A Novel Crypto-Biometric Scheme for Establishing Secure Communication Sessions Between Two Clients

Sanjay G. Kanade Dijana Petrovska-Delacrétaz
Bernadette Dorizzi
Institut Mines-TELECOM: TELECOM SudParis,
Département Electronique et Physique, 9 Rue Charles Fourier, 91011, Evry, France.
E-mail: {Sanjay.Kanade,Dijana.Petrovska,Bernadette.Dorizzi}@it-sudparis.eu

Abstract: Biometrics and cryptography are two tools which have high potential for providing information security and privacy. A combination of these two can eliminate their individual shortcomings, such as non-revocability, non-diversity, and privacy issues in biometrics and need of strong authentication in cryptography. Crypto-biometric systems combine techniques from biometrics and cryptography for these purposes, and more interestingly, to obtain biometrics based cryptographic keys. In this paper, we address the problem of sharing these keys. We propose a crypto-biometric scheme in which two clients can share a session key securely and establish a secure communication session. The scheme involves a Central Authority for Registration and Authentication (CARA) with which the clients are registered. The CARA stores biometric data only in transformed, cancelable form, allowing for easy revocation of the templates and protecting privacy. There are two distinctive features of this protocol (1) it achieves mutual authentication and starts secure communication between *two clients* which may be previously unknown to each other, and (2) this protocol works even if the two clients use different biometric modalities in the same (as well as in different) session.

1 Introduction and Background

Nowadays, information exchange via electronic means is a widely employed task. While the transfer of infirmation is a day-to-day need, it is also required to protect the privacy of this information. The information may be sensitive and be meant for use of only designated entities. In order to protect the privacy of this information, its transmission is generally secured through cryptographic means. The information is first converted into unreadable form through a process called as encryption before sending it. The receiver needs to perform a decryption operation to retrieve the information after receiving it. The encryption and decryption operations depend on long cryptographic keys. Generally, only those who have the correct keys in possession can recover the transmitted information. However, because these keys are long (e.g., the Advanced Encryption Standard (AES) [aes01] requires keys of sizes 128, 192, or 256 bits), these need to be stored somewhere. Therefore, in order to maintain the secrecy and privacy of the information, these keys should be kept secret and access control mechanisms are required to share the keys only with the designated entities.

Traditionally, knowledge (e.g., passwords) or possession (e.g., tokens) based authentication is used in cryptographic systems. These authenticators are assigned to the user identity, and thus, are not strongly associated with the user identity. Therefore, it is possible that the authenticator gets stolen or lost. It can also be willfully shared making it easy for the user to repudiate. Biometrics, defined as automatic recognition of persons based on their physical or behavioral characteristics, can help in this regard. In biometrics, person's biological (e.g., fingerprint, iris, face, etc.) or behavioral (e.g., signature, gait, etc.) characteristics are used to establish his identity. These characteristics are strongly bound to the user's identity and are difficult to steel and/or forge. Because of this ability of biometrics, in recent years (since 1998), researchers have been trying to combine it with cryptographic systems in order to obtain cryptographic keys strongly linked to the user's identity. Such systems combining biometrics with cryptography are denoted as crypto-biometric (or biometric crypto) systems. Details about crypto-biometric systems can be found in [Mar10, KPDD12].

A straight-forward and the easiest way to integrate biometrics into cryptographic systems is first to carry out biometrics based user verification, and on successful verification, release a stored cryptographic key. However, this mode of employment results in a two-stage system the link between them being the biometric system verification result. This result is a one bit (yes/no) response. In this way, it forms a bottle-neck in the system and can be easily attacked (e.g., by a Trojan horse replacing the biometric system module to replace the one-bit information).

Additionally, biometric system have problems of their own such as non-revocability, non-diversity, and possibility of privacy compromise. Non-revocability relates to the fact that biometric characteristics are permanently associated with the user. If the biometric information stored in a database is compromised, it cannot be replaced with a new one. Therefore, it becomes unusable in that system and possibly in all other biometric systems based on that characteristic. Moreover, the templates obtained from the same biometric characteristic stored in different databases are substantially similar resulting in lack of diversity. This can allow cross-database matching and can compromise privacy.

The problems of non-revocability, non-diversity, and possibility of privacy compromise of biometric systems can be resolved with the techniques denoted as cancelable biometrics [RCCB07, LN07, BSW07, KPDD09]. A general idea behind these systems is to apply a user specific (one-way) transformation to the reference biometric template before storing it in the database. The same transformation is applied to the biometric information at the verification time and the comparison is done in the transformed domain. Since the transformation is unique for each user, in case of compromise, it can be changed and the compromised template can be revoked. However, the verification result in this case is also a one-bit (yes/no) response. Therefore, the problem of weak link between biometrics and cryptography described above still exists in these type of systems and these systems cannot provide strong cryptographic keys.

Fortunately, there are other ways of combining biometrics with cryptography, in which, a multi-bit cryptographic key is obtained with the help of biometrics. The key thus obtained is denoted as crypto-biometric key. One way to obtain these crypto-biometric keys is to extract it directly from biometric information. These systems are denoted as biometrics

based cryptographic *key generation* systems. Some examples of key generation systems are [DFM98, MRW99, ATIS09]. Since the keys are multi-bit information, the entropy is much higher than using the classical biometric verification system.

Other widely studied approach of obtaining crypto-biometric keys is to bind a random bit-string with the biometric data during enrollment and regenerate it using another set of authentic biometric data at the time of verification. This method is denoted as *key regeneration* or *key binding* [JNN08]. Some examples of these system can be found in [JW99, JS02, DRS04, HAD06, KCK+08].

However, when it comes to applications to cryptography, the crypto-biometric systems still need some mechanism to share the crypto-biometric keys. There are two main types of cryptography: symmetric-key cryptography and public-key cryptography. In symmetric-key cryptography, the same key is used for encryption and decryption. Therefore, both (or all) the parties involved in cryptographic information exchange need to have this symmetric key. On the other hand, public-key cryptography involves a pair of keys, a public key and a private key, which are mathematically related. Generally, the public key is shared with others and is used for encryption. The private key is kept secret and is required to decrypt the information encrypted using the associated public key. However, the public-key cryptography cannot be used for real-time applications because of its speed and hence, in widely used protocols such as the Transport Layer Security (TLS) [DR08], a symmetric key is shared with the help of public-key cryptography. Moreover, for security reasons, a new symmetric key, called as session key, is used during each communication session.

Many systems can be found in literature which can obtain crypto-biometric keys. However, there are very few which address the problem of using them for establishing secure communication sessions. Some of these systems are summarized below.

Boyen et al. [BDK+05] proposed a biometrics based remote authentication protocol in which fuzzy extractors [Boy04] are used. Tang et al. [TBCP08] also proposed an authentication protocol based on fuzzy extractors. This protocol provides security by employing the ElGamal public-key cryptosystem [Elg84]. It can generate and share Cryptographic keys while preserving some aspects of the user privacy. However, both these systems require storage of classical biometric templates. Additionally, the Tang et al. [TBCP08] scheme needs a secure communication link between the parties for exchanging information.

Ueshige and Sakurai [US06] proposed a one-time authentication protocol which can create biometric authentication based secure sessions. In this protocol, a one-time transformation is generated which is unique to the session. This transformation is applied to the stored templates as well as to the fresh biometric data. The comparison between the two transformed templates is carried out to establish the authenticity of the subject. Bringer et al. [BCI+07] employed the Goldwasser-Micali cryptosystem [GM82] for biometric authentication. This system allows the biometric comparison to be carried out in the encrypted domain. In order to protect the privacy, the system makes sure that the biometric data stored in the database cannot be explicitly linked to any user identity, but it only detects whether the data belonging to an identity is present in the database. Recently Barni et al. [BBC+10] proposed a scheme for privacy preserving authentication based on fin-

gerprints. This scheme employs the ElGamal cryptosystem which facilitates biometric comparison in encrypted domain. Upmanyu et al. [UNSJ10] proposed a blind authentication protocol which is also based on homomorphic encryption. The drawback of these authentication protocols is that they can only authenticate the subject. But they cannot produce the cryptographic keys required for secure communication.

The "Secure Ad-hoc Pairing with Biometrics: SAfE" protocol proposed by Buhan et al. [Buh08] employs the fuzzy extractor scheme and can be used to establish a secure link between two parties. This protocol is different than the others described above because it does not involve a biometric template database or server. However, the drawback of this protocol is that it shares the biometric data between the two parties and requires mutual trust among them. It also requires a secure channel for exchanging the biometric data.

Abid and Afifi [AA09] proposed an ePassport authentication protocol based on elliptic curve cryptography. They proposed to employ biometrics, specifically fingerprints, to securely generate the parameters of the elliptic curve. These parameters are used for the ePassport bearer's authentication. The practical difficulty of this approach is that it requires a stable input from biometrics.

Following the concept of session keys, Scheirer and Boult [SB08, SB09] proposed "bipartite biotokens". In this scheme, their earlier proposal of revocable biotokens [BSW07] is combined with fuzzy vaults [JS02] which enables to securely share keys using biometrics. A series of transformations is shared between the client and the server. A new transformation (in succession) is applied in every communication session. The bipartite biotokens are session specific and make it possible to share session specific data between two parties.

Recently, we proposed a multi-Biometrics based Session-Key Generation and Sharing (BSKGS) protocol [KPDD11]. This protocol has important features such as: (1) secure generation and sharing of multi-biometrics based session keys, (2) cancelability/revocability, template diversity, and privacy protection, (3) mutual authentication between the two parties, (4) no sharing of biometric data and other sensitive information.

However, this protocol cannot work in two situations: (1) to establish a secure communication link between two parties or clients which are unknown to each other, and (2) when these two parties do not want to use a common biometric modality. The BSKGS protocol above is for establishing secure communication session between a client and a server where the client is, *a priori*, enrolled with the server. Additionally, the two parties may not be willing to use the same biometric modality. There may be situations where one of the parties does not possess a particular biometric modality which the other party intends to use, e.g., one may lack voice.

In this paper, we address these two issues. Here, we propose a crypto-biometric scheme which can establish secure communication sessions between two clients which are enrolled in a common database with biometric modalities of their choice. It uses the BSKGS protocol from [KPDD11] and inherits all its features. Moreover, the two parties do not need to use the same biometric modality. They can choose their own biometric modality to authenticate with.

This paper is organized as follows: the multi-biometrics based session key generation

and sharing (BSKGS) protocol from [KPDD11] is first summarized in Section 2. The proposed scheme for establishing secure communication sessions between two clients is then presented in Section 3. Security analysis of this scheme is given in Section 4. Finally, the conclusions and perspectives are given in Section 5.

2 Multi-Biometrics Based Session-Key Generation and Sharing (BSKGS) Protocol

This protocol for multi-biometrics based session key generation and sharing, shown in Fig. 1, was recently proposed by the authors in [KPDD11]. It uses the multi-biometrics based key regeneration system [KPDD10] for obtaining crypto-biometric keys. Figure 1 shows a schematic diagram of this protocol.

The enrollment process, which is securely carried out off-line, is not shown in Fig. 1. During enrollment, individual cancelable templates (collectively denoted as θ_i^c for simplicity) of the user i for different modalities are generated and stored. In addition, a part of the transformation key, K_i^x, is also stored.

At the time of authentication and session establishment, following procedure is performed:

1. The client and the server decide on the security level and choice of biometric modalities to use for authentication during the current session.
2. The client captures fresh biometric data and first creates cancelable templates using his transformation key. Using these cancelable templates and a randomly generated key K_r, he can create a new locked code θ_{lock} using the algorithm in [KPDD10]. The random key K_r is hashed twice to obtain $H(H(K_r))$ and is sent to the server along with θ_{lock}.
3. The server attempts to regenerate a trial value K_r' of the random key, from the locked code θ_{lock}, K_i^x, and the stored cancelable templates θ_i^c.
4. A comparison between double hashed version of the random and the regenerated keys (i.e., between $H(H(K_r))$ and $H(H(K_r'))$) is carried out. Ideally, if the server has the template of the client (or conversely, if the client provides correct authentication information) it can regenerate the random key correctly. If the two hash values are equal, the server considers the client to be genuine and sends a single hashed version of the regenerated key, $H(K_r')$, to the client.
5. When the client receives the single hashed version $H(K_r')$, it is compared with $H(K_r)$. If these are found to be equal, then the client can be assured that the server has actually received the key K_r. Now they can start secure communication with K_r as the crypto-biometric session key.

As can be noted, this protocol establishes secure communication session between the client and the server. The scenario we are addressing in this paper is communication between two clients where this protocol cannot work.

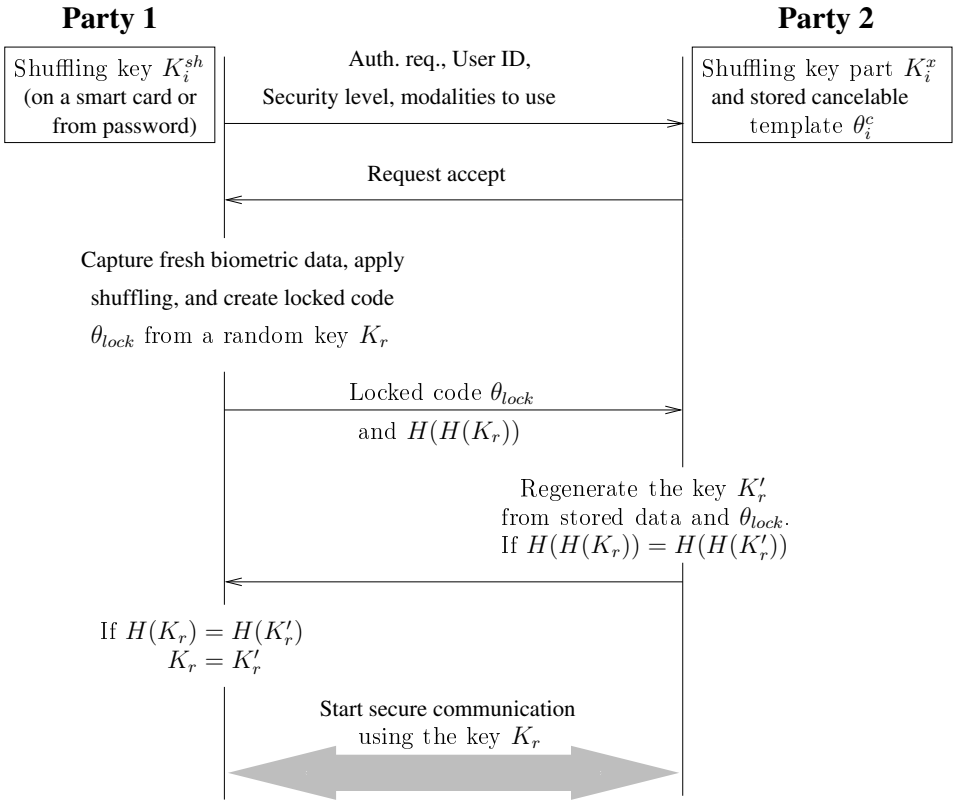

Figure 1: Multi-biometrics based Session Key Generation and Sharing (BSKGS) protocol [KPDD11].

3 Proposed Protocol for Establishing Secure Session Between Two Parties

The proposed crypto-biometric scheme involves a Central Authority for Registration and Authentication (CARA) with which the parties need to be registered. As in the BSKGS protocol, the client registration procedure is carried out off-line at a secure place. During registration, CARA saves cancelable templates of each client in a database.

When two parties, Client A and Client B, want to communicate with each other securely, they follow the protocol shown in Fig. 2 which has following steps:

1. Client A sends a request for secure communication to Client B.
2. Client B responds with a accept signal.
3. Client A then communicates with CARA to establish a secure session by employing the BSKGS protocol and obtains a session key K_A^s. Similarly, Client B obtains his

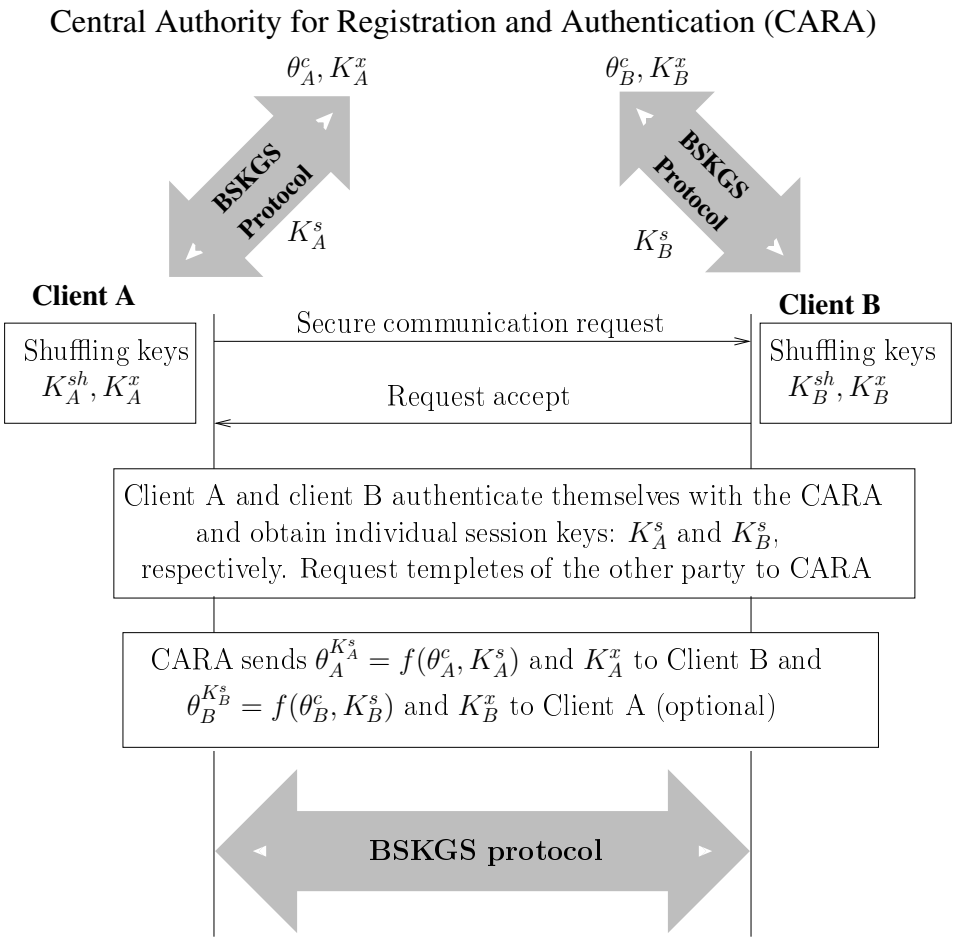

Figure 2: Proposed scheme for establishing secure communication sessions between two clients.

session key K_B^s from CARA.

4. Client A informs CARA about the forthcoming communication request between A and B.

5. CARA then applies the cancelable transformation on the stored template θ_A^c of Client A based on his session key K_A^s to obtain $\theta_A^{K_A^s}$. Note that the template θ_A^c of Client A is already a cancelable template. Which means that the transformation is applied a second time on the biometric data. This double transformed data $\theta_A^{K_A^s}$ along with the shuffling key part K_A^x is sent to Client B.

6. Client B now has a cancelable template $\theta_A^{K_A^s}$ of Client A. Client A has all the data necessary to obtain $\theta_A^{K_A^s}$, which include his own biometric information, his first

transformation key which he obtains during enrollment with CARA, and the current session key K_A^s. With this information, Client A and Client B follow the BSKGS protocol above to generate a crypto-biometric session key and start secure communication with that key.

In this way, the two clients can share a session specific cryptographic key with the help of CARA. Note that, in the protocol shown in Fig. 2, only client B obtains a cancelable template of client A. There is no obligation on the clients to use the same biometric modality. In fact, the Client A and Client B can decide which biometric modalities to use for authentication with the CARA. CARA will send a template corresponding to that modality to the other client. This is an important feature of the proposed scheme which can allow people to chose their own biometric modality for authentication. It is also a practically viable solution since the two clients may not be able to use the same biometric modality because of physical or health issues.

4 Security Analysis

Security of the proposed cryptosystem relies on the security of the the BSKGS protocol and the key regeneration system it uses. The key regeneration system used in this protocol was proposed by the authors in [KPDD10]. This key regeneration system can obtain long crypto-biometric keys based on multi-biometrics (illustrated by iris and facial biometrics combination in particular). The entropy of this scheme is estimated using the method described by Hao et al. [HAD06]. It calculates the degrees of freedom in the biometric data by the procedure given in [Dau03] and then based on the sphere packing bound, calculates the number of brute force attacks needed to obtain the key from the template without having the specific authentication data. The entropy estimated in this way is 183 bits. This entropy indicates the difficulty an attacker will have in obtaining the crypto-biometric key when he has access to the locked code templates without having the required authentication data of the clients. Note that the initial data transmission takes place through unprotected links. However, the data transferred at that time is communication requests, locked codes, and hash values of the random keys, none of which reveals the information about the session key or biometric data.

Both the clients are needed to be registered with the CARA in order to start secure communication. Additionally, both must authenticate themselves with CARA to obtain the temporary cancelable templates of the other party using the BSKGS protocol. Thus, an attacker cannot obtain the templates of any client (e.g., Client A) without having authentication data of the other client (e.g., Client B).

There is an option that Client A can also request a cancelable template of Client B from CARA. In this case, the BSKGS protocol is run twice between Client A and Client B. This additional step can significantly enhance the security of the system.

Even if an attacker obtains the temporary cancelable template of a client, e.g., of Client A, it has to be used in that session only. The template that is transferred by CARA to the other

client B is generated by applying a transformation on the stored cancelable templates. The transformation key used for this operation is the temporary session key of Client A which is not sent to Client B. Thus the attacker cannot obtain the biometric data even if he obtains the temporary cancelable template.

5 Conclusions and Perspectives

The crypto-biometric system proposed in this paper facilitates secure communication between two clients with the help of a Central Authority for Registration and Authentication (CARA). They can achieve mutual authentication which is backed up by the involvement of biometrics. The two parties do not need to use the same biometric modality for authentication. The biometric data is stored in cancelable form at the CARA and is not shared with anyone. A new transformation is applied to the cancelable data before sharing it with others. In this way, the system possesses revocability, diversity, and privacy properties.

The proposed system can be used for secure communication between two clients. It has a potential to replace existing protocols such as TLS. Alternatively, it can be used along with the existing protocols adding another layer of security.

References

[AA09] Mohamed Abid and Hossam Afifi. Towards a Secure e-Passport Protocol Based on Biometrics. *Journal of Information Assurance and Security (JIAS) (Special Issue on Access Control and Protocols)*, 4(4):338–345, 2009.

[aes01] Advanced Encryption Standard (AES), November 2001.

[ATIS09] Savvas Argyropoulos, Dimitrios Tzovaras, Dimosthenis Ioannidis, and Michael G. Strintzis. A Channel Coding Approach for Human Authentication From Gait Sequences. *IEEE Transactions on Information Forensics and Security*, 4(3):428 – 440, 2009.

[BBC+10] Mauro Barni, Tiziano Bianchi, Dario Catalano, Mario Di Raimondo, Ruggero Donida Labati, Pierluigi Failla, Dario Fiore, Riccardo Lazzeretti, Vincenzo Piuri, Fabio Scotti, and Alessandro Piva. Privacy-Preserving Fingercode Authentication. In *The 12th ACM Workshop on Multimedia and Security (MM&Sec10)*, Rome, Italy, Sept 2010.

[BCI+07] Julien Bringer, Hervé Chabanne, Malika Izabachène, David Pointcheval, Qiang Tang, and Sébastien Zimmer. An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication. In *The 12th Australasian Conference on Information Security and Privacy (ACISP '07)*, 2007.

[BDK+05] Xavier Boyen, Yevgeniy Dodis, Jonathan Katz, Rafail Ostrovsky, and Adam Smith. Secure Remote Authentication Using Biometric Data. In *Eurocrypt*, 2005.

[Boy04] Xavier Boyen. Reusable Cryptographic Fuzzy Extractors. In *11th ACM Conference on Computer and Communications Security (CCS)*, 2004.

[BSW07] T. E. Boult, W. J. Scheirer, and R. Woodworth. Revocable Fingerprint Biotokens: Accuracy and Security Analysis. In *IEEE Conference on Computer Vision and Pattern Recognition*, pages 1–8, June 2007.

[Buh08] Ileana Buhan. *Cryptographic Keys from Noisy Data*. PhD thesis, University of Twente, Netherlands, 2008.

[Dau03] John Daugman. The Importance of Being Random: Statistical Principles of Iris Recognition. *Pattern Recognition*, 36(2):279–291, February 2003.

[DFM98] G. I. Davida, Y. Frankel, and B. J. Matt. On enabling secure applications through offline biometric identification. In *Proceedings of the IEEE Symposium on Privacy and Security*, pages 148–157, 1998.

[DR08] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. Request for Comments: 5246, Internet Engineering Task Force (IETF), August 2008.

[DRS04] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *Proceedings of the Eurocrypt 2004*, pages 523–540, 2004.

[Elg84] Taher Elgamal. A Public Key Cryptosystem and a Siggnature Scheme Based on Discrete Logarithms. In *Crypto*, pages 10–18, 1984.

[GM82] Shafi Goldwasser and Silvio Micali. Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information. In *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*, 1982.

[HAD06] Feng Hao, Ross Anderson, and John Daugman. Combining Crypto with Biometrics Effectively. *IEEE Transactions on Computers*, 55(9):1081–1088, 2006.

[JNN08] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar. Biometric Template Security. *EURASIP Journal on Advances in Signal Processing*, (Article ID 579416):17 pages, 2008.

[JS02] A. Juels and M. Sudan. A fuzzy vault scheme. In A. Lapidoth and E. Teletar, editors, *Proc. IEEE Int. Symp. Information Theory*, page 408. IEEE Press, 2002.

[JW99] A. Juels and M. Wattenberg. A Fuzzy Commitment scheme. In *Proceedings of the Sixth ACM Conference on Computer and communication Security (CCCS)*, pages 28–36, 1999.

[KCK+08] Sanjay Kanade, Danielle Camara, Emine Krichen, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi. Three Factor Scheme for Biometric-Based Cryptographic Key Regeneration Using Iris. In *The 6th Biometrics Symposium (BSYM)*, September 2008.

[KPDD09] Sanjay Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi. Cancelable Iris Biometrics and Using Error Correcting Codes to Reduce Variability in Biometric Data. In *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, June 2009.

[KPDD10] Sanjay Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi. Obtaining Cryptographic Keys Using Feature Level Fusion of Iris and Face Biometrics for Secure User Authentication. In *IEEE CVPR Workshop on Biometrics*, June 2010.

[KPDD11] Sanjay Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi. Multi-biometrics Based Crypto-biometric Session Key Generation and Sharing Protocol. In *ACM Workshop on Mumtimedia and Security (MM&Sec)*, 2011.

[KPDD12] Sanjay Ganesh Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi. *Enhancing Information Security and Privacy by Combining Biometrics with Cryptography*. Morgan & Claypool Publishers, June 2012.

[LN07] Alessandra Lumini and Loris Nanni. An improved BioHashing for human authentication. *Pattern Recognition*, 40(3):1057–1065, March 2007.

[Mar10] Martin Drahansky. *Biometric Cryptography Based on Fingerprints: Combination of Biometrics and Cryptography Using Information from Fingerprints*. LAP LAMBERT Academic Publishing, 2010.

[MRW99] F. Monrose, M.K. Reiter, and R. Wetzel. Password hardening based on keystroke dynamics. In *Proceedings of the Sixth ACM Conference on Computer and communication Security (CCCS)*, pages 73–82, 1999.

[RCCB07] Nalini K. Ratha, Sharat Chikkerur, Jonathan H. Connell, and Ruud M. Bolle. Generating Cancelable Fingerprint Templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):561–572, April 2007.

[SB08] W. J. Scheirer and T. E. Boult. Bio-Cryptographic Protocols with Bipartite Biotokens. In *Biometric Symposium*, 2008.

[SB09] W. J. Scheirer and T. E. Boult. Bipartite Biotokens: Definitions, Implementation, and Analysis. In *International Conference on Biometrics (ICB)*, 2009.

[TBCP08] Qiang Tang, Julien Bringer, Hervé Chabanne, and David Pointcheval. A Formal Study of the Privacy Concerns in Biometric-Based Remote Authentication Schemes. In *Information Security Practice and Experience Conference (ISPEC)*, 2008.

[UNSJ10] Maneesh Upmanyu, Anoop M. Namboodiri, Kannan Srinathan, and C. V. Jawahar. Blind Authentication: A Secure Crypto-Biometric Verification Protocol. *IEEE Transactions on Information Forensics and Security*, 5(2):255–268, June 2010.

[US06] Yoshifumi Ueshige and Kouichi Sakurai. A Proposal of One-Time Biometric Authentication. In H. R. Arabnia and S. Aissi, editors, *Security and Management*, 2006.