Christopher Wolf, Stefan Lucks, Po-Wah Yau (Eds.)

WEWoRC 2005

Western European Workshop on Research in Cryptology

July 5–7, 2005

in Leuven, Belgium

TECHNISCHE
INFORMATIONSBIBLIOTHEK
UNIVERSITÄTSBIBLIOTHEK
HANNOVER

Gesellschaft für Informatik 2005

Contents

Efficient Electronic Gambling: An Extended Implementation of the *Toolbox for Mental Card Games*
Heiko Stamer 1

Algebraic Attacks and Annihilators
Frederik Armknecht 13

A Secure Network Storage System with Information Privacy
SeongHan Shin, Kazukuni Kobara and Hideki Imai 22

A cryptosystem " à la " ElGamal on an elliptic curve over $\mathbb{F}_p[\varepsilon]$
Marie Virat 32

A Scanning Tool for PC Root Public Key Stores
Adil Alsaid and Chris J. Mitchell 45

State Recovery Attacks on Pseudorandom Generators
Andrey Sidorenko and Berry Schoenmakers 53

Related-Cipher Attacks on Block Ciphers with Flexible Number of Rounds
Jaechul Sung, Jongsung Kim, Changhoon Lee and Seokhie Hong 64

Collision attacks on processors with cache and countermeasures
Cédric Lauradoux 76

Applications of Partial Hiding in RSA
Eabhnat Ní Fhloinn and Michael Purser 86

Publicly Verifiable Secret Sharing from Paillier's Cryptosystem
Alexandre Ruiz and Jorge L. Villar 98

Issues on Designing a Cryptographic Compiler
Stefan Lucks, Nico Schmoigl, Emin İslam Tatlı 109

Analysis of simplified variants of SHA-256
Krystian Matusiewicz, Josef Pieprzyk, Norbert Pramstaller, Christian Rechberger, Vincent Rijmen 123