电 子 科 技 大 学

UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY OF CHINA

博士学位论文

DOCTORAL DISSERTATION

论文题目

User Authentication and Key agreement Protocols for Mobile Environments

学科专业 Information Security

学　　号 201514220113

作者姓名 Alzubair Hassan Abdullah Mohamed Tahir

指导教师 李发根

分类号 K825.1-64 密级 公开

UDC[注1] 676.874

学 位 论 文

User Authentication and Key agreement Protocols for Mobile Environments

（题名和副题名）

Alzubair Hassan Abdullah Mohamed Tahir

（作者姓名）

指导教师 李发根、教授、电子科技大学

、、

、、

、、

（姓名、职称、单位名称）

申请学位级别 博士 学科专业 Information Security

提交论文日期 2015年9月24日 论文答辩日期 2018年3月31日

学位授予单位和日期 电子科技大学 2017年6月7日

答辩委员会主席

评阅人

注1：注明《国际十进分类法UDC》的类号。

User Authentication and Key agreement Protocols for Mobile Environments

A Doctor Dissertation Submitted to

University of Electronic Science and Technology of China

Discipline: Information Security

Author: Alzubair Hassan Abdullah Mohamed Tahir

Supervisor: Prof. Li Fagen

School: School of Computer Science and Engineering

独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。据我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得电子科技大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

作者签名：_____ 日期：　　年　　月　　日

论文使用授权

本学位论文作者完全了解电子科技大学有关保留、使用学位论文的规定，有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许论文被查阅和借阅。本人授权电子科技大学可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密的学位论文在解密后应遵守此规定）

作者签名：_____ 导师签名：_____

日期：　　年　　月　　日

Contents

List of Figures

List of Tables

Chapter 1 Introduction

In this chapter, background and significance of client-server and multi-server environments, athentication, and key agreement are introduced. Then, the problem statement and research contributions are discussed. The general outline of the thesis is given at the [1] end.

Chapter 2 Literature Review

Chapter 3 An efficient Certificateless User Authentication and Key Exchange Protocol for Client-Server Environment

Chapter 4 Identity-Based User Authenticated Key Agreement Protocol for Multi-Server Environment with Anonymity

Chapter 5 A heterogeneous User Authentication Protocol with Key Agreement for Mobile Client-Server Environment

Chapter 6 Conclusion

Acknowledgements

References

[1] R. Amin, G. Biswas. Design and analysis of bilinear pairing based mutual authentication and key agreement protocol usable in multi-server environment[J]. Wireless Personal Communications, 2015, 84(1):439–462

[2] R. Schmohl, U. Baumgarten. Mobile services based on client-server or p2p architectures facing issues of context-awareness and heterogeneous environments[M]. 2007, 578–584

[3] L. Cao, W. Ge. A Secure and Efficient Multi-Factor Mutual Certificateless Authentication with Key Agreement Protocol for Mobile Client-Server Environment on ECC without the third-party[J]. International Journal of Security and Its Applications, 2016, 10(10):215–226

[4] W. Diffie, M. Hellman. New directions in cryptography[J]. IEEE transactions on Information Theory, 1976, 22(6):644–654

[5] R. L. Rivest, A. Shamir, L. Adleman. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2):120–126

[6] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE transactions on information theory, 1985, 31(4):469–472

[7] A. Shamir. Identity-based cryptosystems and signature schemes[M]. 1984, 47–53

[8] D. Boneh, M. Franklin. Identity-based encryption from the Weil pairing[M]. 2001, 213–229

[9] D. Boneh, M. Franklin. Identity-based encryption from the Weil pairing[J]. SIAM journal on computing, 2003, 32(3):586–615

[10] D. Giri, P. Srivastava. An Improved Remote User Authentication Scheme with Smart Cards using Bilinear Pairings.[J]. IACR Cryptology ePrint Archive, 2006, 2006:274

[11] G. Fang, G. Huang. Improvement of recently proposed remote client authentication protocols[M]. 2006

[12] M. L. Das, A. Saxena, V. P. Gulati, et al. A novel remote user authentication scheme using bilinear pairings[J]. Computers & Security, 2006, 25(3):184–189

[13] Y.-M. Tseng, T.-Y. Wu, J.-D. Wu. A pairing-based user authentication scheme for wireless clients with smart cards[J]. Informatica, 2008, 19(2):285–302

[14] T. Goriparthi, M. L. Das, A. Saxena. An improved bilinear pairing based remote user authentication scheme[J]. Computer Standards & Interfaces, 2009, 31(1):181–185

[15] T.-Y. Wu, Y.-M. Tseng. An efficient user authentication and key exchange protocol for mobile client–server environment[J]. Computer Networks, 2010, 54(9):1520–1530

[16] E. Yoon, K. Yoo. A new efficient ID-based user authentication and key exchange protocol for mobile client-server environment[M]. 2010, 1–4

[17] H. Debiao, C. Jianhua, H. Jin. An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security[J]. Information Fusion, 2012, 13(3):223–230

[18] S. H. Islam, G. Biswas. Comments on ID-based client authentication with key agreement protocol on ECC for mobile client-server environment[M]. 2011, 628–635

[19] D. He. An efficient remote user authentication and key agreement protocol for mobile client–server environment from pairings[J]. Ad Hoc Networks, 2012, 10(6):1009–1016

[20] J.-L. Tsai, N.-W. Lo. Provably secure and efficient anonymous ID-based authentication protocol for mobile devices using bilinear pairings[J]. Wireless Personal Communications, 2015, 83(2):1273–1286

[21] L. Wu, Y. Zhang, Y. Xie, et al. An Efficient and Secure Identity-Based Authentication and Key Agreement Protocol with User Anonymity for Mobile Devices[J]. Wireless Personal Communications, 2016:1–17

[22] M.-b. Hou, Q.-l. Xu. Secure certificateless-based authenticated key agreement protocol in the client-server setting[M]. 2009, 960–965

[23] S. S. Al-Riyami, K. G. Paterson. Certificateless public key cryptography[M]. 2003, 452–473

[24] D. Boneh, B. Lynn, H. Shacham. Short signatures from the Weil pairing[J]. Journal of cryptology, 2004, 17(4):297–319

[25] M. Jakobsson, D. Pointcheval. Mutual authentication for low-power mobile devices[M]. 2001, 178–195

[26] J. C. Choon, J. H. Cheon. An identity-based signature from gap Diffie-Hellman groups[M]. 2003, 18–30

[27] M. Bellare, P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols[M]. 1993, 62–73

[28] D. He, B. Huang, J. Chen. New certificateless short signature scheme[J]. IET Information Security, 2013, 7(2):113–117

[29] D. Pointcheval, J. Stern. Security proofs for signature schemes[M]. 1996, 387–398

[30] D. Pointcheval, J. Stern. Security arguments for digital signatures and blind signatures[J]. Journal of cryptology, 2000, 13(3):361–396

[31] M. Scott. Computing the Tate pairing[M]. 2005, 293–304

[32] G. Bertoni, L. Breveglieri, M. Venturi. Power aware design of an elliptic curve coprocessor for 8 bit platforms[M]. 2006, 5–341

[33] G. Bertoni, L. Breveglieri, M. Venturi. ECC hardware coprocessors for 8-bit systems and power consumption considerations[M]. 2006, 573–574

[34] M. Scott, N. Costigan, W. Abdulwahab. Implementing cryptographic pairings on smartcards[M]. 2006, 134–147

[35] L.-H. Li, L.-C. Lin, M.-S. Hwang. A remote password authentication scheme for multiserver architecture using neural networks[J]. IEEE Transactions on Neural Networks, 2001, 12(6):1498–1504

[36] I.-C. Lin, M.-S. Hwang, L.-H. Li. A new remote user authentication scheme for multi-server architecture[J]. Future Generation Computer Systems, 2003, 19(1):13–22

[37] W.-J. Tsaur, C.-C. Wu, W.-B. Lee. A smart card-based remote scheme for password authentication in multi-server Internet services[J]. Computer Standards & Interfaces, 2004, 27(1):39–51

[38] W.-S. Juang. Efficient multi-server password authenticated key agreement using smart cards[J]. IEEE Transactions on Consumer Electronics, 2004, 50(1):251–255

[39] C.-C. Chang, J.-S. Lee. An efficient and secure multi-server password authentication scheme using smart cards[M]. 2004, 417–422

[40] Y.-P. Liao, S.-S. Wang. A secure dynamic ID based remote user authentication scheme for multi-server environment[J]. Computer Standards & Interfaces, 2009, 31(1):24–29

[41] H.-C. Hsiang, W.-K. Shih. Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment[J]. Computer Standards & Interfaces, 2009, 31(6):1118–1123

[42] S. K. Sood, A. K. Sarje, K. Singh. A secure dynamic identity based authentication protocol for multi-server architecture[J]. Journal of Network and Computer Applications, 2011, 34(2):609–618

[43] X. Li, Y. Xiong, J. Ma, et al. An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards[J]. Journal of Network and Computer Applications, 2012, 35(2):763–769

[44] W. Han. Weaknesses of a dynamic identity based authentication protocol for multi-server architecture[J]. CoRR, 2012, abs/1201.0883

[45] E.-J. Yoon, K.-Y. Yoo. Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem[J]. The Journal of Supercomputing, 2013, 63(1):235–255

[46] M. K. Khan, D. He. A new dynamic identity-based authentication protocol for multi-server environment using elliptic curve cryptography[J]. Security and Communication Networks, 2012, 5(11):1260–1266

[47] W. Han, Z. Zhu. An ID-based mutual authentication with key agreement protocol for multiserver environment on elliptic curve cryptosystem[J]. International Journal of Communication Systems, 2014, 27(8):1173–1185

[48] D. He, D. Wang. Robust Biometrics-Based Authentication Scheme for Multiserver Environment[J]. IEEE Systems Journal, 2015, 9(3):816–823

[49] H. Shen, C. Gao, D. He, et al. New biometrics-based authentication scheme for multi-server environment in critical systems[J]. Journal of Ambient Intelligence and Humanized Computing, 2015, 6(6):825–834

[50] Y.-M. Tseng, S.-S. Huang, M.-L. You. Strongly secure ID-based authenticated key agreement protocol for mobile multi-server environments[J]. International Journal of Communication Systems, 2017, 30(11):e3251–n/a

[51] S. D. Galbraith, K. Harrison, D. Soldera. Implementing the Tate pairing[M]. 2002, 324–337

[52] A. J. Menezes, T. Okamoto, S. A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field[J]. iEEE Transactions on information Theory, 1993, 39(5):1639–1646

[53] L. Chen, K. Harrison, A. Moss, et al. Certification of public keys within an identity based system[M]. 2002, 322–333

[54] H. Shen, C. Gao, D. He, et al. New biometrics-based authentication scheme for multi-server environment in critical systems[J]. Journal of Ambient Intelligence and Humanized Computing, 2015, 6(6):825–834

[55] L.-H. Li, L.-C. Lin, M.-S. Hwang. A remote password authentication scheme for multiserver architecture using neural networks[J]. IEEE Transactions on Neural Networks, 2001, 12(6):1498–1504

[56] P. Jiang, Q. Wen, W. Li, et al. An anonymous and efficient remote biometrics user authentication scheme in a multi server environment[J]. Frontiers of Computer Science, 2015, 9(1):142–156

[57] H. Lin, F. Wen, C. Du. An improved anonymous multi-server authenticated key agreement scheme using smart cards and biometrics[J]. Wireless Personal Communications, 2015, 84(4):2351–2362

[58] Y.-P. Liao, C.-M. Hsiao. A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients[J]. Future Generation Computer Systems, 2013, 29(3):886–900

[59] D. He, S. Zeadally, N. Kumar, et al. Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(9):2052–2064

[60] H. Zhu. A provable one-way authentication key agreement scheme with user anonymity for multi-server environment[J]. KSII Transactions on Internet and Information Systems (TIIS), 2015, 9(2):811–829

[61] S. Jangirala, S. Mukhopadhyay, A. K. Das. A Multi-server environment with secure and efficient remote user authentication scheme based on dynamic ID using smart cards[J]. Wireless Personal Communications, 2017, 95(3):2735–2767

[62] J.-L. Tsai, N.-W. Lo. A chaotic map-based anonymous multi-server authenticated key agreement protocol using smart card[J]. International Journal of Communication Systems, 2015, 28(13):1955–1963

[63] A. Irshad, M. Sher, S. A. Chaudhary, et al. An efficient and anonymous multi-server authenticated key agreement based on chaotic map without engaging Registration Centre[J]. The Journal of Supercomputing, 2016, 72(4):1623–1644

[64] P. Pleva. A Revised Classification of Anonymity[J]. arXiv preprint arXiv:1211.5613, 2012

[65] W.-S. Juang. Efficient multi-server password authenticated key agreement using smart cards[J]. IEEE Transactions on Consumer Electronics, 2004, 50(1):251–255

[66] A. Hassan, N. Eltayieb, R. Elhabob, et al. A Provably Secure Certificateless User Authentication Protocol for Mobile Client-Server Environment[M]. 2017, 592–602

[67] R. Canetti, H. Krawczyk. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels[M]. Springer, 2001, 453–474

[68] B. LaMacchia, K. Lauter, A. Mityagin. Stronger Security of Authenticated Key Exchange[M]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, 1–16

[69] A. De Caro, V. Iovino. jPBC: Java pairing based cryptography[M]. 2011, 850–855

[70] F. Wu, L. Xu, S. Kumari, et al. A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security[J]. Journal of Ambient Intelligence and Humanized Computing, 2017

[71] J. Daemen, V. Rijmen. The design of Rijndael: AES-the advanced encryption standard[M]. Springer Science & Business Media, 2013

[72] A. Hassan, N. Eltayieb, R. Elhabob, et al. A Provably Secure Certificateless User Authentication Protocol for Mobile Client-Server Environment[M]. 2016, 592–602

[73] K.-A. Shim, Y.-R. Lee, C.-M. Park. EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks[J]. Ad Hoc Networks, 2013, 11(1):182–189

[74] S. S. M. Chow, S.-M. Yiu, L. C. K. Hui. Efficient Identity Based Ring Signature[M]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, 499–512

[75] A. Sui, S. S. M. Chow, L. C. K. Hui, et al. Separable and Anonymous Identity-Based Key Issuing[M]. 2005, 275–279

[76] J. Herranz, G. Sáez. New identity-based ring signature schemes[M]. 2004, 27–39

[77] A. Hassan, N. Eltayieb, R. Elhabob, et al. An efficient certificateless user authentication and key exchange protocol for client-server environment[J]. Journal of Ambient Intelligence and Humanized Computing, 2017:1–15

[78] M. Bellare, P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols[M]. 1993, 62–73

[79] A. Fiat, A. Shamir. How to prove yourself: Practical solutions to identification and signature problems[M]. 1986, 186–194

[80] R. Canetti, O. Goldreich, S. Halevi. The random oracle methodology, revisited[J]. Journal of the ACM (JACM), 2004, 51(4):557–594

[81] M. Bellare, A. Boldyreva, A. Palacio. An uninstantiable random-oracle-model scheme for a hybrid-encryption problem[M]. 2004, 171–188

[82] R. L. Rivest, A. Shamir, Y. Tauman. How to leak a secret[M]. 2001, 552–565