The relation between the secrecy rate of biometric template protection and biometric recognition performance

Raymond N.J. Veldhuis
University of Twente
PO Box 217, 7500AE Enschede, The Netherlands
r.n.j.veldhuis@utwente.nl

Abstract

A theoretical result relating the maximum achievable security of the family of biometric template protection systems known as key-binding systems to the recognition performance of an optimal biometric recognition system that is optimal in Neyman-Pearson sense is derived. The relation allows for the computation of the maximum achievable key length from the Receiver Operating Characteristic (ROC) of the optimal biometric recognition system. Illustrative examples that demonstrate how the shape of the ROC impacts the security of a template protection system are presented and discussed.

1. Introduction

We will present a theoretical result that relates the maximum achievable security of a family of biometric template protection systems to the recognition performance of an optimal biometric recognition system. Biometric template protection refers to a class of systems that store biometric features in a form that, ideally, does not reveal information about the underlying biometric data. The principles of biometric template protection have been reviewed and discussed in [25, 12, 20]. Its concept and terminology have been standardised by ISO in [10]. An overview of this standard and of performance metrics related to biometric template protection systems is given in [23]. Currently ISO is standardising the performance metrics of biometric template protection [11].

Encryption schemes such as fuzzy commitment [14] and fuzzy fault [13] have been embedded in biometric recognition systems for the purpose of template protection. These systems are also referred to as key-binding systems. A block diagram of a generic key-binding system is shown above the dashed line in Figure 1, e.g. [9, 30]. This block diagram, which is common in information theoretical papers on biometric template protection, differs from the representation that has been standardised in [10], but can easily be mapped onto it. At enrolment, a secret binary key $S$ is combined with biometric features $x$ – conveniently arranged into a vector and denoted by a bold symbol – by an encoder ENC. This results in the helper data $w$. Ideally, the helper data does not reveal information about the biometric features, nor about the secret. Therefore, it can be stored in the clear. At verification, the decoder DEC combines the helper data with biometric features $y$ in order to reconstruct the secret. The reconstructed secret $S'$ can then be compared with the original secret $S$ and if and only if $S = S'$ it will be decided that features $x$ and $y$ originate from the same biometric source, e.g. the same finger or iris of the same individual. Since biometric features from the same biometric source are likely to exhibit within subject variations, it cannot be guaranteed that $x = y$. Therefore, the encoder and decoder have error-correcting capabilities.

Figure 1. Block diagrams of a key-binding biometric system (above dashed line) and a biometric comparison system (below dashed line).
In order to protect the secret $S$ it is hashed before storage and the comparison is done after hashing $S'$. Obviously, a longer secret yields a better security.

A key-binding system can be seen as a noisy channel transmitting a secret $S$ from an enrolment station to a verification station, with the within-subject variability of the biometric features determining the quality of the channel. According to Shannon’s Channel Capacity Theorem, e.g. [22] or another textbook on information theory, errorless transmission is feasible if the length of the secret per pair of features $(x, y)$, further denoted as the secrecy rate $R$, is below the channel capacity. In [11] the reciprocal of $R$, called Successful Attack Rate (SAR), is proposed as a standard performance metric for the secrecy of a biometric template protection system.

For key-binding systems it has been shown in [2] that the channel capacity, or equivalently the maximum achievable secrecy rate $R^*$, is equal to the mutual information between the biometric features $x$ and $y$, given that they originate from the same biometric source. Outside the context of biometric template protection, the mutual information between biometric features can be regarded as a quantifier for the information content of the biometric data. An alternative quantifier for this is the Kullback-Leibler distance between the population feature distribution and the feature distribution of an individual proposed in [1].

The maximum achievable secrecy rate of a key-binding system is an information-theoretical asymptotic upper bound that depends solely on the joint probability density of the biometric input features. For all sorts of practical reasons the maximum achievable secrecy rate may be hard to achieve. It may even be hard to compute, for it requires that the joint probability density functions of $x$ and $y$ be known. Expressions for the maximum achievable secrecy rate have been derived for the case that the biometric features have Gaussian distributions in [6, 30].

The helper data $w$ should not reveal information about the secret nor about the enrolled biometric features $x$. However, due to the presence of error correction, some of this information will leak. This can be quantified in terms of the mutual information between helper data and enrolled biometric features and the mutual information between helper data and secret. The trade-off between leakage and the successful attack rate is discussed in [17, 9, 30, 29]. In this paper we will not consider leakage nor any other of the desired properties of biometric template protection systems such as unlinkability and irreversibility [23, 11], but we will focus on the relation between the maximum achievable secrecy rate and the optimal biometric recognition performance.

The block diagram below the dashed line in Figure 1 shows a biometric comparator, which is the heart of any biometric recognition system. A biometric comparator produces a comparison score $s$, which is compared to a predefined threshold $t$. Without loss of generality we take the comparison score to be a similarity score. If it is above the threshold it is decided that the biometric features $x$ and $y$ result from the same biometric source – this is called a match. Otherwise, the decision is that the biometric features result from different biometric sources – called a nonmatch. Because of the inherent variability of biometric features, the biometric comparator can make two types of errors: a false match or a false nonmatch. The trade-off between the probabilities of these errors is controlled by varying the threshold $t$. The recognition performance of a biometric comparator is often expressed by the Receiver Operating Characteristic (ROC). The ROC plots the probability of a true match – the true-match rate, i.e. 1 minus the probability of a false nonmatch – as a function of the probability of a false match – the false-match rate. A biometric comparator that is optimal in Neyman-Pearson sense maximises the true-match rate at a given false-match rate [27]. The ROC of the optimal biometric comparator will be denoted as the maximum achievable ROC. Taking the likelihood ratio, or any monotonic function of it, as the score value will result in a biometric comparator that is optimal in Neyman-Pearson sense [4, 6, 27].

Like the maximum achievable secrecy rate of a key-binding system, the maximum achievable ROC is also a theoretical upper bound that depends solely on the joint probability of the biometric input features. For the same reasons as mentioned for mutual information it may be hard to achieve or to compute.

The secrecy rate of template protection systems has been related to indicators for the biometrics recognition performance by, for instance [15, 16], but this was only done for a specific class of systems based on quantised feature vectors and under the assumption that the biometric features have a joint Gaussian probability density. To our best knowledge, no relation has been published that allows for the computation of the maximum achievable secrecy rate from biometric performance characteristics. The main novelty of this paper is, therefore, the presentation of a simple relation between the maximum achievable secrecy rate $R^*$ of a key-binding system and the maximum achievable ROC $\tau^*(\alpha)$, with $\alpha$ denoting the false-match rate, given by

$$R^* = \int_0^1 \frac{d\tau^*(\alpha)}{d\alpha} \log_2 \left( \frac{d\tau^*(\alpha)}{d\alpha} \right) d\alpha. \quad (1)$$

This relation can be used to compute $R^*$ from $\tau^*(\alpha)$. As a second result, it will be shown that (1) implies that the maximum achievable secrecy rate increases with the overall biometric performance.

In the remainder of this paper these results will be derived and discussed, and some illustrating examples based on realistic data will be presented. In Section 2 it will be shown that the mutual information equals the statistical ex-
2. Mutual information and the likelihood ratio

The maximum achievable secrecy rate of a key-binding system is given by the mutual information between a pair of biometric features originating from the same biometric source [2]. It is given by

$$I(x; y | S) = \int f_{x,y}(x, y | S) \log_2 \left( \frac{f_{x,y}(x, y | S)}{f_x(x | S) f_y(y)} \right) \, dx \, dy.$$  \tag{2}

The underlined symbols, e.g. $\underline{x}$, denote random variables. The function $f_{x,y}(x, y | S)$ is the probability density of the feature pair $(x, y)$ given that the features originate from the same biometric source. This condition is denoted by $S$. The product $f_x(x | S) f_y(y)$ is the probability density of $(x, y)$ under the condition that the features originate from different sources, denoted by $D$. There are no conditions on the probability density functions other than that the integral in (2) converges.

The argument of the logarithm in (2) is identical to the likelihood ratio

$$l(x, y) = \frac{f_{x,y}(x, y | S)}{f_x(x | S) f_y(y)},$$  \tag{3}

which, when used as a similarity score, optimally discriminates pairs $(x, y)$ of biometric features originating from the same biometric source from pairs originating from different biometric sources in Neyman-Pearson sense [4, 6, 27].

The equations for the mutual information in (2) and for the likelihood ratio in (3) do not put restrictions on the nature of the features $x$ and $y$. Each can be derived from a single biometric sample, but it is, for instance, also allowed that each vector contains the features of more biometric samples or that $x$ and $y$ originate from heterogenous biometric sources such as from a visible-light and a near-infrared facial image.

According to (2), the mutual information $I(x; y | S)$ is by definition the statistical expectation of the log-likelihood ratio under the condition $S$ that the features originate from the same biometric source. I.e.

$$I(x; y | S) = \mathbb{E} \{ \log_2(l(x, y | S)) | S \}.$$  \tag{4}

with $\mathbb{E} \{ \cdot \}$ denoting the statistical expectation. In what follows, we will use this property to obtain a relation between $I(x; y | S)$ – and thus the maximum achievable secrecy rate – to the maximum achievable ROC of a biometric comparator.

3. Interpreting the ROC as a probability

The similarity score $\underline{s}$ resulting from a biometric comparison is a random variable because it depends on the random inputs $\underline{x}$ and $\underline{y}$ of the biometric comparator. The comparator can operate under the two conditions: $S$ – the inputs originate from the same biometric source – and $D$ – the inputs originate from different biometric sources. Let the set of possible score outcomes be $S$. The false-match rate and the true-match rate are, respectively, defined by

$$\text{fmr}(t) = \Pr(\underline{s} \geq t | D), \quad t \in S,$$  \tag{5}

$$\text{tmr}(t) = \Pr(\underline{s} \geq t | S), \quad t \in S,$$  \tag{6}

with $\Pr \{ E \}$ denoting the probability of an event $E$, and $t$ the decision threshold of the biometric comparator. The ROC is defined as the set of pairs $\{ \text{fmr}(t), \text{tmr}(t) | t \in S \}$, or equivalently as a function $\tau(\alpha) = \text{tmr}(t)$ for $t$ such that $\text{fmr}(t) = \alpha$. For classifiers that are optimal in Neyman-Pearson sense, it has been shown, e.g. [27], that the ROC is a concave function of $\alpha$. For $\text{fmr}(t) = \alpha$ we have

$$\tau(\alpha) = \text{tmr}(t) = \Pr(\underline{s} \geq t | S) = \Pr(\text{fmr}(\underline{s}) \leq \text{fmr}(t) | S) = \Pr(\text{fmr}(\underline{s}) \leq \alpha | S).$$  \tag{7}

The step between the second and the third line of the derivation can be taken because $\text{fmr}(t)$ is monotonically non-increasing with $t$. The result (7) implies that, if we use the false-match rate characteristic $\text{fmr}$ to define a mapping of the score $\underline{s}$ to a random variable $\underline{\alpha}$, defined by

$$\underline{\alpha} = \text{fmr}(\underline{s}),$$  \tag{8}

then

$$\tau(\alpha) = \Pr(\underline{\alpha} \leq \alpha | S).$$  \tag{9}

Therefore, the ROC is the probability distribution of $\underline{\alpha}$ given that the input samples are from the same biometric source and its derivative $\frac{d\tau(\alpha)}{d\alpha}$ is the corresponding probability density function. A similar result was derived in [18]. Note that $\underline{\alpha}$ computed by (8) is a dissimilarity score, whereas $\underline{s}$ is a similarity score.
4. The maximum achievable secrecy rate

The maximum achievable ROC will be denoted by \( \tau^*(\alpha) \). It is a well-known property of maximum achievable ROCs [27] that

\[
    l(x, y) = \frac{d \tau^*(\alpha)}{d \alpha}, \text{ for } \alpha = \text{fmr}(l(x, y)),
\]

which expresses the likelihood ratio as a function of the dissimilarity score \( \alpha \). This, with (4) and the result from Section 3 that \( \frac{d \tau^*(\alpha)}{d \alpha} \) is the probability density of \( \alpha \) in (10) given that the input samples are from the same biometric source leads to our first main result

\[
    R^* = \mathbb{E}\{\log_2(l(x, y)|S)\} = \mathbb{E}\left\{\log_2\left(\frac{d \tau^*(\alpha)}{d \alpha}\bigg|_{\alpha=\tilde{\alpha}}\right) \middle| S\right\} = \int_0^1 \frac{d \tau^*(\alpha)}{d \alpha} \log_2\left(\frac{d \tau^*(\alpha)}{d \alpha}\right) d\alpha
\]

with \( \alpha^*(\tau) \) the inverse of \( \tau^*(\alpha) \). Equations (11) and (12) present two equivalent forms of the result. The first one is in terms of the maximum achievable ROC and the second, slightly more compact one, is in terms of its inverse, or quantile function. Cf. [28] for a derivation of the last step.

We will show now that the maximum achievable secrecy rate increases with the overall biometric performance, which is our second main result. The result (11) can also be written as

\[
    R^* = -h(\alpha|S),
\]

with \( h(\alpha|S) \) the differential entropy of the dissimilarity score \( \alpha \) computed by (8) given that the input samples are from the same biometric source. Note that, unlike the entropy of a discrete random variable, the differential entropy can be negative. Equation (13) states that the maximum achievable secrecy rate decreases with increasing differential entropy of \( \alpha \) given that the input samples are from the same biometric source. Indeed, the ROC \( \tau(\alpha) = \alpha \) of a fully random classifier has \( h(\alpha|S) = 0 \) and cannot convey a secret, whereas a perfect classifier is characterised by \( \frac{d \tau(\alpha)}{d \alpha} = \delta(\alpha) \) and, therefore, \( h(\alpha|S) = -\infty \), allowing for an infinitely long secret. We formalise our result as follows:

If the maximum achievable ROCs of two types of biometric feature sets, denoted by A and B, are given by \( \tau^*_A(\alpha) \) and \( \tau^*_B(\alpha) \), respectively, and their maximum achievable secrecy rates by \( R^*_A \) and \( R^*_B \), respectively, then

\[
    \tau^*_B(\alpha) \leq \tau^*_A(\alpha), \quad \alpha \in [0, 1] \Rightarrow R^*_B \leq R^*_A.
\]

This indeed expresses that the maximum achievable secrecy rate increases with the overall biometric performance. The proof is as follows. On the interval \( \alpha \in [\alpha_1, \alpha_2] \) we replace \( \tau^*_A(\alpha) \) by a chord that is a tangent of \( \tau^*_B(\alpha) \). Because a maximum achievable ROC is concave, the probability density \( \frac{d \tau^*_A(\alpha)}{d \alpha} \) is monotonically non-increasing. Replacing \( \tau^*_A(\alpha) \) on \( \alpha \in [\alpha_1, \alpha_2] \) by a chord is equivalent to replacing \( \frac{d \tau^*_A(\alpha)}{d \alpha} \) on \( \alpha \in [\alpha_1, \alpha_2] \) by its average on that interval. The thus modified ROC is still concave. It can be shown that this replacement increases the differential entropy. This can be understood intuitively because a segment of \( \frac{d \tau^*_A(\alpha)}{d \alpha} \) is replaced by a uniform density, which has maximum differential entropy. In subsequent steps, other segments of the modified \( \tau^*_A(\alpha) \) are replaced by chords that are also tangents of \( \tau^*_B(\alpha) \). After each step \( \tau^*_B(\alpha) \) is better approximated by the new modification of \( \tau^*_A(\alpha) \) and the differential entropy has increased. This procedure will converge to a situation where the modified \( \tau^*_A(\alpha) \) is identical to \( \tau^*_B(\alpha) \) while the differential entropy has increased. This implies that the differential entropy of \( \tau^*_B(\alpha) \) is higher than that of \( \tau^*_A(\alpha) \) and therefore the maximum achievable secrecy rate of feature type B must be below that of feature type A.

5. Discussion

As is true for all information theoretic bounds, the expressions for \( R^* \) as given in (11) and (12) must be interpreted with some care. In particular, estimating \( R^* \) form an ROC \( \tau(\alpha) \) obtained in an evaluation experiment may lead to an incorrect result due to design choices, modelling errors, estimation errors, and sensitivity of (11) to deviations of \( \tau^*(\alpha) \) as we will explain below.

Design choices The ROC \( \tau^*(\alpha) \) in (11) and (12) reflects the recognition performance of an optimal, i.e. likelihood-ratio based, classifier and is solely based on knowledge of the joint probability density functions of the input signals. For good pragmatic and practical reasons of complexity and robustness and because these probability functions are unknown, many biometric recognition systems are not based on the likelihood ratio, but on alternative classifiers based on, for instance, Euclidean distance, total absolute distance, or support vector machines. As a result, the ROC of such systems will be below the maximum achievable ROC and \( R^* \) will be underestimated, because of (14).

Modelling errors Biometric recognition systems that are actually likelihood-ratio based have been proposed, e.g. [21, 4, 24], but it is questionable for two reasons whether their measured ROCs can be considered optimal, despite the good recognition results that have been reported for those systems. The first reason is that the design of these likelihood-ratio classifiers is based on (often Gaussian)
model assumptions for the biometric features, which may not be valid. The second reason is that the model parameters are obtained in a training process and they may not be fully representative for the testing data. These reasons have as an effect that the measured ROC will also be below the maximum achievable one and \( R^\ast \) will again be underestimated because of (14). The same two objections, in fact, also hold for estimating the \( R^\ast \) by computing \( I(x; y|S) \) from estimated probability density functions.

**Estimation errors**  Even when the biometric comparator has an ROC close to \( \tau^\ast(\alpha) \), care must be taken because a measured ROC is noisy, due to the fact that the number of score values that it is computed from is necessarily finite. A large set of testing data is therefore recommended to obtain an accurate ROC. Moreover, a measured ROC contains steps, because it is computed via empirical approximations [3] of \( \mathrm{tfrm}(t) \) and \( \mathrm{tfmr}(t) \), based on counting the scores exceeding the threshold \( t \). These steps will lead to infinite values of \( \frac{d \tau(\alpha)}{d \alpha} \) and divergence of the integrals in (11) and (12). These steps, including the one at \( \alpha = 0 \), can be avoided by a proper smoothing that guarantees the necessary concave character of an maximum achievable ROC, for example by taking the convex hull of the estimated ROC [8].

**Sensitivity**  The region where \( \frac{d \tau(\alpha)}{d \alpha} \gg 1 \) , i.e. \( \alpha \) close to 0, largely determines the outcome of (11). Because of the differentiation and the steepness of a good ROC, the result is very sensitive to deviations of the estimated \( \tau(\alpha) \) from \( \tau^\ast(\alpha) \) in this area, whether they be due to design choices, modelling errors, or measurement errors. Unfortunately, this is the most inaccurate part of an estimated ROC due to the limited numbers of scores exceeding high thresholds. In Section 6 we will demonstrate how a small change in \( \tau(\alpha) \) in this range can lead to a large change in the estimated secrecy rate.

### 6. Examples

In this section we will study the effect of the shape of \( \tau^\ast(\alpha) \) on \( R^\ast \) by computing \( R^\ast \) for two prototypical types of ROCs. We will also discuss to what extent these types of ROCs can model the behaviour of good biometric systems and be used to estimate their secrecy rate.

The first type of ROC lies close to the line \( \tau = 1 \) and is tangential to it for low similarity score values, but it is not tangential to the line \( \alpha = 0 \) for high similarity scores. This type is further denoted as TT (Top Tangential). The second type lies close to the line \( \alpha = 0 \) and is tangential to it for high similarity score values, but it is not tangential to the line \( \tau = 1 \). This type is further denoted as LT (Left Tangential). We choose a simple parametrisation for each of the ROCs. For the top tangential ROCs we define

\[
\tau_{TT}^\ast(\alpha; m) = 1 - (1 - \alpha)^m,
\]

and for the left tangential ROCs

\[
\tau_{LT}^\ast(\alpha; m) = \alpha^\frac{1}{m}.
\]

Figure 2 shows examples of each type, for \( m = 20 \). Note that one type of ROC can be obtained from the other by mirroring it about the line \( \alpha + \tau = 1 \). Consequently, for the same \( m \) \( \tau_{TT}^\ast(\alpha; m) \) and \( \tau_{LT}^\ast(\alpha; m) \) have the same area under curve AUC and the same Equal-Error Rate (EER), which are common indicators of biometric recognition performance.

The performances at a few points of operations of four biometrics systems that have been evaluated in large-scale tests have been plotted in Figure 3, together with plots of \( \tau_{TT}^\ast(\alpha; m) \) and \( \tau_{LT}^\ast(\alpha; m) \). The top graph shows \( \tau_{TT}^\ast(\alpha; m) \) and \( \tau_{LT}^\ast(\alpha; m) \) for \( m = 4500 \) together with the EER points and the true-match rates at false-match rates \( 10^{-2} \), \( 10^{-3} \), and \( 10^{-4} \) of two methods that perform well in the one-to-one comparison of the FVC Ongoing [7] fingerprint verification context. The discs represent the performance of the method EMB9300 that gives the highest true-match rate at a false-match rate of \( 10^{-4} \). The filled squares represent the performance of the method TigerAFIS that gives the highest true-match rate at a false-match rate of \( 10^{-2} \). These figures have been derived from the ones published on https://biolab.csr.unibo.it/fvcongoing/ on November 20, 2014. The performance of the method EMB9300 in the range \( \alpha \in [10^{-4}, 10^{-2}] \) seems well modelled by \( \tau_{LT}^\ast(\alpha; 4500) \). The performance of the method TigerAFIS...
might be better modelled by a mixture of $\tau_{TT}^*(\alpha;m)$ and $\tau_{LT}^*(\alpha;m)$.

The bottom graph in Figure 3 shows $\tau_{LT}^*(\alpha;m)$ for $m = 215$ together with the true-match rates at false-match rates $10^{-2}, 10^{-3},$ and $10^{-4}$ of the methods that performed well in the controlled experiment on the high-resolution dataset for one-to-one algorithms in the face recognition vendor test (FRVT) 2006 [19]. The discs represent the performance of the method NV1–1to1 that gives the highest true-match rate at a false-match rate of $10^{-4}$. The filled squares represent the performance of the method V–1to1 that gives the highest true-match rate at a false-match rate of $10^{-2}$. These figures have been derived from [19, page 43]. The performance of the method V–1to1 in the range $\alpha \in [10^{-4}, 10^{-2}]$ seems well modelled by $\tau_{LT}^*(\alpha;215)$. The true-match rates for the four methods that are plotted in Figure 3 are listed in the first four data rows of Table 1.

The explicit expressions for $\tau_{TT}^*(\alpha;m)$ and $\tau_{LT}^*(\alpha;m)$ allow for an analytic computation of the corresponding secrecy rates as a function of $m$. For the top tangential ROCs in (15) we obtain

$$R_{TT}^*(m) = \log_2(m) - \frac{m - 1}{m \log(2)}, \quad (17)$$

and for the left tangential ROCs in (16)

$$R_{LT}^*(m) = \frac{m - 1}{\log 2} - \log_2(m). \quad (18)$$

Although the EER and AUC of these types of ROC depend on $m$ in the same way, this is not the case for their respective maximum secrecy rates. The maximum secrecy rate of the left tangential ROC increases much faster with increasing $m$ than that of the top tangential ROC. Figure 4 plots the maximum secrecy rates resulting from the top tangential (top graph) and the left tangential (bottom graph) ROCs as a function of equal error rate. The figure is obtained by computing the EER and maximum secrecy rates for various values of the parameter $m$. It is clear from these graphs that at realistic EERs in the range $[10^{-3}, 10^{-2}]$ orders of magnitude higher secrecy rates can be obtained if the ROC is left tangential than if it is top tangential. In fact, the maximum achievable secrecy rate are much higher than anything that has been reported to be obtained by a real system.

![Image of Figure 3: Top graph: A top tangential ROC $\tau_{TT}^*(\alpha;m)$ (solid) and left tangential ROC $\tau_{LT}^*(\alpha;m)$ (dashed), both with $m = 4500$ and 4 points of operation of the algorithms EMB9300 (discs) and TigerAFIS (filled squares) derived from https://biolab.csr.unibo.it/fvcongoing/. Cf. [7]. Bottom graph: A left tangential ROC $\tau_{LT}^*(\alpha;m)$ (dashed), with $m = 215$ and 3 points of operation of the algorithms NV1–1to1 (discs) and V–1to1 (filled squares) derived from [19, page 43].](image1)

![Image of Figure 4: Top graph: The maximum achievable secrecy rate $R^*$ as a function of EER for top tangential rocs $\tau_{TT}^*(\alpha;m)$. Bottom graph: The maximum achievable secrecy rate $R^*$ as a function of EER for left tangential rocs $\tau_{LT}^*(\alpha;m)$. The disc and filled squares show $R^*$ for the methods EMB9300 and V1–1to1 under the assumption that their ROCs can be modelled by $\tau_{LT}^*(\alpha;m)$ from (16). The (open) circle and square show $R^*$ of these respective methods under the more modest assumption that their ROCs can be modelled piece wise linearly.](image2)

Table 1. True-match rates at various points of operation and estimated secrecy rates of four biometrics systems that have been evaluated in large-scale tests.

<table>
<thead>
<tr>
<th></th>
<th>EMB9300</th>
<th>TigerAFIS</th>
<th>NV1–1to1</th>
<th>V–1to1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_{TT}^*$ [#bits]</td>
<td>6479</td>
<td>13.2</td>
<td>12.5</td>
<td>301</td>
</tr>
<tr>
<td>$R_{PW}^*$ [#bits]</td>
<td>13.2</td>
<td>13.2</td>
<td>12.5</td>
<td>12.7</td>
</tr>
</tbody>
</table>

![Table 1: True-match rates at various points of operation and estimated secrecy rates of four biometrics systems that have been evaluated in large-scale tests.](table1)
From Figure 3 it seems that the methods EMB93000 and V–1to1 have true-match rates that seem well-modeled by a left tangential ROC in the range $\alpha \in [10^{-3}, 10^{-2}]$. If that behaviour could be extrapolated towards $\alpha = 0$, then these methods would have the high maximum secrecy rates $R_{LT}^*$ given in the fifth row of Table 1 and that are plotted in Figure 4. The disc in this figure indicates the true-match rate for EMB9300 and the filled square that for V–1to1. However, these high secrecy rates are mostly a consequence of the steep departure from $\alpha = 0$ by the model ROC $\tau^*(\alpha)$.

A slight change of the ROC near $\alpha = 0$ may lead to much more pessimistic results. If, for instance, the ROCs are approximated piece-wise linearly by straight lines connecting the measured points, then the maximum achievable secrecy rate would drop to the mere 12–13 bits presented in the last row of Table 1 and in Figure 4 by the open symbols. This drop is mostly caused by the change of behaviour for the ROCs at low false-match rates, which confirms the observation made in Section 5 that $R^*$ is sensitive to the shape of the ROC near $\alpha = 0$.

From the examples presented in this section it can be concluded that for a high $R^*$, if possible, features should be selected that result in an ROC with a left-tangential character that is steep for low $\alpha$. At the same time, a measured ROC must be interpreted with care, because of the sensitivity of $R^*$ to (errors in) the shape of the ROC at low values of $\alpha$.

7. Conclusions

A new relation between the maximum achievable secrecy rate of a key-binding biometric template protection system and the maximum achievable ROC of a biometric comparator has been presented. This relation allows for the computation of the maximum achievable secrecy rate from the maximum achievable ROC.

Both the maximum achievable secrecy rate and the maximum achievable ROC are functions of the probability density functions of pairs of biometric features. Practical biometric template protection systems and practical biometric comparators may not be able to achieve those bounds. Moreover, the underlying probability densities may be unknown and estimated ROCs may be inaccurate, in particular in the critical range of low false-match rates. Therefore, an estimate of the secrecy rate based on a measured ROC must be interpreted with care.

We have shown that the shape of the ROC, in particular the steepness for low false-match rates, has a great impact on the maximum achievable bit rate. If possible, the designer of a key-binding template protection system should try to use features that result in an ROC that is steep at low false-match rates. Other characteristics, such as equal-error rate, area under curve or false-nonmatch rate at a certain false-match rate are less relevant.

The fact that the maximum achievable secrecy rate, and thus the protection of the biometric data, depends on the recognition performance of the biometric may be undesirable, because privacy reasons may demand that biometric modalities with a weaker recognition performance need a strong protection as well. A solution to this problem is to perform the complete biometric recognition in the encrypted domain, for instance by applying homomorphic encryption. Results following this approach have been presented in [26, 5].

References


