A. Brömme, C. Busch, C. Rathgeb and A. Uhl (Eds.): BIOSIG 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 233

Improvement of Fuzzy Vault for Multiple Fingerprints with Angles

Matthias Neu[1], Ulrike Korte[2] and Markus Ullmann[3]

Abstract: In this paper we analyse an enhanced fuzzy vault scheme for fingerprints with minutia angles that claims to be correlation resistant. During our analysis of this scheme we found a new attack concerning the integration of chaff points with angles, termed angle-correlation attack, which is presented. Moreover, we introduce an improved fuzzy vault scheme for multiple fingers, which is resistant against "traditional" correlation attacks. We broadly analyse our scheme concerning usual attacks (brute-force, "traditional" correlation attacks and in addition angle-correlation attacks). We show that angle-correlation attacks are more or less negligible for our fuzzy vault approach for multiple fingers with minutiae angles.

Keywords: Fuzzy Vault, Biometric Template Protection, Fingerprint Recognition, Minutiae Angles, Multiple Fingers, Angle-Correlation Attack

1 Introduction

Biometric data are private information. Therefore, privacy issues for biometrics are an important issue. Template protection schemes have been an active field of research since the first publication of the fuzzy commitment scheme 1999 [JW99]. Due to intrinsic errors during the capturing of biometrics data template protection schemes apply cryptography and error correction principles to protect the biometric data. Template protection schemes have to require the following privacy properties: irreversibility and unlinkability. Irreversibility means that the protected template prevents the recovery of the original biometrics unless a sufficient similar feature data is provided for comparison. Unlinkability implies that two protected templates from the same biometric data cannot be linked, see [CS09].

Besides the fuzzy commitment scheme the fuzzy vault scheme is broadly analysed, especially for the application of fingerprints. In [Cl03] we find the first fuzzy vault construction. This concept only uses the position of pre-aligned minutiae. For example in [NJP07] this construction was extended by minutiae angles. [Me10] developed a fuzzy vault concept for multiple fingerprints only based on minutiae positions and a relative alignment. In contrast to these concepts the solution of [Li08] is based on alignment-independent features.

All these constructions presented before are vulnerable against correlation attacks as demonstrated in [KY08]. Therefore, [Ta13a] presented the first fuzzy vault fingerprint solu-

[1] University of Applied Sciences Bonn-Rhein-Sieg, D-53757 St. Augustin, https://www.h-brs.de, matthias.neu@h-brs.de
[2] Federal Office for Information Security, D-53133 Bonn, https://www.bsi.bund.de, ulrike.korte@bsi.bund.de
[3] Federal Office for Information Security, D-53133 Bonn, https://www.bsi.bund.de, University of Applied Sciences Bonn-Rhein-Sieg, D-53757 St. Augustin, https://www.h-brs.de markus.ullmann@bsi.bund.de, markus.ullmann@h-brs.de

tion that was not susceptible to correlation attacks. This approach uses an absolute pre-alignment method based on a directed reference point and a quantization mechanism of the minutiae positions based on a grid. Then all grid positions not used by quantized minutiae are occupied by chaff points. In this approach [Ta13a] is generalized by also using minutiae's angles and minutiae's types. The correlation resistance is achieved by using all points of the quantization grid. In [Ta15] another correlation attack resistant fuzzy vault fingerprint solution is proposed, based on three alignment-independent features. Several multi-biometric fusion strategies for biometric template protection are published, e.g., in [NJ08], and [Me10], but without an analysis of the impact of the fusion level on privacy protection. In [MKK12] four different multi-biometric fusion strategies are presented and analysed with respect to their impact on security and recognition accuracy. In this paper, a multi finger vault approach with angles is developed as a generalisation of the feature-level fusion concept of [Me10] and [MKK12], which are only based on minutiae positions.

In Section 2 we introduce a new class of attacks concerning minutiae angles, termed angle-correlation attack. Next, we show that the mentioned fuzzy vault approach [Me16] is vulnerable against this new attack. As a consequence, angles of chaff points should not be chosen at random for single finger fuzzy vault schemes, as proposed in [Me16].

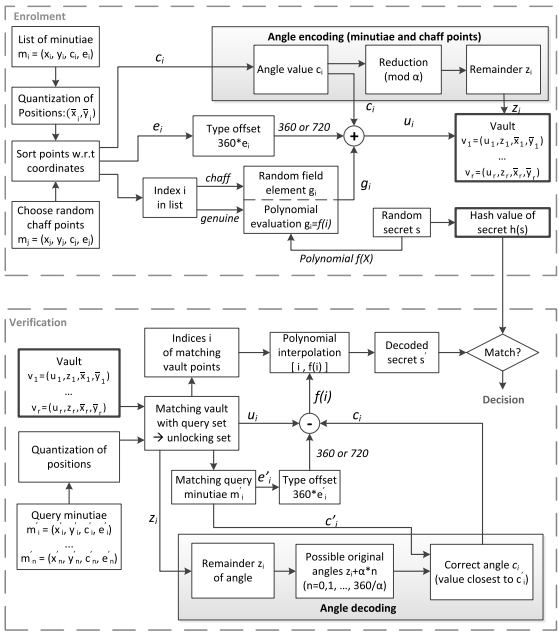

Fig. 1: Enrolment and verification process, obtained from [Me16]

One fingerprint has only a very restricted entropy. Therefore, fuzzy vault constructions for multiple fingers are of interest. We suggest an improved fuzzy vault scheme for multiple fingers with minutiae angles which is resistant against "traditional" correlation attacks pointed out in [KY08]. We show that the correlation of angles of chaff points can be used to enhance the performance of this scheme for multiple fingers. Moreover, we analyse the potential of angle-correlation attacks for our scheme for multiple fingerprints. We demonstrate that angle-correlation attacks are more or less negligible for our fuzzy vault scheme for multiple fingers with minutiae angles. The following sections of this paper are organized as follows: Section 2 provides a brief overview of the analysed fuzzy vault scheme for fingerprints with angles. Subsequently, our improved fuzzy vault scheme for multiple fin-

gers with minutiae angles is presented and analysed in Section 3. Finally, in Section 4 we summarize our results and give an outlook.

2 Fuzzy Vault for Fingerprints with Minutiae Angles resistant against "traditional" Correlation Attacks

For one finger this paper is based on the approach of fuzzy vault for fingerprints with minutiae angles resistant against "traditional" correlation attacks according to [Me16] and on the alignment solution according to [Ta13a]. The minutiae templates are created by the minutiae extracted from these pre-aligned fingerprint samples, which are used as enrolment and query minutiae templates in the fuzzy vault encoding (enrolment) and decoding (verification) process, as explained in chapter 3 of [Me16]. Consider a fingerprint minutiae enrolment template containing N minutiae $m_i = (x_i, y_i, c_i, e_i)$, where (x_i, y_i) are the horizontal and vertical coordinates of the position of minutiae and c_i is the angle of minutiae m_i and e_i is the type of minutiae for $0 < i < N+1$. Minutiae points are quantized according to a rectangular grid with bin spacing q_x and q_y in the direction of image width and image height, respectively as shown in Figure 2. The quantized values $(\bar{x}_i, \bar{y}_i)$ are the centres of the corresponding cell in which the minutiae is to be found. In order to minimize verification errors due to inaccurately measured minutiae angles, we store, for each genuine point, the remainder $c_i \; mod \; \alpha$ in the vault, where the parameter α is a divisor of 360. For chaff points, the remainder $z_i = c_i \; mod \; \alpha$ of a randomly chosen angle c_i, is stored. Details are shown in Figure 1.

2.1 Security

A security analysis of the fuzzy vault schemes with minutiae angles is given in [Me16], too. Here, we sketch the brute force attack because it is needed to perform the angle-correlation attack. First the attacker has to randomly choose k+1 vault points

$\left\{ \left(u_{i_1}, z_{i_1}, \bar{x}_{i_1}, \bar{y}_{i_1}\right), \cdots, \left(u_{i_{k+1}}, z_{i_{k+1}}, \bar{x}_{i_{k+1}}, \bar{y}_{i_{k+1}}\right) \right\}$ (the degree of the secret polynomial is k), guess for each point the original angle c_j, $j \in \{i_1, \cdots, i_{k+1}\}$, of the corresponding minutiae in consideration of its remainder z_j. Then the attacker has to recover the polynomial $f'(x)$ through interpolation from the set of points $\left\{ \left(i_1, u_{i_1} - c_{i_1}\right), \cdots, \left(i_{k+1}, u_{i_{k+1}} - c_{i_{k+1}}\right) \right\}$. If the value of the hash of $f'(x)$ matches the hash value of the vault template, the attack is successful, otherwise the attacker has to retry this process. The number of needed recovery attempts can be estimated as $\frac{\binom{r}{k+1} * (360/\alpha)^{k+1}}{\binom{t}{k+1}}$. r is the number of elements in the vault, t is the number of minutiae points in the vault and k is the degree of the polynom, see [Me16].

2.2 Angle-Correlation Attack

The aim of the angle-correlation attack is to distinguish genuine from chaff points in a given fuzzy vault based on the angle information. Given are two different pre-aligned vaults V_1 and V_2 which are constructed based on the same quantization (quantization grid and angle remainder $mod \; \alpha$) from different pre-aligned fingerprints of the same finger.

The minutiae angles of two corresponding minutiae from different (pre-aligned) fingerprints from the same finger c_i and $\tilde{c}_i$ are quite the same; this property is also valid for the remainder $z_i = c_i \; mod \; \alpha$ respective $\tilde{z}_i$. In contrast, angles of chaff points γ are chosen at random. As a consequence, th e remainder $z_i = \gamma_i \; mod \; \alpha$ is also a random value, too.

Step 1: The attacker needs a set of vault template pairs $\{(V_1, V_1'), (V_2, V_2'), ...\}$. V_i and V_i' are created from fingerprints of the same finger.

Step 2: The attacker randomly chooses a vault template pair $\left(V_j, V_j'\right)$.

Step 3: For each corresponding vault point pair $\left((u_i, z_i, \bar{x}_i, \bar{y}_i), \left(u_i', z_i', \bar{x'}_i, \bar{y'}_i\right)\right)$ of those vault templates the value $DIFF_i = diff(z_i \bmod \alpha, z_i' \bmod \alpha)$ where $diff$ is the function defined by formula (1) is calculated.

Step 4: The attacker creates the sorted list $(DIFF_{i_1}, DIFF_{i_2}, ..., DIFF_{i_r})$ where $DIFF_{i_j} \leq DIFF_{i_{j'}} \Leftrightarrow j \leq j', \; j, j' \in \{1, ..., r\}$ and chooses the first g elements of this list and performs a brute force attack on the vault V_j based on the corresponding set of points $\left\{(u_{i_1}, z_{i_1}, \bar{x}_{i_1}, \bar{y}_{i_1}), \cdots, \left(u_{i_g}, z_{i_g}, \bar{x}_{i_g}, \bar{y}_{i_g}\right)\right\}$. $g \geq k+1$ can be freely chosen. Repeat step 2 if the brute force attack was not successful.

real angle value	$\gamma, \; \delta \in \{0, \cdots, 359\}$
remainder value	$\gamma^{\sim} = \gamma \; mod \; (\alpha), \; \delta^{\sim} = \delta \; mod \; (\alpha)$
angle difference	$\lvert\gamma - \delta\rvert = \theta \leq \alpha/2 \Rightarrow diff(\gamma^{\sim}, \delta^{\sim}) = \theta$
function $min(\gamma, \delta)$	$min(\gamma, \delta) = \gamma$, if $\gamma \leq \delta$ $min(\gamma, \delta) = \delta$, otherwise
function $max(\gamma, \delta)$	$max(\gamma, \delta) = \gamma$, if $\gamma \geq \delta$ $max(\gamma, \delta) = \delta$, otherwise

Tab. 1: Angle relation

$$diff(\gamma^{\sim}, \delta^{\sim}) := min(|\gamma^{\sim} - \delta^{\sim}|, \; |(min(\gamma^{\sim}, \delta^{\sim}) + \alpha) - max(\gamma^{\sim}, \delta^{\sim})|) \qquad (1)$$

The described attack does not break every vault. In order to estimate the performance of the attack it is necessary to calculate (a) how long an attempt on a single vault pair would take and (b) how many attempts are needed for a successful experiment on average:
(a) If the set $\left\{(u_{i_1}, z_{i_1}, \bar{x}_{i_1}, \bar{y}_{i_1}), \cdots, \left(u_{i_g}, z_{i_g}, \bar{x}_{i_g}, \bar{y}_{i_g}\right)\right\}$ contains $x \geq k+1$ genuine points the expected number of interpolations is: $\frac{\binom{g}{k+1} * (360/\alpha)^{k+1}}{\binom{x}{k+1}}$ otherwise the brute force attack is not successful, i.e., all $\binom{g}{k+1} * (360/\alpha)^{k+1}$ possible interpolations would be performed.
(b) Let p be the probability of a successful attempt. To have a 50 % chance of success with the entire attack $avg(p) = \begin{cases} 1, p \geq 0.5 \\ \frac{log(0.5)}{log(1-p)}, p < 0.5 \end{cases}$ attempts are needed.

q_x	20 px
q_y	30 px
t	35
length of horizontal axis of the ellipsis	213 px
length of vertical axis of the ellipsis	293 px

Tab. 2: Chosen parameter of the quantization grid and region of interest

α	k	bf-security	angle-correlation
30°	4	$2^{34.36}$	$2^{30.4}$
40°	4	$2^{32.28}$	$2^{27.9}$
90°	5	$2^{31.84}$	$2^{23.27}$

Tab. 3: Angle-Correlation Attack

Given the configuration defined in Table 2 which has been adopted from [Fe15] the results presented in Table 3 have been calculated based on the MYCT-100 database. It can be seen that the strength of the angle-correlation attacks strongly depends on the value of α. For small α values the angle-correlation attack is slightly better than brute force (bf-security) but with bigger α values the difference grows. Even though this attack is better than brute force, it does not break the scheme in the way the "traditional" correlation attack did with the fuzzy vault scheme without the usage of quantization. A detailed analysis is presented in [Ne16]. But it is shown, that angle-correlation attacks have to be regarded in a security analysis beside brute force attacks, smart polynomial attacks and false accept attacks if angles are used in fuzzy vault schemes, too.

3 Multiple Finger Vault with Angles

3.1 Preliminary Considerations

To enhance the practical security of template protection schemes, multiple fingers could be used. Such an extension was presented in [Me10]. The basic idea is to create a single vault template for each finger during enrolment but to use always the same polynomial. During an authentication the query minutiae sets are matched against the reference vault templates, first. Next, all matching elements can be combined in a matching set. The consequence is that the degree of the polynomial could be increased significantly if multiple fingers are used. Moreover, in [Me10] several actions have been performed (which can't be performed if quantization is used) to reduce the ratio of wrong matches to correct matches [Ne16]. But in [Me10] no quantization is used. So this scheme is still highly vulnerable to "traditional" correlation attacks. The scheme described in Section 2 uses quantization but also offers real information of the fingerprint template in form of the public angle remainder c_i mod α of every vault point. Our fuzzy vault scheme for multiple fingerprints is based on the scheme described in Section 2. But we suggest making additionally use of the exactness of the public remainder c_i mod α during verification without revealing more sensitive information in the vault template. So we use the correlation of angles during verification to improve the achievable security for our multiple fingers scheme.

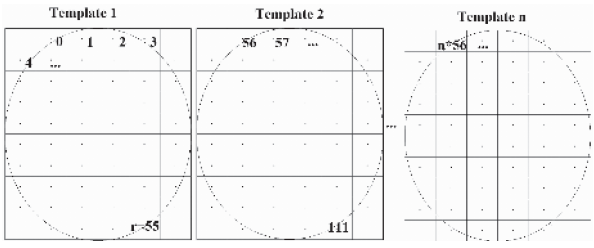

Fig. 2: Numeration of the quantization grid

During enrolment n pre-aligned fingerprint templates from n different fingers from one human being are gathered to create the protected template. For the k'th fingerprint the minutiae are represented as $m_{k,i} = (x_{k,i}, y_{k,i}, c_{k,i})$. $(x_{k,i}, y_{k,i})$ are the cartesian coordinates of the position and $c_{k,i}$ is the associated angle of the i'th minutiae of the k'th finger. Given the quantization parameters q_x and q_y and the specified ellipsis the number of grid cells r for all fingerprints is uniform. To guarantee that every grid cell of all n templates has a different index number a continuous numeration of the grid cells is suggested. Grid cells for the $l'th$ template are numbered from $(l-1)*r+1$ to $l*r$ (Figure 2).

In the next step for each fingerprint template a vault template is produced according the process described in Section 2 with the new numeration taken into consideration. In order to obscure genuine minutiae in the vault, the unused points of the quantization grid are added to the minutiae list and are regarded as chaff points. During enrolment the secret polynomial $f(x)$ is created and used for all templates to construct the according vaults. Finally, the multiple fingerprint vault consists of n single vaults.

3.2 Verification

First, n pre-aligned query fingerprint minutiae templates are gathered. For the k'th fingerprint template the minutiae are represented as $m'_{k,j} = (x'_{k,j},\ y'_{k,j},\ c'_{k,j})$. Next the verification process according to Section 2 is performed for each corresponding query fingerprint template - vault pair until the sets of points $R_k = \{(i, f(i))\}$, which have been used to recover the secret polynomial in the single fingerprint scheme, are evaluated. Additionally, for every point $(i, f(i)) \in R_k$ the remainder $z_{k,i} = c_{k,i} \bmod \alpha$ is taken out of the vault and the remainder $z'_{k,j} = c'_{k,j} \bmod \alpha$ is calculated. Next, the value $d_{k,i} = diff(z_{k,i}, z'_{k,j})$ is calculated where diff is defined in Equation 1. In the next step every point $(i, f(i)) \in R_k$ whose calculated value $d_{k,i}$ is larger than tp, where tp is a new tolerance-parameter, is removed from the set R_k resulting in the set R'_k. After that the sets R'_k are merged together resulting in the set R' on which the reconstruction of the secret polynomial is performed as described in [Me16]. The filtering step of the calculated value of the diff-function helps to improve the ratio of correct matchings to false matchings during verification (i.e., points in the reconstruction set R which can be resolved to a point on the secret polynomial to points which can't). This method enables to significantly increase the degree of the polynomial which results in a higher security level of the vault template.

3.3 Angle-correlation attack

Due to quantization the vault is resistant against the "traditional" cross-matching performed on the exactness of the cartesian coordinates of the minutiae points included in a vault. In order to extend the angle-correlation attack, described in Section 2.2, to the multiple vault scheme some changes have to be made. In step 2 the vault pairs $\left(V_j, V'_j\right)$ are pairs of the multiple vault template containing n single vaults i.e. $V_j = \left\{v_{j,1}, \cdots, v_{j,n}\right\}, V'_j = \left\{v'_{j,1}, \cdots, v'_{j,n}\right\}$. In the following for each pair $(v_{j,s}, v'_{j,s}), s \in \{1, \cdots, n\}$ the set $R = \left\{\left(u_{s,i_1}, z_{s,i_1}, \bar{x}_{s,i_1}, \bar{y}_{s,i_1}\right), \cdots, \left(u_{s,i_g}, z_{s,i_g}, \bar{x}_{s,i_g}, \bar{y}_{s,i_g}\right)\right\}$ is calculated as described in step 3-4. Next, all n sets are merged into one set on which the brute force attack is performed.

3.4 Analysis

To test the performance of the presented multiple finger vault scheme the MCYT-100 database was used which contains 12 fingerprints of 10 fingers of 100 persons. Here, a fuzzy vault scheme with four fingers is regarded.

To create a vault the fingerprints of the finger with the indices 0-3 and 5-8 were used, which results in $2*6 = 12$ 4-finger vaults for every person, because for each finger 6 samples were used for enrolment and 6 for verification. Of each vault template one genuine verification experiment was performed which resulted in $100*12 = 1200$ genuine verification attempts in total.

α	tp	k	FNMR	brute force security
30°	5°	15	0.0873	$2^{109.88}$
40°	5°	18	0.0985	$2^{122.883}$
90°	8°	29	0.0924	$2^{160.664}$

Tab. 4: Brute force security with chaff point filtering

α	k	FNMR	brute force security
30°	10	0.0814	$2^{75.271}$
40°	11	0.0951	$2^{77.192}$
90°	13	0.0891	$2^{68.479}$

Tab. 5: Brute force security without chaff point filtering

In order to optimize the parameters k, tp and α the configuration given in Table 2 was used. k is the degree of the polynomial, tp is the filter parameter and α is the angle quantization parameter. A verification is counted as successful if the chance of a correct verification with 60000 interpolations (according to [Ta13b] $2^{16} = 65536$ interpolations were a practical count in 2013) is at least 90 %. For each of the values $\alpha = 30°, \alpha = 40°, \alpha = 90°$ the optimized parameters k and tp were calculated resulting in the following brute-force security values under the prerequisite of FNMR being smaller than 10 % (Table 4). For comparison purposes the same tests were performed without the filtering step to show its benefit for our multiple finger vault scheme (Table 5). To estimate the performance of the presented angle-correlation attack against the 4-finger vault depending on the α parameter for each parameter combination, estimated in the previous step, 1179 attack attempts were calculated (Table 6). p is the success probability of an angle-correlation attack attempt on a single 4-finger vault pair. Table 6 shows that the brute force security rises with the value of α but the needed interpolations for an attack are nearly quite the same. Therefore, it seems to be the best choice to use small values of α even if high brute force security values can be achieved with larger α values.

α	g	p	interpolations needed per experiment	interpolations needed per attack	brute force security
30°	10	0.0551	$2^{92.206}$	$2^{95.817}$	$2^{109.88}$
40°	10	0.0381	$2^{92.206}$	$2^{96.024}$	$2^{122.883}$
90°	10	0.0025	$2^{87.65}$	$2^{95.742}$	$2^{160.664}$

Tab. 6: Needed interpolation for a successful vault attack

4 Conclusion and Outlook

The performed tests do not represent an optimization of the parameters of the proposed scheme but show its potential and the dependency of the angle-correlation attack from the value of α. Further analysis is needed to optimize the attack. Besides that, the filtering of the minutiae quality offers potential to improve the security level (i.e., allow a higher degree of the secret polynomial) of the scheme. Concerning the fuzzy vault scheme described in Section 2, the false accept attack and the statistical attack, which make use of the correlation of the minutiae position and its remainder angle ([Ne16]), are most effective. For completeness, the effectiveness of both attacks on our scheme should still be analysed in detail, too.

5 Acknowledgement

We thank our colleagues Ralph Breithaupt and Norbert Jung for valuable remarks.

References

[Cl03] Clancy, T. Charles: Secure Smartcard-Based Fingerprint Authentication. In: ACM Workshop on Biometrics: Methods and Applications. pp. 45–52, 2003.

[CS09] Cavoukian, Ann; Stoianov, Alex: Biometric encryption: The new breed of untraceable biometrics. Biometrics: Theory, Methods, and Applications, pp. 655–718, 2009.

[Fe15] Federal Office for Information Security: , BioKeyS-KBEinweg, Project Final Report, Version 1.0, July 31th, 2015.

[JW99] Juels, Ari; Wattenberg, Martin: A fuzzy commitment scheme. In: Proceedings of the 6th ACM conference on Computer and communications security. ACM, pp. 28–36, 1999.

[KY08] Kholmatov, Alisher; Yanikoglu, Berrin: , Realization of correlation attack against the fuzzy vault scheme, 2008.

[Li08] Li, Jianjie; Yang, Xin; Tian, Jie; Shi, Peng; Li, Peng: Topological structure-based alignment for fingerprint fuzzy vault. In: Pattern Recognition, 2008. ICPR 2008. 19th International Conference on. IEEE, pp. 1–4, 2008.

[Me10] Merkle, Johannes; Ihmor, Heinrich; Korte, Ulrike; Niesing, Matthias; Schwaiger, Michael: Performance of the Fuzzy Vault for Multiple Fingerprints (Extended Version). CoRR, abs/1008.0807, 2010.

[Me16] Merkle, Johannes; Butt, Moazzam; Korte, Ulrike; Busch, Christoph: Correlation-resistant Fuzzy Vault for Fingerprints. In: Proceedings of the GI Sicherheit. GI, pp. 11–22, 2016.

[MKK12] Merkle, Johannes; Kevenaar, Tom; Korte, Ulrike: Multi-modal and multi-instance fusion for biometric cryptosystems. In: Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the. IEEE, pp. 1–6, 2012.

[Ne16] Neu, Matthias: , Analysis of a Fuzzy Vault Finger Scheme with Angles, 2016. Bachelor Thesis.

[NJ08] Nandakumar, Karthik; Jain, Anil K: Multibiometric template security using fuzzy vault. In: Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on. IEEE, pp. 1–6, 2008.

[NJP07] Nandakumar, Karthik; Jain, Anil K; Pankanti, Sharath: Fingerprint-based fuzzy vault: Implementation and performance. Information Forensics and Security, IEEE Transactions on, 2(4):744–757, 2007.

[Ta13a] Tams, Benjamin: Absolute Fingerprint Pre-Alignment in Minutiae-Based Cryptosystems. In (Brmme, Arslan; Busch, Christoph, eds): BIOSIG. volume 212 of LNI. GI, pp. 75–86, 2013.

[Ta13b] Tams, Benjamin: Attacks and Countermeasures in Fingerprint Based Biometric Cryptosystems. CoRR, abs/1304.7386, 2013.

[Ta15] Tams, Benjamin; Merkle, Johannes; Rathgeb, Christian; Wagner, Johannes; Korte, Ulrike; Busch, Christoph: Improved Fuzzy Vault Scheme for Alignment-Free Fingerprint Features. In: Biometrics Special Interest Group (BIOSIG), 2015 International Conference of the. IEEE, pp. 1–12, 2015.