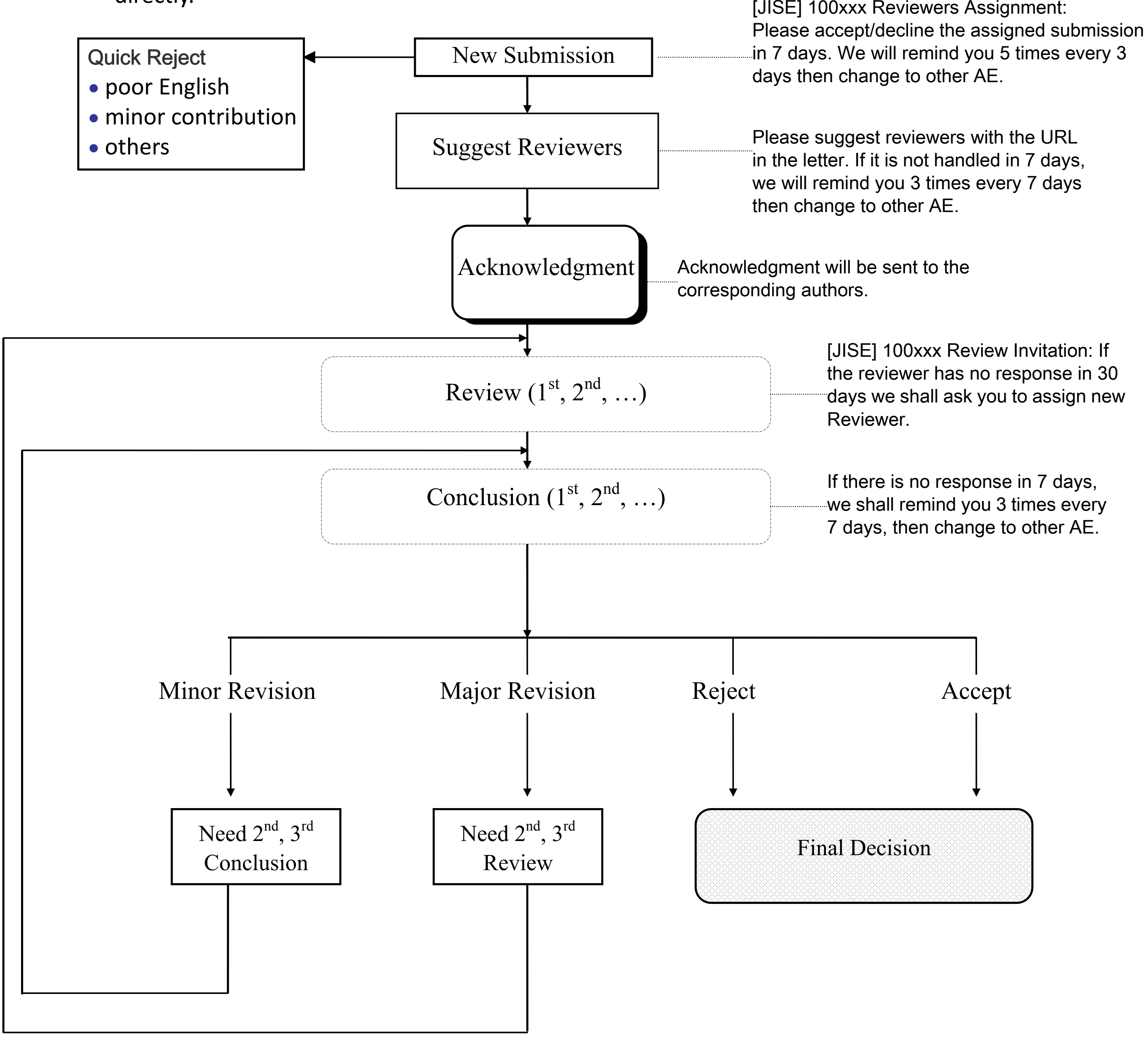
User's Guide for Associate Editor (AE) Online System

The functions for Associate Editor Online System consist of:
(1) Accept/Decline Assignment, (2) Paper Assignment, (3) Review Conclusion, (4) Submission Status, (5) All Submissions, (6) Review Status (by paper, by reviewer), (7) Add Reviewers, (8) Return

- **Overview of the review process:** The auto-submission system will send you Letters (emails) and you could handle the submission with the URL in the letter (email). If it is not handled in 7 days, we will send you reminders on a regular basis.
  - **Quick Reject:** papers with poor English or very minor contribution could reject it directly.



[JISE] 100xxx Reviewers Assignment: Please accept/decline the assigned submission in 7 days. We will remind you 5 times every 3 days then change to other AE.

Please suggest reviewers with the URL in the letter. If it is not handled in 7 days, we will remind you 3 times every 7 days then change to other AE.

Acknowledgment will be sent to the corresponding authors.

[JISE] 100xxx Review Invitation: If the reviewer has no response in 30 days we shall ask you to assign new Reviewer.

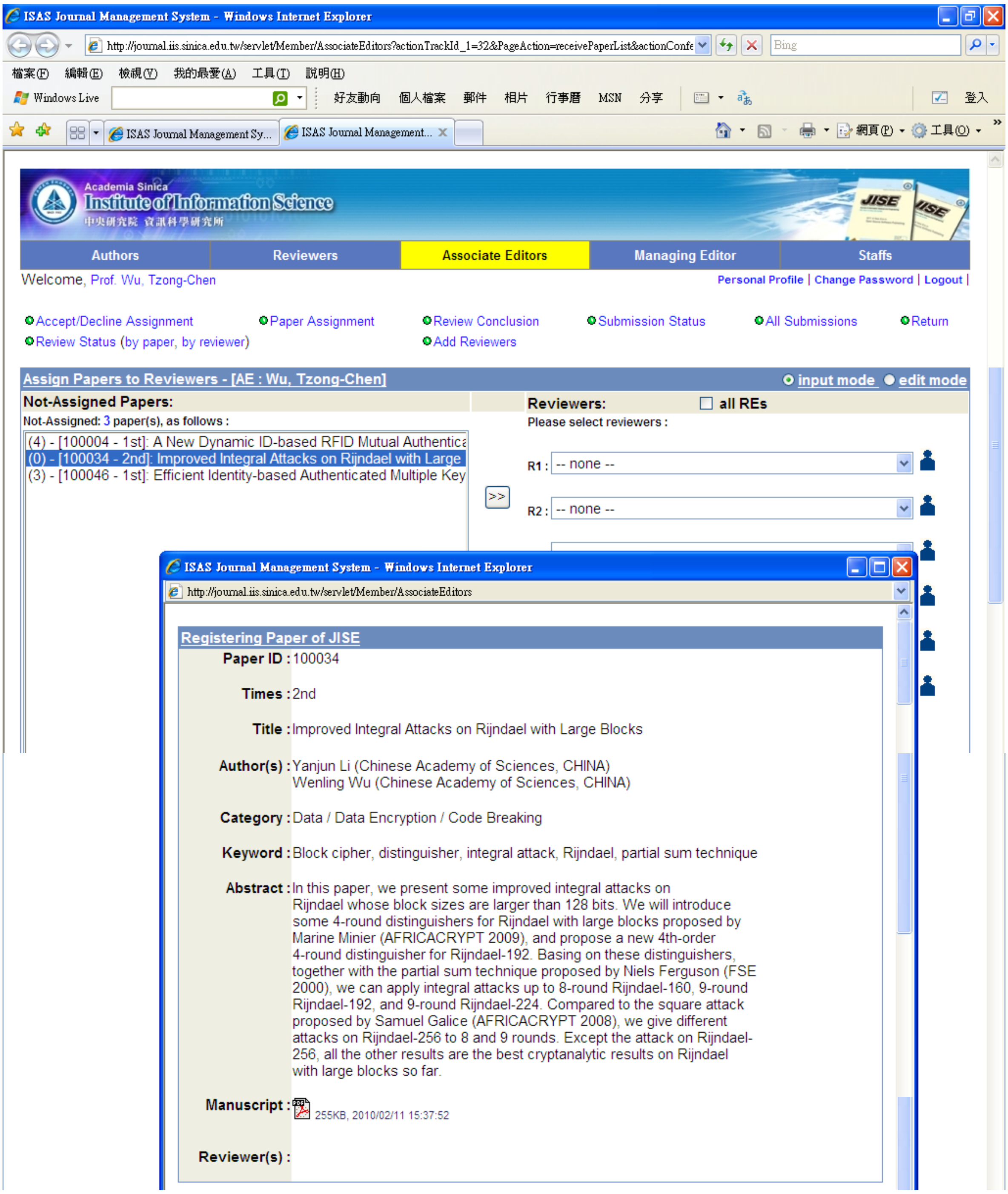
If there is no response in 7 days, we shall remind you 3 times every 7 days, then change to other AE.

(1) **Accept/Decline Assignment:** Please press the button to decide whether you would like to handle this submission.

(2) **Paper Assignment:**

(i) Please select an unassigned submission in the left column which shows “(0)”, where “(0)” means none of the reviewers have been assigned; “(4)” means 4 reviewers have already been assigned.

All the information for this submission will be shown as follows and by clicking “Manuscript” you can read the full text of this submission.



ISAS Journal Management System - Windows Internet Explorer
http://journal.iis.sinica.edu.tw/servlet/Member/AssociateEditors?actionTrackId_1=32&PageAction=receivePaperList&actionConfe
Bing
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
Windows Live 好友動向 個人檔案 郵件 相片 行事曆 MSN 分享 登入
ISAS Journal Management Sy... ISAS Journal Management...
網頁(P) 工具(O)
Academia Sinica
Institute of Information Science
中央研究院 資訊科學研究所
JISE
Authors
Reviewers
Associate Editors
Managing Editor
Staffs
Personal Profile | Change Password | Logout |
Accept/Decline Assignment
Paper Assignment
Review Conclusion
Submission Status
All Submissions
Return
Review Status (by paper, by reviewer)
Add Reviewers
○ input mode ● edit mode
>>
ISAS Journal Management System - Windows Internet Explorer
http://journal.iis.sinica.edu.tw/servlet/Member/AssociateEditors

Welcome, Prof. Wu, Tzong-Chen

Assign Papers to Reviewers - [AE : Wu, Tzong-Chen]

Not-Assigned Papers:

Not-Assigned: 3 paper(s), as follows :

(4) - [100004 - 1st]: A New Dynamic ID-based RFID Mutual Authentica
(0) - [100034 - 2nd]: Improved Integral Attacks on Rijndael with Large
(3) - [100046 - 1st]: Efficient Identity-based Authenticated Multiple Key

Reviewers: □ **all REs**

Please select reviewers :

R1 : -- none --

R2 : -- none --

Registering Paper of JISE

Paper ID : 100034

Times : 2nd

Title : Improved Integral Attacks on Rijndael with Large Blocks

Author(s) : Yanjun Li (Chinese Academy of Sciences, CHINA)
Wenling Wu (Chinese Academy of Sciences, CHINA)

Category : Data / Data Encryption / Code Breaking

Keyword : Block cipher, distinguisher, integral attack, Rijndael, partial sum technique

Abstract : In this paper, we present some improved integral attacks on Rijndael whose block sizes are larger than 128 bits. We will introduce some 4-round distinguishers for Rijndael with large blocks proposed by Marine Minier (AFRICACRYPT 2009), and propose a new 4th-order 4-round distinguisher for Rijndael-192. Basing on these distinguishers, together with the partial sum technique proposed by Niels Ferguson (FSE 2000), we can apply integral attacks up to 8-round Rijndael-160, 9-round Rijndael-192, and 9-round Rijndael-224. Compared to the square attack proposed by Samuel Galice (AFRICACRYPT 2008), we give different attacks on Rijndael-256 to 8 and 9 rounds. Except the attack on Rijndael-256, all the other results are the best cryptanalytic results on Rijndael with large blocks so far.

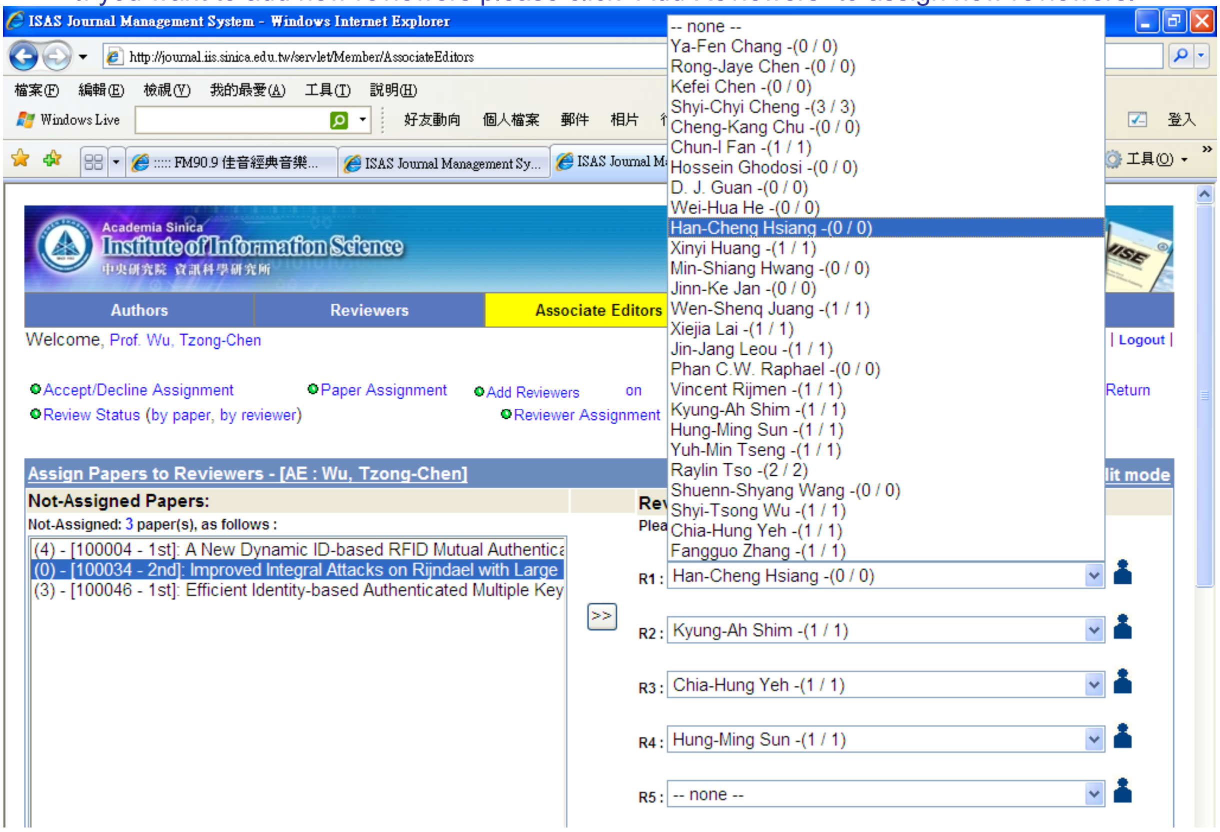
Manuscript : 255KB, 2010/02/11 15:37:52

Reviewer(s) :

(ii) Please assign 3 or 4 reviewers. The reviewers' list in the field of this submission will be shown when you click ⌄ 👤. After you have selected 3-4 reviewers, please click ">>" then the review invitations will be sent to the assigned reviewers.

* All the reviewers in our database will be shown when you select ☐ all REs

* If you want to add new reviewers please click "Add Reviewers" to assign new reviewers.



ISAS Journal Management System - Windows Internet Explorer

http://journal.iis.sinica.edu.tw/servlet/Member/AssociateEditors

Academia Sinica Institute of Information Science 中央研究院 資訊科學研究所

Authors | Reviewers | Associate Editors

Welcome, Prof. Wu, Tzong-Chen | Logout |

Accept/Decline Assignment · Paper Assignment · Add Reviewers · Return

Review Status (by paper, by reviewer) · Reviewer Assignment

Assign Papers to Reviewers - [AE : Wu, Tzong-Chen]

Not-Assigned Papers:

Not-Assigned: 3 paper(s), as follows :

(4) - [100004 - 1st]: A New Dynamic ID-based RFID Mutual Authentica

(0) - [100034 - 2nd]: Improved Integral Attacks on Rijndael with Large

(3) - [100046 - 1st]: Efficient Identity-based Authenticated Multiple Key

-- none --
Ya-Fen Chang -(0 / 0)
Rong-Jaye Chen -(0 / 0)
Kefei Chen -(0 / 0)
Shyi-Chyi Cheng -(3 / 3)
Cheng-Kang Chu -(0 / 0)
Chun-I Fan -(1 / 1)
Hossein Ghodosi -(0 / 0)
D. J. Guan -(0 / 0)
Wei-Hua He -(0 / 0)
Han-Cheng Hsiang -(0 / 0)
Xinyi Huang -(1 / 1)
Min-Shiang Hwang -(0 / 0)
Jinn-Ke Jan -(0 / 0)
Wen-Sheng Juang -(1 / 1)
Xiejia Lai -(1 / 1)
Jin-Jang Leou -(1 / 1)
Phan C.W. Raphael -(0 / 0)
Vincent Rijmen -(1 / 1)
Kyung-Ah Shim -(1 / 1)
Hung-Ming Sun -(1 / 1)
Yuh-Min Tseng -(1 / 1)
Raylin Tso -(2 / 2)
Shuenn-Shyang Wang -(0 / 0)
Shyi-Tsong Wu -(1 / 1)
Chia-Hung Yeh -(1 / 1)
Fangguo Zhang -(1 / 1)

R1 : Han-Cheng Hsiang -(0 / 0)

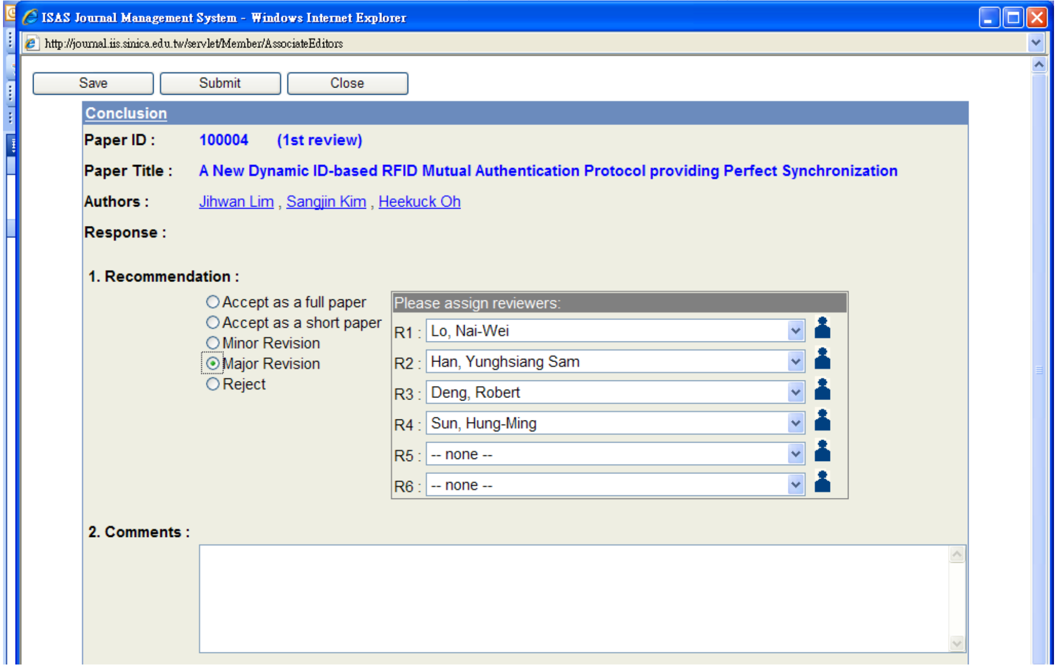
R2 : Kyung-Ah Shim -(1 / 1)

R3 : Chia-Hung Yeh -(1 / 1)

R4 : Hung-Ming Sun -(1 / 1)

R5 : -- none --

(3) **Review Conclusion:** Please make conclusion and your comments will be sent to the authors. Please notice that if a second review is required you have to select "major revision" as follows.



ISAS Journal Management System - Windows Internet Explorer

http://journal.iis.sinica.edu.tw/servlet/Member/AssociateEditors

Save | Submit | Close

Conclusion

Paper ID : 100004 (1st review)

Paper Title : A New Dynamic ID-based RFID Mutual Authentication Protocol providing Perfect Synchronization

Authors : Jihwan Lim , Sangjin Kim , Heekuck Oh

Response :

1. Recommendation :

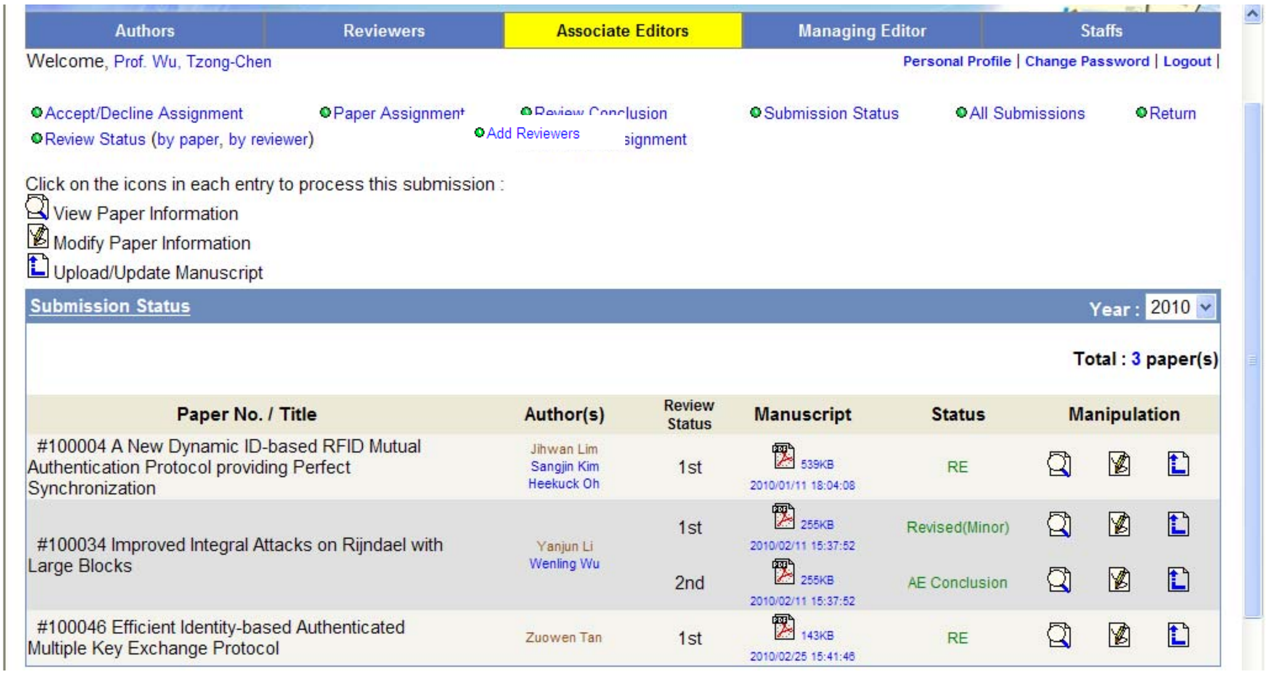
○ Accept as a full paper
○ Accept as a short paper
○ Minor Revision
● Major Revision
○ Reject

Please assign reviewers:

R1 : Lo, Nai-Wei
R2 : Han, Yunghsiang Sam
R3 : Deng, Robert
R4 : Sun, Hung-Ming
R5 : -- none --
R6 : -- none --

2. Comments :

(4) **Submission Status:** to check the status of all the submissions handled by you.
Status “RE” means “under review by the reviewers”
“Revised” means “under revision by the author”
“AE Conclusion” means “under conclusion by the associate editor”



Welcome, Prof. Wu, Tzong-Chen

Personal Profile | Change Password | Logout |
Accept/Decline Assignment
Paper Assignment
Review Conclusion
Submission Status
All Submissions
Return
Review Status (by paper, by reviewer)
Add Reviewers
signment

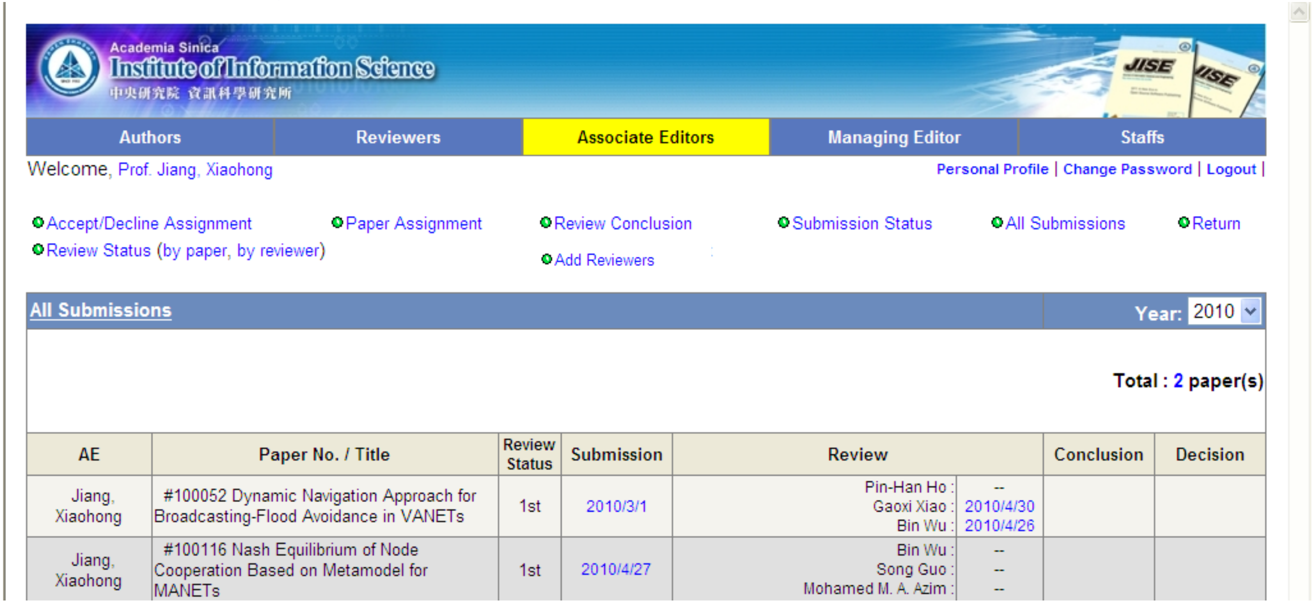
Click on the icons in each entry to process this submission :
- View Paper Information
- Modify Paper Information
- Upload/Update Manuscript

Submission Status — Year : 2010

Total : 3 paper(s)

Paper No. / Title	Author(s)	Review Status	Manuscript	Status	Manipulation
#100004 A New Dynamic ID-based RFID Mutual Authentication Protocol providing Perfect Synchronization	Jihwan Lim Sangjin Kim Heekuck Oh	1st	539KB 2010/01/11 18:04:08	RE	
#100034 Improved Integral Attacks on Rijndael with Large Blocks	Yanjun Li Wenling Wu	1st	255KB 2010/02/11 15:37:52	Revised(Minor)	
		2nd	255KB 2010/02/11 15:37:52	AE Conclusion	
#100046 Efficient Identity-based Authenticated Multiple Key Exchange Protocol	Zuowen Tan	1st	143KB 2010/02/25 15:41:46	RE	

(5) **All Submissions:** It shows the dates of the review process. When they finished the review and fill out the form, the dates will be recorded on the status.


Academia Sinica
Institute of Information Science
中央研究院 資訊科學研究所
JISE
Authors
Reviewers
Associate Editors
Managing Editor
Staffs

Welcome, Prof. Jiang, Xiaohong

Personal Profile | Change Password | Logout |
Accept/Decline Assignment
Paper Assignment
Review Conclusion
Submission Status
All Submissions
Return
Review Status (by paper, by reviewer)
Add Reviewers

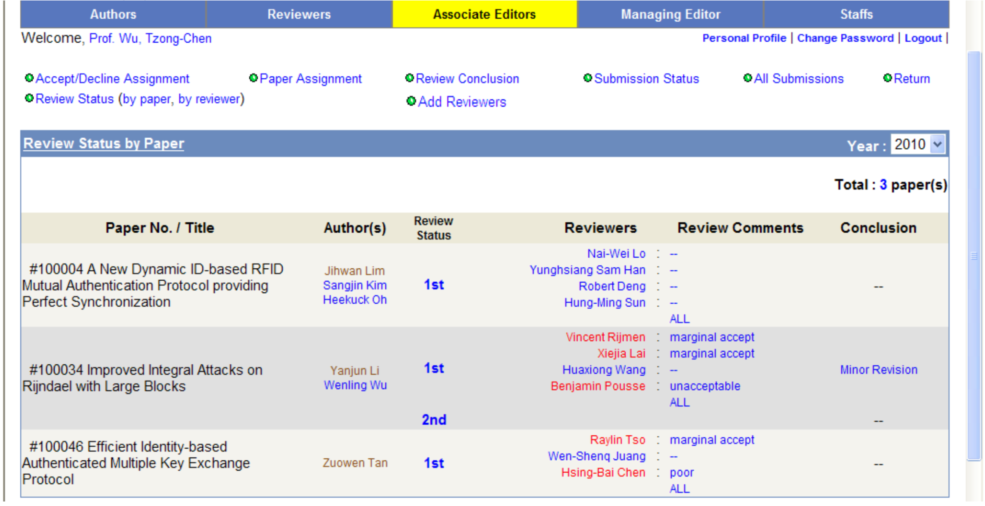
All Submissions — Year: 2010

Total : 2 paper(s)

AE	Paper No. / Title	Review Status	Submission	Review		Conclusion	Decision
Jiang, Xiaohong	#100052 Dynamic Navigation Approach for Broadcasting-Flood Avoidance in VANETs	1st	2010/3/1	Pin-Han Ho : Gaoxi Xiao : Bin Wu :	-- 2010/4/30 2010/4/26		
Jiang, Xiaohong	#100116 Nash Equilibrium of Node Cooperation Based on Metamodel for MANETs	1st	2010/4/27	Bin Wu : Song Guo : Mohamed M. A. Azim :	-- -- --		

(6) Review Status (by paper, by reviewer):

(i) Review Status by paper: You could check all the review comments for each submission handled by you.



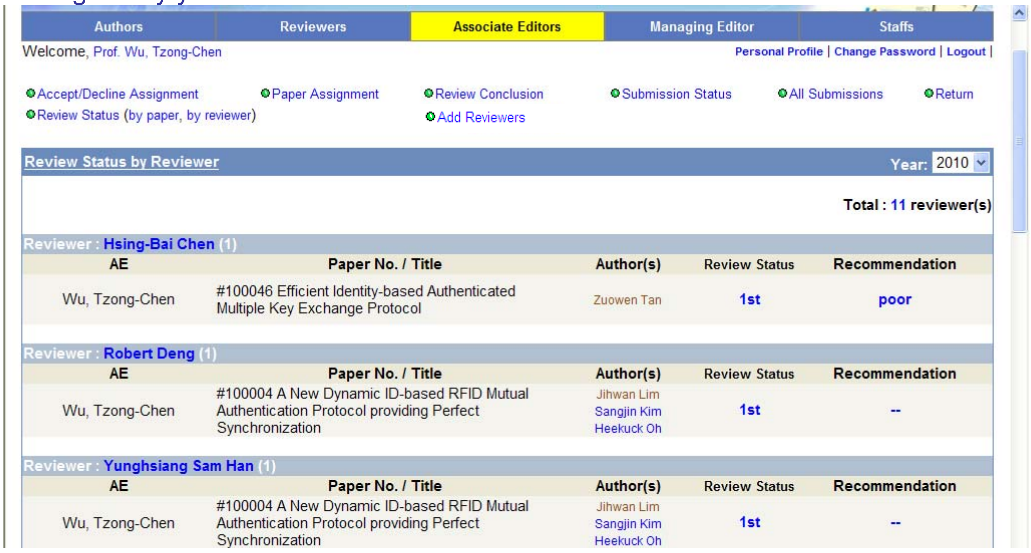
Welcome, Prof. Wu, Tzong-Chen

Review Status by Paper — Year : 2010

Total : 3 paper(s)

Paper No. / Title	Author(s)	Review Status	Reviewers	Review Comments	Conclusion
#100004 A New Dynamic ID-based RFID Mutual Authentication Protocol providing Perfect Synchronization	Jihwan Lim Sangjin Kim Heekuck Oh	1st	Nai-Wei Lo Yunghsiang Sam Han Robert Deng Hung-Ming Sun	: -- : -- : -- : -- ALL	--
#100034 Improved Integral Attacks on Rijndael with Large Blocks	Yanjun Li Wenling Wu	1st	Vincent Rijmen Xiejia Lai Huaxiong Wang Benjamin Pousse	: marginal accept : marginal accept : -- : unacceptable ALL	Minor Revision
		2nd			--
#100046 Efficient Identity-based Authenticated Multiple Key Exchange Protocol	Zuowen Tan	1st	Raylin Tso Wen-Sheng Juang Hsing-Bai Chen	: marginal accept : -- : poor ALL	--

(ii) Review Status by reviewer: You could check the review status of each reviewer assigned by you.



Welcome, Prof. Wu, Tzong-Chen

Review Status by Reviewer — Year: 2010

Total : 11 reviewer(s)

Reviewer : Hsing-Bai Chen (1)

AE	Paper No. / Title	Author(s)	Review Status	Recommendation
Wu, Tzong-Chen	#100046 Efficient Identity-based Authenticated Multiple Key Exchange Protocol	Zuowen Tan	1st	poor

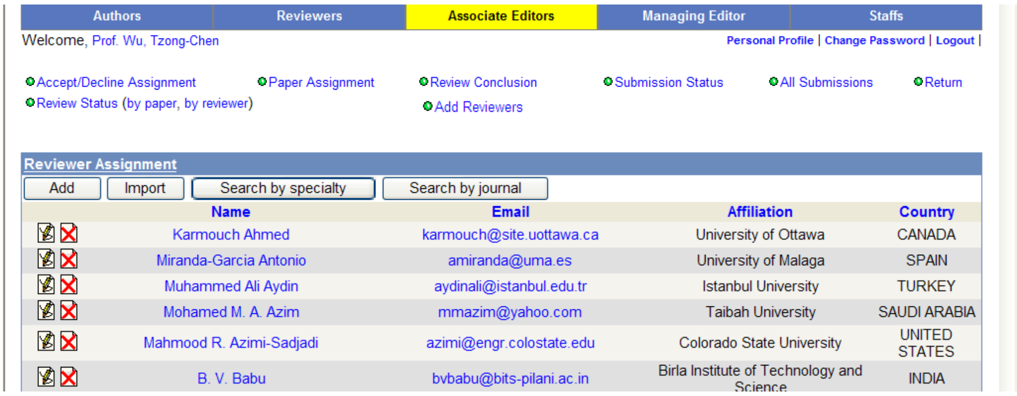
Reviewer : Robert Deng (1)

AE	Paper No. / Title	Author(s)	Review Status	Recommendation
Wu, Tzong-Chen	#100004 A New Dynamic ID-based RFID Mutual Authentication Protocol providing Perfect Synchronization	Jihwan Lim Sangjin Kim Heekuck Oh	1st	--

Reviewer : Yunghsiang Sam Han (1)

AE	Paper No. / Title	Author(s)	Review Status	Recommendation
Wu, Tzong-Chen	#100004 A New Dynamic ID-based RFID Mutual Authentication Protocol providing Perfect Synchronization	Jihwan Lim Sangjin Kim Heekuck Oh	1st	--

(7) Add Reviewers: You could add new reviewers not in our database.



Welcome, Prof. Wu, Tzong-Chen

Reviewer Assignment

	Name	Email	Affiliation	Country
✎ ☒	Karmouch Ahmed	karmouch@site.uottawa.ca	University of Ottawa	CANADA
✎ ☒	Miranda-Garcia Antonio	amiranda@uma.es	University of Malaga	SPAIN
✎ ☒	Muhammed Ali Aydin	aydinali@istanbul.edu.tr	Istanbul University	TURKEY
✎ ☒	Mohamed M. A. Azim	mmazim@yahoo.com	Taibah University	SAUDI ARABIA
✎ ☒	Mahmood R. Azimi-Sadjadi	azimi@engr.colostate.edu	Colorado State University	UNITED STATES
✎ ☒	B. V. Babu	bvbabu@bits-pilani.ac.in	Birla Institute of Technology and Science	INDIA

(8) Return: Back to previous page.