

ASIACRYPT 2007 - RUMP SESSION

Program

Title	Authors / Presenter	Affiliation	Minutes	Time*
Opening Remarks	Aggelos Kiayias	University of Connecticut, USA	1	7.00
IACR Business Meeting	staff		1	7.02
The 2nd International Conference on Information Theoretic Security	Rei Safavi-Naini	University of Calgary, Canada	3	7.04
Group encryption on malicious machines	Mirek Kutyłowski, Anna Lauks	Wroclaw University of Technology, Poland	5	7.08
When AES blinks	Martin Hlavac	Charles University in Prague, Czech Republic	5	7.14
Asiacrypt 2008	Lynn Batten and Josef Pieprzyk	Deakin and Macquarrie U., Australia	1	7.20
Protocols lounge wiki	C.Boyd and M.C.Gorantla and J. Gonzalez	QUT, Brisbane, Australia	3	7.22
BREAK			25	7.25
Batch Verification of Signatures	Susan Hohenberger	Johns Hopkins U., USA	5	7.50
FSE 2008	Thomas Baignères and Serge Vaudenay	EPFL, Switzerland	1	7.56
Pairing 2008	Tsuyoshi Takagi	Future U. Hakodate, Japan	1	8.00
Zcipher Algorithm	Ilya O. Levin	-	3	8.02
How Compilers Can Make Z/pZ Faster	Stephen M. Watt	University of Western Ontario	3	8.06
EnRUPT – an all-in-one symmetric cryptographic primitive	Sean O'Neil	VEST, France	3	8.10
Aliens and/or Collisions?	Florian Mendel and Christian Rechberger and Vincent Rijmen	IAIK, Graz University of Technology, Austria	3	8.14
END			63	8.17

** a 1 minute speaker swapping allowance is included*