Advances in Cryptology – ASIACRYPT 2006

12th International Conference on the Theory and Application of Cryptology and Information Security
Shanghai, China, December 3-7, 2006
Proceedings

Springer
# Table of Contents

## Attacks on Hash Functions

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finding SHA-1 Characteristics: General Results and Applications</td>
<td>1</td>
</tr>
<tr>
<td><em>Christophe De Cannière, Christian Rechberger</em></td>
<td></td>
</tr>
<tr>
<td>Improved Collision Search for SHA-0</td>
<td>21</td>
</tr>
<tr>
<td><em>Yusuke Naito, Yu Sasaki, Takeshi Shimoyama, Jun Yajima, Noboru Kunihira, Kazuo Ohta</em></td>
<td></td>
</tr>
<tr>
<td>Forgery and Partial Key-Recovery Attacks on HMAC and NMAC Using Hash Collisions</td>
<td>37</td>
</tr>
<tr>
<td><em>Scott Contini, Yiqun Lisa Yin</em></td>
<td></td>
</tr>
</tbody>
</table>

## Stream Ciphers and Boolean Functions

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Guess-and-Determine Attack on the Self-Shrinking Generator</td>
<td>54</td>
</tr>
<tr>
<td><em>Bin Zhang, Dengguo Feng</em></td>
<td></td>
</tr>
<tr>
<td>On the (In)security of Stream Ciphers Based on Arrays and Modular Addition</td>
<td>69</td>
</tr>
<tr>
<td><em>Souradyuti Paul, Bart Preneel</em></td>
<td></td>
</tr>
<tr>
<td>Construction and Analysis of Boolean Functions of $2t + 1$ Variables with Maximum Algebraic Immunity</td>
<td>84</td>
</tr>
<tr>
<td><em>Na Li, Wen-Feng Qi</em></td>
<td></td>
</tr>
</tbody>
</table>

## Biometrics and ECC Computation

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Sketch for Biometric Templates</td>
<td>99</td>
</tr>
<tr>
<td><em>Qiming Li, Yagiz Sutcu, Nasir Memon</em></td>
<td></td>
</tr>
<tr>
<td>The 2-Adic CM Method for Genus 2 Curves with Application to Cryptography</td>
<td>114</td>
</tr>
<tr>
<td><em>P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, A. Weng</em></td>
<td></td>
</tr>
<tr>
<td>Extending Scalar Multiplication Using Double Bases</td>
<td>130</td>
</tr>
<tr>
<td><em>Roberto Avanzi, Vassil Dimitrov, Christophe Doche, Francesco Sica</em></td>
<td></td>
</tr>
</tbody>
</table>
ID-Based Schemes

HIBE With Short Public Parameters Without Random Oracle
Sanjit Chatterjee, Palash Sarkar

Forward-Secure and Searchable Broadcast Encryption with Short Ciphertexts and Private Keys
Nuttapong Attrapadung, Jun Furukawa, Hideki Imai

On the Generic Construction of Identity-Based Signatures with Additional Properties
David Galindo, Javier Herranz, Eike Kiltz

Public-Key Schemes

On the Provable Security of an Efficient RSA-Based Pseudorandom Generator
Ron Steinfeld, Josef Pieprzyk, Huaxiong Wang

On the Security of OAEP
Alexandra Boldyreva, Marc Fischlin

Relationship Between Standard Model Plaintext Awareness and Message Hiding
Isamu Teranishi, Wakahla Ogata

RSA and Factorization

On the Equivalence of RSA and Factoring Regarding Generic Ring Algorithms
Gregor Leander, Andy Rupp

Trading One-Wayness Against Chosen-Ciphertext Security in Factoring-Based Encryption
Pascal Paillier, Jorge L. Villar

A Strategy for Finding Roots of Multivariate Polynomials with New Applications in Attacking RSA Variants
Ellen Jochemsz, Alexander May

Construction of Hash Function

Indifferentiable Security Analysis of Popular Hash Functions with Prefix-Free Padding
Donghoon Chang, Sangjin Lee, Mridul Nandi, Moti Yung
Multi-Property-Preserving Hash Domain Extension and the EMD Transform ................................. 299
   Mihir Bellare, Thomas Ristenpart

Combining Compression Functions and Block Cipher-Based Hash Functions ...................................... 315
   Thomas Peyrin, Henri Gilbert, Frédéric Muller, Matt Robshaw

Protocols

A Scalable Password-Based Group Key Exchange Protocol in the Standard Model ............................ 332
   Michel Abdalla, David Pointcheval

A Weakness in Some Oblivious Transfer and Zero-Knowledge Protocols ........................................ 348
   Ventzislav Nikov, Svetla Nikova, Bart Preneel

Almost Optimum Secret Sharing Schemes Secure Against Cheating for Arbitrary Secret Distribution ........ 364
   Satoshi Obana, Toshinori Araki

Block Ciphers

KFC - The Krazy Feistel Cipher ........................................ 380
   Thomas Baignères, Matthieu Finiasz

Generic Attacks on Unbalanced Feistel Schemes with Contracting Functions .................................... 396
   Jacques Patarin, Valérie Nachef, Côme Berbain

New Cryptanalytic Results on IDEA ............................. 412
   Eli Biham, Orr Dunkelman, Nathan Keller

Signatures

New Approach for Selectively Convertible Undeniable Signature Schemes ........................................ 428
   Kaoru Kurosawa, Tsuyoshi Takagi

Simulation-Sound NIZK Proofs for a Practical Language and Constant Size Group Signatures ............ 444
   Jens Groth
XIV Table of Contents

Analysis of One Popular Group Signature Scheme 460
Zhengjun Cao

Author Index 467