Cryptographic Keys from Dynamic Hand-signatures with Biometric Secrecy Preservation and Replaceability

[12]Yip Wai Kuan, [2]Alwyn Goh, [12]David Ngo CL, [12]Andrew Teoh BJ

[1]Fac. of Info. Science & Tech., Multimedia University, Jln Ayer Keroh Lama, 75450 Melaka, Malaysia
{yip.wai.kuan04, david.ngo, bjteoh}@mmu.edu.my
[2]Corentix Technologies Sdn Bhd, B-5-06, Kelana Jaya, Petaling Jaya, 47301 Selangor, Malaysia
alwyn@corentix.com

Abstract

We propose a method of extracting cryptographic key from dynamic handwritten signatures that does not require storage of the biometric template or any statistical information that could be used to reconstruct the biometric data. Also, the keys produced are not permanently linked to the biometric hence, allowing them to be replaced in the event of key compromise. This is achieved by incorporating randomness which provides high-entropy to the naturally low-entropy biometric key using iterative inner-product method as in Goh-Ngo, and modified multiple-bit discretization that deters guessing from key statistics. Our proposed methodology follows the design principles of block ciphers to result in unpredictable key space and secure construction.

1. Introduction

It is widely believed that the use of biometric as the keys in cryptographic protocols may be the solution to the issues of poor security in password-based access systems and stolen private keys. In this paper, we consider utilizing dynamic handwritten signature as biometric for key transformation because it is a physically and universally accepted method of authentication. We propose that a secure and good cryptographic key extraction technique from dynamic handwritten signature should have the following requirements:-

- No signature template storage. Most handwritten signature verification schemes require a template of the signature to be stored for comparison later. This provides no security in the event the template is stolen as the user, inconveniently, must register a new signature.
- Refreshable keys. Previous methods of Monrose [1-2], Davida [3] and Chang et al [4] methods derive keys straight from biometrics to be used in various cryptosystems. Again, in the event of compromised key, the user has to change his biometrics, which is not feasible for physiological biometrics like face, iris and fingerprint. Keys that can be replaced in the event of key compromise will be an important consideration for integration into cryptographic protocols.
- Secrecy protection. Throughout the transformation process, no statistical information that can be used for reconstruction of the biometric data should be revealed.
- Unpredictable key space. It should not be possible for an adversary to perform a statistical extraction of key space patterns based on intercepting multiple keys. The keys should be sufficiently different in terms of bits from non-genuine keys, and should be uniformly distributed.
- Secure transformation. The transformation process should follow good security design principles as described by Shannon [5], to promote robustness against cryptanalysis. The transformation from dynamic signature to cryptographic key should not be reversible to thwart attempts in recovering the biometric.
- Error correction. Since every capture of the hand-signatures is not exact, a tolerable application of correction is needed to ensure that the keys are stable enough to be used as cryptographic keys.

2. Literature Review

Biometric to cryptographic bitstrings transformation method is a relatively new direction of research, spurred on by the need to incorporate biometrics data into cryptographic algorithms and protocols. Key generation from voice passphrase was proposed by Monrose et al [1][2] and uses a scalable vector of biometric features in conjunction with a randomized lookup table generated using generalized secret sharing scheme. The biometrics iris identification in Davida et al [3] uses a different approach in that error correction codes are used. During enrollment, a digital signature that links the iris biometric is generated and stored onto a trusted authority distributed smartcard. Chang et al [4] utilised user-dependent statistics to generate multiple bits which allow for more compact and distinguishable keys. The feature space is divided into multiple segments allowing more than one bits to be assigned depending on the number of segments specified by tuning the segment width and boundaries. The main security issue with these schemes is that the

0-7695-2475-3/05 $20.00 © 2005 IEEE

keys are permanently associated with the biometric eg. when stolen a new biometric need to be used which is not possible for physiological biometrics. Additional token may be combined with the biometric to allow cancelable key as in Soutar et al [6], which combines the Fourier transforms of biometric images with a random digital key enabling the key, or bioscrypt to be modified later in the event of key loss. However, the scheme did not explain in a satisfactory manner the cryptographic security of the transformations and there were not results published. Goh et al [7] introduced cancelable keys via inner product between randomized token and face data and is advantageous in comparison to Soutar et al as the step is a one-way process. Juels-Wattenberg [8] extended the work in Davida et al [3] by introducing the idea of a fuzzy commitment. A difference vector is computed by taking the difference between the biometric key and a reissuable secret. At verification step, the test biometric is added to the difference vector to recover the secret that will be decoded back to the original secret using error correction code. Next, Juels-Sudan [9] improved the earlier version by incorporating polynomial-based secret sharing on the secret message in their "fuzzy vault" scheme. Clancy et al [10] implemented the fuzzy vault scheme on fingerprints but also pointed out that a perfect Juels-Sudan vault scheme is not possible to be implemented and presented methods to improve and optimally configure the vault for fingerprint data.

The first biometrics hash on dynamic hand-signature was proposed by Vielhauer et al [11,12] which uses a 50-feature-parameter set from dynamic hand-signature and an interval matrix to store the upper and lower threshold permissible for correct identification. Another scheme similar to Vielhauer and Chang et al is Feng-Chan [13] which also uses specific boundaries for each user. The scheme uses 43 features (but not all are published) and reported 8% EER but the uniqueness of the output vector is only 1 in 2^{40}. The limited feature extraction using parameter-based approach in these methods could not support use in cryptographic systems as they are small in key space, the keys are not cancelable and more importantly, they have generally low-entropy. They are also not secure due to storage of user specific statistical boundaries that could be used to recover the biometric features. Yip et al [14] combines the methods of Goh-Ngo and Chang to enable longer and cancelable keys but however, the user-specific key statistics required to correct the feature vector allows an adversary to easily guess the most probable combination from the compromised user boundaries information and reduced number of segments eg. smaller space.

3. Proposed Method

Our method incorporates the inner product-based mixing with random token, multiple-bit discretization and permutation to result in replaceable cryptographic keys, in addition to a longer and unpredictable key space. We improved on earlier work in [14], particularly in the area of security, by (1) using population-wide instead of user-specific boundaries for multiple-bits discretization, (2) forcing the number of segments in discretization space to be of be 2^n so that an adversary has to search all possible space, (3) permutating the pre-keys to deter multiple keys attack, and (4) using error correction codes to compensate for the loss of accuracy due to (1) and (2). The outline of the proposed method (Fig 1) can be loosely divided into three sections: (1) Feature extraction whereby the raw data is processed into a compact representation, (2) Biometric hashing whereby the extracted feature is combined in an irreversible step to result in a binarised pre-key vector and (3) Correction where the pre-key is restored within a permissible threshold to the template key.

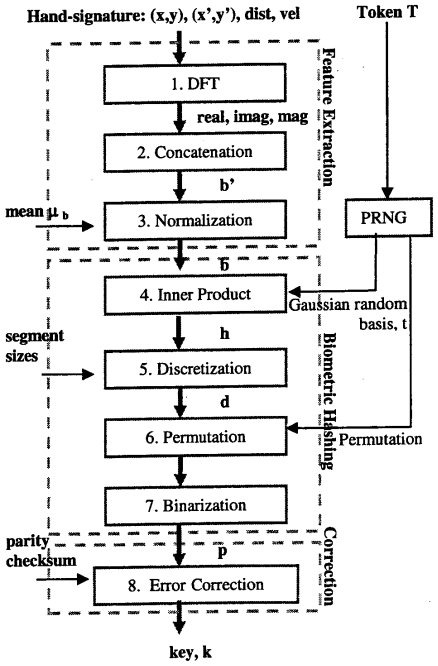

Fig 1: Proposed method

The detailed steps are as follows:-

Step 1. Discrete Fourier Transformation (DFT), first proposed for hand-signature feature extraction by Chan-Kamins [15], is the process of transforming a time series into frequency domain and can be implemented with the Fast Fourier Transform algorithm [16]. The DFT is useful as it provides a translation invariant conversion of the positional and velocity hand-signature signals. A discrete sequence x can be represented by a Fourier integral of form:

$$x(n)=\frac{1}{2\pi}\int_{-\pi}^{\pi}X(e^{j\omega})e^{j\omega n}d\omega \qquad \text{with } j=\sqrt{-1} \quad \text{[Eq. 1]}$$

that represents x as a superposition of infinitesimally small complex sinusoids. Conversely, the Fourier transformation of a discrete time sequence x is defined to be

$$X(e^{j\omega})=\sum_{n=0}^{\infty}x(n)e^{-j\omega n} \qquad \text{[Eq. 2].}$$

In general, the Fourier transformation is a complex-valued function of ω and can be expressed in rectangular form as

$$X(e^{j\omega})=X_R(e^{j\omega})+jX_I(e^{j\omega}) \quad \text{[Eq. 3]}$$

or in the polar form as

$$X(e^{j\omega}) \rightleftharpoons |X(e^{j\omega})|\,e^{\angle X(e^{j\omega})} \qquad \text{[Eq. 4]}$$

where $|X(e^{j\omega})|=\sqrt{X_R^2+X_I^2}$ is the magnitude and $\angle X(e^{j\omega})=\tan^{-1}\frac{X_I}{X_R}$ is the angle of the Fourier transform.

In our experiment, we found that the real, imaginary and magnitude DFT of the complex input of positional information (x+yj) and component velocity (x'+y'j), and real input dist (= $\sqrt{x^2+y^2}$) and vel (=$\sqrt{(x')^2+(y')^2}$) gave the lowest error rates (in terms of Euclidean distance measurement). We also did not perform any additional steps to the raw signals as we noticed that pre-processing using spline interpolation would not improve the performance as also confirmed in [17] because it would introduce spurious points that distort the signals. Each of the transform, z are then normalized by dividing with its norm.

Step 2. Concatenation of the truncated DFTs of the raw signals to form the biometric feature b'. Truncation involves extracting the 13 most significant amplitudes of the DFT as shown in Chan-Kamins. For complex input, the DFT will be non-symmetric hence the first and last 13 significant amplitudes signal were also extracted. For real input, only the first 13 amplitudes are considered.

Step 3. Normalization, by subtraction of the mean vector (obtained at training of 10 signature samples from population), is necessary to ensure that all the biometric feature vectors are centered at the origin. This guarantees that the normalized biometric feature, b, will have zero mean.

Step 4. Iterative inner product as in [7], is easily implemented as the successive inner products, $h_i = \langle t_i \mid b \rangle$ for i = 1,..,r where $1 < r < b_{length}$. The process projects b onto a random subspace and its random basis is formed by random vectors $t_1, t_2, .., t_r$. The important pre-requisite for vectors t_i is that $t_i \perp t_j$ for $i \neq j$ and $t_i \neq t_j$ so that they are all linearly independent. The orthogonalization of the random vectors be can be straightforwardly implemented with Gram-Schmidt process. This guarantees that the projected vector elements will also be randomly independent of each other. The random vectors are generated based on a stored token, T using some pseudo-random number generation (PRNG) following the Gaussian distribution zero mean and unit variance. Again, after projection, h will be normalized to (-1,1).

Step 5. Discretization is an error correction step where the projected vector in real space is transformed into the an index space. Because biometric data are not exact, we consider only those elements that fall within a certain deviation from the mean value to be genuine. This is achieved by dividing the vector element space into 2^n segments by adjusting to the standard deviation (stdev) and the implementation is outlined below:-

- At enrollment, compute population-wide $\text{stdev}_i = \sqrt{\left(\sum_{k=1,u=1}^{K,U}[h_{i,k,u}-\overline{h_{i,k,u}}]\right)/KU}$ for K=10 number of training sample, U number of users and mean $\overline{h_{i,k,u}}$, for each element in h.
- Then estimate and store the number of segments $n_i = \{N \mid \min\{\text{abs}[\frac{1-(-1)}{2^N}-(\text{stdev}_i \times 2 \times k)]\}, N=1..10\}$ for $i=1..b_{length}$.
- At verification, the discretized vector for random projected test input h is $d_i = \left\lfloor \frac{[h_i-(-1)].2^{n_i}}{1-(-1)} \right\rfloor$.

Step 6. Permutation is necessary to provide diffusion into the key space so that the influence of each element is spread to other parts of the pre-key, p. Again, we utilize the PRNG to retrieve another random sequence of indices s (generated based on stored token as the seed), by index sorting. The permutated vector is $p_i = d_{s_i}$.

Step 7. Binary representation is taken in Gray coding, $p_i = \text{gray}(p_i')$ because the consecutive Gray codes differs by 1 bits by Hamming distance, and hence will allow indices (from test input) near to the genuine segment to be corrected later in Step 8, provided that the distances are within a certain permissible threshold.

Step 8. Correction is applied to p to correct it into the template key without compromising the secrecy of the actual key itself. This is done using error correction codes such as Reed-Solomon (RS) or Hamming Error Correction. During enrollment, majority voting is used to determine the template key eg. for every bit, if the majority for all the training pre-keys are 1, set the template key to 1 and vice versa. Then, a parity checksum is generated based on the template key, and only this checksum is stored hence preserving the secrecy of the template key. At verification, the user appends the parity checksum to the test pre-key to hopefully decode it (as closely as possible) into the template key k. If more than a certain threshold of bits are different, the code will not correct ie. the cases of impostors or different users.

4. Security of the Proposed Method

Shannon [5] has outlined several principles of computationally secure cryptosystems: (1) Confusion, (2) Diffusion and (3) Product principles. The basic idea behind these principles is to obscure the redundancies in a plaintext (biometrics) so that the ciphertext (key) will be unpredictable. Confusion conceals the relationship between the biometrics and the key so that a cryptanalyst cannot derive the statistical patterns by studying the keys. Diffusion on the other hand, dissipates the effect of each element of the biometrics over the key space and can be implemented using permutation or a combination of variant permutations. Finally, the Product principle states that the systematic cascading of different types of ciphers in a single cryptosystems will increase the cipher strength provided if the product ciphers are associative but not commutative (forward-only transformation). These principles are typically employed in cipher blocks such as IDEA or DES [18]. In our scheme, the confusion principle is applied in the iterative inner product-discretization step and is analogous to the S-box construction in IDEA which uses multiplication but in binary space. The core transformation of the former uses inner product which is an irreversible process since solving inner products for its individual components is an intractable problem ie. cannot be solved in polynomial time.

Proposition 1: Factoring inner products of biometric vector, b and random vectors, $t=\{t_i\}_{i=1}^{r}$, is an intractable problem if $1 < r < b_{length}$, even if t is known.

Proof: The iterative inner products $\{h_i =< t_i \mid b >\}_{i=1}^{r}$ form r system of equations where $t_i \perp t_j$ for $i \neq j$ and $t_i \neq t_j$. Since there are length(b) number of unknowns and only $r < b_{length}$ number of equations, the system of equations has infinite number of solutions and hence, b is not recoverable in polynomial time. Therefore, factoring b from the inner product h and t is an intractable problem.

The discretization step quantizes the random projected vector space into the 2^n space, and hence, is an irreversible substitution process. The diffusion principle used in the permutation step of our method is analogous to the P-box construction in basic block ciphers. Instead of using a pre-set permutation, we utilized the random sequence generated from the stored token to spread the effect of the distribution evenly. Note that this process is linear and hence can be reversed easily but the reversed result h will not reveal anything about the biometric data, b, due to Prop 1.

Proposition 2: The sequence of iterative inner product, discretization, permutation and binarization obeys the Product principle.

Proof: The iterative inner product can be defined with individual function $R_i: \mathbb{R}^d \times \mathbb{R}^d \rightarrow (-1,1)$, discretization with $D:(-1,1)^n \rightarrow \mathbb{Z}_{2^q}^n$, permutation $P:\mathbb{Z}_{2^q}^n \times \pi(n) \rightarrow \mathbb{Z}_{2^q}^n$ with $\pi(n)$ permutation index, and binarization $B:\mathbb{Z}_{2^q}^n \rightarrow \{0,1\}^*$ for some positive integer q, d size of biometric feature, and n size of the inner product vector. Because R is irreversible from Prop 1 and range D ≠ domain $\{R_i\}_{i=1}^{n}$ so $R \times D$ is non-commutative. Because D is a lossy function, $D \times P$ is non-commutative. Also, P is permutated with random sequence from token T so P is not reversible as long as T is unknown. Hence, $P \times B$ is non-commutative. Therefore, sequence of $\{R_i\}_{i=1}^{n} \times D \times P \times B$ is a non-commutative or one-way function that obeys the Product principle.

5. Empirical Results

There are a few important criteria for measuring the unpredictability of cryptosystems: (1) Completeness [19], (2) the Avalanche effect [20] and (3) Bit-independence [21]. Completeness of a cryptosystems can be guaranteed if each output bit is dependant on all the input elements and not subsets of the input. Meanwhile, the Avalanche effect requires that changing an element in the plaintext should affect the change in the key space with approximately probability of one half.

Proposition 3: Each change in the key is dependent on entire input biometric, b.
Proof: In the iterative inner product step, the random vector t_i is applied to b in individual inner product $h_i = <t_i \mid b>$ for $i = 1,..,r < b_{length}$. Since $t_i \neq t_j$, every h_i is dependent on all (and not a subset) of b.

Proposition 4: The bits of the output pre-key are independent.
Proof: The inner product of biometric b and token t can be decomposed into the orthogonal and parallel (to random vector t_i) components $h_i = <b \mid t_i> = <b \mid t_i^{\perp}> + <b \mid t_i^{\parallel}>$. The requirement that $t_i \perp t_j$ for $i \neq j$ and $t_i \neq t_j$ guarantees that $t_j^{\parallel} \perp t_i^{\parallel}$ and hence, $\forall h_i$ are independent.

Next, we consider the empirical results of the keys produced from the proposed method. We use the hand-signature database from SVC 2004 [22] for Task 1 (without pressure information). Fig 2a-b considered the Hamming distances of the pre-keys for the genuine users, skilled forgers and random forgers. Fig 2a shows the distribution for different token scenario while the worst case scenario of the forgers using stolen tokens is depicted in Fig 2b, both for k=2. The selection of optimal configuration k=2 was done based on the mean distribution of the various users (Fig 3) and the equal error rates (EER) (see Fig 4) for varying k. The chosen configuration has the lowest EER for the worst case scenario of skilled forgery with stolen token. Note that in Fig 3, the mean of 0.5 for the random user (with different token) case is consistent with the Avalanche effect. Because the skilled forgeries (with different tokens) are more similar to the genuine user case, its distribution is about 0.4. The EERs for random and skilled forgery (with different token) are 0% and <=2%. The lowest EER between genuine and skilled forgery with stolen token is ~14.1% and genuine and random curves is ~6.4%.

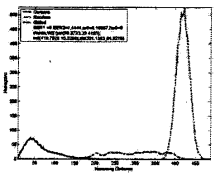

Fig 2a: Different Token Scenario (k=2)

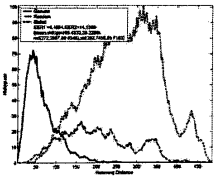

Fig 2b: Same Token Scenario (k=2)

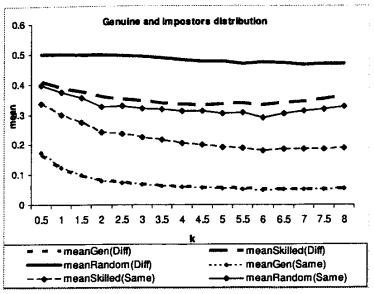

Fig3: Mean distribution of genuine & impostor (no correction)

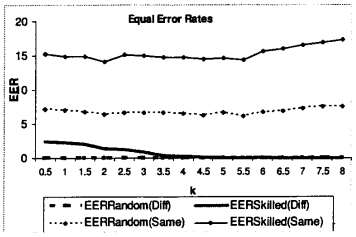

Fig 4: Equal error rates (no correction)

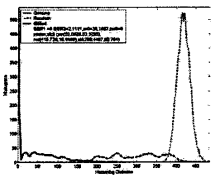

Fig 5a: Different Token scenario (k=2), corrected

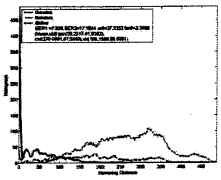

Fig 5b: Same Token scenario (k=2), corrected

Fig 5a & 5b show the effect of error correction using RS with symbol size M=6, code size K=33, for both optimal and worst cases respectively. This configuration is selected based on the mean distribution and EER shown in Fig 6 & 7 using various correction codes of RS and Hamming. Note that for the different token scenario, although the genuine and skilled forgery distributions shifted towards zero, the random forgery remains at 0.5 as with the no-correction case. From Fig 6, Hamming is not a suitable choice as the skilled forgeries were over corrected. For the worst case of stolen tokens, both the skilled and random impostor distribution shifted left, and have higher skilled EER ~17% and Random EER ~7% using the best configuration. The experiments suggest that the stolen tokens pose a security risk and hence, when a user discovers that his token has been lost, should

replace and register for new token. The replacement of token will not involve revealing the information about the actual biometrics ie. the user need not change his signature.

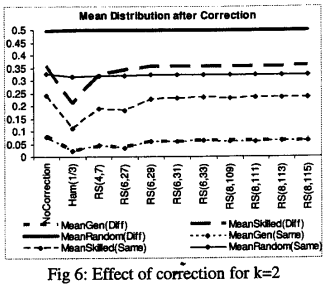

Fig 6: Effect of correction for k=2

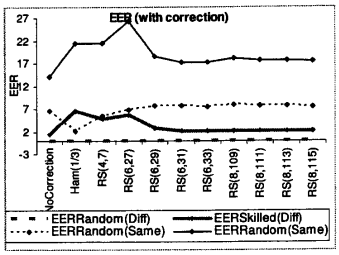

Fig 7: Equal error rates (after correction)

6. Conclusion

We believe that the use of block cipher principles in our method is a significant contribution to the design of secure biometric authentication not realizable in conventional biometric key generation system that required template and/or key statistics storage and where the keys are non-replaceable. The experiment results confirm the proposed method demonstrates high unpredictability of key space and as long as the tokens are not stolen, cryptanalysis will be reduced to only brute-force attack on the key space. The one-way transformation and non-storage of user-specific statistics guarantee that an adversary cannot recover the biometric feature vector from the stolen keys.

7. References:

[1] Monrose, F., Reiter, M.K., Li, Q. & Wetzel, S. (2001). Cryptographic Key Generation from Voice, Proceedings of the 2001 IEEE Symposium on Security and Privacy, May 2001.

[2] Monrose, F., Reiter, M.K., Li, Q., Lopresti, D.P. & Shih, C. (2002). Toward Speech-Generated Cryptographic Keys on Resource Constrained Devices, Proceedings of the 11th USENIX Security Symposium, 2002

[3] Davida, G., Frankel, Y., Matt, B.J. & Peralta, R. (1999). On the Relation of Error Correction and Cryptography to an Off Line Biometric Based on Identification Scheme, WCC99, Paris

[4] Chang, Y.C., Zhang, W. & Chen, T. (2004). Biometric-based Cryptographic Key Generation, IEEE Conference on Multimedia and Expo, Taiwan

[5] C. E. Shannon (1949), Communication Theory of Secrecy Systems, *Bell Systems Technical Journal*, Vol. 28, pp.656-715

[6] Soutar, C., Roberge, D., Stoianov, A., Gilroy, R. & Kumar, B.V.K.V. (1998). Biometric Encryption Using Image Processing. SPIE 3314: pp 178-188

[7] Goh, A. & Ngo, D.C.L. (2003). Computation of Cryptographic Keys from Face Biometrics, 7th IFIP CMS 2003, Torino, Springer-Verlag LNCS2828

[8] Juels, A. & Wattenberg, M. (1999). A Fuzzy Commitment Scheme, in Proc. 6th ACM Conf. Computer and Communications Security, G. Tsudik, Ed., 1999, pp.28-36

[9] Juels, A. & Sudan, M. (2002). A Fuzzy Vault Scheme, in Proc. IEEE Int. Symp. Information Theiry, A. Lapidoth & E. Teletar, Eds., 2002, p.408

[10] Clancy, T.C., Kiyavash, N. & Lin, D.J. (2003). Secure Smartcard-based Fingerprint Authentication, ACM SIGMM 2993 Multimedia, Biometrics Methods & Applications Workshop, pp.45-52

[11]Vielhauer, C. & Steinmetz, R. & Mayerhorf, A. (2002). Biometric Hash based on Statistical Features of Online Signatures, 16th ICPR 2002.

[12] Vielhauer, C. & Steinmetz, R. (2004). Handwriting: Feature Correlation Analysis for Biometric Hashes, EURASIP Journal on Applied Signal Processing, Special Issue on Biometric Signal Processing, Volume 2004, Number 4.

[13] Feng, H. & Chan, C.W. (2002). Private Key Generation from On-line Handwritten Signatures, Information Management and Computer Security, MCB UP Limited, pp. 159-164.

[14] Yip, W.K., Goh, A., Ngo, D. & Teoh, A. (2005). Efficient Generation of Replaceable Cryptographic Keys from Dynamic Handwritten Signatures, ICBA 2006, Hong Kong (accepted)

[15] Chan, F.L. & Kamins, D. (1989). Signature Recognition Through Spectral Analysis, Pattern Recognition, Vol. 22, Issue 1, pp. 39-44

[16] Cooley, J.W. & Tukey, J.W. (1965). An Algorithm for Machine Calculation of Complex Fourier Series, Math. Comp., 19, 297–301

[17] Lei, H. & Govindaraju, V. (2004). A Study of the Consistency of Features for On-line Signature Verification, SSPR, Portugal

[18] Schneider, B. (1996). Applied Cryptography, 2nd Edition, John Wiley, 1996

[19] Kam, J. and Davida, G. (1979). Structured Design of Substitution-Permutation Encryption Networks. IEEE Transactions on Computers. C-28(10): 747-753.

[20] Feistel, H. (1973). Cryptography and Computer Privacy. Scientific American. 228(5): 15-23.

[21] Webster, A.F. & Tavares, S.E. (1986). On the Design of S-Boxes, CRYPTO 85, Springer-Verlag, NY, pp. 523-534.

[22] SVC 2004: First International Signature Verification Competition, http://www.cs.ust.hk/svc2004/