

## Paper 1:

### Efficient multicast stream authentication for the fully adversarial network model

**Christophe Tartary and Huaxiong Wang**

Division of ICS, Department of Computing  
Macquarie University, NSW 2109 Australia  
Email: {ctartary,hwang}@ics.mq.edu.au

---

## Paper 2:

### Aggregate Designated Verifier Signatures and Application to Secure Routing

**Raghav Bhaskar**

Projet CODES - INRIA Rocquencourt  
78153 Le Chesnay cedex, France  
E-mail: raghav.bhaskar@inria.fr

**Javier Herranz**

Centrum voor Wiskunde en Informatica (CWI)  
Kruislaan 413, P.O. Box 94079, NL-1090 GB Amsterdam, The Netherlands  
E-mail: Javier.Herranz@cwi.nl

**Fabien Laguillaumie**

Projet TANC - INRIA Futurs  
Ecole Polytechnique, 91128 Palaiseau cedex, France  
E-mail: laguillaumie@lix.polytechnique.fr

---

## Paper 3:

### LIP: A Lightweight Inter-layer Protocol for Preventing Packet Injection Attacks in Mobile Ad-Hoc Network

**Hung-Yuan Hsu**

Department of Computer Science and Engineering,  
The Pennsylvania State University, United States  
E-mail: hhsu@cse.psu.edu

\*Corresponding author

**Sencun Zhu**

Department of Computer Science and Engineering,  
The Pennsylvania State University, United States  
E-mail: szhu@cse.psu.edu,

**Ali R. Hurson**

Department of Computer Science and Engineering,  
The Pennsylvania State University, United States  
E-mail: hurson@cse.psu.edu,

---

## Paper 4:

### On the Design of Secure Protocols for Hierarchical Sensor Networks

Leonardo B. Oliveira\*

University of Campinas (UNICAMP), Brazil  
Supported by FAPESP grant 2005/00557-9  
E-mail: leob@ic.unicamp.br

\*Corresponding author

Hao Chi Wong

Palo Alto Research Center (PARC), CA,  
E-mail: hcwong@parc.com

Antonio A. F. Loureiro

Federal University of Minas Gerais (UFMG), Brazil  
E-mail: loureiro@dcc.ufmg.br

Ricardo Dahab

University of Campinas (UNICAMP), Brazil  
E-mail: rdahab@ic.unicamp.br

---

## Paper 5:

### Server Side Hashing Core Exceeding 3 Gbps of Throughput

**Harris E. Michail\***

Department of Electrical and Computer Engineering,  
University of Patras, Greece, GR-26500 Patra  
E-mail: michail@vlsi.ee.upatras.gr

\*Corresponding author

**George A. Panagiotakopoulos**

Department of Electrical and Computer Engineering,  
University of Patras, Greece, GR-26500 Patra  
E-mail: gpanagiotak@upnet.gr

**Vasilis N. Thanasoulis**

Department of Electrical and Computer Engineering,  
University of Patras, Greece, GR-26500 Patra  
E-mail: vthanasouli@upnet.gr

**Athanasios P. Kakarountas**

Department of Electrical and Computer Engineering,  
University of Patras, Greece, GR-26500 Patra  
E-mail: kakaruda@vlsi.ee.upatras.gr

**Costas E. Goutis**

Department of Electrical and Computer Engineering,  
University of Patras, Greece, GR-26500 Patra  
E-mail: goutis@vlsi.ee.upatras.gr

---

## Paper 6:

### Preventing or Utilizing Key Escrow in Identity-Based Schemes Employed in MobileAd Hoc Networks

Katrin Hoepfer

Department of Electrical and Computer Engineering

University of Waterloo

Waterloo, Ontario, N2L 3G1, Canada

E-mail: [khoepfer@calliope.uwaterloo.ca](mailto:khoepfer@calliope.uwaterloo.ca)

\*Corresponding author

Guang Gong

Department of Electrical and Computer Engineering

University of Waterloo

Waterloo, Ontario, N2L 3G1, Canada

E-mail: [ggong@calliope.uwaterloo.ca](mailto:ggong@calliope.uwaterloo.ca)

---

## Paper 7:

### On Security Proof of McCullagh-Barreto's Key Agreement Protocol and its Variants

Zhaohui Cheng

School of Computing Science, Middlesex University

The Burroughs, Hendon, London, UK

E-mail: [m.z.cheng@mdx.ac.uk](mailto:m.z.cheng@mdx.ac.uk)

Liqun Chen

Hewlett-Packard Laboratories

Filton Road, Stoke Gird, Bristol, UK

E-mail: [liqun.chen@hp.com](mailto:liqun.chen@hp.com)

---

## Paper 8:

### Cryptanalysis of an Elliptic Curve Cryptosystem for Wireless Sensor Networks

**Kevin M. Finnigin**

Ft. George Meade, Maryland 20755, USA

E-mail: [kevinfinnigin@yahoo.com](mailto:kevinfinnigin@yahoo.com)

**Barry E. Mullins\*, Richard A. Raines, Henry B. Potoczny**

Department of Electrical and Computer Engineering,  
Air Force Institute of Technology, Wright-Patterson AFB, Ohio 45433-7765, USA  
E-mail: {Barry.Mullins, Richard.Raines, Henry.Potoczny}@afit.edu  
\*Corresponding author

---

## Paper 9:

### Pseudonym-Based Cryptography for Anonymous Communications in Mobile Ad-hoc Networks

Dijiang Huang  
Computer Science and Engineering  
Arizona State University  
Tempe, AZ 85287-8809 USA  
E-mail: dijiang@asu.edu

---

## Paper 10:

### Strong Password-Based Authentication in TLS using the Three-Party Group Diffie-Hellman Protocol

Michel Abdalla  
D epartement d'Informatique,  
Ecole normale sup erieure, Paris, France  
E-mail: Michel.Abdalla@ens.fr  
Emmanuel Bresson  
Cryptology department,  
CELAR Technology Center, Bruz Cedex, France  
E-mail: Emmanuel.Bresson@m4x.org  
Olivier Chevassut  
Lawrence Berkeley National Laboratory, Berkeley, CA, USA  
E-mail: OChevassut@lbl.gov

Bodo M oller  
Horst G ortz Institute for IT Security, Lehrstuhl f ur Kommunikationssicherheit,  
Ruhr-Universit at Bochum, Bochum, Germany  
E-mail: bmoeller@acm.org

David Pointcheval  
D epartement d'Informatique,  
Ecole normale sup erieure, Paris, France  
E-mail: David.Pointcheval@ens.fr

Abstract: The Internet has evolved into a very hostile ecosystem