Rump Session Talks at AES2

SPEAKER	**TITLE**
Miles Smid (for Don Johnson)	Future Resiliency of AES Candidates
Ross Anderson	Smartcard Implementation Issues
Orr Dunkelman	Serpent-p and Serpent-p-ns
Ian Harvey	DFC Attack
Kazumaro Aoki	Optimized Software Implementation of E2
Adi Shamir	A Better Answer to W. Diffie’s Question
Bruce Schneier	Comments on Biham’s “Minimal Secure Round” Variant
Shiho Moriai	Comparison of Randomness Provided by AES Candidates
Johan Borst	Weak Keys of Crypton
Doug Whiting	AES Candidates on Merced
Niels Ferguson	An Emergency Mode for AES
Takeshi Shimoyama	Security of S-boxes Against Higher Order Differential Attack
David Wagner	Equivalent Keys in HPC
Ron Rivest	An Alternative Key Schedule for RC6
Chae Hoon Lim	A Hardware Design of Crypton Version 1.0
Bruce Schneier	The Case Against Multiple Algorithms in AES Standards
Gary Graunke	Critical Path Opcode Analysis Vs. Current
Carl Ellison	A New Metric for the AES