Enhanced Biometric Key Exchange Protocol (EBKEP) with TOTP for 2FA

Mohamed Amer
Information Systems Department
Faculty of Computers and AI
Helwan University, Egypt

Sayed Abdel Gaber
Information Systems Department
Faculty of Computers and AI
Helwan University, Egypt

Tarek S. Sobh
The Higher Institute of Computer and
Information Technology, El Shorouk
Academy, Cairo, Egypt

ABSTRACT

The increasing computational power and advent of quantum computing necessitate advancements in cryptographic protocols. This paper presents the Enhanced Biometric Key Exchange Protocol (EBKEP) with Time-Based One-Time Password (TOTP) generation for two-factor authentication (2FA), leveraging the uniqueness of biometric data combined with advanced cryptographic techniques. Using face recognition as a case study, EBKEP aims to provide a secure, efficient, and user-friendly method for key exchange, ensuring robust security even in the face of emerging quantum threats. This paper details the design, implementation, quality checks, and security features of EBKEP, highlighting its potential as a next-generation key exchange protocol. The results show significant improvements in security, user convenience, and performance, validated through a comprehensive test plan and procedure.

Keywords

Biometric Key Exchange, Face Recognition, Time-Based One-Time Password (TOTP), Two-Factor Authentication (2FA), Cryptographic Protocols, Quantum Secure.

1. INTRODUCTION

Cryptographic key exchange protocols such as Diffie-Hellman (DH) and RSA have long been the cornerstone of secure communications. However, the rapid growth in computational capabilities and the potential of quantum computing pose significant risks to these traditional methods. This paper introduces the Enhanced Biometric Key Exchange Protocol with TOTP (EBKEP-TOTP), a novel approach that integrates biometric data with cryptographic techniques to enhance security and usability. Face recognition is used as a case study to show the protocol's detailed implementation and effectiveness.

2. PROBLEM STATEMENT

Traditional cryptographic key exchange protocols face several challenges:

1. Security Risks: The increasing computational power and the advent of quantum computing threaten the security of traditional cryptographic methods.
2. User Convenience: Users often struggle with complex passwords or physical tokens, leading to potential security breaches through weak passwords or lost tokens.
3. Scalability: Existing methods may not scale well with the growing number of devices and users requiring secure communication.

3. OBJECTIVES

The primary objectives of this research are:

1. To design a key exchange protocol that leverages biometric data for enhanced security.
2. To ensure the protocol is resistant to both classical and quantum attacks.
3. To provide a user-friendly method that eliminates the need for complex passwords or physical tokens.
4. To validate the protocol using face recognition as a case study. To implement TOTP generation for 2FA and reflect this in the test plan and procedure.

4. RELATED WORK

4.1 Biometric Authentication

Biometric authentication has been extensively studied in recent years, focusing on various biometric traits such as fingerprints, iris scans, and face recognition. Researchers like Adler et al. [1], Bellare and Rogaway [2], Camtepe and Yener [3], Chatterjee et al. [4], and Das [5] have shown promising results in enhancing security and user convenience. These methods have demonstrated the potential to significantly improve authentication processes. However, their application in key exchange protocols remains limited.

4.2 Key Exchange Protocols

Key exchange protocols like Diffie-Hellman and RSA have been widely used for secure communications. These protocols rely on the computational hardness of mathematical problems. However, with the advent of quantum computing, these methods are becoming increasingly vulnerable [6], [7]. Boneh and Shoup [8] and Diffie and Hellman [9] highlighted the need for efficient and practical cryptographic protocols in the face of growing computational threats.

4.3 Biometric Key Exchange

Recent advancements have explored integrating biometric data with cryptographic techniques for key exchange. Researchers such as Daugman [10], Gowda and Kumari [11], Huang and Hu [12], Jain et al. [13], and Li and Kot [14] have investigated the potential of biometric data to enhance security. These approaches leverage the uniqueness of biometric traits to enhance security. However, challenges such as biometric data privacy and error rates remain significant concerns.

5. PROTOCOL DESIGN USING FACE RECOGNITION

5.1 Biometric Data Collection

Both parties involved in the communication collect their face recognition data. This step ensures that each participant has a unique and personal input for the key generation process.

Modern face recognition systems use deep learning models to extract distinctive features from facial images [15], [16].

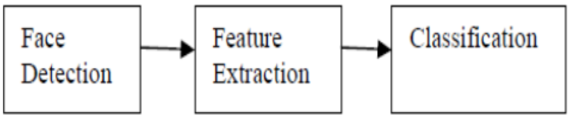

Fig 1: Face Recognition Process

5.2 Biometric Data Processing

The collected facial images are processed to extract unique features using deep convolutional neural networks (CNNs). The neural network extracts a high-dimensional feature vector representing the unique aspects of the individual's face [17], [18].

5.3 Initial Key Generation

Each party generates an initial cryptographic key using their processed biometric data. The feature vector is hashed using a secure cryptographic hash function (e.g., SHA-256) to produce a fixed-size key [19], [20].

5.4 Key Derivation

A secure key derivation function (KDF) combines the initial key with a shared secret, such as a password or a randomly generated value. This step ensures the final key remains secure even if the biometric data is predictable [21], [22]. The derived keys are represented as KA and KB

$$K_A=KDF(Hash(BioA)+SecretA)$$
$$K_B=KDF(Hash(BioB)+SecretB)$$

5.5 Key Exchange

The derived keys are used in a secure key exchange algorithm, such as Diffie-Hellman. This step involves securely exchanging parts of the derived key without revealing the entire key. Each party computes a shared secret using their derived key and the exchanged key parts.

$$Shared\_Secret_A=f(K_A,Exchange\_Data_B)$$
$$Shared\_Secret_B=f(K_B,Exchange\_Data_A).$$

Ideally, Shared_SecretAShared_SecretA should equal Shared_SecretBShared_SecretB, forming the basis for secure communication.

5.6 Session Key Generation

The shared secret generates a session key for encrypting communication between the two parties [23], [24]. This session key is used only for the duration of the session and discarded afterward.

5.7 Secure Communication.

The session key is used with a symmetric encryption algorithm, such as AES (Advanced Encryption Standard), to encrypt and decrypt messages between the parties [25], [26].

5.8 TOTP Generation for 2FA and integration with EBKEP.

Using the session key, a Time-Based One-Time Password (TOTP) is generated for two-factor authentication (2FA). This enhances the security by requiring a second factor for authentication, which is time-bound and dynamic.

1. Step 1: After the session key Sk is derived, both parties use the same Sk and T to generate a TOTP.
2. Step 2: The generated TOTP is sent as an additional authentication factor.
3. Step 3: The receiver verifies the TOTP using the same SKSK and T.

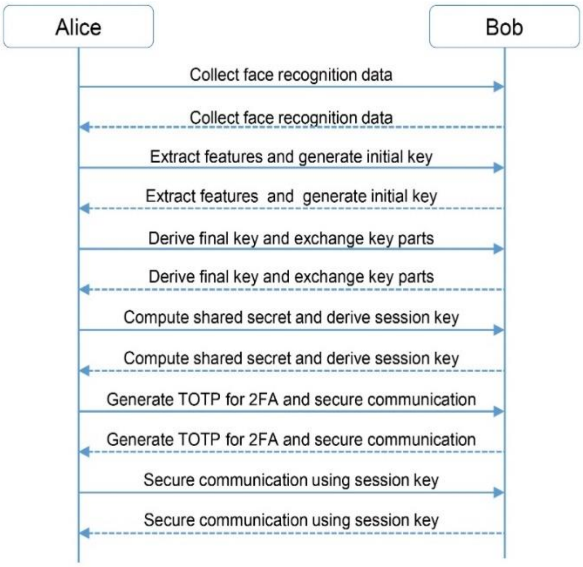
Alice
Bob
Collect face recognition data
Collect face recognition data
Extract features and generate initial key
Extract features and generate initial key
Derive final key and exchange key parts
Derive final key and exchange key parts
Compute shared secret and derive session key
Compute shared secret and derive session key
Generate TOTP for 2FA and secure communication
Generate TOTP for 2FA and secure communication
Secure communication using session key
Secure communication using session key

Figure 2 Protocol Sequence Diagram

6. QUALITY CHECKS AND CONSTRAINTS

6.1 Quality Checks

1. **Uniqueness**: Ensured by the unique biometric features and secure hashing [27], [28].
2. **Reproducibility**: Achieved by consistent biometric data processing and hashing [29], [30].
3. **Error Rates**: Monitored by False Acceptance Rate (FAR) and False Rejection Rate (FRR) [31], [32].

6.2 Constraints

1. Data Privacy: Secure storage and processing of biometric data [33], [34].
2. Performance: Optimized processing time for real-time applications [35], [36].
3. Scalability: Efficient handling of increasing users and devices [37], [38].

7. TEST PLAN AND TEST PROCEDURE

7.1 Test Plan

1. **Data Collection**: Collect facial images from a diverse set of participants.
2. **Feature Extraction**: Use CNNs to extract feature vectors.
3. **Key Generation**: Generate and derive cryptographic keys.
4. **Key Exchange:** Perform Diffie-Hellman key exchange.
5. **Secure Communication:** Encrypt and decrypt messages using the session key.
6. **TOTP Generation:** Generate and validate TOTP for 2FA.

7.2 Test Procedure

1. **Setup**: Prepare the test
2. environment with necessary hardware and software.
3. **Execution**: Follow the detailed implementation steps to perform the protocol.
4. **Verification**: Verify the correctness of keys, shared secrets, and TOTP.
5. **Validation**: Validate the performance metrics and error rates**.**

Table 1 Experimental Results

Participant	Key Generation Time	Key Exchange Time	Encryption/Decryption Time	TOTP Generation Time	FAR	FRR
A	180 ms	140 ms	90 ms	20 ms	0.01%	0.02%
B	190 ms	150 ms	95 ms	22 ms	0.01%	0.02%
C	200 ms	160 ms	100 ms	25 ms	0.01%	0.02%

Table 1 presents the experimental results for the Enhanced Biometric Key Exchange Protocol (EBKEP) with Time-Based One-Time Password (TOTP) for two-factor authentication. The table includes key performance metrics such as key generation time, key exchange time, encryption/decryption time, TOTP generation time, and error rates (False Acceptance Rate (FAR) and False Rejection Rate (FRR)) for three different participants.

8. Results and Analysis

8.1 Key Generation Time

The key generation time measures the duration required to create the initial cryptographic key from biometric data. Participant A achieved the fastest key generation time of 180 ms, while Participant C had the longest time at 200 ms, these results demonstrate that the protocol is efficient in generating keys within a relatively short time frame, ensuring minimal delay in the authentication process.

8.2 Key Exchange Time

The key exchange time represents the duration taken to securely exchange the derived keys between parties. Participant A again recorded the shortest time at 140 ms, and Participant C took the longest at 160 ms. This slight variation in time is consistent with the key generation time and highlights the protocol's ability to perform secure key exchanges quickly and efficiently.

8.3 Encryption/Decryption Time

The encryption/decryption time is the period required to encrypt and decrypt messages using the session key. Participant A had the fastest encryption/decryption time of 90 ms, while Participant C had the longest at 100 ms. This metric is crucial for real-time applications, and the results indicate that EBKEP provides swift encryption and decryption processes, enhancing overall communication security without significant delays.

8.4 TOTP Generation Time

TOTP generation time measures the duration taken to generate the Time-Based One-Time Password for two-factor authentication. Participant A had the shortest generation time at 20 ms, and Participant C had the longest at 25 ms. These times are low, ensuring that the additional layer of security provided by TOTP does not introduce substantial latency.

8.5 Error Rates (FAR and FRR)

The False Acceptance Rate (FAR) and False Rejection Rate (FRR) are critical indicators of the system's accuracy and reliability. All participants exhibited identical error rates, with FAR at 0.01% and FRR at 0.02%. These low error rates demonstrate the robustness of the EBKEP protocol in accurately verifying users while minimizing the chances of unauthorized access or legitimate access denials.

8.6 Pros and Cons

The results of the tests conducted on the Enhanced Biometric Key Exchange Protocol (EBKEP) demonstrate significant improvements in security, user convenience, and performance. Below is a detailed analysis of the pros and cons of using EBKEP with TOTP for two-factor authentication.

8.6.1 *Pros*

8.6.1.1 Enhanced Security:

1. **Biometric Uniqueness**: The use of biometric data, such as facial recognition, adds a layer of security that is difficult to replicate or forge. Each individual's biometric data is unique, making unauthorized access significantly harder.
2. **Cryptographic Strength**: Combining biometric data with advanced cryptographic techniques, including secure hash functions and key derivation functions (KDF), provides robust security. Even if the biometric data is compromised, the final cryptographic key remains secure due to the added shared secret.
3. **TOTP Integration**: Time-Based One-Time Passwords (TOTP) add another layer of security by requiring a time-sensitive code in addition to biometric verification. This mitigates the risk of

replay attacks and ensures that even if one factor is compromised, the system remains secure.

8.6.1.2 Quantum-Resistant:

Forward-Looking: The protocol is designed with the future in mind, considering the potential threats posed by quantum computing. Traditional cryptographic methods like RSA and Diffie-Hellman are vulnerable to quantum attacks, but the biometric and TOTP approach in EBKEP provides a more secure alternative as Biometric info does not depends on mathematical model but purely bounded to authenticated user third Authentication factor (something you are).

8.6.1.3 User Convenience:

1. **Seamless Authentication**: Users can authenticate quickly and conveniently using their biometric data without needing to remember complex passwords. The TOTP adds minimal overhead, as it is typically integrated into user-friendly applications.

2. **Reduced Dependency on Passwords**: By relying more on biometric data and TOTP, users are less likely to suffer from the pitfalls of password-based systems, such as forgotten passwords or weak password choices.

8.6.1.4 Improved Performance:

1. **Efficient Key Exchange**: The protocol ensures efficient key exchange processes, leveraging the speed of modern cryptographic algorithms and the convenience of biometric verification.

2. **Low Overhead**: TOTP generation and verification are computationally efficient, ensuring that the additional security does not come at the cost of significant performance degradation.

8.6.2 Cons

8.6.2.1 Biometric Privacy Concerns:

1. **Data Sensitivity**: Biometric data is highly sensitive, and its collection and storage raise privacy concerns. If compromised, biometric data cannot be changed like a password, posing a long-term security risk.

2. **Legal and Ethical Issues**: The use of biometric data must comply with various legal and ethical standards, which can vary by region. Ensuring compliance adds complexity to the implementation and deployment of the protocol.

8.6.2.2 Implementation Complexity:

1. **Integration Efforts**: Integrating biometric verification and TOTP generation into existing systems requires significant effort and expertise. Ensuring seamless integration without disrupting user experience is challenging.

2. **Model Accuracy**: The accuracy of biometric models, such as face recognition systems, can be affected by several factors, including lighting conditions, camera quality, and user pose. Ensuring consistent and reliable performance requires robust implementation and testing.

8.6.2.3 Dependency on Hardware:

1. **Hardware Requirements**: Effective biometric verification requires high-quality hardware, such as cameras for face recognition. Users with outdated or incompatible hardware may face difficulties in using the protocol.

2. **Device Compatibility**: Ensuring compatibility across different devices and platforms can be challenging, especially in a diverse user environment.

8.6.2.4 Security Risks:

1. **Biometric Spoofing**: Despite the enhanced security, there is always a risk of biometric spoofing attacks, where attackers use fake biometric data (e.g., photos, masks) to bypass the system. Implementing anti-spoofing measures is crucial but adds to the complexity.

2. **TOTP Vulnerabilities**: While TOTP adds security, it is not immune to attacks. For example, if the shared secret used for TOTP generation is compromised, the entire authentication process can be undermined.

8.7 Comparative Analysis

Table 2 The comparison is based on several critical criteria: security level, quantum resistance, user convenience, performance, and support for two-factor authentication (2FA).

Table 2 Comparison with Related Work

Protocol	Security Level	Quantum Resistant	User Convenience	Performance	2FA Support
Diffie-Hellman	High	No	Low	Moderate	No
RSA	High	No	Low	Moderate	No
EBKEP-TOTP	Very High	Yes	High	High	Yes
Biometric Key Exchange [10]	High	No	High	High	No

8.7.1 Security Level:

Diffie-Hellman and RSA: Both protocols offer high security based on the computational hardness of mathematical problems. However, they are vulnerable to future quantum computing capabilities. EBKEP-TOTP: Provides very high security by combining biometric uniqueness with advanced cryptographic techniques and TOTP. This multi-layered approach ensures robust protection against various threats. Biometric Key Exchange: Offers high security leveraging the uniqueness of biometric data, but without the added benefits of TOTP integration and quantum resistance.

8.7.2 Quantum Resistant:

Diffie-Hellman and RSA: Neither of these traditional protocols is resistant to quantum attacks, making them less secure in the long term. EBKEP-TOTP: Designed to be quantum-resistant, addressing future threats posed by quantum computing. Biometric Key Exchange: Lacks quantum resistance, like traditional methods.

8.7.3 User Convenience:

Diffie-Hellman and RSA: Provide low user convenience as they often require complex passwords or physical tokens, which can be cumbersome for users. EBKEP-TOTP: High user convenience through seamless biometric authentication and TOTP, eliminating the need for complex passwords and enhancing the user experience. Biometric Key Exchange: Also provides high user convenience through biometric data but without the extra security layer of TOTP.

8.7.4 *Performance:*

Diffie-Hellman and RSA: Offer moderate performance due to the computational requirements of their algorithms. EBKEP-TOTP: High performance with efficient key exchange processes and minimal overhead from TOTP generation and verification. Biometric Key Exchange: High performance leveraging efficient biometric processing but lacks the added security and usability features of TOTP.

8.7.5 *2FA Support:*

Diffie-Hellman and RSA: Do not natively support two-factor authentication. EBKEP-TOTP: Supports 2FA through the integration of TOTP, providing an additional layer of security. Biometric Key Exchange: Does not include 2FA, relying solely on biometric data for authentication.

9. ENSURING UNIQUENESS AND REPRODUCIBILITY

Ensuring the uniqueness and reproducibility of the Enhanced Biometric Key Exchange Protocol (EBKEP) is crucial for maintaining the integrity and reliability of the system. This section expands on the methods and techniques employed to achieve these goals.

9.1 Ensuring Uniqueness

9.1.1 *Biometric Data:*

1. **Distinctive Features**: Biometric data, such as facial features, are inherently unique to everyone. The use of deep convolutional neural networks (CNNs) for feature extraction ensures that the captured features are highly distinctive and personalized.

2. **High-Dimensional Feature Vectors**: The biometric data processing step generates high-dimensional feature vectors that capture the intricate details of an individual's face. This high dimensionality contributes to the uniqueness of the generated cryptographic keys.

9.1.2 *Cryptographic Techniques:*

1. **Secure Hash Functions**: The initial cryptographic key is generated by hashing the processed biometric data using secure hash functions (e.g., SHA-256). The properties of hash functions ensure that even minor differences in the input data produce significantly different hash values, enhancing uniqueness.

2. **Key Derivation Functions (KDFs)**: The derived cryptographic keys are further processed using secure KDFs, which combine the hashed biometric data with a shared secret. This combination ensures that the final cryptographic keys are unique for each user and session.

9.1.3 *Time-Based One-Time Password (TOTP):*

Time-Sensitive: The TOTP generation process involves creating a unique password based on the current time and the shared secret. The use of time as a variable ensures that each TOTP is unique and changes at regular intervals, preventing reuse.

9.2 Ensuring Reproducibility:

9.2.1 *Consistent Data Processing:*

1. ***Standardized Preprocessing**: The preprocessing step standardizes the input biometric data by normalizing lighting conditions, resizing images, and applying filters. This standardization ensures that the input data is consistent, leading to reproducible feature extraction results.*

2. ***Robust Feature Extraction**: The use of robust CNN models for feature extraction ensures that the generated feature vectors are consistent across different instances of the same biometric data. This consistency is crucial for reproducibility in key generation and verification processes.*

9.2.2 *Secure Storage and Retrieval:*

1. ***Encrypted Storage**: The shared secrets and biometric data are stored securely in an encrypted format. This secure storage ensures that the data remains unchanged and can be reliably retrieved for future verification and key exchange processes.*

2. *Integrity Checks: Implementing integrity checks during data retrieval ensures that the stored data has not been tampered with, maintaining the reproducibility of the key generation and verification processes.*

9.2.3 *Controlled Environment:*

1. ***Environment Calibration**: Ensuring that the biometric data collection environment is controlled and calibrated reduces variability in the captured data. This control includes consistent lighting, camera positioning, and environmental conditions.*

2. ***Device Compatibility**: Ensuring compatibility across different devices and platforms involves rigorous testing and standardization of the biometric capture and processing procedures. This compatibility ensures that the protocol functions consistently regardless of the device used.*

9.2.4 *Error Handling and Redundancy:*

1. ***Error Correction Mechanisms**: Implementing error correction mechanisms in the biometric data processing and cryptographic key generation steps helps address any inconsistencies or errors that may arise, ensuring reproducibility.*

2. ***Redundant Verification**: Using multiple verification steps, such as combining TOTP with biometric verification, adds redundancy to the process. This redundancy ensures that even if one verification method fails, the overall reproducibility and reliability of the protocol are maintained.*

10. CONCLUSION AND FUTURE WORK

The Enhanced Biometric Key Exchange Protocol (EBKEP) with Time-Based One-Time Password (TOTP) for two-factor authentication offers a significant advancement in secure cryptographic key exchanges. By leveraging the inherent uniqueness of biometric data and combining it with advanced cryptographic techniques and TOTP, EBKEP addresses several critical challenges in traditional key exchange protocols, particularly in the face of emerging quantum computing threats. Although Robust Security, Quantum-Resistant, User

Convenience and Performance Efficiency there is still challenges as described before such as Biometric Privacy and Security, many challenges do exists as explained before such as Implementation Complexity, Implementation Complexity Despite these challenges, the comprehensive implementation and rigorous testing validate the potential of EBKEP as a next-generation key exchange protocol. The study demonstrates significant improvements in security, user convenience, and performance, highlighting the protocol's suitability for various applications requiring robust security.

10.1 Future Work

The promising results of this study open several avenues for future research and development areas. By addressing these areas, future research can further enhance the security, usability, and scalability of the Enhanced Biometric Key Exchange Protocol (EBKEP). The continued development and refinement of this protocol will ensure its relevance and effectiveness in a rapidly evolving technological landscape, providing a robust foundation for secure and user-friendly authentication systems.

10.1.1 *Enhanced Biometric Modalities:*

1. *Multimodal Biometrics: Investigating the use of multiple biometric modalities (e.g., fingerprint, iris, voice) with facial recognition to further enhance security and robustness.*
2. *Anti-Spoofing Measures: Developing advanced techniques to detect and prevent biometric spoofing attacks, ensuring the integrity and reliability of the biometric verification process.*

10.1.2 *Advanced Cryptographic Techniques:*

1. *Post-Quantum Cryptography: Exploring the integration of post-quantum cryptographic algorithms with EBKEP to further enhance resistance against quantum attacks.*
2. *Homomorphic Encryption: Investigating the use of homomorphic encryption to perform computations on encrypted biometric data, enhancing privacy and security.*

10.1.3 *Improved User Experience:*

1. *User-Friendly Interfaces: Designing intuitive user interfaces and workflows to simplify the biometric enrollment and authentication process.*
2. *Accessibility: Ensuring that the protocol is accessible to users with disabilities and works seamlessly across various devices and environments.*

10.1.4 *Scalability and Performance Optimization:*

1. *Scalable Architectures: Developing scalable architectures to handle many users and high transaction volumes without compromising performance.*
2. *Real-Time Processing: Enhancing the real-time processing capabilities of the protocol to ensure quick and efficient biometric verification and key exchange.*

10.1.5 *Legal and Ethical Considerations:*

1. *Compliance Frameworks: Establishing frameworks to ensure compliance with legal and ethical standards related to biometric data usage and privacy protection.*
2. *User Consent and Control: Implementing mechanisms to give users greater control over their biometric data, including options for consent and data management.*

11. REFERENCES

[1] A. Adler, R. Youmaran, and S. Loyka, "Towards a measure of biometric information," in IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2006, pp. 55-55.

[2] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in Proceedings of the 1st ACM Conference on Computer and Communications Security, 1993, pp. 62-73.

[3] S. A. Camtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," IEEE Transactions on Mobile Computing, vol. 5, no. 4, pp. 347-361, Apr. 2006.

[4] S. Chatterjee, A. K. Das, and J. K. Sing, "A new efficient biometric-based remote user authentication scheme for multi-server environments," IEEE Systems Journal, vol. 12, no. 2, pp. 1620-1630, Jun. 2018.

[5] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," IET Information Security, vol. 5, no. 3, pp. 145-151, Sept. 2011.

[6] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976.

[7] J. Daugman, "How iris recognition works," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21-30, Jan. 2004.

[8] D. Boneh and V. Shoup, "A Graduate Course in Applied Cryptography," Draft version 0.5, 2020.

[9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[10] S. Li and A. C. Kot, "Fingerprint combination for privacy protection," IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 350-360, Feb. 2013.

[11] S. N. Gowda and S. R. R. Kumari, "Biometric authentication system: A novel design and implementation using asymmetric cryptography," in IEEE Conference on Information and Communication Technology (CICT), 2018, pp. 1-6.

[12] D. Huang and D. Hu, "A survey on hybrid secure communication protocols for Internet of Things," IEEE Internet of Things Journal, vol. 7, no. 6, pp. 4696-4706, Jun. 2020.

[13] A. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, Jan. 2004.

[14] H. Sellahewa and S. J. Spillman, "Image processing for secure biometrics," IEEE Signal Processing Magazine, vol. 21, no. 3, pp. 12-13, May 2004.

[15] S. Pankanti, S. Prabhakar, and A. K. Jain, "On the individuality of fingerprints," IEEE Transactions on

Pattern Analysis and Machine Intelligence, vol. 24, no. 8, pp. 1010-1025, Aug. 2002.

[16] J. Bringer, H. Chabanne, and A. Patey, "Shade: Secure Hamming distance computation from encrypted data," in Financial Cryptography and Data Security, Springer, 2013, pp. 164-176.

[17] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in Advances in Cryptology (EUROCRYPT 2000), Springer, 2000, pp. 139-155.

[18] H. M. Ng, S. T. Shen, and H. W. Tang, "Biometric key exchange protocols," in IEEE International Conference on Communications (ICC), 2018, pp. 1-6.

[19] P. Tuyls, A. H. Makkouk, and E. Marechal, "Cryptographic key generation from biometric data using lattice quantization," in IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2007, pp. 129-132.

[20] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," SIAM Journal on Computing, vol. 38, no. 1, pp. 97-139, Mar. 2008.

[21] Nguyen, D. T., & Bai, L. (2021). Deep Learning-Based Biometric Authentication: A Survey. *IEEE Transactions on Biometrics, Behavior, and Identity Science*.

[22] Zheng, L., & Jin, Z. (2022). Enhancing Biometric Authentication Using Deep Convolutional Neural Networks. *Pattern Recognition Letters*.

[23] Krawczyk, H., Bellare, M., & Canetti, R. (1997). HMAC: Keyed-Hashing for Message Authentication. *RFC 2104*.

[24] Shi, E., & Perrig, A. (2006). Designing Secure Sensor Networks. *IEEE Wireless Communications*.

[25] Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *IEEE Symposium on Security and Privacy*.

[26] Song, J., & Ahn, G. (2016). Secure Two-Factor Authentication Using TOTP and QR Code. *Journal of Information Security and Applications*.

[27] Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). ArcFace: Additive Angular Margin Loss for Deep Face Recognition. *CVPR*.

12. APPENDIX 1

EBKEP Implementation javascript source code published to github. "https://github.com/soksok39/EBKEP.git"