

# WEWoRC 2005 – Programme

WEWoRC Chairs: Christopher Wolf, Stefan Lucks, Po-Wah Yau

June 29, 2005

## Monday, July 4

**17.30–18.30** Registration (*Entrance Hall ESAT*)

**18.00–19.30** Welcome Reception (*Room 00.62*)

## Tuesday, July 5

**8.30– 8.45** Registration (*Room 00.54 / Auditorium A*)

**8.45– 9.00** Introduction (*Room 00.54 / Auditorium A*)

**9.00–10.00** Session on **Pairing-Based Cryptography**

*Session Chair: Gregory Neven (Room 00.54 / Auditorium A)*

EMELINE HUFSCMITT, DAVID LEFRANC, HERVÉ SIBERT: A Zero-Knowledge Identification Scheme in Gap Diffie-Hellman Groups

D. NALI, C. ADAMS, A. MIRI: Hierarchical Identity-Based Signcryption with Public Ciphertext Authenticity and Forward Security

**10.00–10.30** *Coffee Break*

**10.30–11.00** Short Talks

**Track A.1:** (*Room 01.57*)

*Session Chair: Elke De Mulder*

TAKAAKI FUJITA, KUNIHIRO  
OKAMOTO, MAKI YOSHIDA, AND  
TORU FUJIWARA: A Watermark  
Detection Scheme Ensuring the  
False Positive Error Probability

SANTA AGRESTE, GUIDO ANDALORO,  
DANIELA PRESTIPINO, LUIGIA  
PUCCIO: Combination of crypto-  
graphic and watermark schemes  
for copyright protection of digital  
images

**Track B.1:** (*Room 01.60*)

*Session Chair: Joe Lano*

PAZ MORILLO, CARLA RÀFOLS: A new  
Certificate-Based Encryption Cho-  
sen Ciphertext Secure

JENS-MATTHIAS BOHLI, JÖRN  
MÜLLER-QUADE, STEFAN  
RÖHRICH: On Group Key Agree-  
ment with Cheater Identification

**11.00–11.10** *Short Break*

**11.10–11.40** Short Talks

**Track A.2:** (*Room 01.57*)

*Session Chair: Elke De Mulder*

AUDREY MONTREUIL, JACQUES  
PATARIN: Computation of the  
“AND” with Cards

HEIKO STAMER: Efficient electronic  
gambling: An extended implemen-  
tation of Schindelhauer’s *Toolbox for  
Mental Card Games*

**Track B.2:** (*Room 01.60*)

*Session Chair: Joe Lano*

TAKESHI GOMI, KAZUKUNI KOBARA,  
TOSHIHISA NAKANO, MASAO  
NONAKA, HIDEKI IMAI: Off-line  
Clone Discovery Using Portable  
Media

MASANORI YOSHIDA, RIE SHIGETOMI,  
HIDEKI IMAI: Revocation of anony-  
mous credentials by short informa-  
tion

**11.40–11.50** *Short Break*

**11.50–12.20** Short Talks

**Track A.3:** (*Room 01.57*)

*Session Chair:* **Charlotte Vikkelsoe**

ADRIAN LEUNG, CHRIS MITCHELL: Towards Secure Zero Configuration

QING ZHANG: A User-centric solution to realise m-payment

**Track B.3:** (*Room 01.60*)

*Session Chair:* **Ellen Jochemsz**

RIE SHIGETOMI, HARUHIRO YOSHIMOTO, HIDEKI IMAI: How visual demonstrations help showing cryptographic algorithms to general audience

CHRISTOPHER WOLF: Multivariate Public Key Schemes

**12.20–14.00** *Lunch*

**14.00–15.30** Session on **Theory**

*Session Chair:* **Svetla Nikova** (*Room 00.54 / Auditorium A*)

FREDERIK ARMKNECHT: Algebraic Attacks and Annihilators

SEONGHAN SHIN, KAZUKUNI KOBARA, HIDEKI IMAI: Password-based Information Retrieval with Privacy

MARIE VIRAT: Around ElGamal encryption cryptosystem on a Weierstrass cubic on  $\mathbf{F}_q[\varepsilon]$

**15.30–16.00** *Coffee Break*

**16.00–17.30** Session on **Hardware-Oriented Cryptography**

*Session Chair:* **Lejla Batina** (*Room 00.54 / Auditorium A*)

PIM TULYS: Key Extraction from Noisy Data: Physical Unclonable Functions

LAURENT LARGER, VLADIMIR UDALTSOV, STÉPHANE POINSOT, PIERRE-AMBROISE LACOURT, NICOLAS GASTAUD: High speed chaotic carrier encrypting at the physical layer

NORBERT PRAMSTALLER, CHRISTIAN RECHBERGER, VINCENT RIJMEN: An Efficient FPGA Implementation of Whirlpool

**17.30–...** Rump Session (*Session Chair:* **Stefan Lucks**): announcements, calls for papers, very recent results, ... (*Room 00.54 / Auditorium A*)

## Wednesday, July 6

### 9.00–10.30 Session on Mobile Security and Key Storage

*Session Chair: Po-Wah Yau (Room 00.54 / Auditorium A)*

ADIL ALSAID, CHRIS J. MITCHELL: A scanning tool for PC root public key stores

ANISH MOHAMMED, CHRIS J. MITCHELL: Privacy aspects of wireless protocols

ANAND S. GAJPARIA: On Location-based services and the  $UCON_{ABC}$  Model

### 10.30–11.00 Coffee Break

### 11.00–11.30 Short Talks

**Track A.4:** (Room 01.57)

*Session Chair: Frederik Armknecht*

ANDREY SIDORENKO, BERRY SCHOEN-  
MAKERS: State Compromise At-  
tacks on Pseudorandom Generators

JAECHUL SUNG, JONGSUNG KIM,  
CHANGHOON LEE, SEOKHIE  
HONG: Related-Cipher Attacks  
on Block Ciphers with Flexible  
Number of Rounds

**Track B.4:** (Room 01.60)

*Session Chair: Rie Shigetomi*

SATOSHI NAKAYAMA, MAKI YOSHIDA,  
SHINGO OKAMURA, AKIRA FUJI-  
WARA, TORU FUJIWARA : An Ef-  
ficient Private and Consistent Data  
Retrieval Protocol

ABDELILAH TABET, SEONGHAN SHIN,  
KAZUKUNI KOBARA, HIDEKI IMAI:  
Formal Verification of Password-  
based Protocol by FDR Model  
Checking

### 11.30–11.40 Short Break

### 11.40–12.10 Short Talks

**Track A.5:** (Room 01.57)

*Session Chair: Frederik Armknecht*

MARION VIDEAU: Symmetric Boolean  
functions with high nonlinearity

AN BRAEKEN: Error-Set Codes, Secret  
Sharing Schemes and Matroids

**Track B.5:** (Room 01.60)

*Session Chair: Simos Xentillis*

KALID ELMUFTI, CHRIS J MITCHELL:  
GSM for mobile SSO to protect user  
privacy

ZINAIDA BENENSON, FELIX C. FREIL-  
ING, DOGAN KESDOGAN: Secure  
Multi-Party Computation with Se-  
curity Modules

### 12.10–14.00 Lunch

### 14.00–... Social Programme (14.00–19.00, details to be announced)

→ 19.30–...: Workshop Dinner in the Troubadour

## Thursday, July 7

### 9.00–10.00 Session on Cryptanalysis

*Session Chair: Nicolas Sendrier (Room 00.54 / Auditorium A)*

CÉDRIC LAURADOUX: Collision attacks on processors with cache and countermeasures

MARINE MINIER: An integral cryptanalysis against a five rounds version of FOX

### 10.00–10.30 *Coffee Break*

### 10.30–11.00 Short Talks

**Track A.6:** (*Room 01.57*)

*Session Chair: Simos Xentillis*

BORISLAV STOYANOV: The 2-adic Summation-Shrinking Generator

ENDRE BANGERTER, ANDY RUPP, AHMAD-REZA SADEGHI: Simplified Hardness Proofs in the Generic Group Model

**Track B.6:** (*Room 01.60*)

*Session Chair: Ellen Jochemsz*

EABHNAT NÍ FHLOINN, MICHAEL PURSER: Applications of Partial Hiding in RSA

JULIA C BATE AND SEONHO SHIN: Group Key Distribution Patterns

### 11.00–11.10 *Short Break*

### 11.10–11.40 Short Talks

**Track A.7:** (*Room 01.57*) *Session Chair:*

*Krystian Matusiewicz*

**Track B.7:** (*Room 01.60*)

*Session Chair: Anand Gajparia*

QIANG TANG, CHRIS J. MITCHELL: Security vulnerabilities of a password-based key establishment protocol

TILL STEGERS: Faugère's F5 Algorithm Revisited

SIMOS XENITELLIS: A list of open-source PKI implementations

GORAN PANTELIĆ, SLOBODAN BOJANIĆ: Managing Security Levels in Smart Card Based Certification

### 11.40–11.50 *Short Break*

### 11.50–12.20 Short Talks

**Track A.8:** (*Room 01.57*)

**Track B.8:** (*Room 01.60*)

*Session Chair: Krystian Matusiewicz* *Session Chair: Anand Gajparia*

SU-JEONG CHOI: Cryptanalysis of Homomorphic Public-Key Cryptosystem

SHENGLAN HU, CHRIS J. MITCHELL: Using Trusted Computing for IP address autoconfiguration in MANETs

ALEXANDRE RUIZ, JORGE VILLAR: An Homomorphic Scheme for Publicly Verifiable Secret Sharing

JAN CAMENISCH, MARKUS ROHE, AHMAD-REZA SADEGHI: Sokrates - A Compiler Framework for Zero-Knowledge Protocols

**12.20–14.00** *Lunch*

**14.00–15.00** Session on **Modelling and Implementing**

*Session Chair: Gregor Leander (Room 00.54 / Auditorium A)*

S. NACHTIGAL, C.J. MITCHELL: Modelling e-business security using business processes

STEFAN LUCKS, NICO SCHMOIGL, EMIN ISLAM TATLI: The Idea and the Architecture of a Cryptographic Compiler

**15.00–15.30** *Coffee Break*

**15.30–17.00** Session on **Hash Functions**

*Session Chair: An Braeken (Room 00.54 / Auditorium A)*

LUIS CARLOS CORONADO GARCÍA: The Subset Sum Problem and (Universal) One-Way Functions based on it

KRYSTIAN MATUSIEWICZ, JOSEF PIEPRZYK: Collisions for simplified variants of SHA-256

NORBERT PRAMSTALLER, CHRISTIAN RECHBERGER, VINCENT RIJMEN: Preliminary Analysis of the SHA-256 Message Expansion

**17.00–17.15** *Closing Remarks Goodbye!*