Crypto 2007 rump session, Tuesday 21 August 2007

Introduction

19:45 Daniel J. Bernstein (chair): Welcome
19:49 Markus Jakobsson (chair of something else): Best-paper award (rump papers not included, sorry)
19:50 Jean-Jacques Quisquater (sponsor): Less known facts about an indentification protocol

Politics

19:56 Susan Landau: The Security Risks Created by the Protect America Act
20:00 Whitfield Diffie and Susan Landau: Privacy on the Line: The Politics of Wiretapping and Encryption (updated and expanded edition)
20:01 Ross Anderson: Does Bob Go to Prison?
20:08 Alexander May, Roberto Avanzi, Christof Paar, Ahmad Sadeghi, Jörg Schwenk, Christopher Wolf: Eurocrypt 2009 in Cologne

Demos

20:10 Manoj Prabhakaran & Mike Rosulek: CRYPTUTOR

Hash functions

20:14 Florian Mendel and Christian Rechberger and Vincent Rijmen: Update on SHA-1
20:19 Gregory Hirshman: Further Musings on the Wang et al. MD5 Collision
20:23 Daniel J. Bernstein: $1000 for best attack this year: http://cr.yp.to/rumba20.html
20:23 Adi Shamir: How to SQUASH Your Data
20:30 Scott Contini, Krystian Matusiewicz, Josef Pieprzyk, Ron Steinfeld, Guo Jian, Huaxiong Wang: Analysis of LASH (Work in Progress)
20:33 Carl Ellison, Victor Miller, Eran Tromer, Rebecca Wright; presented by Cryptoc Hoir: On the design and cryptanalysis of a one-way hash
20:40 Break

Cryptanalysis

21:00 Eli Biham, Orr Dunkelman, Sebastiaan Indesteege, Nathan Keller, Bart Preneel: How to Steal Cars - A Practical Attack on KeeLoq
21:05 Dan Shumow, Niels Ferguson: On the Possibility of a back door in the NIST SP800-90 Dual Ec Prng
21:09 Bob Silverman: Optimal Sieving Regions for the Lattice Sieve
21:12 Igor Semaev: Average versus Worst in Solving Sparse Algebraic Equations
21:17 Andy Clark, Tony Sale: A Colossal Challenge
21:22 Tanja Lange, Christof Paar: SHARCS 07 Announcement

Encryption

21:24 Christof Paar et al.: The only Rump Session Talk with Pamela Anderson
21:30 Christof Paar: Announcement CHES 2007
21:32 Philip Zimmermann: ZRTP: Media Path Key Agreement for Secure VoIP
21:37 Thomas Baignères, Serge Vaudenay: FSE 2008 announcement
21:38 Ronald Cramer, Carles Padro: Public Key Cryptography, PKC 2008
21:40 Chris Peikert and Brent Waters: Lossy Trapdoor Functions
21:47 Nicko van Someren: nCipher is hiring Cryptographic Security Architects - nicko@ncipher.com
21:47 Jon Callas, Tamzen Cannoy, Nicko Van Someren: Economics and Cryptography: Integrity checks as a solution to factoring sub-primes
21:54 Break

Conclusion

22:15 Alexandra Boldyreva: Face Paradox and Cryptanalysis of Several Face Recognition Protocols
22:18 Yevgeniy Dodis: TCC 2008 announcement
22:19 David Freeman: Constructing Pairing-Friendly Ordinary Genus 2 Curves
22:25 Alexandra Boldyreva, Craig Gentry, Adam O'Neill, Dae Hyun Yum: Ordered Multisignatures and Identity-Based Sequential Aggregate Signatures
22:29 Dan Boneh, Craig Gentry, Mike Hamburg: Space-Efficient IBE without Pairings
22:34 Masayuki Abe: ASIACCS 2008 CFP
22:35 Tal Malkin: CT-RSA 2008 announcement
22:36 Ivan Damgård; presented by Jesper Buus Nielsen: ICALP 2008, Cryptographer's Track
22:38 Ivan Damgård, Jesper Buus Nielsen: Multiparty Computation Goes Live
22:44 Juan Garay and Jonathan Katz and Chiu-Yuen Koo and Rafail Ostrosvky: Round Complexity of Authenticated Broadcast with a Dishonest Majority
22:50 Juan Garay, Aggelos Kiayias and Hong-Sheng Zhou: Sound and Fine-grained Specification of Ideal Functionalities
22:56 Manoj Prabhakaran & Mike Rosulek: Trusted Parties & Their Twins
23:02 Good night!