

# IET Information Security

(formerly IEE Proceedings Information Security)

## Special Issue on Group-Oriented Cryptographic Protocols

Group-oriented cryptographic protocols are foundational for the security of various group applications, like digital conferencing, groupware, group communication systems, computer-supported collaborative work-flow systems, multi-user information distribution and sharing, data base and server replication systems, peer-to-peer and ad-hoc groups, group-based admission and access management, electronic voting and election, applications in federative or distributed environment, etc. A variety of cryptographic techniques and assumptions provides a solid basis for the design of provably secure group-oriented cryptographic protocols, which is an important and challenging task. Formal security models for group-oriented cryptographic protocols require consideration of a large number of potential threats resulting from the attacks on the communication channel and from the misbehavior of some protocol participants. These challenges and the emerging development of multi-party and group-oriented applications are just some reasons for setting up a new cryptographic workshop, solely dedicated to the security issues of cryptographic protocols used in these scenarios. The editors of this special issue invite contributions reporting on cryptographic foundations, formal security models, and actual design of all kinds of group-oriented cryptographic protocols, schemes, and applications, including:

- Access and admission control in groups
- Anonymity and privacy in group communications
- Broadcast and multicast communication security
- Cryptographic group-oriented protocols
- Electronic election and voting
- Formal security models (proofs) for group-oriented cryptographic protocols
- Group key exchange/distribution
- Group-oriented signatures
- Secure multi-party computation
- Security in distributed group applications
- Security in mobile and ad hoc groups
- Security in peer-to-peer groups
- Trust management in groups

### Guest Editor

Dr David Pointcheval

ENS-DI

45, rue d'Ulm

75230 PARIS Cedex 05

France

david.pointcheval@ens.fr

### Submission Details

The deadline for submissions is 30 September 2007.

Manuscripts should not exceed 4000 words (excluding references, tables and figures).

All manuscripts should be submitted online at <http://mc.manuscriptcentral.com/ifs>

More information for authors can be found at:

<http://www.iee.org/Publish/Support/Auth/authproc.cfm>

---

All former IEE journals are now published by the Institution of Engineering and Technology (IET), a new institution formed by the joining together of the IEE (Institution of Electrical Engineers and the IIE (Institution of Incorporated Engineers). The new institution is the inheritor of the IEE brand, products and services.