

PROCEEDINGS OF CRYPTO '92

TABLE OF CONTENTS

Session I: Digital Signatures and Identification I

Provably Unforgeable Signatures Jurjen N. E. Bos, David Chaum	1
New Constructions of Fail-Stop Signatures and Lower Bounds Eugène van Heijst, Torben P. Pedersen, Birgit Pfitzmann	15
Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes Tatsuaki Okamoto	31
An Efficient Digital Signature Scheme Based on an Elliptic Curve Over the Ring Z_n Tatsuaki Okamoto, Atsushi Fujioka, Eiichiro Fujisaki	54

Session II: The Digital Signature Standard

Designing and Detecting Trapdoors for Discrete Log Cryptosystems Daniel M. Gordon	66
Response to Comments on the NIST Proposed Digital Signature Standard (Invited) Miles E. Smid, Dennis K. Branstad	76

Session III: Applications and New Problems

Wallet Databases with Observers David Chaum, Torben Pryds Pedersen	89
Making Electronic Refunds Safer Rafael Hirschfeld	106
Fair Public-Key Cryptosystems Silvio Micali	113
Pricing via Processing or Combatting Junk Mail Cynthia Dwork, Moni Naor	139

Session IV: Secret Sharing I

On the Information Rate of Secret Sharing Schemes Carlo Blundo, Alfredo De Santis, L. Gargano, Ugo Vaccaro	148
---	-----

New General Lower Bounds on the Information Rate of Secret Sharing Schemes Doug R. Stinson	168
Universally Ideal Secret Sharing Schemes Amos Beimel, Benny Chor	183
Session V: Theory I	
Perfect Zero-Knowledge Arguments for NP can be Based on General Complexity Assumptions Moni Naor, Rafail Ostrovsky, Ramarathnam Venkatesan, Moti Yung	196
Low communication 2-Prover Zero-Knowledge Proofs for NP Cynthia Dwork, Uri Feige, Joe Kilian, Moni Naor, Muli Safra	215
Invariant Signatures and Non-Interactive Zero-Knowledge Proofs are Equivalent Shafi Goldwasser, Rafail Ostrovsky	228
On the Discrepancy between Serial and Parallel of Zero-Knowledge Protocols Kouichi Sakurai, Toshiya Itoh	246
Session VI: Cryptographic Functions	
On the Design of SP Networks from an Information Theoretic Point of View M. Sivabalan, Stafford Tavares, L. E. Peppard	260
Partially-Bent Functions Claude Carlet	280
Session VII: Digital Signatures and Identification II	
Practical Approaches to Attaining Security Against Adaptively Chosen Ciphertext Attacks Yuliang Zheng, Jennifer Seberry	292
On the Security of the Permuted Kernel Identification Scheme Thierry Baritaud, Mireille Campana, Pascal Chauvaud, Henri Gilbert	305
Session VIII: Computational Number Theory	
Massively Parallel Computation of Discrete Logarithms Daniel M. Gordon, Kevin S. McCurley	312
A Quadratic Sieve on the n -Dimensional Cube René Peralta	324
Efficient Multiplication on Certain Nonsupersingular Elliptic Curves Willi Meier, Othmar Staffelbach	333

Speeding up Elliptic Cryptosystems by Using a Signed Binary Window Method Kenji Koyama, Yukio Tsuruoka	345
On Generation of Probable Primes by Incremental Search Jørgen Brandt, Ivan Damgård	358
Session IX: Cryptography Education	
Kid Krypto (Invited) Michael Fellows, Neal Koblitz	371
Session X: Theory II	
On Defining Proofs of Knowledge Mihir Bellare, Oded Goldreich	390
Public Randomness in Cryptography Amir Herzberg, Michael Luby	421
Necessary and Sufficient Conditions for Collision-Free Hashing Alexander Y. Russell	433
Certifying Cryptographic Tools: The Case of Trapdoor Permutations Mihir Bellare, Moti Yung	442
Session XI: Key Distribution	
Protocols for Secret Key Agreement by Public Discussion Based on Common Information Ueli M. Maurer	461
Perfectly-Secure Key Distribution for Dynamic Conferences Carlo Blundo, Alfredo De Santis, Amir Herzberg, Shay Kuten, Ugo Vaccaro, Moti Yung	471
Session XII: DES	
Differential Cryptanalysis of the Full 16-Round DES Eli Biham, Adi Shamir	487
Iterative Characteristics of DES and S^2 DES Lars R. Knudsen	497
DES is not a Group Keith W. Campbell, Michael J. Wiener	512
A High-Speed DES Implementation for Network Applications Hans Eberle	521

Session XIII: Secret Sharing II

Threshold Schemes with Disenrollment	540
Bob Blakley, G. R. Blakley, Agnes H. Chan, James L. Massey	
Non-Existence of Homomorphic General Sharing Schemes for Some Key Spaces	549
Yair Frankel, Yvo Desmedt, Mike Burmester	
An t-Span Generalized Secret Sharing Scheme	558
Lein Harn, Hung-Yu Lin	

Session XIV: Rump Session

Provable Security Against Differential Cryptanalysis	566
Kaisa Nyberg, Lars R. Knudsen	
Content-Addressable Search Engines and DES-like Systems	575
Peter C. Wayner	
FFT-Hash-II is not yet Collision-free	587
Serge Vaudenay	