Post-Print: Research on Three-Factor Remote Identity Authentication Protocol Based on Bilinear Mapping

Authors: Wei Chunying, Guo Zhonghua

Date: 2018-11-29T00:00:00+00:00

Abstract

To enhance the security of authentication in multi-server environments and reduce computational complexity, a three-factor authentication protocol based on bilinear pairing is proposed. The three factors include biometric information, smart cards, and bilinear pairing-based passwords. The proposed protocol comprises six phases: system setup, server registration, user registration, login, authentication and key agreement, and password update, wherein the biometric factor and smart card serve as core factors involved in the registration, login, authentication, and password change phases. Formal proof in the Oracle model validates the security of the proposed protocol, demonstrating that adversaries cannot obtain tokens, passwords, biometric feature information, etc., and that key agreement and mutual authentication can be achieved. Compared with other related protocols, the proposed protocol exhibits certain advantages in terms of security features, smart card storage cost, communication cost, and other aspects.

Full Text

Preamble

Vol. 37 No. 1
Application Research of Computers
ChinaXiv Cooperative Journal

Research on a Three-Factor Remote Authentication Protocol Based on Bilinear Mapping

Wei Chunying, Guo Zhonghua
(College of Physics and Electronic-Electrical Engineering, Ningxia University, Yinchuan 750021, China)

Abstract: To improve the security of authentication in multi-server environments and reduce computational complexity, this paper proposes a three-factor authentication protocol based on bilinear mapping. The three factors include biometric information, smart cards, and bilinear mapping cryptography. The proposed protocol comprises six stages: system setup, server registration, user registration, login, authentication and key agreement, and password update. Among these, biometric factors and smart cards serve as core components involved in the registration, login, authentication, and password change phases. Formal verification using the Oracle model confirms the protocol' s security: adversaries cannot obtain identifiers, passwords, or biometric feature information, while the protocol achieves both key agreement and mutual authentication. Compared with related protocols, the proposed protocol offers advantages in security features, smart card storage costs, and communication costs.

Keywords: multi-server; authentication; bilinear mapping; biometric information; smart card; formal verification

0 Introduction

The rapid development of modern network communication technologies has substantially enhanced online services[1], significantly improving service quality. Applications such as email, e-healthcare, online banking, and e-commerce have become integral to daily life. However, most of these services operate over untrusted channels, creating opportunities for malicious actors. Consequently, security issues including privacy, integrity, and confidentiality are paramount, with identity authentication[2] serving as a critical prerequisite for online services and representing a key research focus and challenge in network security.

Authentication protocols can be categorized based on server distribution into single-server and multi-server environments. In single-server environments, users must register with each application server individually, with the primary drawback being the need to remember multiple passwords and identifiers for different servers, resulting in poor user experience. This scenario is suitable for applications with special security considerations, such as certain healthcare security systems[3]. Multi-server environments eliminate this complexity, allowing users to access multiple servers through a single registration.

Multi-server authentication has been extensively studied. For instance, literature[4] proposed a robust two-factor authentication protocol for multi-server environments utilizing smart cards and elliptic curve cryptography, capable of resisting various potential network attacks. Literature[5] analyzed this protocol, demonstrating its vulnerability to impersonation attacks, password guessing attacks, and privileged insider attacks, and proposed an improved two-factor protocol to address these weaknesses. Related research[6] indicates that two-factor authentication protocols lack sufficient reliability because users typically select low-entropy passwords vulnerable to dictionary attacks. Literature[7] addressed the inability of existing cross-trust domain key agreement protocols to meet network demands by proposing a cross-autonomous domain key agreement protocol using different public parameters and PKG master keys, though employing fewer factors. Literature[8] examined the authentication protocol from literature[9], identifying its vulnerability to smart card loss attacks and server impersonation attacks, and proposed an improved authentication protocol based on biometric features and extended chaotic mapping.

Current research often employs bilinear pairing or point multiplication to reduce complexity. This paper also utilizes bilinear pairing to propose a three-factor remote authentication protocol[10] based on bilinear mapping, incorporating biometric features, smart cards, and passwords. Analysis results demonstrate that the proposed protocol achieves high security and computational efficiency.

---

1 Protocol Description

1.1 System Setup Phase

The registration center (RC) selects a random number and retains it as a secret key. It computes , where P is a generator of group G1. RC publishes {ê, G1, G2, q, P, PubRS, H(.), h(.)} as public parameters.

1.2 Server Registration Phase

When a new application server SSj joins the multi-server environment to provide services to remote users Ui, the following steps occur: Server SSj selects an identity identifier SIDj ($1 < j < m$), where m represents the total number of servers in the environment, and sends SIDj to RC. Upon receiving SIDj, RC computes and sends Sj to SSj through a secure channel while publishing Pubj as a public parameter.

1.3 User Registration Phase

When remote user Ui wishes to access server SSj’ s services, Ui must register with RC through the following steps:

a) User Ui selects IDi and PWi, inputs biometric features Bi via a sensor, and sends {UIDi, HPWi, Bi} to RC through a secure channel.

b) Upon receiving the registration message, RC computes . RC generates a unique identifier (TIDi) for each user and calculates PIDi = h(TIDi||SRS). RC then stores {PIDi, UIDi} and a status bit (0, 1) in the database, where the status bit indicates the user’ s state. Finally, RC generates a smart card containing {TIDi, bi, Regi, Si, PubRS, H(.), h(.), H1} and sends it to Ui through a secure channel.

1.4 Login Phase

When user Ui wishes to log in to server SSj, the following steps are executed:

a) Ui inserts the smart card into a terminal and inputs IDi, PWi, and Bi. The smart card reader computes and checks whether it holds. If valid, the biometric information is correct; otherwise, the connection is aborted. The smart card then computes and compares it with the stored Regi. If they match, Ui has entered correct {IDi, PWi}, and the process continues.

b) The smart card generates a random number ri and computes . The smart card reader then sends the login message M1={Ri, TIDi, SIDj, di} to RC through an insecure channel.

1.5 Verification and Key Agreement Phase

This phase executes the following steps:

a) Upon receiving M1, RC first checks whether the user exists in the database. If not, RC terminates the session; if the user exists, RC retrieves UIDi from the database and proceeds.

b) RC computes and checks whether both conditions hold. If both are satisfied, RC continues; otherwise, the session is terminated.

c) RC generates a random nonce ni and computes . RC then sends message M2 ={Li, Ki, SIDj, Ti} to SSj through a public channel.

d) After receiving M2 from RC, SSj computes and checks whether it holds. If valid, user Ui and registration center RC are authenticated as trustworthy to server SSj; if not, the session is terminated. Subsequently, SSj generates ci, and sends M3 ={SIDj, Ki, Di, Ei} to user Ui through an insecure channel.

e) Upon receiving M3 from SSj, Ui computes , and checks whether it holds. If valid, RC and SSj pass Ui’ s identity verification. Additionally, user Ui computes and sends message M4={Vi, Oi} to SSj through an insecure channel.

f) After receiving M4 from Ui, the server computes and checks whether it holds. If valid, the session key is established and both SSj and Ui can communicate using the shared key SK; otherwise, the session is terminated.

1.6 Password Change Phase

In this phase, users can replace old password PWi with new password without any assistance from the registration center:

a) User Ui inserts the smart card into a terminal and inputs IDi, PWi, and biometric information Bi on a specific device.

b) The smart card reader computes and checks whether it holds. If valid, the biometric information is correct; otherwise, the session is aborted.

c) The smart card computes and checks whether it holds. If not, the smart card rejects the password change request; if valid, the smart card prompts user Ui to enter a new password . Finally, the smart card replaces the old {Regi, Si} in its memory with , completing the password change phase.

---

2 Oracle Formal Security Proof

This section presents formal security analysis using the Random Oracle Model[11] (ROM) to prove that adversary A cannot obtain identifier IDi, password PWi, biometric features Bi, or session key SK in the proposed protocol. Definitions 1-4 first explain negligible functions, collision resistance, and Reveal oracles, followed by proofs of these definitions.

Definition 1 (Negligible Function): For all positive integers d, if there exists an integer k0 such that for every k k0, h(k) < k-d, then h(k) is called a negligible function.

Definition 2 (Collision Resistance): The definition of collision resistance is , where represents the adversary’ s success probability in time period t, and denotes the number of queries executed by adversary A.

Definition 3 (Reveal Oracle 1): This Reveal Oracle unconditionally provides input re from hash output y, i.e., y = h(re).

Definition 4 (Reveal Oracle 2): Given public parameters , this oracle outputs the private key x.

Theorem 1: Assuming the hash function acts as a random oracle, adversary A knows communication messages {SIDj, Yi, Ki, Vi} but still cannot retrieve IDi and session key SK.

Proof: First, assume A can retrieve IDi and SK using the experimental algorithm “Cryptanalysis and Improvement of a Three-Factor Remote Authentication Scheme for Multi-server Environments[12]” (CITRASM). The success probability of CITRASM is expressed as:

where Pr(.) represents the success probability of Algorithm 1. The advantage function is defined as , where the maximum depends on the number of queries qr1 executed by the Reveal Oracle in time interval t1. If , the adversary can retrieve Ui’ s IDi and SK. This condition only holds if the adversary can invert the one-way hash function[13]. Since deriving input from a hash function is computationally infeasible in polynomial time, . Therefore, the proposed protocol can prevent A from obtaining Ui’ s IDi and session key SK.

Theorem 2: Assuming the hash function acts as a random oracle, adversary A obtains smart card parameters Ci, Ei, G and communication messages Di, SIDi, DIDi, Ti. A still cannot compute user password PWi, biometric key SPi, or private key x.

Proof: This proof is similar to Theorem 1. Assume A can compute user password PWi, biometric key SPi, and private key x. A obtains communication messages {Di, SIDi, DIDi, Ti} from the public channel and extracts values {Ci, Ei, G} from the smart card. Then A executes an algorithm to compute PWi, SPi, and x.

The advantage function is defined as:

where the maximum depends on the number of queries qr2 executed by the Reveal Oracle in time interval t2. If , the adversary can compute PWi, SPi, and x. This condition only holds if the adversary can invert the one-way hash function. Since deriving input from a hash function is computationally infeasible in polynomial time, . This demonstrates that the proposed scheme can prevent A from obtaining PWi, SPi, and x.

Algorithm 2: 1. Input: < SIDj, G, Di, DIDi, Ti, Ci, Ei > 2. Result: 1 or 0 3. Apply Reveal Oracle on Di to obtain information SIDj, IDi, Pi, and Ai 4. Compute 5. If , then apply Reveal Oracle on to obtain information x 6. Apply Reveal Oracle on Ki to obtain information Pi, Wi, IDi, SIDj, and RSj 7. Compute 8. If , then is the correct identity for user Ui 9. Apply Reveal Oracle on to obtain PWi and SPi 10. If , then is the correct password for Ui and is the correct biometric key 11. Else return 0 (False) 12. End if

---

3 Performance Analysis

This chapter compares the proposed protocol with several related protocols in terms of security features, smart card storage costs, communication costs, computational overhead, and estimated time.

3.1 Smart Card Storage Cost and Communication Cost Comparison

Table 1 compares the proposed protocol with others in smart card storage and communication costs (in bits). For evaluation, this paper assumes IDi, PWi, random nonce, and hash functions are all 160 bits, and key encryption/decryption operations are 512 bits. Table 1 shows that protocols[4,5] have lower smart card storage and communication costs than the proposed protocol. However, these two-factor protocols[4,5] cannot resist certain attacks such as user untraceability and privileged insider attacks, nor do they provide security features like user anonymity, forward secrecy, efficient login phases, or password change phases. Therefore, incurring some additional cost for better security features and functionality is justified.

Table 1. Comparison of Smart Card Storage Cost and Communication Cost (/bits) | Protocol | Smart Card Storage Cost | Communication

Cost | |——-|—————|————-| | Two-factor authentication[4] | | | | Two-factor improvement[5] | | | | Cross-identity authentication[7] | | | | Three-factor authentication[9] | | | | Three-factor improvement[8] | | | | Proposed protocol | | |

3.2 Security Comparison

The ability to resist password guessing attacks (A1), user anonymity (A2), server impersonation attacks (A3), privileged insider attacks (A4), smart card loss attacks (A5), forward secrecy (A6), user untraceability attacks (A7), and session key recovery attacks (A8) are evaluated. Table 2 shows that literature[4] is vulnerable to password guessing attacks, privileged insider attacks, and server impersonation attacks—the most attack types. Literature[5] improves upon[4] and can resist A1, A3, and A4 attacks but fails against user untraceability and key recovery attacks. Literature[8] improves upon[9] and is more reliable against smart card loss attacks. Both literature[8,9] demonstrate good security against these eight attacks. Literature[7] ranks next, strengthening the password factor without using smart cards. The proposed protocol provides better security protection, resisting more attacks and exhibiting robust security characteristics (though not all attack types are enumerated).

Table 2. Comparison of Security Characteristics | Protocol | A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 | |——-|—|—|—|—|—|—|—|—| | Literature[4] | | | | | | | | | | | Literature[5] | | | | | | | | | | | Literature[7] | | | | N/A | | | | | | Literature[8] | | | | | | | | | | | Literature[9] | | | | | | | | | | | Proposed protocol | | | | | | | | |

3.3 Computation Cost and Estimated Time Comparison

For accurate comparison of computation costs, this paper defines symbols as shown in Table 3 , which also provides single-operation computation times from literature[14].

Table 3. Symbolic Definition | Symbol | Definition | Single Computation Time (s) | |—-|——|—————-| | Th | Hash function operation | | | Tme | Modular exponentiation operation | | | Ts | Symmetric key encryption/decryption | | | Tpm | Point multiplication operation | | | Tbp | Bilinear pairing operation | | | Tbh | Bio-cryptographic hash function | | | Tfe | Fuzzy extractor operation | |

The proposed protocol' s computation costs are 7Th + 3Tpm + 1Tfe for registration and 23Th + 12Tpm + 1Tfe for login/authentication. Other protocols[4,5,7-9] have computation costs for registration and authentication phases as shown in Table 4 . The execution time of one fuzzy extractor function equals one elliptic curve point multiplication. The proposed protocol ranks in the medium-to-high range, placing in the upper tier among three-factor approaches.

Table 4. Comparison of Computation Cost and Estimated Time |

Protocol | Registration Phase | Authentication Phase | Total Execution Time (s) | |——-|————-|—————|——————-| | Literature[4] | 13Th + 4Tme | | | | Literature[5] | 6Th + 7Tme | | | | Literature[7] | 12Th + 14Ts + Tme | | | | Literature[8] | 6Th + 4Tpm + 2Tbh | 18Th + 11Tpm + 3Tbp + 1Tbh | | | Literature[9] | 6Th + 6Tpm + 4Tbh | 18Th + 12Tpm + 4Tbp + 1Tbh | | | Proposed protocol | 7Th + 3Tpm + 1Tfe | 23Th + 12Tpm + 1Tfe | |

---

4 Conclusion

In multi-server environments, this paper proposes a three-factor remote authentication protocol where the three factors play crucial roles throughout the authentication process, significantly enhancing security. Formal proof verifies that adversaries cannot obtain identifiers, passwords, or biometric information. Additionally, the proposed protocol does not lag behind other protocols in terms of computational overhead. Future work will focus on further reducing the protocol' s space and time complexity while maintaining essential security features, and extending the protocol to other environments such as healthcare and cloud computing.

References

[1] Shuai Qinghong, Miao Miao. Online payment and electronic banking [M]. Beijing: Machinery Industry Press, 2015.

[2] Tan Zhihua. Research on efficient model checking of network authentication protocol [D]. Changsha: Hunan University, 2011.

[3] Amin R, Islam S H, Biswas G P, et al. Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for e-health care systems [J]. Journal of Medical Systems, 2015, 39 (11): 1-21.

[4] Pippal R S, Jaidhar C D, Tapaswi S. Robust smart card authentication scheme for multi-server architecture [J]. Wireless Personal Communications, 2013, 72 (1): 729-745.

[5] Wei Jianghong, Liu Wenfen, Hu Xuexian. Cryptanalysis and improvement of a robust smart card authentication scheme for multi-server architecture [J]. Wireless Personal Communications, 2014, 77 (3): 2255-2269.

[6] Long Liping, Chen Weijian, Yang Yongjun, et al. Double factors based authentication protocol for RFID [J]. Computer Engineering and Design, 2013, 34 (11): 3726-3730.

[7] Zhang Xue, Li Guangsong, Han Wenbao, et al. Identity-based authenticated

key agreement protocol cross autonomous domains [J]. Journal of Sichuan University: Engineering Science Edition, 2015, 47 (4): 125-131.

[8] Qu Juan, Li Yanping, Wu Xili. Cryptanalysis and improvement of two multi-server remote user authentication schemes using smart cards [J]. Journal of Computer Applications, 2015, 35 (8): 2199-2204.

[9] Choi Y, Nam J, Lee D, et al. Security enhanced anonymous multi-server authenticated key agreement scheme using smart cards and biometrics [J]. Scientific World Journal, 2014, 37 (4): 281-292.

[10] Chen Xiaofeng, Feng Dengguo. Direct anonymous attestation based on bilinear maps [J]. Journal of Software, 2010, 21 (8): 2070-2078.

[11] Lei Qi, Shang Tao, Liu Jianwei. Security analysis for arbitrated quantum signature scheme based on random oracle model [J]. Journal of Cryptologic Research, 2016, 4 (6): 619-628.

[12] Tang Yonglong. A user authentication protocol based on multiple factors [J]. Journal of Networks, 2014, 9 (10): 1081-1090.

[13] Yang Yijun. Research on irreversible transformation of fingerprint security authentication [D]. Shenzhen: Shenzhen University, 2015.

[14] Chiou Shinyan, Ying Zhaoqin, Liu Junqiang. Improvement of a privacy authentication scheme based on cloud for medical environment [J]. Journal of Medical Systems, 2016, 40 (4): 101-115.

Note: Figure translations are in progress. See original paper for figures.