

Saeed Ullah Jan

# An Improved Lightweight Privacy Preserving Authentication Scheme for SIP-Based-VoIP Using Smart Card



**Anchor Academic Publishing**

*disseminate knowledge*

**Jan, Saeed Ullah: An Improved Lightweight Privacy Preserving Authentication Scheme for SIP-Based-VoIP Using Smart Card, Hamburg, Anchor Academic Publishing 2017**

PDF-eBook-ISBN: 978-3-96067-628-7

Druck/Herstellung: Anchor Academic Publishing, Hamburg, 2017

**Bibliografische Information der Deutschen Nationalbibliothek:**

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

**Bibliographical Information of the German National Library:**

The German National Library lists this publication in the German National Bibliography. Detailed bibliographic data can be found at: <http://dnb.d-nb.de>

All rights reserved. This publication may not be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publishers.

---

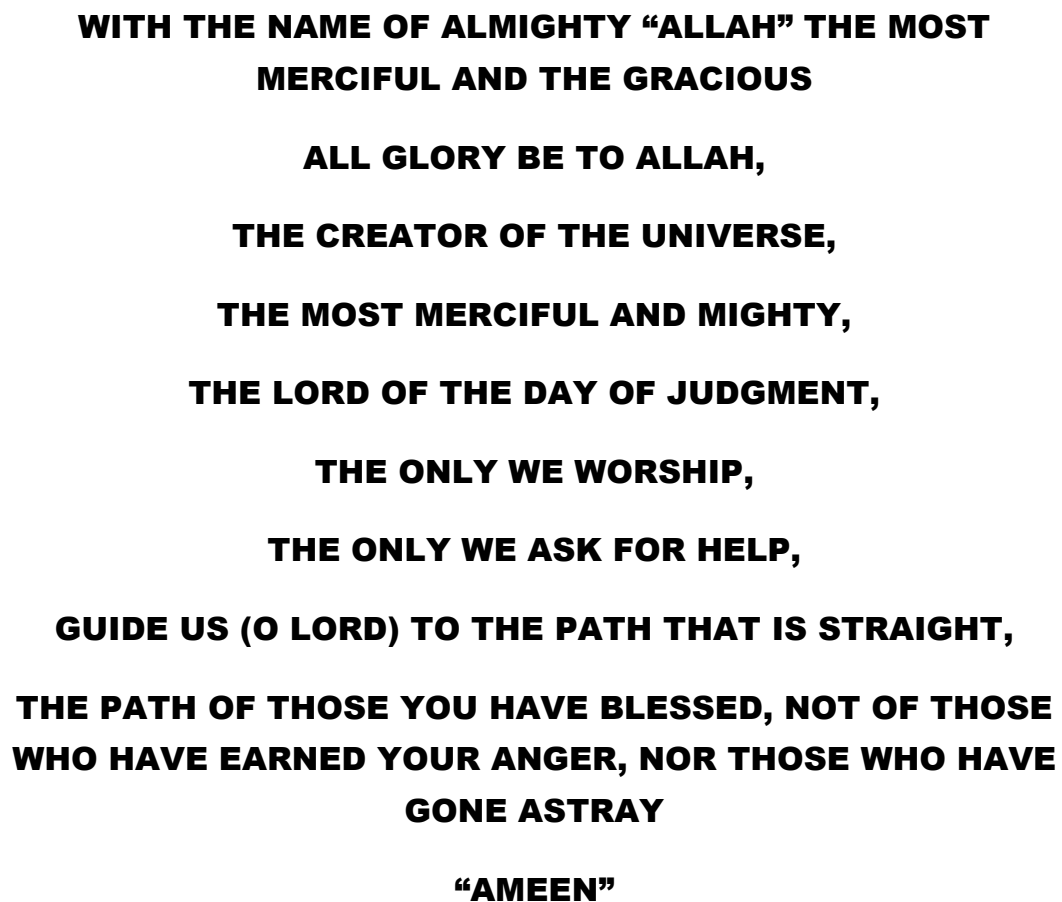
Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Bearbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden und die Diplomica Verlag GmbH, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

Alle Rechte vorbehalten

© Anchor Academic Publishing, Imprint der Diplomica Verlag GmbH  
Hermannstal 119k, 22119 Hamburg  
<http://www.diplomica-verlag.de>, Hamburg 2017  
Printed in Germany

A decorative border resembling a scroll, with rounded corners and a thick black outline. The top and bottom edges are slightly curved, and there are small circular accents at the corners, one at the top-left and one at the bottom-left, which are shaded grey.

**WITH THE NAME OF ALMIGHTY “ALLAH” THE MOST  
MERCIFUL AND THE GRACIOUS**

**ALL GLORY BE TO ALLAH,  
THE CREATOR OF THE UNIVERSE,  
THE MOST MERCIFUL AND MIGHTY,  
THE LORD OF THE DAY OF JUDGMENT,  
THE ONLY WE WORSHIP,  
THE ONLY WE ASK FOR HELP,  
GUIDE US (O LORD) TO THE PATH THAT IS STRAIGHT,  
THE PATH OF THOSE YOU HAVE BLESSED, NOT OF THOSE  
WHO HAVE EARNED YOUR ANGER, NOR THOSE WHO HAVE  
GONE ASTRAY**

**“AMEEN”**

## *Dedication*

*This thesis is dedicated:*

*To*

*The Holiest Man Ever Born,*

*Prophet Muhammad (صلى الله عليه وسلم)*

*∫*

*To*

*MY Parents and Family*

*I am most appreciative of my parents, family and love of my life, whose affection has always been the source of encouragement for me, and whose prayers have always been a key to my success.*

*∫*

*To*

*My Beloved colleagues*

*Who were always there for me and made my life at UOM easier and fun.*

*∫*

*To*

*My Honorable Teachers*

*Whose are beacon of knowledge and a constant source of inspiration for my whole life span.*

## **Acknowledgements**

First of all I would like to thank ALMIGHTY ALLAH for his countless blessing to complete my studies. At the leading edge, I would like to thank my supervisor Dr. Fawad Qayum who shared a lot of his experience and ideas with me. I appreciate his professionalism, planning, and constant involvement in my research. I cherish the time we spent in discussions and in the laboratory hammering over problems. Working under him has sharpened my research skills and increased my enthusiasm to work in cryptography.

I am grateful to Dr. Sohail Abbas for his encouragement, advice, and help whenever needed. I am thankful to the Department of Computer Science Research Lab and the Software Engineering Department for offering me a fabulous environment to work and study. I would like to take this opportunity to acknowledge Dr Sohail Abbas and lab mates who made my stay at University of Malakand exciting and unforgettable. I acknowledge the help received from him on innumerable occasions. I would especially like to thank him for helping me out with various tool flows for the discussions that we had on technical as well as non- technical topics. I thank Dr Shakeel Arshad, Dr Siffat Ullah, Dr Sami Ur Rahman and Dr Sehat Ullah for working along with me on several courses and assignments.

I am grateful to Dr Ajab Khan and Dr Siffat Ullah Khan for giving me this opportunity to further my studies. I would like to acknowledge the help received from my colleague, Mr Aziz Ur Rahman, who took care of things while I was away. I would like to thank my brothers and my family for the love and encouragement I received. Without their support this thesis would not have been possible. I would like to thank my friend Mr Aziz Ur Rahman and Mr. Muhammad Salim for his prayers and for being my role model for hard work.

**SAEED ULLAH JAN**

## Abstract

In the past few years, secure information sharing became very popular in the area of immigration, military applications, healthcare, education, foreign affairs, etc. As secure communication utilizes both wireless and wired communication mechanizations for exchanging sensitive information, so security and privacy of the information exchange cannot be easily compromised. To moderate the security, integrity, authenticity, and privacy issues related to information exchange, numerous authentication mechanisms have been recommended by different researcher in the literature in recent times, but are vulnerable to prospective security flaws such as masquerade, insider, replay, impersonation, password guessing, server spoofing, denial-of-service attacks and in addition failed to deliver mutual authentication.

In the past few years we have also seen a balanced growth in the acceptance of VoIP (Voice over IP) facilities, because the numerous Web and VoIP applications depend on huge and extremely distributed infrastructures to process requests from millions of users in an appropriate manner. Due to their extraordinary desires, these large-scale Internet applications have frequently surrendered security for other objectives such as performance, scalability and availability. As a result, these applications have characteristically favored weaker, but well-organized security mechanisms in their foundations. Session Initiation Protocol (SIP) is an application and presentation layers signaling protocol that initiates, modifies, and terminates IP-based multimedia sessions. Implementing SIP for secure communication has been a topic of study for the past decade, and several proposals are available in the research domain. However, security aspects are not addressed in most of these proposals, because SIP is exposed to several threats and faces security issue at these layers. Probes for SIP (Session Initiation Protocol) servers have been conveyed for many years, and to gather more details about these activities we simply design a scheme for SIP servers in a network and composed data about some popular attacks. What will follow is an explanation of our interpretations and guidance on how to prevent these attacks from being successful.

Biometrics a new field of research has also been materialized in this research, entitled "a three-factor authentication scheme" in which one factor is biometrics. In biometric cryptosystems the benefits of biometric confirmation are presented to basic cryptographic key supervisory systems to enhance security. Anyhow, this research delivers a general outline of the basics, permitting to biometrics as well as cryptography. This work also gives biometric cryptosystems based on iris biometrics and using smart card as well as a password for authentication.

# Table of Contents

<b>1. Introduction.....</b>	<b>1</b>
1.1 Overview .....	1
1.1.1 One-Factor Authentication Scheme.....	1
1.1.2 Two-Factor Authentication Scheme .....	1
1.1.3 Three-Factor Authentication Scheme .....	2
1.2 Cryptology.....	2
1.2.1 Symmetric Cryptography .....	3
1.2.2 Key Generation Technique.....	3
1.2.3 Symmetric Encryption and Decryption .....	4
1.2.4 One-Way Digital Hash-Function.....	4
1.2.5 Asymmetric Cryptography .....	5
1.3 Voice over Internet Protocol (VoIP) .....	7
1.3.1 Session Initiation Protocol (SIP) .....	8
1.3.2 H.323 .....	11
1.4 Smart Card.....	11
1.4.1 Background of Smart Card.....	11
1.4.2 Standard Selection for Smart Card .....	13
1.4.3 Application of Smart-Card .....	14
1.4.4 Types of Smart Card.....	14
1.5 ProVerif an Automated Software Toolkit .....	15
1.6 BioHashing Technique.....	15
1.7 Common Adversary Model (CAM).....	17
1.8 XOR ( $\oplus$ ) Bitwise-Operations.....	18
1.9 BAN-Logic.....	19
1.10 Chapter Summary.....	19
<b>2. Literature Review .....</b>	<b>21</b>
2.1 Overview .....	21
2.2 Kim and Kue Scheme.....	21
2.2.1 Registration Phase .....	22
2.2.2 Login Phase .....	22
2.2.3 Cryptanalysis of Kim and Kue Scheme.....	23
2.3 He et al.'s Scheme.....	23

2.3.1	Registration Phase .....	23
2.3.2	Login Phase .....	24
2.3.3	Authentication Phase .....	24
2.3.4	Password Change Phase .....	24
2.3.5	Cryptanalysis of He et al.'s Scheme .....	25
2.4	Das et al.'s Scheme .....	25
2.4.1	Registration Phase .....	25
2.4.2	Login Phase .....	25
2.4.3	Verification Phase.....	26
2.4.4	Password Change Phase .....	26
2.4.5	Cryptanalysis of Das et al.'s Scheme .....	26
2.5	An's Scheme .....	26
2.5.1	Registration Phase .....	27
2.5.2	Login Phase .....	27
2.5.3	Authentication Phase .....	28
2.5.4	Cryptanalysis of An's Scheme .....	29
2.6	Park et al.'s Scheme .....	29
2.6.1	Registration Phase .....	29
2.6.2	Login Phase .....	30
2.6.3	Authentication Phase .....	30
2.6.4	Cryptanalysis of Park et al.'s Scheme .....	31
2.7	Zhu-Xu-Feng's Scheme .....	31
2.7.1	Initial Phase .....	31
2.7.2	Registration Phase .....	31
2.7.3	Login Phase .....	31
2.7.4	Authentication Phase .....	32
2.7.5	Cryptanalysis of Zhu-Xu-Feng's Scheme .....	32
2.8	Song's Scheme .....	33
2.8.1	Initialization Phase .....	33
2.8.2	Registration Phase .....	34
2.8.3	Login Phase .....	34
2.8.4	Authentication Phase .....	34
2.8.5	Cryptanalysis of Song's Scheme .....	35



2.9 Wu et al.'s Scheme [19] .....	35
2.9.1 Initialization Phase .....	35
2.9.2 Registration Phase .....	35
2.9.3 Login & Authentication Phases .....	36
2.9.4 Password or Biometrics Change Phase .....	37
2.9.5 Cryptanalysis of Wu et al.'s Scheme .....	37
2.10 Lee et al.'s Scheme .....	37
2.10.1 Registration Phase .....	38
2.10.2 Login & Authentication Phases .....	39
2.10.3 Password Change Phase .....	40
2.10.4 Cryptanalysis of Lee et al.'s Scheme .....	40
2.11 Lue et al.'s Scheme .....	40
2.11.1 Registration Phase .....	41
2.11.2 Login & Verification Phases .....	42
2.11.3 Password Change Phase .....	43
2.11.4 Cryptanalysis of Lue et al Scheme .....	43
2.12 Tsai et al.'s Scheme [25] .....	43
2.12.1 Working of Tsai et al. scheme .....	43
2.12.2 The Server Registration Phase .....	44
2.12.3 The User Registration Phase .....	44
2.12.4 The Login and Authentication Phase .....	45
2.12.5 Cryptanalysis of Tsai et al. Scheme .....	45
2.13 Wu-Xu-Xiong Scheme .....	47
2.13.1 Registration Phase .....	48
2.13.2 Login and Authentication Phases .....	48
2.13.3 Password Change Phase .....	50
2.13.4 Card Revocation Phase .....	50
2.13.5 Cryptanalysis of Wu-Xu-Xiang Scheme .....	50
2.14 Lipping Zhang et al.'s Scheme .....	50
2.14.1 Initialization Phase .....	51
2.14.2 Registration Phase .....	51
2.14.3 Login Phase .....	52
2.14.4 Authentication Phase .....	52

2.14.5 Password or Biometric Updating Phase .....	53
2.14.6 Cryptanalysis of Lipping Zhang et al.'s Scheme.....	54
2.15 Zhang et al.'s Scheme .....	54
2.15.1 Registration Phase .....	55
2.15.2 Login and Authentication Phases .....	56
2.15.3 Password Change Phase .....	58
2.16 Zhang et al.'s Protocol Analysis .....	58
2.16.1 Working Procedure of the Scheme.....	58
2.16.2 Biometric Extraction and Password Guessing Attacks .....	59
2.16.3 User Anonymity Violation .....	59
2.16.4 Replay Attack and Denial-of-Service Attack .....	60
2.17 Chapter Summary.....	60
<b>3. Proposed Solution .....</b>	<b>61</b>
3.1 Overview .....	61
3.2 Proposed Scheme .....	61
3.2.1 Registration Phase .....	64
3.2.2 Login and Authentication Phases .....	65
3.2.3 Password Change Phase .....	67
3.3 Chapter Summary.....	68
<b>4. Security Analysis.....</b>	<b>69</b>
4.1 Overview .....	69
4.2 Formal Security Analysis .....	69
4.2.1 BAN Logic .....	70
4.2.2 Rules of BAN Logic .....	70
4.2.3 BAN Method for Protocol Analysis .....	72
4.2.4 BAN-Logic Postulates .....	72
4.2.5 BAN Idealized Form .....	75
4.3 Proposed Protocol Analysis .....	75
4.3.1 BAN Goals for the Proposed Scheme .....	76
4.3.2 BAN Idealized form for the Proposed Scheme .....	76
4.3.3 BAN Assumptions for the Proposed Scheme.....	76
4.4 ProVerif Implementation.....	78
4.4.1 Proposed Protocol Verification Using ProVerif.....	78

4.5 Informal Security Analysis.....	83
4.5.1 Denning-Sacco Attack.....	83
4.5.2 Stolen-Verifier Attack .....	84
4.5.3 Insider Attack .....	84
4.5.4 Password Disclosure Attack .....	84
4.5.5 Certified-Key Guarantee.....	84
4.5.6 Man-in-the-Middle Attack.....	84
4.5.7 Mutual Authentication.....	85
4.5.8 Online Password Guessing Attack .....	85
4.5.9 Offline Password Guessing Attack.....	85
4.5.10 Biometrics Security .....	85
4.5.11 Resist Replay Attack .....	86
4.5.12 Strong User Anonymity.....	86
4.5.13 Resist Denial-of-Service Attack .....	86
4.6 Chapter Summary.....	87
<b>5. Performance Analysis.....</b>	<b>88</b>
5.1 Overview .....	88
5.1.1 Attack Resistance and Functionality Analysis .....	88
5.1.2 Storage Overhead Analysis .....	89
5.1.3 Computation Cost Analysis.....	90
5.1.4 Communication Cost Analysis .....	91
5.2 Chapter Summary.....	92
<b>6. Conclusion and Future Work .....</b>	<b>93</b>
<b>Bibliography .....</b>	<b>95</b>

## List of Figures

Figure- 1: Symmetric Cryptography .....	3
Figure- 2: Symmetric Encryption/Decryption .....	4
Figure- 3: A Diagrammatic Representation of Single-Way Hash Function .....	4
Figure- 4: Asymmetric Cryptography.....	5
Figure- 5: Public Key Infrastructure .....	6
Figure- 6: Conventional Public Key Infrastructure .....	6
Figure- 7: Elliptic Curve Cryptography [25] .....	7
Figure- 8: VoIP Application Scenarios.....	8
Figure- 9: SIP's Messages Structure.....	8
Figure- 10: Flow Chart Representation for SIP Callee.....	10
Figure- 11: Participants using H.323 .....	11
Figure- 12: A Typical Smart Card .....	12
Figure- 13: A Ring-Shaped Smart Card.....	12
Figure- 14: The Chip, Dimension and Standards Selection for Smart Card.....	13
Figure- 15: Smart Cards Types .....	14
Figure- 16: ProVerif Model .....	15
Figure- 17: Insecure Bio-Metric Extraction.....	16
Figure- 18: Biometric data with hashing .....	16
Figure- 19: Adversary Control over Distributed System [80] .....	17
Figure- 20: XOR-Logic Circuit .....	18
Figure- 21: XOR Technique for Error Correction .....	18
Figure- 22: The Registration.....	51
Figure- 23: Login and Authentication Phases.....	53
Figure- 24: Iris BioHashing Technique .....	62
Figure- 25: Biometric Template Storing Stages .....	63

## List of Tables

Table- 1: Notations Used for Kim and Kue Scheme .....	21
Table- 2: Notations Used for the Scheme .....	23
Table- 3: Notations Used for the Scheme .....	25
Table- 4: Notations Used for An's Scheme .....	27
Table- 5: Notations Used for Park et al.'s Scheme .....	29
Table- 6: Notations Used for Zhu-Xu-Feng's Scheme .....	31
Table- 7: Notation Used for Song's Scheme .....	33
Table- 8: Notations used by Wu et al.'s Protocol .....	35
Table- 9: Notations Used for Lee et al.'s Scheme .....	38
Table- 10: Notations Used for Lue et al.'s Scheme .....	41
Table- 11: Notation used for Tsai et al.'s Scheme .....	44
Table- 12: Notations used in Wu-Xu-Xiong Scheme .....	47
Table- 13: Notations used Lipping Zhang et al.'s Scheme .....	51
Table- 14: Notation Used for Zhang et al.'s Scheme .....	55
Table- 15: Notation used for the Proposed Scheme .....	64
Table- 16: Notations used by Burrows, Abadi and Needham .....	70
Table- 17: Protocol steps and its descriptions .....	75
Table- 18: The Functionality Comparison .....	89
Table- 19: Storage Overhead .....	89
Table- 20: Computational Coast Analysis of Different Schemes .....	91