Crypto 2004 Rump Session Program

7:00 Introduction
Stuart Haber

Session 1: Hash function collisions

7:05 New results on SHA-0 and SHA-1
Eli Biham, Rafi Chen

7:20 Collisions in SHA-0
Antoine Joux

7:35 Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD
Xiaoyun Wang, Xuejia Lai (& Dengguo Feng, Hongbo Yu)

7:50 **Break**

8:00 **Session 2**

Elliptic curves

8:00 More, weaker fields for ECC
Edlyn Teske (& Alfred Menezes)

8:04 Performance improvements in Java-based elliptic-curve point counting
Andrew Burnett

8:06 Using isogenies in cryptosystems
David Jao (& Ramarathnam Venkatesan)

8:09 How to give a timeless rump-session presentation
D.J. Bernstein

8:09 Almost-Ramanujan graphs and random reducibility of DLOG among isogenous elliptic curves
David Jao (& Stephen Miller, Ramarathnam Venkatesan)

8:12 **Announcements**

8:12 NIST withdrawal of DES
John Kelsey

8:13 SASC - State of the Art of Stream Ciphers
Matt Robshaw

8:14 PKC 2005
Serge Vaudenay

8:15 TCC 2005
Joe Kilian

8:16 Eurocrypt 2005
Ivan Damgard

8:17 Pervasive security workshop
Steve Weis

8:18 **Block ciphers**

8:18 The Galois/counter mode operation of AES
Scott Fluhrer for David McGrew, John Viega

8:21 Timeless rump-session presentations reconsidered
D.J. Bernstein

8:21 Foolproof block-cipher design
John Black

8:25 Grey-box implementation of block ciphers preserving the confidentiality of their design
Emmanuelle Dottax (& Vincent Carlier, Hervé Chabanne)

8:28 Whitening the AES S-box
Nicloas Courtois

8:31 Elastic block ciphers
Debra Cook (& Moti Yung, Angelos Keromytis)

8:34 Eliminating random permutation oracles in the Even-Mansour cipher
Zulfikar Ramzan (& Craig Gentry)

8:35 **RSA**

8:35 Stop overestimating RSA bandwidth!
Dan Bernstein

8:40 On the difference RSA assumption and its applications
Shouhuai Xu (& Gene Tsudik)

8:43 SPA-based attack against the modular reduction within a partially secured RSA-CRT implementation
Helmut Kahl

8:45 Universally composable TRSPs without random oracles
D.J. Bernstein

8:45 **Miscellaneous**

8:45 Resilient threshold ring signatures
Shouhuai Xu (& Moti Yung)

8:48 Secret key agreement from weak secret bits
Thomas Holenstein

8:51 The Muadja streaming MAC
Greg Rose (& Philip Hawkes, Michael Paddon)

8:54 On corrective patterns for the SHA-2 family
Philip Hawkes (& Michael Paddon, Greg Rose)

8:57 On a construction of nonlinear feedback shift registers with short cycles
Werner Schindler (& Le Van Ly)

8:59 **Break**

9:15 **Session 3**

9:15 **Protocols**

9:15 Additive visual voting
David Chaum

9:20 How to cheat at chess: An analysis of the Internet chess club
John Black (& Martin Cochran, Ryan Gardner)

9:23 Oblivious transfers of zero knowledge
Nicko van Someren

9:27 This space for rent
D.J. Bernstein

9:27 Reusable proofs of work
Hal Finney

9:31 Steganography with imperfect sampling
Mira Meyerovich (& Anna Lysyanskaya)

9:34 Mining data from anonymous transactions
Moti Yung (& Aggelos Kiayias, Shouhuai Xu)

9:37 **Crypto & the physical world**

9:37 Hidden world in an open eye: A corneal problem
Jean-Jacques Quisquater (& Ko Nishino, Shree K. Nayar)

9:42 Different security philosophies for physical random number generators
Werner Schindler (& Wolfgang Killmann)

9:46 How to design an RFID protocol?
Gildas Avoine

9:50 **Theory**

9:50 Cryptography in NC0
Yuval Ishai (& Benny Applebaum, Eyal Kushilevitz)

9:53 Mercurial commitments and zero-knowledge sets from general assumptions
Anna Lysyanskaya, Tal Malkin (& Alexander Healy, Leo Reyzin)

9:56 Towards Kolmogorov-optimal signature schemes
Craig Gentry (& Zulfikar Ramzan)

9:59 Computational PIR and OT with logarithmic total communication
Craig Gentry (& Zulfikar Ramzan)

10:02 On the (im)possibility of basing cryptography on imperfect randomness
Yegeniy Dodis (& Shien Jin Ong, Manoj Prabhakaran, Amit Sahai)

10:03 On obfuscating proximity queries
Adam Smith (& Yegeniy Dodis)

10:04 **More encryption**

10:04 A note on an encryption scheme of Kurosawa and Desmedt
Victor Shoup (& Rosario Gennaro)

10:09 Fuzzy identity-based encryption
Brent Waters

10:13 Exact security of the Regev cryptosystem
Melissa Chase

10:16 **Attacks**

10:16 Impossible fault analysis of RC4
Eli Biham (& Louis Granboulan, Phong Nguyen)

10:20 Inc.rease your ke.y size by 100-400 bits for FR.EE! Overn.ight deli.very!
D.J. Bernstein

10:20 Breaking hidden identities
Jean-Jacques Quisquater

10:23 Side-channel cryptanalysis on XTR public-key cryptosystems
Dong-Guk Han (& Tetsuya Izu, Jongin Lim, Kouichi Sakurai)

10:26 The advantage of a rich vocabulary
Christophe de Cannière

10:30 Crypto 2004 AES challenge
Jim Hughes

10:33 **Good night!**