# Asiacrypt 2005 Rump Session

7 December 2005

Chair: Bart Preneel

- Gideon Yuval, R. Venkatesan (Microsoft Research): Stretch and compress: A secure hash construction
- Zulfikar Ramzan (DoCoMo) On truncating hash function outputs
- Stuart Haber (HP Labs), Pandurang Kamat (Rutgers University): Content integrity service for long-term digital archives
- Moses Liskov (The College of William & Mary): A practical, lightweight water marking scheme
- Eli Biham, Orr Dunkelman, Nathan Keller (Technion): Recovering the S-boxes of 24-round reduced GOST (or how to combine the cycle structure with slide attacks)
- Tom Berson (Anagram Labs): Skype cryptosystem overview
- Xuejia Lai (Shanghai Jiaotong University): Asiacrypt 2006 announcement.