob, who start communication by exchanging public keys, should be provided with means to trust that the received public key does indeed belong to either Alice or Bob. Avoiding attacks by *masquerading* false keys is thus an important task of key management. The provisions for this task are a mixture of cryptography and protocol administration.

It is probably the most important achievement of modern cryptography that the problems of secure information exchange have been reduced to primitives, endowed with well-defined properties, and security is asserted on base of such properties, which can be verified by the cryptologist in the whole world. Hence, the possibility of attacks to a cryptographically secured environment can be also grouped in types of attacks based on well-defined *attack-scenarios*. It is the presence of these attack-scenarios which help establish the trust into cryptographic solutions, which end up being standardized and used world-wide. A typical, very important *standard* in this context is the *TLS/SSL standard*, which is the cryptographic standard of the world wide web and provides secure communication facilities based on variable tool-kit primitives.

One may conclude that the first decades of public key cryptography provided a reliable system of well scrutinized primitives for addressing each of the problems A–D. The algorithms for public key encryption, hashes and secret key algorithms as well as the protocols for key management of the last decades are resistant to direct attacks, beyond reasonable doubt.[2]

[2]We must not mistake "beyond reasonable doubt" for "provable certainty". There is no mathematical proof for the lack of efficient attacks to the state of the art primitives, and even if such one would be provided, it would always be connected to a fixed context of application. But new attacks can be invented, which were not thought of. Confidence relays on the intensive long time research in the public academic domain, spent on the related cryptologic questions.

At the present day, cryptology offers protocols and primitives that are

C1. *Reliable*: They are well researched and secure within any reasonable doubt.
C2. Providing *scalable security* in the sense that it is possible in any of the primitives, to adapt to increased performance of computers, by modifying the length of keys in such a way that the expected time necessary to perform well-defined attacks on a given primitive stays unchanged.
C3. *Deterministic* in the sense that on the same input they will always produce the same output. The notion of security if based on the provision that an attack on a primitive should require computation time which range beyond hundreds of years, under the most favorable circumstances and using the best algorithms to date. *Even the lowest accepted level of security is beyond doubt*, and the primitives are rejected as soon as theoretical advances show any vulnerability allowing for attacks that can be performed in less than decades or even centuries.

2.1. Recent evolution. After these achievements have been completed in the 90-es, the challenges of security moved to more volatile topics. The most important are

H1. The definition of trust: in an open environment, who should security protect against whom? Can one trust the user more or the vendor providing some token or hardware, that requires secure identification, which may be stolen?
H2. Viruses and denial of service attacks: both are attacks against an operation system that can either spread over the whole internet or focus on certain target intranets, leading to a blockage of their functionality by overload.
H3. Hacker intrusions of intranets. These are often performed with the purpose of commercial espionage and use any kind of vulnerabilities of operating system, security implementations of even individual authentic users of the intranet.

Developing countermeasures to these very real and corrosive kinds of attacks is an endeavour that requires all the apparatus of cryptology but reaches well beyond: it is the modern task of security engineering.

One may thus observe that cryptology has offered its best and became now part of the more complex task of IT security engineering. Paradoxically, the development and spread of secure applications lead at the opposite end of complexity to new challenges. Since applications are mostly independent and coming from various vendors, the typical user of a large intranet becomes soon confronted with the requirement to secure his identification with respect to a multitude of software, each requiring *safe passwords* from him. This challenges human memory and it mostly happens that users choose to bypass security prescriptions for passwords, by either writing them down or reusing the same password. This leads to user driven vulnerabilities.

2.2. The advent of biometry. In this context, biometry entered the scene with the promise which is best reflected in the paradigm *you are what you are* as opposed to *you are what you know* or *what you have*. Indeed, in a cryptographical frame, the user is authenticated either by knowledge of some secret, such as the password of some key, or by means of a token that carries this secret information for him. Assuming he has control on these access modalities, cryptology guarantees secure use. However, the control is

relativized by the reasons stated above. Therefore biometry suggests to identify a person physically, by some specific traits that distinguish him uniquely. These can be fingerprints or iris, face or writing mechanics, vein geometry or voice — a multitude of physical and behavior traits have been proposed and investigated in order to uniquely identify a person. The wish becomes one to remove the responsibility for identification information from the user and defer it to technology. The user presents his physical appearance and trusts the system that it may well identify him and not allow intrusions or any other kind of abuse of information related to him. The approach was motivated by the success achieved in *image processing* during the previous decades, which made the identification by means such as fingerprint, iris or face recognition quite reliable.

However, the advent of biometry and its increasing actual use in security contexts raises a series of important questions:

B1. Unlike cryptographic authentication, the biometric authentication is not deterministic. It is based on comparing real time acquired data — such as images of fingers, iris or a face, against *templates* stored in a database. It is certainly likely that the new data best matches the one of the template of the individual stored in the data base; this is however only true within a certain stochastic measure of doubt. The actual deterministic certainty is replaced by an error distribution of false acceptances and false rejects. By deciding acceptance scores, the system can adjust false accepts against false rejects — it will not be able though, to remove any probability of error. This is the *stochastic nature* of biometric identification.

B2. Unlike passwords, which can be replaced when compromised, biometric traits cannot be changed. As a consequence, the world -wide system using one kind of biometry cannot be reliably factored into more secure areas, by use of advanced and expensive technology: A template acquired in a weak system can be used for impersonating a user in any other system. As mentioned in the introduction, the consequences of the biometric identification data being *unique and unrenewable* should be investigated in the context of high security applications of biometry.

B3. Most important, the presence of a non-vanishing probability of a false match becomes the de facto measure of *active information entropy* present in some type of biometric recognition. We describe in this paper some attacks, which confirm practically what one can well imagine by common sense: In presence of a certain probability of a false match, one can use databases of templates for successfully impersonating a legitimate user.

B4. Due to the statistical nature of identification, there is some lack of formal accuracy also in the definition of identification — although in practice, the identification process is well understood. The key notion used in discussing security of the identification data is the notion of *reversibility*, which vaguely describes the capacity of an entity to recover identification data from a protected storage. One of the important issues addressed in this paper is the fact that an adequate definition of reversibility is statistical and should not be connected to the complete identification data stored, but instead, to a sufficient amount of information in order to enable an *impersonation* attack. We shall also show that this perspective shows once again the relevance of false-accept attacks.

Although these concerns raise *serious caveats* for the use of biometry, its user friendliness leads to a continuous propagation of the idea of using it in secure applications. It is therefore the task of research to develop affordable measures for meeting the two polar expectations: security versus commodity.

Certainly, the concerns about low entropy in biometric data are known, but the vague idea of *application for lower or medium security concerns* was brought up as an alternative. This breaks the fundamental principle C3 of security: Suddenly one seems willing to accept secure contexts, in which attacks can be performed in very short time, yet expecting that the outcome is not sufficiently important for motivating such attacks. This could be a defendable point of view, when the security context is, for instance, a small intranet in which users are satisfied with a formal protection; or when biometry protects access to some areas or institutions. However, the consequences in view of B2, namely the uniqueness and irreplaceability of biometric traits are poorly thought through. In plain words, a successful attack on a system of little security relevance may endow an attacker with the capacity of impersonating a target in any other application of biometric security, and this consequence calls for analysis.

As an alternative, a separate branch of activity has been dedicated to a mixture of cryptography and biometry, in which cryptography is supposed to well protect the templates of biometry. However, this quite theoretical area of research operates with the questionable notion of biometric traits being *public data*. This assumption does take into account B2. and the possibility of compromising biometric traits — it is though questionable, what the overall amount of security based on public data may be. Most problematic is the fact that despite intense work, the possibility to uncouple biometric from cryptographic security in these settings, and thus breaking the weakest part in the chain has received no convincing answer yet.

Another approach, which shall be discussed more in detail in this paper, considers biometry as some kind of passwords. They allow access to resources, and, like passwords, should be stored under some one way transformation. This works without problem in the deterministic context: The user presents a password, and its hash value is stored. The hash value to the same password will always be the same, but an attacker cannot recover the password from knowing the hash. In biometry though, any transformation of the template that can allow both to hide the data from intruders and to perform identification, will mostly have at least a loss in the recognition accuracy as a consequence. Therefore, even in the context in which unprotected template matching provides quite a low entropy and thus protection levels, the requirement for password protection leads to an additional loss of entropy, and thus even lower security.

These questions are actively discussed in the literature of the last decade. The community of biometry security is a mixed one, ranging from engineers with good expertise in image processing and practical implementations of biometric systems, to specialists of information theory and cryptology which bring new ideas from their domains, while treating biometry as a black box yielding an amount of entropy. The responsibility that the entropy be measurable and sufficient is deferred to applicants — which often are not trained for establishing such complex measures. In fact, no mathematical or statistical stringent definition of entropy can be accurately applied in the context. It is one of the

points which we shall make in this paper, that the de facto entropy of some biometric template is simply given by the equal error rate of the system, i.e. the balanced probability of false accepts and false rejects. This leads to a realistic, albeit quite low quantity. A further concern of the incipient biometric security research should be the one of giving some accurate definitions of attacks. Like in the case of cryptographic security, these attacks should specify clearly:

A1. What resources does one assume that the intruder may dispose of?
A2. What advantage does the intruder wish to gain?
A3. In what way does one evaluate the success of an attack?

3. Biometric recognition. In this section we introduce the basic concepts of automatic biometric recognition systems. We summarize the setting in general terms with the intention to be accessible to readers who are not familiar with biometry. For a more comprehensive reference, we refer the interested reader to [10].

We shall start with one of the most popular examples of a biometric modality.

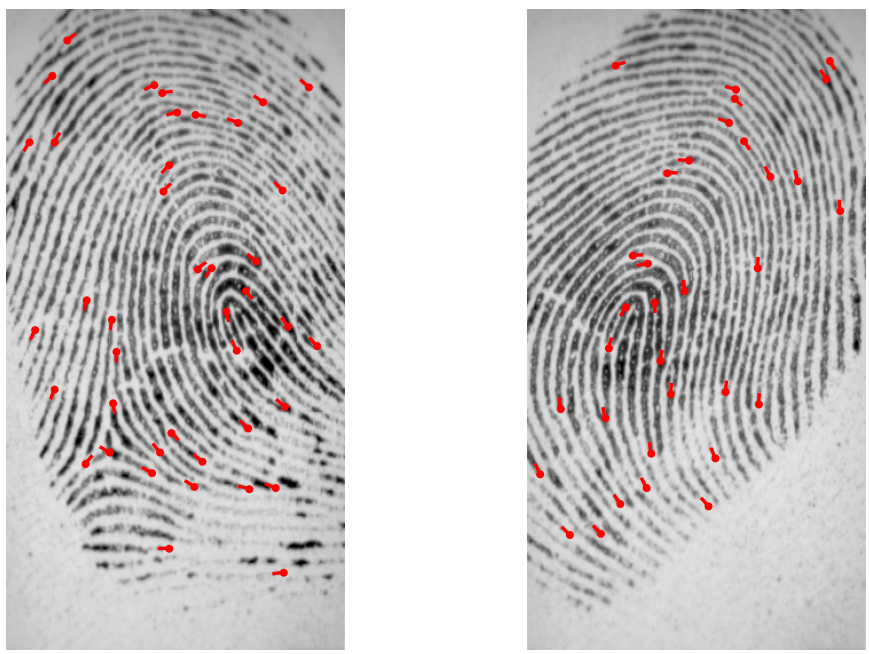


Fig. 1. Two matching fingerprints and its minutiae

3.1. Example: Fingerprints. One popular and well-known biometric modality that can be used for biometric recognition is the fingerprint modality. A *fingerprint* is given by the traces that the ridges of a finger leave on a surface. These days, digital scanners can be used (including specific fingerprint sensors) to obtain a digitized image, i.e. the *fingerprint image* of these traces. A standardized type of fingerprint features are *minutiae*, i.e. features derived from the positions at which a fingerprint ridge ends abruptly or where it bifurcates, i.e. a *minutiae ending* or *minutiae bifurcation*, respectively (see Fig. 1). These minutiae positions are typically attached with a *minutia angle*. Given two minutiae sets,

i.e. two *minutiae templates*, comparison may be performed by adopting methods for registering two-dimensional point clouds. Many methods for minutiae template comparison utilize a pre-alignment step in which, before a comparison score is derived, both minutiae sets are aligned such that matching minutiae are expected to be spatially in agreement. For further details as well as for a comprehensive overview on fingerprints we refer the reader to [16].

3.2. Comparison. We continue with describing the topic in general terms without restriction to a certain biometric modality.

Assume we are given two *biometric templates* (e.g. *minutiae* estimated from a scan of a finger) for which we want to decide whether they are *matching* or not.[3] This decision problem may be usefully conceptualized as the problem of finding a binary function that outputs a binary match decision. An ideal such function would output *match* for all matching templates while, at the same time, outputs *non-match* for all non-matching templates are given. Such a perfect biometric decision function may not exist due to the stochastic nature of biometric measurements — an inherent property already mentioned in Section 2.2. In this section, we consider this situation in more detail.

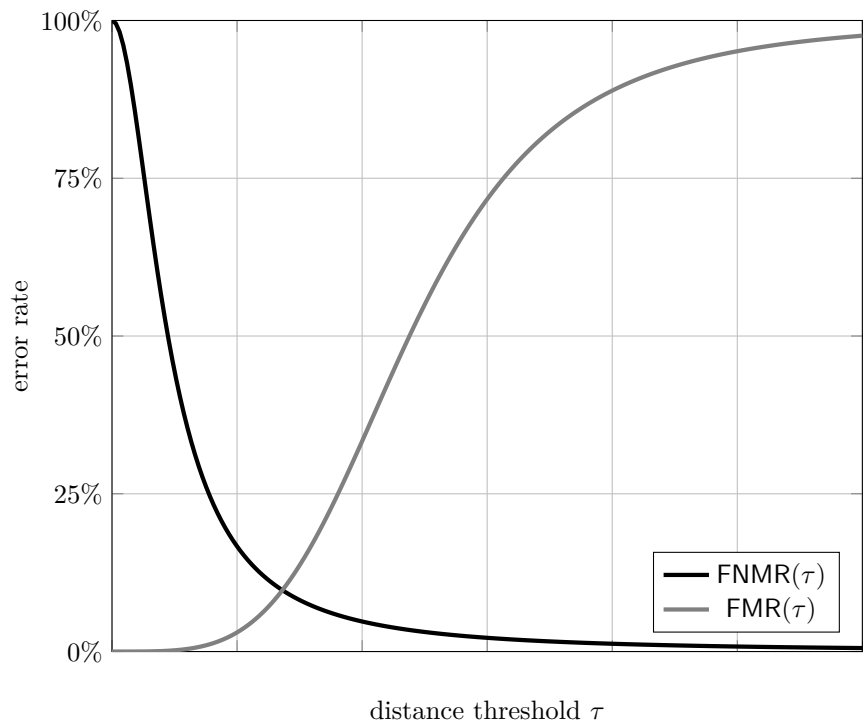


Fig. 2. Visualization of a biometric comparison system's decision error rates in dependence of the chosen distance threshold τ. These are the false non-match rate and the false match rate being functions in τ and denoted by $\mathsf{FNMR}(\tau)$ and $\mathsf{FMR}(\tau)$, respectively

[3]Two templates are said to *match* iff they have been derived from the same *biometric instance*, e.g. finger.

A biometric comparison decision may be derived on base of an underlying distance function

$$\mathsf{dist} : \mathbf{U} \times \mathbf{U} \to \mathbb{R}_{\geq 0} \tag{1}$$

whose value is correlated with the (dis)similarity of the input template pair, i.e. the more two templates differ from each other the higher is the value of this distance function. Given a threshold τ, on biometric comparison we may decide two biometric templates to match if and only if they have a distance at most τ; otherwise, these two biometric templates are considered not to match. To obtain a biometric comparison decision we have to deal with two kind of errors: *false non-match rate* and *false match rate*. The first refers to the probability of two matching templates being falsely recognized as non-matching and the second to the probability that two non-matching templates are falsely recognized as matching. Both error rates can be considered as functions in τ (see Fig. 2). More specifically, the false non-match rate may be defined as

$$\mathsf{FNMR}(\tau) = \mathbb{P}(\mathsf{dist}(Q, R) > \tau \,|\, \text{matching } Q \text{ and } R) \tag{2}$$

and the false match rate as

$$\mathsf{FMR}(\tau) = \mathbb{P}(\mathsf{dist}(Q, R) \leq \tau \,|\, \text{non-matching } Q \text{ and } R). \tag{3}$$

By definition $\mathsf{FNMR}(\cdot)$ is a decreasing function and $\mathsf{FMR}(\cdot)$ is increasing fulfilling

$$\mathsf{FNMR}(\tau) \to 0 \text{ and } \mathsf{FMR}(\tau) \to 1 \text{ as } \tau \to \infty \tag{4}$$

and it seems hard to believe that false decisions can be avoided in biometric system. Instead we aim at finding a good trade-off between these two error probabilities by choosing a suitable threshold τ.[4]

3.3. Authentication. The biometric authentication problem can be considered as a generalization of the comparison problem in which not only a one-to-one decision is required but a one-to-many decision. That is, given a dataset **DB** of reference templates and a query template Q, decide whether there exists a matching $R \in \mathbf{DB}$. Using a biometric comparison function, we may solve the biometric authentication problem in a straightforward way by successively applying it to all reference templates; if the result for (at least) one reference template is a match, we may decide that there exists a matching reference template. The error rates of such an authentication decision can be expressed in terms of the $\mathsf{FNMR}(\cdot)$ and $\mathsf{FMR}(\cdot)$. Most notably, the false match rate may be significantly higher for large $|\mathbf{DB}|$. Furthermore, it is important to note that typically the evaluation of a discriminative distance function dist leading to low error rates can easily be comparably time-consuming.

To overcome the above problems one may decide to attach a username along with the reference templates; on authentication, the user provides a fresh query template and his username; then, a biometric comparison decision is derived for the query template and

[4] At a glance, one may consider the *equal error rate*, i.e. the error rate at the threshold where $\mathsf{FNMR}(\cdot)$ and $\mathsf{FMR}(\cdot)$ are equal, as a reasonable trade-off. However, we stress that the kind of application may dictate how to bound error probabilities: For example, it may be unacceptable that an impostor gains access to a nuclear power plant with probability equals to the equal error rate in case it turns out to be 0.5%.

for the reference template attached with the username; if the result is positive, access is granted and otherwise, denied. Though this approach can avoid the aforementioned issues, it may be associated with some of the user convenience problems of mere password-based authentication that biometry is intended to resolve. For example, the user still has to remember a username or has to carry a smartcard that he might lose. To overcome these issues, we may nonetheless attempt to establish full biometric-based authentication systems.

In an automatic biometric authentication system one typically filters out a short list from **DB** using a fast distance function. In this way, many non-matching reference templates can be dismissed and a time-consuming biometric decision must be applied to a significant fraction of **DB** only. The problem of generating a shortlist falls under the term *biometric identification* and is affected by another error rate.

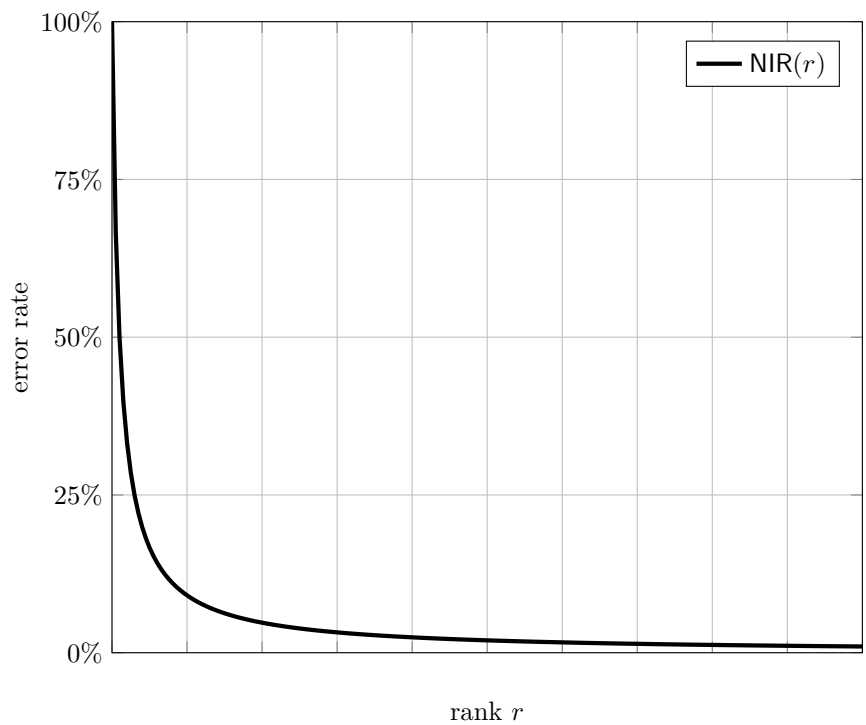


Fig. 3. Visualization of a biometric comparison system's negative identification rate

3.4. Identification. Assume that a user provides his query template Q with which an authentication server aims to filter out a shortlist of matching candidates from a database of reference templates $\mathbf{DB} = \{R_1, \ldots, R_N\}$ as part of an authentication process. Therefore, the authentication server can utilize a distance function

$$\mathsf{qdist} : \mathbf{U} \times \mathbf{U} \to \mathbb{R}_{\geq 0} \tag{5}$$

being faster, though less reliable, than the verification distance function dist from (1). The server knows in advance how many elements r the shortlist will contain each having

distance to Q belonging to the r smallest among all templates from **DB**; more specifically, the server computes the distances $d_j = \mathsf{qdist}(Q, R_j)$ and sorts them such that $d_{j_1} \leq \ldots \leq d_{j_N}$; finally, the shortlist is chosen as

$$\mathbf{S} = \{R_{j_1}, \ldots, R_{j_r}\}. \tag{6}$$

If **S** contains a reference template matching with Q, then after successively applying a more reliable verification process to the elements from **S**, the user will be accepted with probability at least $1 - \mathsf{FNMR}$. The probability that a matching reference template is not contained in **S** is defined as the *negative identification rate* and can be considered as a function in r denoted by $\mathsf{NIR}(r)$. In a good identification scheme $\mathsf{NIR}(r)$ quickly approaches 0 already for small r/N (see Fig. 3 for an illustration).

4. Biometric security. A biometric authentication system requires biometric information to be stored on a database, personal devices, or smartcards. Biometric security is concerned with the task to ensure that the biometric templates of enrolled users' will be used for no other but the intended purpose, e.g. authentication; and since biometric information may contain sensitive information, a legitimate requirement for biometric systems is to guarantee anonymity/privacy of users. To reach these goals we may develop techniques for storing biometric templates in a transformed protected way (*private template*) such that they leak no significant information unless a reasonably similar (probably matching) template is given.

Requirements of protected biometric information are prescribed by international standards [9]. These include the

- *irreversibility requirement* which is to guarantee that no *significant* information about the original biometric template can be determined from the private templates while, at the same time, allowing efficient private template generation (one-way property). We discuss in Section 5 some weaknesses and sharpening of this notion.
- *unlinkability requirement* in which it must not be possible to decide with reasonable accuracy whether two private templates have been generated from matching templates; in such a way, it can, in particular, be ensured that the activity of an individual being registered at multiple biometric systems cannot be traced back, which otherwise might result in privacy problems. It is important to note that the standard [9] dictates unlinkability even for private templates generated from identical (not only matching) biometric templates.

These requirements look similar to those of a classical cryptographic application. It is, however, important to note that private templates must have another obvious property as well; namely, they must be

- *usable* meaning that they allow genuine authentication with a low false non-match rate FNMR.

We shall continue with outlining some of the popular existing approaches and techniques proposed for implementing biometric template protection.

4.1. Cancelable biometrics. Roughly speaking, a *cancelable biometric* is generated from a biometric template by passing it through a repeatable but irrevertible transform $\mathsf{CB}(\cdot)$. On comparison, the query template is input to the same transformation such that a comparison decisions can be derived on base of a distance function operating in the encrypted domain. Ratha *et al.* [21] were the first who proposed the concept of applying non-invertible transforms to achieve biometric template protection.

4.1.1. *Hill-climbing.* A serious problem concerning the irreversibility requirement of cancelable biometrics is the inherent problem of *hill-climbing attacks* [1]. Therefore, assume that an intruder could intercept a private cancelable biometric-based template $\mathsf{CB}(R)$ and has access to the distance function dist on which base comparison scores are derived in the cancelable biometric's encrypted domain. To revert $\mathsf{CB}(R)$, the intruder might attempt to find a template Q such that $\mathsf{dist}(\mathsf{CB}(R), \mathsf{CB}(Q))$ becomes minimal, i.e. zero. This problem can be usefully conceptualized as an optimization problem in which the target function

$$\mathbf{U} \to \mathbb{R}_{\geq 0}, \quad x \mapsto \mathsf{dist}(\mathsf{CB}(R), \mathsf{CB}(x)), \tag{7}$$

is to be minimized. Approaches that pose a potential threat for a cancelable biometric-based system are given by well-known numerical and statistical optimization strategies: *steepest descent methods*, *convex optimization*, *simulated annealing* etc.

One may argue that a solution to the above optimization problem does not necessarily imply recovery of the original template nor recovery of a similar template. Yet, it is now a widely accepted notion that for a cancelable biometric it is feasible to exploit hill-climbing to generate (at least) a falsely matching template of which distance falls below the system comparison threshold. In such a way, an impostor can create an artificial biometric instance (e.g. a gummy finger) from which he can hope that a falsely matching biometric template can be extracted on authentication. Thus, this increases an impostor's chance to get successfully authenticated in a cancelable biometrics-based system.

It is due to the threat given by hill-climbing attacks that, in a server/client scenario, the mere use of cancelable biometrics do not pose a suitable measure on the server-side to be sufficiently convinced that an authenticating client is in fact legitimate. In other words, cancelable biometrics are not suitable to operate in *verification mode* (though it has the potential to run in a secure identification mode). A possible alternative or supplement is given by the concept of a biometric cryptosystem.

4.2. Biometric cryptosystems. The concept of a *biometric cryptosystem* can be outlined as follows: A cryptographic key is bound to the biometric template in a way that the key hides the template and vice versa, thereby generating a private template; on verification, using a sufficiently similar query template, verifiable information about the cryptographic key can be reconstructed. We continue by describing the functioning of a specific such biometric cryptosystem.

4.2.1. *Fuzzy commitment scheme.* In 1999, Juels and Wattenberg [13] proposed the *fuzzy commitment scheme*. Assume that a biometric sample is encoded as an n-length feature vector $w \in \mathbf{F}^n$ with entries in a finite field $\mathbf{F}$; furthermore, let $c \in \mathbf{C}$ be a codeword

encoding a cryptographic key chosen from a linear error-correcting code $\mathbf{C} \subset \mathbf{F}^n$.[5] On enrollment, the feature vector w and the codeword c are used to obfuscate the other by publishing the *fuzzy commitment* $\mathbf{f} = w + c$. From $\mathbf{f}$ it should be hard to recover the feature vector w or the codeword c. Typically, one also stores a cryptographic hash $h(c)$ of the correct codeword along with $\mathbf{f}$. On verification, using another feature vector $v \in \mathbf{F}^n$, the difference $\mathbf{f} - v = c + (w - v)$ can be corrected to c if $|w - v| \leq (\delta - 1)/2$ where $|\cdot|$ denotes the *Hamming weight* of a vector and δ denotes the minimal distance of the code $\mathbf{C}$; the recovery of the correct codeword can be verified using the hash $h(c)$. Otherwise, if $|w - v| > (\delta - 1)/2$, then, most likely, an attempt to decode $w - v$ produces a decoding failure.

Recovery attacks. If we assume, for simplicity, that biometric feature vectors are distributed uniformly among all $w \in \mathbf{F}^n$, then finding the correct template w from the record $\mathbf{f}$ is as hard as iterating through all codewords in $\mathbf{C}$ or, if accessible, reverting the cryptographic hash $h(c)$ [13]. It is important to note, that the assumption that feature vectors are distributed uniformly among all $\mathbf{F}^n$ typically leads to severe overestimation of the real system security. Later in the context of the similar *fuzzy vault scheme* (Section 4.2.2) we will discuss the problem in more detail.

Linkage attacks. Simoens *et al.* [25] analyzed the *decodability attack* conflicting with the *unlinkability requirement* for the important case in which the code $\mathbf{C}$ is linear: Given two fuzzy commitments $\mathbf{f}_1 = w_1 + c_1$ and $\mathbf{f}_2 = w_2 + c_2$ known to an impostor, he might try to determine whether w_1 and w_2 stem from the same instance: Since $\mathbf{f}_1 - \mathbf{f}_2 = (c_1 - c_2) + (w_1 - w_2)$ and since $\mathbf{C}$ is linear, the intruder can decode $\mathbf{f}_1 - \mathbf{f}_2$ to $c_1 - c_2$ if $\mathbf{f}_1$ and $\mathbf{f}_2$ are *related*, i.e. if $|w_1 - w_2| \leq (\delta - 1)/2$; otherwise, in most cases an attempt to decode $\mathbf{f}_1 - \mathbf{f}_2$ will fail. Thus, just from decodability of $\mathbf{f}_1 - \mathbf{f}_2$ the intruder can distinguish related from non-related records.

Kelkboom *et al.* [14] proposed to apply record-specific but public permutation processes $P_1, P_2 \in \mathbf{F}^{n \times n}$ (here we use matrix representation of the permutation processes for notational convenience) to the feature vectors before private template generation. Then, determining whether two records $\mathbf{f}_1 = c_1 + P_1 w_1$ and $\mathbf{f}_2 = c_2 + P_2 w_2$ are related cannot be decided from decodability of $\mathbf{f}_1 - \mathbf{f}_2$.

However, Kelkboom *et al.* [14] have overlooked that by applying public permutation processes, they inadvertently generate another vulnerability also analyzed in [25] that conflicts with the unlinkability and irreversibility requirement.[6] In the following we summarize the problem by describing the simple connection between [14] and [25]. Let $G \in \mathbf{F}^{n \times k}$ be the generator matrix of the code $\mathbf{C}$. Since the permutation processes P_1 and P_2 are public the adversary can consider $P_1^{-1}\mathbf{f}_1$ and $P_2^{-1}\mathbf{f}_2$ as two fuzzy commitments protecting w_1 and w_2 built over codes $\mathbf{C}_1$ and $\mathbf{C}_2$ generated by the matrices $G_1 = P_1^{-1}G$ and $G_2 = P_2^{-1}G$, respectively. There exist codewords $c_1' \in \mathbf{C}_1$ and $c_2' \in \mathbf{C}_2$ (specifically,

[5] For details on error-correcting codes we refer to one of the good textbooks available in the literature, for example [2].

[6] We did not find this observation mentioned in the literature except in slides that we have found online: `http://www.cosic.esat.kuleuven.be/vandermeulen/slides/van-der-meulen-seminar_2011-12-07.pdf`

$c'_1 = P_1^{-1}c_1$ and $c'_2 = P_2^{-1}c_2$) such that $P^{-1}\mathbf{f}_1 = c'_1 + w_1$ and $P_2^{-1}\mathbf{f}_2 = c'_2 + w_2$. Assume that $e = w_1 - w_2$ is the error pattern between the feature vectors correctly guessed by an attacker. Then, the linear system $(G_1|G_2)m^\top = \mathbf{f}_1 - \mathbf{f}_2 - e$ is solvable. Write $m^\top = (m_1^\top | - m_2^\top)$ with $m_1, m_2 \in \mathbf{F}^k$ for a solution to $c'_1 = G_1 m_1$ and $c'_2 = G_2 m_2$. Finally, using the relations $w_1 = P_1^{-1}\mathbf{f}_1 - c'_1$ and $w_2 = P_2^{-1}\mathbf{f}_2 - c'_2$ the protected feature vectors can even be recovered.

One may argue that the above attack requires the error pattern e to be guessed correctly which may be infeasible for large $|e|$. Moreover, the attack can only yield an advantage if the rank of $(G_1|G_2)$ is smaller than n which assumes that $k < n/2$. We stress, however, that the international standard [9] explicitly requires unlinkability even if $|e| = 0$ in which case the error pattern is known to be zero. Furthermore, a typically high intra-class variance of biometric measurements easily requires that $k \ll n$ which easily results in the property that $(G_1|G_2)$ is of rank much smaller than n.

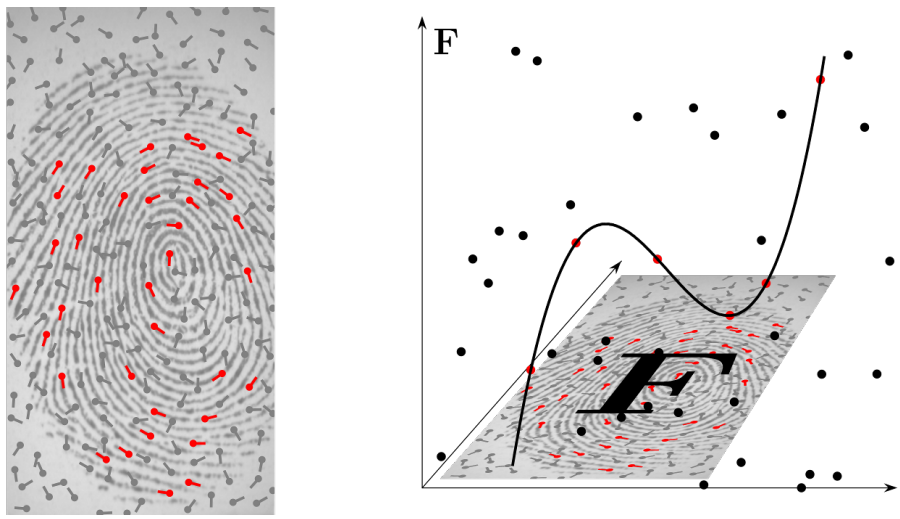
We may ask whether linkage attacks in a fuzzy commitment scheme can be prevented by replacing the permutation processes by another kind of transform preserving the Hamming distance. In fact, when applying a record-specific field permutation $\mathbf{F} \to \mathbf{F}$ component-wisely to each feature vector, no known attack appears to be feasible for sufficiently large $|\mathbf{F}|$. On the other hand, many implementations to the fuzzy commitment scheme operate with binary fuzzy commitment schemes in which $|\mathbf{F}| = 2$. For this important case, we can, however, prove that each transformation preserving the Hamming distance essentially assumes to be a permutation process (see Claim A.1 in the appendix) and the above attack cannot be prevented by this means.

One may argue that other measures may be applied to prevent linkage attacks in a binary fuzzy commitment scheme (e.g. using non-linear codes, extracting record-specific feature bits only, etc.). Yet, we stress that the problem mentioned above is hardly discussed in the literature and may therefore conclude that achieving unlinkability in a fuzzy commitment scheme belongs to the open questions and challenges in biometric security.

4.2.2. *Fuzzy vault scheme.* In 2002, Juels and Sudan proposed the *fuzzy vault scheme* [11, 12]. Instead of assuming that biometric templates are encoded as fixed-length feature vectors, in a fuzzy vault scheme one assumes that biometric templates are encoded as sets encoding elements in an underlying finite field $\mathbf{F}$. An example of a biometric modality of which features are predestined to be represented as sets are fingerprint minutiae: Each minutia can be encoded as a binary bit string that encodes an element from a binary finite field.

Given a set of s reference features (e.g. minutiae) encoded as $\mathbf{A} \subset \mathbf{F}$, the private template is generated as follows. As in other biometric cryptosystems, a cryptographic key is generated at random and bound to $\mathbf{A}$. Therefore, the key is encoded as a polynomial of degree smaller than k (where $k \ll s$) with coefficients in $\mathbf{F}$, i.e. $f \in \mathbf{F}[X]$. The set of *genuine pairs* $\mathbf{G} = \{(a, f(a)) \,|\, a \in \mathbf{A}\}$ is generated of which abscissas encode the feature elements and of which interpolation polynomial is equal to f. Thereby, the cryptographic key has been bound to the feature set. To hide the genuine pairs, a certain number of spurious chaff pairs $\mathbf{C} = \{(x, y)\}$ is generated such that the $x \notin \mathbf{A}$ encode spurious chaff features where the y are chosen uniformly at random with $y \neq f(x)$. The union

$\mathbf{V} = \mathbf{G} \cup \mathbf{C}$ essentially represents the private template from which it should be hard to distinguish the genuine pairs from the chaff; in a typical implementation, we also store a cryptographic hash value $h(f)$ along with $\mathbf{V}$ to allow safe verification.



(a) (b)

Fig. 4. Visualization of a minutiae-based fuzzy vault:
(a) A fingerprint's genuine minutiae (red) are hidden among a large number of chaff minutiae (gray);
(b) genuine minutiae are bound to a cryptographic key encoded as a polynomial

On verification, given a vault record $(\mathbf{V}, h(f))$ and a query feature set,[7] those vault pairs $\mathbf{U} \subset \mathbf{V}$ are extracted of which abscissa encode a feature well approximated by an element in the query set. If the reference template protected by the vault and the query set are matching, then we expect $\mathbf{U}$ to contain a significant amount of genuine pairs lying on the graph of the secret polynomial f. In particular, if $\mathbf{U}$ contains at least $(|\mathbf{U}|+k)/2$ genuine pairs, then f can be recovered efficiently using algorithms for decoding Reed–Solomon codes [7].[8] Note that the correctness of f can be verified using $h(f)$. If successful, we may accept and, otherwise, reject the verification attempt.

Recovery attacks. An attacker who has intercepted a vault record $(\mathbf{V}, h(f))$ might try to find the secret polynomial $f \in \mathbf{F}[X]$; if successfully found, he may reconstruct the feature set by checking which vault pairs $(x, y) \in \mathbf{V}$ lies on the graph of f, i.e. $y = f(x)$. The converse works, too: If an attacker is able to recover the feature set $\mathbf{A}$, then he may compute the interpolation polynomial of those vault pairs of which abscissa values are contained in $\mathbf{A}$; this interpolation polynomial will be equal to f. Thus, without loss of

[7] In presences of a minutiae-based fuzzy vault a mechanism must be implemented in which a correct alignment of the query minutiae is approximated; for example, see [19, 26]. For simplicity, we do not discuss such methods but stress their importance.

[8] There exist polynomial-time algorithm that can successfully recover f if there are more than $\sqrt{(k-1)|\mathbf{U}|}$ genuine pairs contained in $\mathbf{U}$ [8].

generality we may try to recover a vault record's secret polynomial (which is equivalent to recovering the feature sets).

There are multiple strategies to derive f from $(\mathbf{V}, h(f))$. For example, the attacker might try to guess f directly which is equivalent to guessing k elements from $\mathbf{F}$ and requires approximately $|\mathbf{F}|^k$ steps. However, there are more efficient ways. In 2009, Mihăilescu *et al.* [18] analyzed the following brute-force attack:

1. Guess k genuine pair candidates randomly from $\mathbf{V}$;
2. compute the candidate pairs' interpolation polynomial f^* which is of degree smaller than k;
3. check whether $h(f^*) = h(f)$ and, if true, return f^*; otherwise, go to Step 1.

The probability that in Step 1 all k guesses are genuine is equal to $p = \binom{s}{k} \cdot \binom{n}{k}^{-1}$ (where $n = |\mathbf{V}|$ and $s = |\mathbf{A}|$) and thus we can expect to successfully recover f from $(\mathbf{V}, h(f))$ after approximately $1/p$ iterations of the above attack yielding a notion of *brute-force security.*

A typical application of the fuzzy vault scheme is the protection of fingerprint features such as minutiae [19] in which $(n, s, k) = (224, 24, 11)$ yielding to a brute-force security of approximately 2^{39}; this is rather low from a cryptographic point of view.

Brute-force security is often used as the mere measure to assess the security in an implementation of a fuzzy vault. However, brute-force security does not exploit the distribution of biometric template features which is typically neither uniformly nor independently distributed. An example of an attack that accounts for the distribution of features is the *false-accept attack* in which we assume that the attacker has access to a sufficiently large database containing feature sets from real biometric data:

1. For each feature set from the database simulate a verification attempt;
2. if successful, return f; otherwise, continue with Step 1.

The probability that a single verification attempt will be successful is equal to the false match rate FMR of the fuzzy vault system. It is important to note that the attacker is not forced to follow a certain verification protocol; he may choose a protocol that minimizes the overall effort in running a false-accept attack. In [26] an analyse of the false-accept attack for a specific implementation to fingerprint is given that results in the observation that brute-force security tends to significantly overestimate any realistic security measure. For example, at a configuration for which brute-force security evaluates to 2^{52}, a false-accept attack suggests a security of only 2^{31}. Since in a fuzzy vault system a false match is equivalent to recovery of the protected biometric template we cannot expect the irreversibility requirement to be met if the false match rate is not sufficiently small. A possible way out could be the fusion of multiple biometric modalities (e.g. multiple fingerprint templates extracted from 4, say, fingers) and implement a multi-biometric fuzzy vault system with a sufficiently small false match rate.

Linkage attacks. In general, the fuzzy vault scheme is vulnerable to a very serious linkage attack [23]. Observe that in a fuzzy vault, the genuine features stem from a biometric sample while the chaff features have been generated at random. If two fuzzy vault record can be intercepted by an intruder protecting templates that stem from the same instance

(e.g. the same finger) we may observe that the genuine vault features in the first record (e.g. red-colored minutiae in Fig. 5(a)) well agree with the genuine vault features in the second record (blue-colored in Fig. 5(b)), i.e. they correlate well as compared to the chaff features (Fig. 5(c) and Fig. 5(d)). This property can be exploited by an intruder to distinguish related from unrelated vault correspondences. Even worse, an intruder who has intercepted two related vault records may even unlock the vaults using the candidate sets of genuine vault features. In fact, for a minutiae-based fuzzy vault implementation, Kholmatov and Yanikoglu [15] demonstrated that an intruder can break two related vault correspondences with success probability of order 60%, which is much too high for a system to fulfill the unlinkability and irreversibility requirement. The possibility of running the so-called *correlation attack* calls for a valid countermeasure.

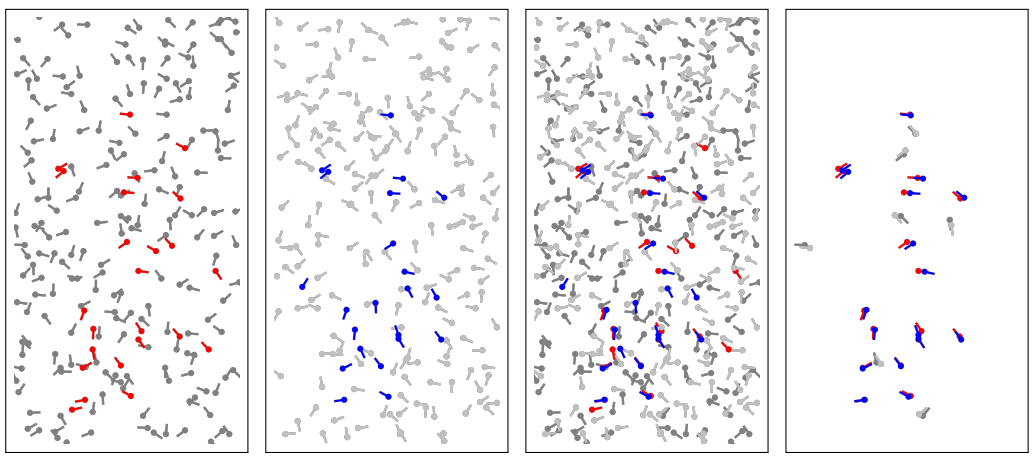
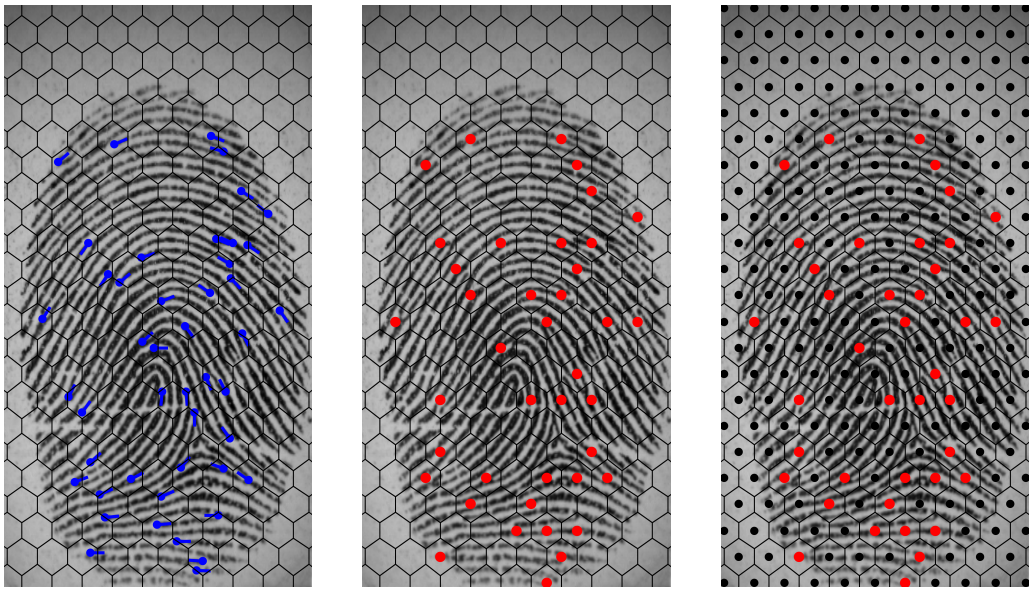


Fig. 5. Visualization of the correlation attack process in a minutiae-based fuzzy vault: those vault minutiae of two related vaults (a) and (b) are correlated (c) and those vault minutiae that well agree have a quite good chance to be genuine minutiae (d) being colored red and blue for the first and second vault, respectively

4.2.3. *Improved fuzzy vault scheme.* The correlation attack in a fuzzy vault scheme yields an advantage to an attacker in linking and breaking two related records due to the fact that the chaff is generated at random while the genuine features stem from the same instance thereby essentially being fixed (up to tolerable noise). We may avoid this issue in a fuzzy vault scheme by a simple yet effective variation, which we describe next, in informal terms, for fingerprint minutiae. A grid (e.g. rectangular or hexagonal) is laid over the fingerprint image; each genuine minutia is rounded to grid coordinates that are then used to build the genuine features, thereby passing the genuine minutia through a quantization scheme (we may also quantize the minutia angles in a similar manner). All other, unoccupied grid coordinates are used as the chaff. Consequently, there is no correlation that can be exploited in an attack, since the feature sets are equal for any two records. On verification, query minutiae must be quantized, too, in order to identify genuine pair candidates from the vault to extract unlocking pairs. We are therefore not able to tolerate noise at the feature level but require a sufficiently number of features

to be exactly measurable. This may negatively affect verification performance but avoids correlation attacks.



(a) (b) (c)

Fig. 6. Visualization of how to make a minutiae-based fuzzy vault resistant against the correlation attack: (a) The genuine minutiae are rounded/quantized as coordinates of a (for example) hexagonal grid (b) and all other unoccupied grid coordinates are used as the chaff (c)

If a maximal number of chaff is used, as above, then a modified fuzzy vault scheme proposed by Dodis *et al.* in 2004 [6, 5] can be used to protect a feature set $\mathbf{A} \subset \mathbf{F}$. Essentially, vault pairs can be encoded by the polynomial

$$V(X) = f(X) + \prod_{a \in \mathbf{A}} (X - a) \tag{8}$$

where $f \in \mathbf{F}[X]$ is a secret polynomial of degree smaller than k as in the original fuzzy vault construction. If $x \in \mathbf{A}$, then $V(x) = f(x)$ and thus $(x, V(x))$ is a genuine pair; otherwise, if $x \notin \mathbf{A}$, then $V(x) \neq f(x)$ and thus $(x, V(x))$ is a chaff pair. In such a way reversibility attacks can be adopted from the original fuzzy vault construction.

Linkage attacks. It is an obvious property of the improved fuzzy vault scheme that the correlation attack cannot be exploited to attack unlinkability. However, in 2013, Blanton and Aliasgari [3] observed that, given $V(X)$ as in (8) and a second record

$$W(X) = g(X) + \prod_{b \in \mathbf{B}} (X - b) \tag{9}$$

protecting the feature sets $\mathbf{A}$ and $\mathbf{B}$ of size s with $\deg(f), \deg(g) < k$, such that $|\mathbf{A} \cap \mathbf{B}| \geq (s + k)/2$, then the set differences $\mathbf{A} \setminus \mathbf{B}$ and $\mathbf{B} \setminus \mathbf{A}$ can be recovered explicitly by solving a system of non-linear equations. In particular, if $\mathbf{A} = \mathbf{B}$, an attacker may observe that the upper $s - k$ coefficients of $V(X)$ and $W(X)$ are equal which is hardly the case for

$\mathbf{A} \neq \mathbf{B}$. We can therefore not guarantee that the improved fuzzy vault scheme fulfills the unlinkability requirement (Section 4).

For the general case $|\mathbf{A} \cap \mathbf{B}| \geq (s+k)/2$, Blanton and Aliasgari argued that recovery of the feature sets' differences is computationally hard since solving a system of non-linear equations is NP hard in general. However, Merkle and Tams [17] observed that the extended Euclidean algorithm can be used to efficiently solve the equations established by Blanton and Aliasgari. In particular, if (without loss of generality $s \geq t$) $R_j = P_j \cdot V + Q_j \cdot W$ denotes the sequence in the extended Euclidean algorithm applied to V and W, then there exists j_0 such that P_{j_0} and Q_{j_0} split into linear factors whose roots coincide with $\mathbf{B} \setminus \mathbf{A}$ and $\mathbf{A} \setminus \mathbf{B}$, respectively.[9]

Merkle and Tams [17] also contribute a discussion on how to prevent linkage attacks in an improved fuzzy vault scheme. In our view, a promising approach is to pass the feature elements through a random but public permutation process $\sigma : \mathbf{F} \to \mathbf{F}$; instead of protecting a non-shuffled feature set $\mathbf{A}$, the shuffled set $\sigma(\mathbf{A}) = \{\sigma(a) \,|\, a \in \mathbf{A}\}$ is protected. Note that, due to the publicity of σ, the verification procedure can be easily adjusted by passing the query feature set through σ as well. Also note that σ can be encoded by a compact seed stored along with the vault record;[10] in such a way, it is not necessary to store the full permutation table. An attacker who has intercepted two vault records $V(X) = f(X) + \prod_{a \in \mathbf{A}}(X - \sigma_1(a))$ and $W(X) = g(X) + \prod_{b \in \mathbf{B}}(X - \sigma_2(a))$ subject to two different field permutations $\sigma_1, \sigma_2 : \mathbf{F} \to \mathbf{F}$ and wants to exploit the attack from [3, 17] to attack unlinkability, requires $|\sigma_1(\mathbf{A}) \cap \sigma_2(\mathbf{B})| \geq (s+k)/2$ to be fulfilled,[11] a probability easily negligible for sufficiently large $|\mathbf{F}|$ and random σ_1, σ_2.

Although an attacker can compute the inverse of public permutation processes, he may, however, not be able to re-order the features protected by a vault record unless and until he has recovered them. Yet, it would be desirable to find a mathematical proof to support this assumption or, alternatively, to find an effective attack exploiting the publicity of the permutation process as a counterexample.

4.2.4. *Other approaches.* There exist other schemes to implement biometric template protection and we briefly give an overview of them. For a comprehensive survey of these schemes and specific implementations thereof we refer to [22].

A first approach to implement biometric template protection goes back to Tomko *et al.* in 1994 [28] in which fingerprint images are protected via Fourier transforms, thereby achieving translation invariance and making it even easier to cope with rotation. However, usability and security issues were discovered quickly. In 1998, Davida *et al.* [4] proposed to extract error-correcting check bits from biometric templates encoded as binary feature vectors which can be used on verification with a sufficiently similar query template to reconstruct the original template of which correctness can be verified by means of a cryptographic hash.[12] In 2004, Dodis *et al.* [6, 5] presented and analyzed a variety of

[9] More specifically, j_0 is such that $\deg(Q_{j_0})$ is minimal where $\deg(Q_{j_0}) + k > \deg(R_{j_0})$.

[10] If a cryptographic hash $h(f)$ is part of the vault record, then $h(f)$ can be used to encode a seed for a field permutation leading avoiding any deflate of record sizes.

[11] The relation $|\mathbf{A} \cap \mathbf{B}| \geq (s+k)/2$ is neither sufficient nor necessary.

[12] The construction of Davida *et al.* [4] is quite similar to the fuzzy commitment scheme [13].

template protection schemes under the term *fuzzy sketch* and *fuzzy extractor* on the basis of error-correcting codes including the improved fuzzy vault scheme (Section 4.2.3).

In the authors' view it seems safe to claim that most schemes considered to implement biometric template protection are based on either the fuzzy commitment scheme, the fuzzy vault scheme or a cancelable biometric approach. In presence of a non-negligible false match rate, the first two schemes cannot guarantee the irreversibility requirement to be met, while in a cancelable biometric-based scheme irreversibility may be affected by hill-climbing attacks. As a result algorithms have been proposed that combine template protection schemes with a user password (e.g. see [27, 20]). If carefully implemented, weaker passwords can be used to reach a similar security level but requiring less effort from system users to memorize them. On the other hand, it seems obvious that data can be protected via keys and that this can increase security while also negatively affecting usability. Furthermore, measuring a zero false match rate for systems with user passwords makes it hard to compare usability and security, the latter often being completely delegated to the assumption that user passwords can be kept secret — a key management problem thus for which biometry has been promoted as a possible way out.

5. Biometric irreversibility. As mentioned above, the condition of irreversibility when applied to biometric cryptosystems such as the fuzzy commitment scheme and the fuzzy vault scheme should imply that a template that is stored indirectly by means of these schemes should not be recoverable. The condition is however flue, since an attacker does in fact not need to be in possession of a perfect recovery in order get falsely verified in front of a fuzzy commitment or a fuzzy vault in order to impersonate another user. Therefore reversibility should rather be defined in a way that is related directly to the most immediate goal of an attack, which is the impersonation attack. We propose here the following statistical definition of reversibility.

DEFINITION 5.1. Let S be a scheme implemented for the protection of biometric templates, which allows identification in protected mode.[13] Consider the template T of a genuine user Alice. We say that the scheme is ε, δ-reversible, if an intruder Eve can succeed with *affordable efforts* and within a success rate of $1 - \varepsilon$ to produce templates that can pass for the template T and thus may be used for an impersonation attack of Alice, and this with a success rate of at least $1 - \delta$.

Certainly, this definition becomes useful if the term of an affordable attack is better connected to notions of complexity. We choose not to do this in this paper, and prefer instead to add some discussion of the notion and of realistic security issues, and the way they may be better expressed and understood in the future, by using improvements of the above definition. The fuzzy schemes mentioned above, for instance, have the property that even on a false match produced by an impostor, he can recover the original biometric template, e.g. encoded as a feature vector or a feature set. In order for a private template

[13] Examples of such schemes are the fuzzy vault and the fuzzy commitment, together with numerous variants thereof. But also cryptographic template protection schemes belong to the larger scope of this definition.

generated with such a biometric cryptosystem to fulfill the standardized irreversibility requirement, a sufficiently low false match rate FMR is required. Otherwise, false accept attacks are a serious limitation to "irreversibility". In fact we already see that the notion of irreversibility becomes impractical, since it allows for no gradual definition, where in reality, the performance of attacks is statistical, it also depends on the quality of the original (private) template, and this behavior must be reflected in the definition.

If an irrevertible biometric verification system has a too coarse FMR, then the system must be designed such that a false match does not allow recovery of the original template. Both the fuzzy commitment scheme and the fuzzy vault scheme do not have this property and one may ask whether there exist a working alternative. In 2012, Simoens *et al.* [24] showed that every verification scheme for binary n-length feature vectors that outputs a positive match decision if and only if a query template is provided that sufficiently agrees (by means of the Hamming distance) with the reference template cannot provide this. More specifically, if an attacker can produce a false accept, he can even fully recover the bits of the reference template within $O(n)$ evaluations of the verification protocol. The attack, called *center search attack*, is outlined in the appendix (Section A.2). One can easily generalize the attack for verification systems working with non-binary feature vectors having entries in a finite set of symbols $\mathbf{S}$ to derive the original template from a false match within $O(|\mathbf{S}| \cdot n)$ evaluations of the verification protocol. Furthermore, since feature sets encoded as subsets of the universe $\mathbf{E}$ can be transformed into binary feature vectors of length $|\mathbf{E}|$ (and vice versa), even constructions for feature sets are vulnerable to the center search attack within $O(|\mathbf{E}|)$ evaluations of the verification protocol (details are given in the appendix in Section A.2). The situation in biometry is somehow related, in as much as it is statistical in nature too. However, the complexity bounds, and the statistical dependencies are of natural and physical origin, unlike the examples in the paper of Simoens *et al.* [24].

5.1. The need for low false match rates. One could try to develop schemes and biometric templates encodings for which center search attacks do not apply. However, as already mentioned in the beginning of Section 5, for the purpose of malicious authentication an adversary may not require to fully recover the original template's encoding but may already be satisfied to just generate a false match. Thus, we advocate to require a sufficiently low false match rate FMR from a secure verification system in order to fulfill the irreversibility requirement. In particular, given the average time for running the verification protocol AVT, an attacker having intercepted a private template can run a false-accept attack as detailed in Section 4.2.2 (page 133); thereby, he can expect to successfully produce a false match after an effort of

$$\frac{\log(0.5)}{\log(1-\mathsf{FMR})} \cdot \mathsf{AVT} \tag{10}$$

and this size must be sufficiently large — ideally within cryptographic bounds — for the irreversibility requirement to be met.

It is an interesting question to investigate whether in biometrical practice, one can consider reversibility attacks as $(1-\varepsilon, 1-\delta)$ *oracles* — i.e. oracles providing a $(1-\varepsilon, 1-\delta)$ reversion of a fixed template T and to improve the characteristics ε, δ by iterated use of

the oracle. One may ask if it is possible to obtain exponentially small ε, δ in polynomially many iterations, for instance. These questions are related to *hill climbing attacks* and *center search attacks* which have been considered in the literature.

6. Summary. In this discussion paper, we gave a motivation for biometry-based authentication systems as an alternative to password-based authentication schemes. We described general approaches that can help in storing biometric information in a protected way. We discussed a problem of a popular technique, the fuzzy commitment scheme, with fulfilling the unlinkability requirement — an important property that is explicitly request by an international standard; but, argued that, in principle, unlinkability may be an achievable goal, e.g. with the improved fuzzy vault scheme. On the other hand, in order for protected biometric to be irrevertible, the false match rate of biometric systems needs to be sufficiently low. We may therefore conclude that the implementation of a usable secure biometric system with convincing estimations of sufficiently low false match rates belongs to the main challenges of future work. It is important to note that the false match rate depends on the relative information that can be extracted from the incorporated biometry and it seems hard to believe that modalities such as single fingerprint can provide a sufficient amount of relative information. Instead multi-finger systems or even multiple biometric modalities should be used. We also proposed a statistical definition for the standard notion of reversibility, and provided evidence for the need to use this approach. This step is considered to be a useful one in the direction of developing formally clear and sound notions of security attacks in the domain of biometry.

A. Appendix

A.1. Ineffectiveness of public feature transforms to prevent linkage attacks in a binary fuzzy commitment scheme

Claim A.1. *Let $T : \{0,1\}^n \to \{0,1\}^n$ be a map that preserves the Hamming distance. Then there exists a permutation matrix $P \in \{0,1\}^{n\times n}$ such that $T(v) = Pv \oplus T(0)$ for every $v \in \{0,1\}^n$.*

Here we denote by $\{0,1\}$ the field with two elements and by $\oplus$ the addition of vectors with coefficients in $\{0,1\}$ which can be interpreted as an exclusive or-operation (note that subtraction is the same as addition over $\{0,1\}$).

By Claim A.1, every transformation through which feature vectors can be passed are permutations plus a constant shifting vector. Due to the publicity of the transformations an adversary can subtract the constant shift from any fuzzy commitment that he has intercepted generating the case in which an affine permutation process is applied.

To prove Claim A.1, first note that T must be bijective (as a map preserving the Hamming distance) since, otherwise, there would exist distinct vectors $v_1, v_2 \in \{0,1\}^n$ with $0 = |T(v_1) \oplus T(v_2)| = |v_1 \oplus v_2| \neq 0$ which is a contradiction.

Let $\hat{T} : \{0,1\}^n \to \{0,1\}^n$, $v \mapsto T(v) \oplus T(0)$. Note that

$$|v \oplus v'| = |T(v) \oplus T(v')| = |T(v) \oplus T(v') \oplus T(0) \oplus T(0)| = |\hat{T}(v) \oplus \hat{T}(v')|;$$

consequently, $\hat{T}$ preserves the Hamming distance, too, and is thus bijective as well. Furthermore, since $|v| = |v \oplus 0| = |T(v) \oplus T(0)| = |\hat{T}(v)|$, $\hat{T}$ also preserves the Hamming weight.

It remains to show that the map $\hat{T}$ is a bit permutation process to which the following lemma is a key.

LEMMA A.2. *Let $\hat{T} : \{0,1\}^n \to \{0,1\}^n$ be a map that preserves the Hamming distance and the Hamming weight. For every list of distinct unity vectors $e_1, \ldots, e_\ell \in \{0,1\}^n$, $0 \leq \ell \leq n$, the equality $\hat{T}(e_1 \oplus \ldots \oplus e_\ell) = \hat{T}(e_1) \oplus \ldots \oplus \hat{T}(e_\ell)$ holds.*

Proof. From the preservation of the Hamming weight it follows that $\hat{T}(0) = 0$, so the statement holds for $\ell = 0$. Furthermore, the mappings $\hat{T}(e_1), \ldots, \hat{T}(e_\ell)$ are unity vectors and pairwise distinct (since $\hat{T}$ preserves the Hamming weight and is bijective). Note that $|\hat{T}(e_1 \oplus \ldots \oplus e_\ell) \oplus \hat{T}(e_j)| = \ell - 1$ and since the $\hat{T}(e_j)$ are all distinct, we obtain

$$\begin{aligned} \ell &> |\hat{T}(e_1 \oplus \ldots \oplus e_\ell) \oplus \hat{T}(e_1)| \\ &> |\hat{T}(e_1 \oplus \ldots \oplus e_\ell) \oplus \hat{T}(e_1) \oplus \hat{T}(e_2)| \\ &\vdots \\ &> |\hat{T}(e_1 \oplus \ldots \oplus e_\ell) \oplus \hat{T}(e_1) \oplus \ldots \oplus \hat{T}(e_\ell)| = 0 \end{aligned}$$

and the statement of the lemma follows. ∎

Due to the fact that every vector in $\{0,1\}^n$ can be written as the sum of unity vectors and applying Lemma A.2 recursively, it follows that $\hat{T}$ is linear and since $\hat{T}$ maps unity vectors to unity vectors, it must be a bit permutation process.

A.2. Center search attack. In this section, we review the center search attack formulated by Simoens *et al.* [24] which can be used to attack irreversibility in a verification system for (binary) feature vectors assuming that a false match is given.

A.2.1. *Attack for feature vectors.* By $\mathsf{hd}(\cdot,\cdot)$ we denote the *Hamming distance* between two binary feature vectors. Assume that an impostor has intercepted a private template generated from $w \in \{0,1\}^n$. By $\mathsf{verify} : \{0,1\}^n \to \{0,1\}$ we denote the biometric verification function accessible by the impostor that, when $v \in \{0,1\}^n$ is input, outputs 1 for $\mathsf{hd}(w,v) \leq \tau$ and 0 otherwise; here τ denotes a certain threshold. If the FMR is sufficiently large, then it is feasible for the impostor to construct a vector v with $\mathsf{verify}(v) = 1$, i.e. such that $\mathsf{hd}(w,v) \leq \tau$. We next show how the impostor can recover w from v after $2n - \tau$ evaluations of verify.

Write $v = (v_1, \ldots, v_n)$ with $v_i \in \{0,1\}$ and let $v^{(0)} = (\neg v_1, .., \neg v_j, v_{j'+1}, \ldots, v_n)$ be such that j' is maximal where $\mathsf{verify}(v^{(0)}) = 1$. Then, $\mathsf{hd}(w, v^{(0)}) = \tau$. Also note that $v^{(0)}$ can be found after at most $n - \tau$ evaluations of verify.

Now, let $v^{(j)}$ be the vector $v^{(0)}$ but with negated j-th entry, i.e. if we write $v^{(0)} = (v_1^{(0)}, \ldots, v_n^{(0)})$, then $v^{(0)} = (v_1^{(0)}, \ldots, v_{j-1}^{(0)}, \neg v_j^{(0)}, v_{j+1}^{(0)}, \ldots, v_n^{(0)})$. The entries of the original feature vector $w = (w_1, \ldots, w_n)$ fulfill $w_j = 1$ if $\mathsf{verify}(v^{(j)}) = 0$ and $w_j = 0$; otherwise if $\mathsf{verify}(v^{(j)}) = 1$, then $w_j = 0$.

In this way, any biometric verification system for binary feature vectors may be revertible if the false match rate FMR is too large. The attack can be easily generalized to

feature vectors with elements from a possibly larger set of symbols $\mathbf{S}$. With this attack, given a falsely matching initial vector, the original vector can be recovered after $|\mathbf{S}| \cdot n - \tau$. Consequently, irreversibility of any such biometric verification system can be successfully attacked after an expected number of at most

$$O(1/\mathsf{FMR}) + |\mathbf{S}| \cdot n - \tau$$

evaluations of the system's verification function.

A.2.2. *Attack for feature sets.* For constructions designed to protect feature sets, the center search attack [24] could be applied, too. Assume that features are encoded as elements from $\mathbf{E}$. By writing $\mathbf{E} = \{\alpha_1, \ldots, \alpha_n\}$ we can represent any feature set $\mathbf{A} \subset \mathbf{E}$ as the binary feature vector $w = (w_1, \ldots, w_n)$ where $w_i = 1$ if $\alpha_i \in \mathbf{A}$ and $w_i = 0$ otherwise. If the verification function outputs 1 if and only if it is input with a query set $\mathbf{B} \subset \mathbf{E}$ where $|\mathbf{A} \cap \mathbf{B}| \geq \omega$, then the center search attack [24] for binary feature vectors can be performed with $\tau = |\mathbf{A}| - \omega$; here we assume that ω is a known bound and also that $|\mathbf{A}|$ is known. In this way, a feature set protected by a private template can be recovered given a falsely matching query set by running $|\mathbf{E}| - \tau$ evaluations of the verification function.

Acknowledgments. B. Tams gratefully acknowledges the support of the Felix Bernstein Institute for Mathematical Statistics in the Biosciences and the Volkswagen Foundation.

References

[1] A. Adler, *Vulnerabilities in biometric encryption systems*, Audio and Video based Biometric Person Authentication, Lecture Notes in Comp. Sci. 3546, Springer, Berlin 2005, 1100–1109.

[2] R. E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge Univ. Press, Cambridge 2003.

[3] M. Blanton, M. Aliasgari, *Analysis of reusability of secure sketches and fuzzy extractors*, IEEE Trans. Inf. Forensics Security 8 (2013), 1433–1445.

[4] G. I. Davida, Y. Frankel, B. J. Matt, *On enabling secure applications through off-line biometric identification*, in: Security and Privacy – 1998 IEEE Symp. on Security and Privacy, IEEE Computer Soc., 1998, 148–157.

[5] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, *Fuzzy extractors: how to generate strong keys from biometrics and other noisy data*, SIAM J. Comput. 38 (2008), 97–139.

[6] Y. Dodis, L. Reyzin, A. Smith, *Fuzzy extractors: how to generate strong keys from biometrics and other noisy data*, in: Advances in Cryptology EUROCRYPT 2004, Lecture Notes in Comput. Sci. 3027, Springer, Berlin 2004, 523–540.

[7] S. Gao, *A new algorithm for decoding Reed–Solomon codes*, in: Communications, Information and Network Security, Springer, Berlin 2002, 55–68.

[8] V. Guruswami, M. Sudan, *Improved decoding of Reed–Solomon and algebraic-geometric codes*, IEEE Trans. Intell. Transp. Syst. 45 (1998), 1757–1767.

[9] ISO/IEC JTC1 SC2 Security Techniques, *ISO/IEC 24745:2011. Information Technology – Security Techniques – Biometric Information Protection*, International Organization for Standardization, 2011.

[10] A. K. Jain, P. Flynn, A. A. Ross, *Handbook of Biometrics*, Springer, New York 2008.
[11] A. Juels, M. Sudan, *A fuzzy vault scheme*, in: Information Theory 2002, Proc. 2002 Internat. Symp. on Information Theory, no. 408.
[12] A. Juels, M. Sudan, *A fuzzy vault scheme*, Design Codes Cryptogr. 38 (2006), 237–257.
[13] A. Juels, M. Wattenberg, *A fuzzy commitment scheme*, in: CCS '99 Proc. of the 6th ACM Conf. on Computer and Communications Security, 1999, 28–36.
[14] E. J. C. Kelkboom, J. Breebaart, T. A. M. Kevenaar, I. Buhan, R. N. Veldhuis, *Preventing the decodability attack based cross-matching in a fuzzy commitment scheme*, IEEE Trans. Inf. Forensics Security 6 (2011), 107–121.
[15] A. Kholmatov, B. Yanikoglu, *Realization of correlation attack against the fuzzy vault scheme*, in: Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, Proc. SPIE 6819 (2008).
[16] D. Maltoni, D. Maio, A. Jain, S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed., Springer, London 2009.
[17] J. Merkle, B. Tams, *Security of the improved fuzzy vault scheme in the presence of record multiplicity*, arXiv:1312.5225.
[18] P. Mihăilescu, A. Munk, B. Tams, *The fuzzy vault for fingerprints is vulnerable to brute force attack*, in: BIOSIG 2009, Proc. of the Special Interest Group on Biometrics and Electronic Signatures (Darmstadt 2009), 43–54.
[19] K. Nandakumar, A. K. Jain, S. Pankanti, *Fingerprint-based fuzzy vault: Implementation and performance*, IEEE Trans. Inf. Forensics Security 2 (2007), 744–757.
[20] K. Nandakumar, A. Nagar, A. Jain, *Hardening fingerprint fuzzy vault using password*, in: Advances in Biometrics (Seoul 2007), Lecture Notes in Comp. Science 4642, Springer, Berlin 2007, 927–937.
[21] N. K. Ratha, J. H. Connell, R. M. Bolle, *Enhancing security and privacy in biometrics-based authentication systems*, IBM Syst. J. 40 (2001), 614–634.
[22] C. Rathgeb, A. Uhl, *A survey on biometric cryptosystems and cancelable biometrics*, EURASIP J. Information Security (2011), no. 3.
[23] W. J. Scheirer, T. E. Boult, *Cracking fuzzy vaults and biometric encryption*, in: Biometrics Symp., IEEE Computer Soc., 2007, 1–6.
[24] K. Simoens, J. Bringer, H. Chabanne, S. Seys, *A framework for analyzing template security and privacy in biometric authentication systems*, IEEE Trans. Inf. Forensics Security 7 (2012), 833–841.
[25] K. Simoens, P. Tuyls, B. Preneel, *Privacy weaknesses in biometric sketches*, in: Security and Privacy – 2009 IEEE Symp. on Security and Privacy, IEEE Computer Soc., 2009, 188–203.
[26] B. Tams, P. Mihăilescu, A. Munk, *Security considerations in minutiae-based fuzzy vaults*, IEEE Trans. Inf. Forensics Security (2015), 985–998.
[27] A. B. J. Teoh, A. Goh, D. C. L. Ngo, *Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs*, IEEE Trans. Pattern Anal. Machine Intell. 28 (2006), 1892–1901.
[28] G. J. Tomko, C. Soutar, G. J. Schmidt, *Fingerprint controlled public key cryptographic system* (1994), US Patent 5,541,994.