Biometric Creation of Digital Signatures and Their Application in Blockchain

Nenad Badovinac(✉) and Dejan Simić

Faculty of Organizational Sciences of the University of Belgrade, Beograd, Serbia
nenad.badovinac@azelija.rs, dejan.simic@fon.bg.ac.rs

Abstract. Blockchain transactions are secured from falsification by appending a digital signature using the PKI (Public key infrastructure). When signing a blockchain transaction, the user must have access to his private key, which must be kept on a hardware or software token. The scientific works analyzed in this paper represent the application of Blockchain technology in payment card system, and in this way the architecture of the system is simplified. The fusion of biometric technology and blockchain technology, which allows a blockchain transaction to be signed without tokens and eliminates the need for a third-party transaction validator, has improved the functionality of current payment card systems. This paper contains three contributions. It is first demonstrated how different biometrically based digital signature models reported in the literature compare, then it is demonstrated how blockchain transactions can be digitally signed using digital signatures made using biometrics, and finally, because biometric digital signature creation methods have not attracted much attention in the scientific public, a detailed comparison of the FIBS (Fuzzy Identity Based Signature) scheme and the Fuzzy signature method was presented as for these two schemes was shown that we can implement them in Blockchain and Payment Card System.

Keywords: Blockchain · Biometrics · Fuzzy signature · PKI · Payment card system

1 Introduction

The process of conventional electronic banking transactions, in terms of withdrawing cash from an ATM (Automated Teller Machine) or paying at a POS (Point of Sale) device implies that the user will insert a chip card into the device. Since the advent of chip cards, technology has advanced, but the process of electronic payment on POS devices has remained the same. Basically, cardholders still have to carry multiple payment cards and adapt to different authorization processes.

In [1], the authors proposed a e-payment model in which the user replaces all his payment cards with one smart card and biometric authentication. They presented a kind of upgrade of the electronic payment model in which the user must enter the PIN and the biometric fingerprint data are used to create it. This concept simplifies the electronic payment process and complies with PSD2 (Payment Services Directive 2), a requirement set out by the European Union SCA (Strong Customer Authentication).

M. Mihić et al. (Eds.): SymOrg 2022, LNNS 562, pp. 3–13, 2023.
https://doi.org/10.1007/978-3-031-18645-5_1

Information must be exchanged during payment card bank transactions between the third-party validator, the cardholder, the merchant, the issuing bank, and the merchant bank. In addition, the merchant pays a fee for accepting and processing payment transactions. For merchants, blockchain technology has simplified and made the process of electronic payment cheaper, eliminating the need for third-party transaction verifiers [2].

Biometric technology enables the cardholder to be authenticated in electronic payment systems, without the need to remember the authentication PINs, because he/she can be authenticated using his/her biometric characteristics [3]. Some of the advantages of this technology are that biometric data cannot be alienated, the user does not need to carry it as a smart card or to remember it as a password.

Creating a decent biometric system might be a difficult process. System designers must be professionals in a variety of scientific disciplines. Also, while building a biometric system, user engagement with the system is a vital factor to consider [4].

In [5], the authors presented the results of comparing modern methods of user biometric authentication on mobile applications. The results showed that Iris has the highest score of user authentication based on biometric data with a score of 8.53, while PIN has the lowest score of 1.02. Fingerprint has a rating of 7.86. It was concluded that the biometric modalities Iris, Face Image and Fingerprint gave the best results in the authentication process on mobile applications.

In this paper, solutions for creating digital signatures using biometric data are analyzed. This analysis will allow us to propose a model of payment card systems with biometrically digitally signed blockchain transactions in further research.

Biometric models of digital signing of blockchain transactions enable digital signing of blockchain transactions of electronic payment suggest biometrically created private and public keys. Table 1 presents the characteristics of methods for creating digital signatures using biometric data. FIBS methods for creating biometrically based digital signatures that use biometric data to sign blockchain transactions are analyzed and presented in Table 2. The basic difference between the FIBS scheme and the Fuzzy signature method is also presented.

Section 2 provides an overview of the available literature describing digital signature models using biometric data. In Sect. 3, a comparison of the biometric-digital signature concept is provided. In Sect. 4, the application of the FIBS biometric scheme is proposed. Section 5 provides a conclusion and Sect. 6 presents the literature used.

2 Literature Review

Blockchain technology allows us to exchange data with a group of people or machines, that is not copied but distributed. This creates a decentralized distribution of data that gives all members access to data at the same time. All data changes are recorded in real time and are transparent. Blockchain stores encrypted blocks of data and then links them in a chain to form a chronological sequence of data that will be shared among members of the Blockchain network. There are Public Blockchain networks that are applied in networks that use for example digital cryptocurrencies, while Private blockchain networks are used by companies, for example banks [6].

In the paper "Blockchain in Payment Card Systems" [28] the application of private blockchain technology in the electronic payment process is presented eliminates the need for third-party validators.

The disadvantage of a conventional Blockchain transaction signature is that there is no confirmation that the creator of the transaction is the actual user under whose name the creator of the transaction signs, since the private key may be used by another person, but only confirms that the transaction's creator has a valid private key.

In scientific paper [7], the authors showed that classical digital signatures are insufficiently secure and therefore proposed new encryption schemes for blockchain transactions. They suggested a more secure signature scheme based on the principle of using the biometric data of the blockchain transaction creator. Instead of conventional methods, it is possible to use biometric methods to create a blockchain transaction's digital signature.

Biometrics is a combination of several technological areas of competence. Some of the areas related to biometrics are pattern recognition, computer programming, experience design, operating systems, and system administration [8], and as such we can implement it with different technologies.

In the available literature, the authors have published methods of biometric private and public key creation. Uludag et al., In [9] presented several techniques for creating a cryptographic key that use user biometric data instead of using a PIN and password. Yao-Jen Chang et al., in [10] uses biometric data to create stable cryptographic keys. They conclude that any biometric cryptosystem, in order to generate trusted keys, must be able to cope with the changes caused by unstable biometric data.

The contribution of the work in relation to the analyzed literature is the synergy created by the simultaneous application of biometrics and blockchain technology, so that payment systems are more convenient to use and more resistant to possible abuses.

In the available literature, there are Fuzzy Identity Based Signature (FIBS) biometric digital signature methods that enable a signer with an identity w to produce a digital signature using his biometric data that can be confirmed using the identity w' if and and only if w and w' are within the acceptable mutual range [11]. In [7, 12], the authors introduce a new idea of digital signature named fuzzy signature, that is a signature system which involves a "noise" string as a private key, such as biometric data. Their contribution is the construction of a Fuzzy signature scheme that has certain homomorphic properties with respect to encrypted keys. The next chapter provides a detailed comparison of existing solutions for creating a digital signature using biometric data.

3 Comparative Analysis of Existing Digital Signature Solutions Using Biometric Data

The presented characteristics of different cryptographic methods for digital signature using biometric data are shown in Table 1. Sashank, Singhvi et al. in [13] for the purpose of correcting errors that occur during extracted unstable biometric data, developed a technique integrated with ReedSolomon codes. Lifang Wu et al. [14] created a biometric cryptosystem that uses biometric facial image data. Nguyen Thi Hoang Lan et al. [15] created a solution that uses a biometric key to encrypt private keys. Ratha et al. [16]

presented a technique for creating biometric identifiers from a fingerprint image. Their technique allows the replacement of the biometric identifier in case the biometric key is compromised. Rathgeb et al. [17] created a cryptographic model that uses unstable biometric characteristics of the iris of the eye to create keys by the Fuzzy method. Hao et al. [18] presented a safe method to apply the biometric characteristics of the iris of the eye in cryptographic applications. Cryptographic keys are created from an image of the iris of the eye that can be stored on a token resistant to unauthorized use, such as a smart card. Yazhuo Gong et al. [19] created a model for generating PKI keys based on the biometric characteristics of the iris of the eye. This technique uses pseudo random numbers to create cryptographic keys. Jo et al. [20] provided an useful technique for generating digital signatures using biometric features. Syh-Yuan Tan et al. [21] presented model, due to the fuzzy characteristic of biometric data, tolerates errors using Lagrang

Table 1. Characteristics of methods for creating private and public keys from biometric data.

Authors and biometric cryptographic methods	Characteristics
Sashank Singhvi et al. [13]	Private-Public keys, Facial biometrics, 128 bitni AES (Advanced Encryption Standard)
Lifang Wu et al. [14]	Private-Public key, Facial biometrics, simetrical 128 DES (Data encryption standard) algoritham. Reed-Solomon algoritham
Nguyen Thi H. L. et al. [15]	Private-Public key, Fingerprint biometric
Ratha et al. [16]	A technique that applies the advantages of Cancelable Biometrics over other approaches. Case studies of this technique have been described
Rathgeb and Uhl [17]	Private-Public key, key construction from Fuzzy biometric data
Hao et al. [18]	Generating biometric PKI key, Iris biometrics Creates 128 bit AES. Combines Hadamard i Reed-Solomon codes to correct errors
Yazhuo Gong et al. [19]	Digital signature from the biometric data of the iris of the eye. Uses pseudo random numbers to create cryptographic keys
Jo i sur. [20]	Digital signature, RSA (Rivest–Shamir–Adleman) kriptospistem, Fingerprint
Syh-Yuan Tan et al. [21]	Fuzzy identification based on identity (FIBI), uses fingerprint biometric feature
Yongjin Wang et al. [22]	Fuzzy generating Key generator. Facial biometrics
Syh-Yuan Tan et al. [23]	Analyze FIBS scheme vulnerability, Facial

polynomial interpolation. Yongjin Wang et al. [22] presented a method for generating a variable cryptographic key based on biometric data of facial images. Syh-Yuan Tan et al. [23] analyzed the shortcomings of FIBS schemes for generating keys from biometric data.

When extracting the biometric data of the same person, a certain instability of the biometric data used to generate the keys is shown. During each extraction of biometric data, the algorithm creates a different private key [24]. From the presented methods from Table 1, the FIBS scheme tolerates errors of biometric data up to a certain level of tolerance defined by the parameter and this method can be used for biometric digital signing of blockchain transactions [11]. Table 2 shows FIBS schemas and Fuzzy signature models, and their cryptographic techniques and characteristics.

Table 2. A comparison of biometric authentication methods with the FIBS method and Fuzzy signature method.

FIBS and Fuzzy signature models' authors	Cryptographic technique and features
Shan X. et al., 2021. [16]	The model uses bilinear pairing and Fuzzy extractor. Safety is based on CDH (Computational Diffie-Hellman assumption)
Xiaojun Z. et al., 2017. [24]	Model je neprobojan u okruženjima ROM (Random-Oracle Model) and EUF-ACMIA (Existential forgery on adaptively designed message and ID assault)
Oday A. et al. 2020. [11]	For message attack, the model includes bilinear pairing
Yanhua Z. et al. 2019. [25]	The model is unbreakable in ROM (Random-Oracle Model) surroundings and SU-sID-CMA (Strongly unforgetable against selectively chosen identity and chosen message attacks)
Kenta T. et al. 2019. [12]	The model uses Diffie–Hellman key exchange protocol Uses Hamming distance

A comparison of two FIBS models was performed in [26]. The first model accepts the error specified by the parameter using the Lagrange polynomial, but the second model corrects the error using the Fuzzy extractor. The authors believe that their approaches can be implemented in environments with restricted computational resources. The authors of [24] introduced their FIBS system, which may be used in cryptographic communication environment that makes use of the fingerprint and iris. The authors of [11] presented their concept for increasing security through the use of multimodal biometrics. The authors of [25] presented their FIBS scheme and showed that it is the quickest of those previously accessible in the scientific literature. The authors in [7, 12] presented the Fuzzy signature method which is a no-identity based digital signature scheme in which

the user can directly use their biometric data as a signing key. The user can generate a public key for verification and signature using their biometric data directly.

The main differences between the Fuzzy signature and the FIBS scheme are that FIBS is a special type of identity-based signature (IBS) in which identity strings can be fuzzy data. There is a trusted-party in the FIBS scheme, and it is usually the KGC – (Key Generation Center), which generates the Master Key as a pair of public / secret keys. Then each user's signature key is generated using his biometric data and a Master Key defined by KGC.

In the FIBS scheme, the user cannot independently generate his own signing key, because a Master Key (generated by a trusted-party) is required. After KGC generates the keys, the user must store them securely. On the other hand, the signing key in the Fuzzy signature technique is the user's biometric data, and in this model the user does not have to worry about storing the Private or Master key, since every time digital signatures are generated, the user's biometric data is analyzed.

3.1 FIBS – Fuzzy Identity Based Signature Model

FIBS use fuzzy biometric data, such as fingerprint biometric data, as a cryptographic key. Traditional digital signature techniques necessitate the use of specified data as a key. FIBS allows an individual with identity w to generate a digital signature that can only be validated with identity w if w and w' are within the threshold.

The Fuzzy identity-based signature model consists algorithms [11]:

- SETUP: The generating method makes use of the security and error tolerance parameters n and d. The Master Key and Public Key are both generated.
- KEYGEN: This method generates private keys using the MasterKey and the user's biometric data (w). The result is a Private Key referring to user w.
- SIGN: the algorithm accepts as inputs Public Key, Private Key and Message.
- VERY: The verification method takes as input the Public Key, the user's biometric data, and the appropriate signature. Returns one bit and if $b = 1$ then the digital signature is correct; otherwise the signature is incorrect.

The first phase – Setup; consists of four steps:

- The Agency for Issuance of Biometric Certificates (BCA) verifies the identity the user's and takes over his biometric data.
- Generating the Public key and the Master key.
- Generation of biometric data in combination with a private key
- The Agency BCA shall issue a PKC (public key certificate) by associating a digital signature with a public key.

Second phase – Transaction generation; The sender creates a transaction containing the recipient's PKC and the hash value of the H data.

Third phase – Sign; The message is signed with the Private key kw. Then, utilizing Fuzzy biometric data, a biometric signature is created from the hash value. This transaction is awaiting Validation.

Phase Four – Transaction Verifications; In this step we check the input data which includes: Public Key, identity w', Hash message and corresponding signature as input. The result will be $b = 1$ or $b = 0$. If $b = 1$ The signature is verified correctly.

3.2 Fuzzy Signature Model

The Fuzzy signature model is presented as a fuzzy signature technique in [24]. The four algorithms (Setup, KeyGen, Sign, Ver) define for a fuzzy key configuration:

- Setup: This is the setup procedure, which takes as input the description of the fuzzy key setting and produces a public parameter pp.
- KeyGen: This is the key generation technique that accepts fuzzy data as input and produces a verification key as output.
- Sign: This is the signing method that takes fuzzy data and message as input and returns a signature as output.
- Ver: This is the verification method that accepts fuzzy data and returns either "accept" or "reject" as an output.

The Fuzzy scheme does not have to store the user's private key on any device or server in the cloud, because the user's biometric data acts as his private key [12].

3.3 Comparison of FIBS Scheme and Fuzzy Signature Methods for Creating a Digital Signature

The analyzed FIBS scheme and Fuzzy signature methods enable a blockchain block is created using a biometric digital signature [7, 11]. Blockchain, on the other hand, is used in electronic payment transactions [28]. We compare two biometric digital signature technologies to consider the electronic payment model using the benefits of biometrically signed blockchain transactions. Fuzzy signature does not require auxiliary parameters in relation to FIBS. Table 3 shows a comparison of the characteristics of the FIBS scheme and the Fuzzy signature.

The main differences between the FIBS scheme and the Fuzzy signature method can also be defined as follows [7, 11, 12, 24–27]:

- In order to obtain his/her signature key, using the FIBS scheme, the user must disclose his/her biometric data to the KGC (Key Generation Center). That is, KGC will know the biometric data of all users and therefore users must have strong trust in KGC. With the Fuzzy signature method, KGC is not needed, because the user can independently generate a Public Key for checking and signing the message (using his own biometrics). Therefore, with the Fuzzy signature method, the user does not have to reveal his biometrics to other entities.
- In the FIBS method, after the user receives the signing key from the KGC, he must store it securely. In the Fuzzy signature method, this is not the case, as there is no additional secret mechanism or device, other than his/her biometrics, that can be measured each time a message needs to be signed.

Table 3. Comparison of FIBS scheme and Fuzzy signature.

Feature	FIBS scheme [11, 24–26]	Fuzzy signature [7, 12, 27]
Application in signing Blockchain transactions	It can be applied for biometric digital signing of blockchain transactions	There is a theoretical concept for applying this method to digitally sign Blockchain transactions
Compromising keys	Possible, Master Key is used that is stored on the smart card or token	Not possible, because the user's biometric data are used for creating the keys
A type of digital sugnature based on identity	Yes	No
There is a reliable third-party	KGC – Key Generation Center	No
Smart card or token needed	Yes, for the secure storage of Master key generated by KGC	No
Generating private key	The user cannot generate the Private Key independently, without KGC	The user generates the private key

- In FIBS, signature verification requires the user's biometric data, since it is used as a verification key. However, biometric data should not be disclosed. In contrast, in the Fuzzy signature method, the digital signature is verified using a verification key derived from the user's biometric data, rather than in the form of pure biometric data.

The main difference between the compared FIBS schemes and the Fuzzy signature from Table 3, that the FIBS scheme uses a KGC as a foreign entity for generate Master Key which must be stored on a smart card or token and thus requires an additional security phase in the process of biometric digital signature creation.

4 Conclusion

Innovative biometric digital signature creation can be implemented in the Blockchain transaction digital signature procedure. By using the user's biometric data, digital keys are created and then it is possible to prove that he/she, with his/her unique biometric data, e.g. fingerprint or face image, is a transaction creator. Analyzing the characteristics of biometric cryptographic methods shown in Table 1, it was established that it is possible to biometrically sign blockchain transactions. Table 2 shows a comparative analysis of FIBS and Fuzzy signature schemes that are available in the literature for biometric creation of digital signatures used in blockchain transactions. Table 3 shows a detailed comparison of the characteristics of these two methods.

In this phase of research we didn't encounter any obstacle of the usability of the proposed schemes, and in the next phases of the research it is necessary to make more formalised assessment of the usability in different blockchain environments.

When applying the model of biometric digital signing of blockchain transactions in electronic card payments, it is possible to create digital keys in the form of an authentication PIN in the presence of the user in front of the biometric scanner.

Examples of conventional digital signature schemes of Blockchain transactions are ECDSA (The Elliptic Curve Digital Signature Algorithm), Schnorr signatures, BLS (Boneh–Lynn–Shacham). Blockchain technology where each miner or validator must verify each signature could not function globally without adequate signature schemes.

When applying Blockchain in which it is necessary to prove that the creator of the transaction is the real user, the conventional verification of digital signatures cannot achieve sufficient security.

In such cases as electronic payment transactions, in which it is necessary to prove that the creator of the transaction is the real user, only biometrically created digital keys for digital signatures can provide a sufficiently secure technology, and they can be obtained in the way shown in Subsect. 3.1.

Conventional signature schemes will probably exist in the near future, but they will inevitably be replaced by the biometric schemes that we investigate in this paper. New cryptographic systems are rarely widely used in the first stages of research and a trial period is needed to test and prove their security assumptions.

Solutions that reduce the usability of Blockchain technology, such as dedicated token devices, appear burdensome to users. The results of the comparative analysis of the available FIBS and Fuzzy signature schemes show their characteristics applicable in blockchain transaction implementation of the Biometric Authentication Model. The scientific literature was analyzed to find a digital signature scheme in which the user's biometric data could be used as a digital signature key, without using an additional mechanism or additional storage device. By combining signature schemes with other suitable cryptographic methods, user authentication schemes and key exchange protocols can be achieved. By constructing a digital signature with the fuzzy signature method, we can achieve user authentication and key exchange based on "biometrics". Therefore, the fuzzy signature method could be the main primitive for the realization of "secure cryptographic communication" based on user biometrics.

References

1. Badovinac, N., Simic, D.: E-payment systems using multi-card smart card. In: Book of Springer Proceedings in series: Springer Proceedings in Business and Economics – XIII Balkan Conference on Operational Research, ISBN 978-3-030-21989-5, 1st edition, pp. 237–249 (2019)
2. Godfrey-Welch, D., Lagrois, R., Law, J., Anderwald, R., Engels, D.: Blockchain in payment card systems. SMU Data Science Review **1**(1), Article 3 (2018)
3. Badovinac, N., Simic. D.: A multimodal biometric authentication (MBA) in card payment systems. In: 2019 International Conference on Artificial Intelligence: Applications and Innovations (IC-AIAI), pp. 23–26. Belgrade, Serbia (2019)
4. Bogicevic, S., M., Milenkovic, I., Jovanovic, B., Simic, D., Minovic, M., Milovanovic, M.: Bringing biometric sensors to the classroom: a fingerprint acquisition laboratory for improving student motivation and commitment. Appl. Sci. **10**, 880 (2020). https://doi.org/10.3390/app10030880

5. Korac, D., Simic, D.: Fishbone model and universal authentication framework for evaluation of multifactor authentication in mobile environment. Comput. Secur. **85**, 313–332 (2019). https://doi.org/10.1016/j.cose.2019.05.011
6. Zutshi, A., Grilo, A., Tahereh, N.: The value proposition of blockchain technologies and its impact on Digital Platforms. Department of Mechanical and Industrial Engineering at NOVA School of Science and Technology. Universidade Nova de Lisboa, Portugal (2021). https://doi.org/10.1016/j.cie.2021.107187
7. Kaga, Y., et al.: A Secure and Practical Signature Scheme for Blockchain Based on Biometrics. In: Liu, J.K., Samarati, P. (eds.) ISPEC 2017. LNCS, vol. 10701, pp. 877–891. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-72359-4_55
8. Milenković, I., Šošević, U., Simić, D., Minović, M., Milovanović, M.: Improving student engagement in a biometric classroom: the contribution of gamification. Univ. Access Inf. Soc. **18**(3), 523–532 (2019). https://doi.org/10.1007/s10209-019-00676-9
9. Umut, U., Sharath, P., Salil, P., Anil, K.J.: Biometric cryptosystems: issues and challenges. In: Proceedings of the IEEE **92**(6), 0018–9219/04 (2004)
10. Yao-Jen, C., Wende, Z., Tsuhan C.: Biometric-based cryptographic key generation. In: 2004 IEEE International Conference on Multimedia and Expo (ICME), 0-7803-8603-5/04/520.002004 IEEE (2004)
11. Oday, A., Abdulhussein, H.A., Darwish, S.M., Othman, Z.A., Tiun, S., Lotfy, A.Y.: Towards a secure signature scheme based on multimodal biometric technology: application for IOT blockchain network. Symmetry 1699 (2020). https://doi.org/10.3390/sym12101699
12. Takahashi, K., Matsuda, T., Murakami, T., Hanaoka, G., Nishigaki, M.: Signature schemes with a fuzzy private key. Int. J. Inf. Secur. **18**(5), 581–617 (2019). https://doi.org/10.1007/s10207-019-00428-z
13. Sashank, R., Venkatachalam, S., Kannan, P., Palanisamy, V.: Cryptography key generation using biometrics. In: 2009 International Conference on Control, Communication and Energy Conservation, pp. 1–6 (2009)
14. Lifang, W., Xingsheng, L., Songlong, Y., Peng, X.: A novel key generation cryptosystem based on face features. In: IEEE 10th International Conference On Signal Processing Proceedings, pp. 1675–1678. Beijing, China (2010). https://doi.org/10.1109/ICOSP.2010.5656719
15. Nguyen, H.L., Nguyen, T.T.: An approach to protect private key using fingerprint biometric encryption key in BioPKI based security system. In: 10th International Conference on Control, Automation, Robotics and Vision, pp. 1595–1599. Hanoi, Vietnam (2008). https://doi.org/10.1109/ICARCV.-2008.4795763
16. Nalini, K., Sharat, C., Jonathan, H., C., Ruud, M.: Generating cancelable fingerprint templates. IEEE Transactions On Pattern Analysis And Machine Intelligence, In: IEEE Published by the IEEE Computer Societ, vol. 29(4) (2007)
17. Rathgeb, C., Uhl, A.: Context-based biometric key generation for Iris. In: Published in IET Computer Vision Received, 8th October (2010). https://doi.org/10.1049/iet-cvi.2010.0176
18. Feng, H., Ross, A., Daugman, J.: Combining crypto with biometrics effectively. IEEE Transactions On Computers **55**(9) (2006)
19. Yazhuo, G., Kaifa, D., Pengfei, S.: PKI key generation based on iris features. In: 2008 International Conference on Computer Science and Software Engineering 978-0-7695-3336-0/08. IEEE (2008). https://doi.org/10.1109/CSSE.2008.1181
20. Jo, J.-G., Seo, J.-W., Lee, H.-W.: Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint. In: Preparata, F.P., Fang, Q. (eds.) FAW 2007. LNCS, vol. 4613, pp. 38–49. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-73814-5_4

21. Syh-Yuan, T., Zhe, J., Andrew, B., Teoh, J., Bok-Min, G., Swee-Huay, H.: On the realization of fuzzy identity-based identification scheme using fingerprint biometrics. Security And Communitaction Networks, In: Published online in Wiley Online Library (2012). https://doi.org/10.1002/sec.408
22. Wang, Y., Plataniotis, K.N.: Fuzzy vault for face based cryptographic key generation. In: 2007 Biometrics Symposium, pp. 1–6 (2007). https://doi.org/10.1109/BCC.2007.4430549
23. Tan, S.Y., Heng, S.H., Goi, B.M.: On the security of two fuzzy identity-based signature schemes. In: 4th IFIP International Conference on New Technologies, Mobility and Security, pp. 1–5 (2011). https://doi.org/10.1109/NTMS.2011.5721040
24. Xiaojun, Z., Chunxiang, X., Yuan, Z.: Fuzzy identity-based signature scheme from lattice and its application in biometric authentication. In: KSII Transactions On Internet And Informations System **11**(5), p. 2762 (2017). https://doi.org/10.3837/tiis.2017.05.025
25. Yanhua, Z., Yupu, H., Yong, G., Yifeng, Y., Huiwen, J.: Efficient fuzzy identity-based signature from lattices for identities in a small (or large) universe. J. Info. Secu. Appl. **47** (2019). https://doi.org/10.1016/j.jisa.2019.04.012
26. Shan, X., You, L., Hu, G.: Two efficient constructions for biometric-based signature in identity-based setting using bilinear pairings. IEEE Access **9**, 25973–25983 (2021). https://doi.org/10.1109/ACCESS.2021.3057064
27. Matsuda, T., Takahashi, K., Murakami, T., Hanaoka, G.: Fuzzy Signatures: Relaxing Requirements and a New Construction. In: Manulis, M., Sadeghi, A.-R., Schneider, S. (eds.) ACNS 2016. LNCS, vol. 9696, pp. 97–116. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39555-5_6
28. Godfrey-Welch, D., Remy L., Jared L.: Blockchain in Payment Card Systems, p. 75205. Southern Methodist University, Dallas, Texas (2018)