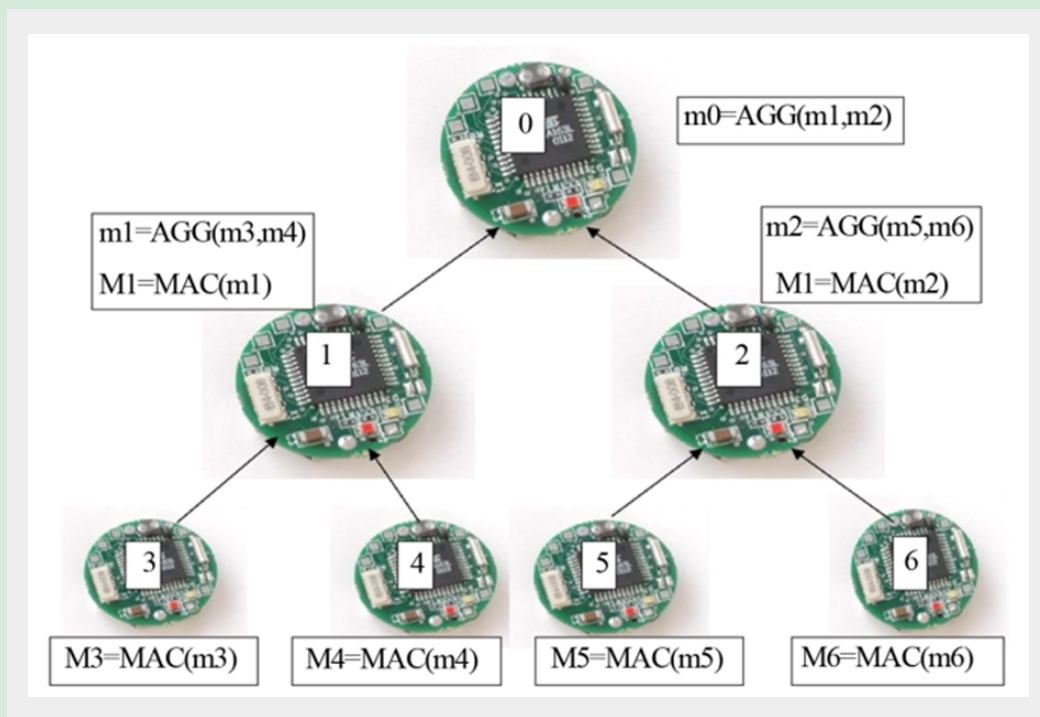




# Journal of Information Security



ISSN: 2153-1234



9 772153 123004 01

# Journal Editorial Board

ISSN: 2153-1234 (Print)    ISSN: 2153-1242 (Online)

<http://www.scirp.org/journal/jis>

---

## Editor-in-Chief

**Prof. Gyungho Lee**

Korea University, South Korea

## Editorial Board (According to Alphabet)

**Prof. Abbaci Azzedine**

Universite Badji Mokhtar, Algeria

**Prof. Chris Cannings**

University of Sheffield, UK

**Dr. Xiaochun Cheng**

Middlesex University, UK

**Dr. Philip W. L. Fong**

University of Calgary, Canada

**Dr. Marina L. Gavrilova**

University of Calgary, Canada

**Prof. Vic Grout**

Glyndwr University, UK

**Dr. Le Gruenwald**

University of Oklahoma, USA

**Prof. Sun-Yuan Hsieh**

National Cheng Kung University, Chinese Taipei

**Prof. Lucas Chi Kwong Hui**

The University of Hong Kong, China

**Prof. Min-Shiang Hwang**

National Chung Hsing University, Chinese Taipei

**Prof. Jiejun Kong**

Beijing Institute of Technology, China

**Dr. Fagen Li**

University of Electronic Science and Technology of China, China

**Dr. Giannis F. Marias**

Athens University of Economics and Business, Greece

**Prof. Stavros D. Nikolopoulos**

University of Ioannina, Greece

**Prof. Changwoo Pyo**

Hongik University, South Korea

**Prof. Sofiene Tahar**

Concordia University, Canada

**Prof. Lina Wang**

Wuhan University, China

**Dr. Ronald D. Williams**

University of Virginia, USA

## TABLE OF CONTENTS

**Volume 5    Number 1**

**January 2014**

**Investigating Approaches of Data Integrity Preservation for Secure Data Aggregation in  
Wireless Sensor Networks**

V. Jariwala, V. Singh, P. Kumar, D. C. Jinwala.....1

**Comparative Evaluation of Elliptic Curve Cryptography Based Homomorphic Encryption  
Schemes for a Novel Secure Multiparty Computation**

S. J. Patel, A. Chouhan, D. C. Jinwala.....12

---

The figure on the front cover is from the article published in *Journal of Information Security*, 2014, Vol. 5, No. 1, pp. 1-11 by Vivaksha Jariwala, *et al.*

## **Journal of Information Security (JIS)**

### **Journal Information**

#### **SUBSCRIPTIONS**

The *Journal of Information Security* (Online at Scientific Research Publishing, [www.SciRP.org](http://www.SciRP.org)) is published quarterly by Scientific Research Publishing, Inc., USA.

#### **Subscription rates:**

Print: \$79 per issue.

To subscribe, please contact Journals Subscriptions Department, E-mail: [sub@scirp.org](mailto:sub@scirp.org)

#### **SERVICES**

##### **Advertisements**

Advertisement Sales Department, E-mail: [service@scirp.org](mailto:service@scirp.org)

##### **Reprints (minimum quantity 100 copies)**

Reprints Co-ordinator, Scientific Research Publishing, Inc., USA.

E-mail: [sub@scirp.org](mailto:sub@scirp.org)

#### **COPYRIGHT**

Copyright©2014 Scientific Research Publishing, Inc.

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as described below, without the permission in writing of the Publisher.

Copying of articles is not permitted except for personal and internal use, to the extent permitted by national copyright law, or under the terms of a license issued by the national Reproduction Rights Organization.

Requests for permission for other kinds of copying, such as copying for general distribution, for advertising or promotional purposes, for creating new collective works or for resale, and other enquiries should be addressed to the Publisher.

Statements and opinions expressed in the articles and communications are those of the individual contributors and not the statements and opinion of Scientific Research Publishing, Inc. We assume no responsibility or liability for any damage or injury to persons or property arising out of the use of any materials, instructions, methods or ideas contained herein. We expressly disclaim any implied warranties of merchantability or fitness for a particular purpose. If expert assistance is required, the services of a competent professional person should be sought.

#### **PRODUCTION INFORMATION**

For manuscripts that have been accepted for publication, please contact:

E-mail: [jis@scirp.org](mailto:jis@scirp.org)



# Journal of Information Security

ISSN 2153-1234 (Print) ISSN 2153-1242 (Online)  
<http://www.scirp.org/journal/jis>

JIS, a quarterly journal, publishes research and review articles in all important aspects of information security. Both experimental and theoretical papers are acceptable provided they report important findings, novel insights, or useful techniques in these areas.

## Editor-in-Chief

Prof. Gyungho Lee

Korea University, South Korea

## Subject Coverage

JIS aims to provide a platform for scientists and academicians all over the world to promote, share, and discuss various new issues and developments in different areas of information security. All manuscripts submitted to JIS must be previously unpublished and may not be considered for publication elsewhere at any time during JIS's review period. Additionally, accepted ones will immediately appear online followed by printed in hard copy. The topics to be covered by Journal of Information Security include, but are not limited to:

Access Control	Intrusion Detection
Anti-Virus and Anti-Worms	Key Management and Key Recovery
Authentication and Authorization	Language-Based Security
Biometric Security	Network Security
Cryptography	Operating System Security
Data and System Integrity	Risk Evaluation and Security Certification
Database Security	Security and Privacy for Social Computing
Distributed Systems Security	Security Evaluation
Electronic Commerce Security	Security for Mobile Computing
Fraud Control	Security Models
Grid Security	Security Protocols
Information Hiding and Watermarking	Signature and Key Agreement Protocol
Information Privacy	Software Security
Information Security Engineering	System Security
Intellectual Property Protection	Trusted Computing and Trustworthy Computing Technology

We are also interested in short papers (letters) that clearly address a specific problem, and short survey or position papers that sketch the results or problems on a specific topic. Authors of selected short papers would be invited to write a regular paper on the same topic for future issues of the *JIS*.

## Notes for Intending Authors

Submitted papers should not have been previously published nor be currently under consideration for publication elsewhere. Paper submission will be handled electronically through the website. All papers are refereed through a peer review process. For more details about the submissions, please access the website.

## Website and E-Mail

<http://www.scirp.org/journal/jis>

E-mail: [jis@scirp.org](mailto:jis@scirp.org)