"Secret Sharing and Cloud Computing", One Day Workshop

June 7, 2011 10:00 - 20:00
Room 111, Institute of Mathematics for Industry (IMI)
Kyushu University, Ito Campus

Organizers: Kirill Morozov (IMI), Tsuyoshi Takagi (IMI)
Contact e-mail: morozov@imi.kyushu-u.ac.jp

10:00-10:10 Opening
10:10-12:00 Tutorials
   - Introduction to Secret Sharing
     Kirill Morozov (Kyushu University)
   - Cryptographic Techniques for Cloud Computing
     Takashi Nishide (Kyushu University)

13:30-14:30 Plenary talk
   Secure Multiparty Computation for Cloud Computing
   Yvo Desmedt (University College London, UK)

14:40-16:25 Invited talks I
   - Business Requirements for Applying Secret Sharing Schemes to Cloud Computing
     Yuji Suga (Internet Initiative Japan)
   - Efficient Secret Sharing Schemes Secure against Cheating
     Satoshi Obana, NEC
   - An XOR-based High-Speed Secret Sharing
     Jun Kurihara (KDDI)

16:40-17:50 Invited talks II
   - On $d$-Multiplicative Non-perfect Secret Sharing
     Maki Yoshida (Osaka University)
   - Rational Secret Sharing with Constant-Round Reconstruction
     Kenji Yasunaga (Tokyo Institute of Technology)

17:50-18:00 Closing of the public sessions
18:00-20:00 Discussion (internal)