Selected Areas in Cryptography

14th International Workshop, SAC 2007
Ottawa, Canada, August 16-17, 2007
Revised Selected Papers
Preface

SAC 2007 was the 14th in a series of annual workshops on Selected Areas in Cryptography. This is the first time this workshop was held at the University of Ottawa. Previous workshops were held at Queen’s University in Kingston (1994, 1996, 1998, 1999, and 2005), Carleton University in Ottawa (1995, 1997, and 2003), University of Waterloo (2000 and 2004), Fields Institute in Toronto (2001), Memorial University of Newfoundland in St. Johns (2002), and Concordia University in Montreal (2006). The intent of the workshop is to provide a stimulating atmosphere where researchers in cryptology can present and discuss new work on selected areas of current interest. The themes for SAC 2007 were:

- Design and analysis of symmetric key cryptosystems
- Primitives for symmetric key cryptography, including block and stream ciphers, hash functions, and MAC algorithms
- Efficient implementations of symmetric and public key algorithms
- Innovative cryptographic defenses against malicious software

A total of 73 papers were submitted to SAC 2007. Of these, one was withdrawn by the authors, and 25 were accepted by the Program Committee for presentation at the workshop. In addition to these presentations, we were fortunate to have two invited speakers:

- Dan Bernstein: “Edwards Coordinates for Elliptic Curves”
- Moti Yung: “Cryptography and Virology Inter-Relationships.” This talk was designated the Stafford Tavares Lecture.

We are grateful to the Program Committee and the many external reviewers for their hard work and expertise in selecting the program. They completed all reviews in time for discussion and final decisions despite events conspiring to compress the review schedule. We apologize if anyone was missed in the list of external reviewers.

We would like to thank the Ontario Research Network for Electronic Commerce (ORNEC) for financial support of the workshop. We would also like to thank Gail Deduk for administrative support and Aleks Essex and Terasan Niyomsataya for technical support.

Finally, we thank all those who submitted papers and the conference participants who made this year’s workshop a great success.

October 2007
Carlisle Adams
Ali Miri
Michael Wiener
14th Annual Workshop on Selected Areas in Cryptography

August 16–17, 2007, Ottawa, Ontario, Canada

in cooperation with the
International Association for Cryptologic Research (IACR)

Conference Co-chairs

Carlisle Adams       University of Ottawa, Canada
Ali Miri            University of Ottawa, Canada
Michael Wiener      Cryptographic Clarity, Canada

Program Committee

Roberto Avanzi       Ruhr University Bochum, Germany
Orr Dunkelman       Katholieke Universiteit Leuven, Belgium
Ian Goldberg        University of Waterloo, Canada
Helena Handschuh    Spansion, France
M. Anwar Hasan      University of Waterloo, Canada
Antoine Joux        DGA, Université de Versailles
                     St-Quentin-en-Yvelines, France
Pascal Junod        Nagravision, Switzerland
Tanja Lange         Technische Universität, Eindhoven, Netherlands
Arjen Lenstra       EPFL, Switzerland
Christof Paar       Ruhr University Bochum, Germany
Bart Preneel        Katholieke Universiteit Leuven, Belgium
Vincent Rijmen      Graz University of Technology, Austria
Matt Robshaw        France Telecom, France
Greg Rose           QUALCOMM, USA
Doug Stinson        University of Waterloo, Canada
Serge Vaudenay      EPFL, Switzerland
Robert Zuccherato   Entrust Inc., Canada

External Reviewers

Abdulaziz Alkhoraidly Elena Andreeva Thomas Baignères
Siavash Bayat-Sarmadi Anja Becker Côme Berbain
Daniel J. Bernstein Eli Biham Olivier Billet
Toni Bluher          Andrey Bogdanov Reinier Broker
VIII Organization

Christophe De Cannière  Yaniv Carmeli  Jaewook Chung
Scott Contini           Christophe Doche  Nevine Ebeid
Thomas Eisenbarth      Lars Elmegaard-Fessel  Andreas Enge
Matthieu Finiasz        Steven Galbraith  Henri Gilbert
Jovan Golic             Johann Grosschadl Tilm Guneysu
Arash Hariri            Phil Hawkes Rafi Hen
Laurent Imbert          Sebastiaan Indesteege Takanori Isobe
David Jacobson          Shaoquan Jiang Marcelo Kaihara
Alexandre Karlov        Shahram Khazaei Mario Lamberger
Cédric Lauradoux        Gregor Leander Kerstin Lemke
Reynald Lercier         Cameron McDonald Florian Mendel
Marine Minier           Bodo Möller Jean Monnerat
Dag Arne Osvik          Elisabeth Oswald Sylvain Pasini
Souradyuti Paul         Raphael Phan Norbert Pramstaller
Emmanuel Prouff         Christian Rechberger Arash Reyhani-Masoleh
Kai Schramm             Yaniv Shaked Martijn Stam
Marc Stevens            Nicolas Theriault Frederik Vercauteren
Martin Vuagnoux         Johannes Wolkerstorfer Hongjun Wu
Huapeng Wu              Brecht Wyseur   Lu Xiao
# Table of Contents

Reduced Complexity Attacks on the Alternating Step Generator ....... 1
   *Shahram Khazaei, Simon Fischer, and Willi Meier*

Extended BDD-Based Cryptanalysis of Keystream Generators ......... 17
   *Dirk Stegemann*

Two Trivial Attacks on TRIVIUM ................................. 36
   *Alexander Maximov and Alex Biryukov*

Collisions for 70-Step SHA-1: On the Full Cost of Collision Search ...... 56
   *Christophe De Cannière, Florian Mendel, and Christian Rechberger*

Cryptanalysis of the CRUSH Hash Function ............................. 74
   *Matt Henricksen and Lars R. Knudsen*

Improved Side-Channel Collision Attacks on AES .................... 84
   *Andrey Bogdanov*

Analysis of Countermeasures Against Access Driven Cache Attacks on
   AES ................................................................. 96
   *Johannes Blömer and Volker Krummel*

Power Analysis for Secret Recovering and Reverse Engineering of
   Public Key Algorithms ........................................... 110
   *Frederic Amiel, Benoit Feix, and Karine Villegas*

Koblitz Curves and Integer Equivalents of Frobenius Expansions ...... 126
   *Billy Bob Brumley and Kimmo Järvinen*

Another Look at Square Roots (and Other Less Common Operations)
   in Fields of Even Characteristic .................................. 138
   *Roberto Maria Avanzi*

Efficient Explicit Formulae for Genus 2 Hyperelliptic Curves over Prime
   Fields and Their Implementations .................................. 155
   *Xinxin Fan and Guang Gong*

Explicit Formulas for Efficient Multiplication in \( \mathbb{F}_{3^m} \) ........ 173
   *Elisa Gorla, Christoph Puttmann, and Jamshid Shokrollahi*

Linear Cryptanalysis of Non Binary Ciphers ............................ 184
   *Thomas Baignères, Jacques Stern, and Serge Vaudenay*

The Delicate Issues of Addition with Respect to XOR Differences ...... 212
   *Gaoli Wang, Nathan Keller, and Orr Dunkelman*
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRHS Equation Systems</td>
<td>232</td>
</tr>
<tr>
<td><strong>Håvard Raddum</strong></td>
<td></td>
</tr>
<tr>
<td>A Fast Stream Cipher with Huge State Space and Quasigroup Filter</td>
<td>246</td>
</tr>
<tr>
<td>for Software</td>
<td></td>
</tr>
<tr>
<td><strong>Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, and Mariko Hagita</strong></td>
<td></td>
</tr>
<tr>
<td>Cryptanalysis of White-Box DES Implementations with Arbitrary</td>
<td>264</td>
</tr>
<tr>
<td>External Encodings</td>
<td></td>
</tr>
<tr>
<td><strong>Brecht Wyseur, Wil Michiels, Paul Gorissen, and Bart Preneel</strong></td>
<td></td>
</tr>
<tr>
<td>Cryptanalysis of White Box DES Implementations</td>
<td>278</td>
</tr>
<tr>
<td><strong>Louis Goubin, Jean-Michel Masereel, and Michaël Quisquater</strong></td>
<td></td>
</tr>
<tr>
<td>Attacks on the ESA-PSS-04-151 MAC Scheme</td>
<td>296</td>
</tr>
<tr>
<td><strong>Georg Illies and Marian Margraf</strong></td>
<td></td>
</tr>
<tr>
<td>The Security of the Extended Codebook (XCB) Mode of Operation</td>
<td>311</td>
</tr>
<tr>
<td><strong>David A. McGrew and Scott R. Fluhrer</strong></td>
<td></td>
</tr>
<tr>
<td>A Generic Method to Design Modes of Operation Beyond the Birthday</td>
<td>328</td>
</tr>
<tr>
<td><strong>David Lefranc, Philippe Painchault, Valérie Rouat, and Emmanuel Mayer</strong></td>
<td></td>
</tr>
<tr>
<td>Passive–Only Key Recovery Attacks on RC4</td>
<td>344</td>
</tr>
<tr>
<td><strong>Serge Vaudenay and Martin Vuagnoux</strong></td>
<td></td>
</tr>
<tr>
<td>Permutation After RC4 Key Scheduling Reveals the Secret Key</td>
<td>360</td>
</tr>
<tr>
<td><strong>Goutam Paul and Subhamoy Maitra</strong></td>
<td></td>
</tr>
<tr>
<td>Revisiting Correlation-Immunity in Filter Generators</td>
<td>378</td>
</tr>
<tr>
<td><strong>Aline Gouget and Hervé Sibert</strong></td>
<td></td>
</tr>
<tr>
<td>Distinguishing Attack Against TPypy</td>
<td>396</td>
</tr>
<tr>
<td><strong>Yukiyasu Tsunoo, Teruo Saito, Takeshi Kawabata, and Hiroki Nakashima</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>409</td>
</tr>
</tbody>
</table>