



Participant Profile

for the
Turkish-German Strategy Workshop 2006
TÜBİTAK Marmara Research Center,
Istanbul- Gebze Turkey
13 – 15 December 2006



International Bureau (IB)
of the Federal Ministry of
Education and Research
(BMBF)

1. Contact details and personal information

Name:	Siddika Berna Örs Yalçın	Phone:	00902122853603
Role/function¹:	Assistant Prof. Dr.	Fax:	00902122853565
Institution:	Istanbul Technical University	E-Mail:	Siddika.Ors@itu.edu.tr
Department:	Electronics and Communication	Website:	www2.itu.edu.tr/~orssi
Address:	Istanbul Technical University, Faculty of Electrical and Electronics Engineering, Maslak Istanbul, Turkey	Organisation type²:	university
Postcode and City:	34469, Istanbul		

¹ **Role/function** e.g. working group leader, managing director, postdoc, PhD etc.

² **Organisation type** e.g. university, research institution, small and medium enterprise (SME), industry etc.

Working Group:

- | |
|---|
| <input type="checkbox"/> 1 Material Technologies |
| <input type="checkbox"/> 2 Biotechnology, Genomics and Food |
| <input type="checkbox"/> 3 Energy |
| <input checked="" type="checkbox"/> 4 Information and Communication Technologies |
| <input type="checkbox"/> 5 Environmental Protection, Climate Change and Sustainable Development |

Areas of activity:

- | | |
|--|--|
| <input checked="" type="checkbox"/> research | <input checked="" type="checkbox"/> training |
| <input checked="" type="checkbox"/> technology development | <input type="checkbox"/> dissemination |
| <input type="checkbox"/> demonstration | <input type="checkbox"/> other: |

Keywords characterising your area of research:

Please choose the appropriate key words (max. 5) from the following list:
<http://www.cordis.lu/fp6/keywords>

- | | |
|----------------------|------------------------|
| 06.01.01.02.00.00.00 | Computer-aided design |
| 06.02.12.00.00.00.00 | Electronic engineering |
| 06.02.12.01.00.00.00 | Smart cards |
| 06.03.14.00.00.00.00 | Information technology |
| 06.03.14.04.01.00.00 | Security systems |



Participant Profile

for the
Turkish-German Strategy Workshop 2006
TÜBİTAK Marmara Research Center,
Istanbul- Gebze Turkey
13 – 15 December 2006



International Bureau (IB)
of the Federal Ministry of
Education and Research
(BMBF)

**Expertise,
technologies and
infrastructures
available in your
institution:**

Research activities / expertise: Hardware design of cryptographic Algorithms, Embedded System Design for Cryptographic Algorithms, Side Channel Attacks

Methods: Design, test, verification

Key technologies: cryptography, hardware design, embedded system design

Infrastructures: Embedded system design lab, Circuit and systems lab

Key publications:

1. S. B. Ors, "Hardware Design of Elliptic Curve Cryptosystems and Side-Channel Attacks", Ph. D. thesis, Katholieke Universiteit Leuven, February 2005 (ISBN: 90-5682-584-4).
2. S. B. Ors, "Design of Multiplier Blocks for DSP Applications Using VHDL", M.Sc. Thesis, Istanbul Technical University, February 1999.
3. E. De Mulder, S. B. Ors, B. Preneel and I. Verbauwhede, "Differential Electromagnetic Attack On An FPGA Implementation Of Elliptic Curve Cryptosystems", *Proceedings of the World Automation Congress*, July 24-26, 2006, Budapest, Hungary
4. E. De Mulder, P. Buysschaert, S. B. Ors, P. Delmotte, B. Preneel, G. Vandenbosch and I. Verbauwhede, "Electromagnetic analysis attack on a FPGA implementation of an elliptic curve cryptosystem", *Proceedings of the International Conference on "Computer as a tool (EUROCON)*, IEEE, November 21-24, 2005 (Second at IEEE Region 8 Student Paper Contest 2005).
5. S. B. Ors, L. Batina, B. Preneel, J. Vandewalle, "Hardware Implementation of an Elliptic Curve Processor over GF(p)", *International Journal of Embedded Systems (IJES)*, Inderscience Publishers, February, 2005.
6. L. Batina, N. Mentens, S. B. Ors, B. Preneel, "Serial multiplier architectures over GF(2ⁿ) for elliptic curve cryptosystems", *Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference (MELECON)*, 2004, 12-15 May 2004, Vol.2, pp: 779 -782.
7. F. Standaert, S. B. Ors, B. Preneel, and J. Quisquater, "Power Analysis Attacks against FPGA Implementations of the DES", *In Proceedings of Field-Programmable Logic and its Applications (FPL)*, Lecture Notes in Computer Science, Springer-Verlag, p. 84-94, 2004.
8. L. Batina, G. Bruin-Muurling, S. B. Ors, "Flexible Hardware Design for RSA and Elliptic Curve Cryptosystems", *Proceedings of Topics in Cryptology - CT-RSA, The Cryptographers' Track at the RSA Conference*, Tatsuaki Okamoto (Ed.), Lecture Notes in Computer Science 2964, pp. 250-263, San Francisco, CA, USA, February 23-27, 2004, Springer_verlag.
9. F. Standaert, S. B. Ors, and B. Preneel, "Power Analysis attack on an FPGA implementation of AES", *In Proceedings of Cryptographic Hardware and Embedded Systems - CHES*, Marc Joye, Jean-Jacques Quisquater (Eds.), Lecture Notes in Computer Science (LNCS), Springer-Verlag, pp. 30-44, 2004.
10. N. Mentens, S. B. Ors, B. Preneel, and J. Vandewalle, "An FPGA Implementation of a Montgomery multiplier over GF(2^m)", *Computing and Informatics*, vol: 23, issue: 5-6, pp. 487-499, 2004.
11. N. Mentens, S. B. Ors, B. Preneel, and J. Vandewalle, "An FPGA Implementation of a Montgomery multiplier over GF(2^m)", *The Proceedings of the 7th IEEE Workshop on Design & Diagnostics of Electronic Circuits & Systems (DDECS)*, pp. 121-128, 2004.
12. N. Mentens, S. B. Ors, and B. Preneel, "An FPGA Implementation of an Elliptic Curve Processor over GF(2^m)", *In Proceedings of the 2004 Great Lakes Symposium on VLSI (GLSVLSI 2004)*, pp. 454-457, 2004.
13. S. B. Ors, F. Gurkaynak, E. Oswald, and B. Preneel, "Power-Analysis Attack on an ASIC AES implementation", *In Proceedings of the International Conference on Information Technology (ITCC 2004)*, 8 pages, 2004.



Participant Profile

for the
Turkish-German Strategy Workshop 2006
TÜBİTAK Marmara Research Center,
Istanbul- Gebze Turkey
13 – 15 December 2006



International Bureau (IB)
of the Federal Ministry of
Education and Research
(BMBF)

14. S. B. Ors, F. Gurkaynak, E. Oswald, and B. Preneel, "Power-Analysis Attack on an ASIC AES implementation", Chapter in *Embedded Cryptographic Hardware: Design and Security*, Nova Science Publishers, 8 pages, 2004.
15. S. B. Ors, E. Oswald, B. Preneel, "Power-Analysis Attacks on an FPGA -- First Experimental Results", *The Proceedings of the 5th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, C. Walter, C. K. Koc and C. Paar (Ed.), 2779 LNCS, pp. 35-50, Cologne, Germany, September 7 - 10 2003, Springer-Verlag.
16. S. B. Ors, L. Batina, B. Preneel, J. Vandewalle, "Hardware Implementation of an Elliptic Curve Processor over $GF(p)$ ", *The Proceedings of the IEEE 14th International Conference on Application-specific Systems, Architectures and Processors (ASAP)*, pp. 433-443, The Hague, The Netherlands, June 24-26, 2003.
17. L. Batina, S. B. Ors, B. Preneel, J. Vandewalle, "Hardware Architectures for Public Key Cryptography", *Elsevier Science Integration, the VLSI Journal*, issue 34, pages 1-64, 2003.
18. S. B. Ors, L. Batina, B. Preneel, J. Vandewalle, "Hardware Implementation of a Montgomery Modular Multiplier in a Systolic Array", *The Proceedings of the 10th Reconfigurable Architectures Workshop (RAW)*, 8 pages, Nice, France, April 22, 2003.
19. S. B. Ors, A. Dervisoglu, Writing VHDL Models of Parallel nxn Bit Multiplication Blocks , *Proceedings of the European Conference on Circuit Theory and Design (ECCTD'99)*, pp 402-405, Aug. 1999, Stresa Italy.
20. S. B. Ors, A. Dervisoglu, Modeling nxn Multiplication Blocks for DSP Applications Using VHDL, *Proceedings of the 25th EUROMICRO Conference*, pp 892-895, Sept. 8-10 1999, Milan, Italy.



Participant Profile

for the
Turkish-German Strategy Workshop 2006
TÜBİTAK Marmara Research Center,
Istanbul- Gebze Turkey
13 – 15 December 2006



International Bureau (IB)
of the Federal Ministry of
Education and Research
(BMBF)

2. Past and present research collaborations

Are you familiar
with the European
Framework
Programme?

Yes

No

- with Framework Programme 5
 with Framework Programme 6
 with Framework Programme 7

EU-projects you are
involved in:

Past projects

**Programme title / contract number / title / acronym / your function
(coordinator / partner / contractor)**

Side Channel Analysis Resistant Design Flow" (EU IST-2002-507270, SCARD),
Coordinator: Technikon Forschungs- und Planungsgesellschaft mbH, Technikon,
Avusturya.

"European Network of Excellence for Cryptology" (EU IST-2002-507932,
ECRYPT) Coordinator: Prof. Bart Preneel.

Present projects

Other international
collaborations:

Research cooperation with Katholieke Universiteit Leuven, Belgium.

Name(s) and
contact details of
potential partners:

**If you would like to suggest the participation of particular partners from the
partner country based on existing contacts or collaboration experience,
you are welcome to indicate their names and contact details below:**

Prof. Dr. Jean-Jacques Quisquater (Group Leader)

Université Catholique de Louvain (UCL) Crypto Group, <http://www.dice.ucl.ac.be/crypto/>
Bâtiment Maxwell
place de Levant, 3
B-1348 Louvain-la-Neuve
Belgium

Prof. Dr. Reinhard Posch (Group Leader)

Institute for applied information processing and communications (IAIK),
<http://www.iaik.tugraz.at/index.php>
Graz University of Technology
Inffeldgasse 16a a-8010 Graz, Austria

Prof. Dr Christof Paar (Grup başkanı)

Communication Security (COSY), <http://www.crypto.ruhr-uni-bochum.de>
Lehrstuhl Kommunikationssicherheit
Gebäude IC 4/132
Ruhr-Universität Bochum
Universitätsstrasse 150
44780 Bochum



Participant Profile

for the
Turkish-German Strategy Workshop 2006
TÜBİTAK Marmara Research Center,
Istanbul- Gebze Turkey
13 – 15 December 2006



International Bureau (IB)
of the Federal Ministry of
Education and Research
(BMBF)

3. Presentation at the Workshop

I will give a presentation at the workshop (approx. 10 min.) to present my institution, my expertise, and my collaboration interests. The contents of my presentations is summarised below (max. 1 page).

Embedded System Design for Security

R&D activities within Istanbul Technical University, Department of Electronics and Communication Engineering

Within the area of embedded system design for security we are active in the fields

- Hardware implementation of cryptographic algorithms
 1. symmetric key cryptography (AES, DES)
 2. public key cryptography (RSA, ECC)
- Smartcard implementation of cryptographic algorithms
 1. symmetric key cryptography (AES, DES)
 2. public key cryptography (RSA, ECC)
- Side channel attacks on the implementation of cryptographic algorithms
- Design with countermeasures to side-channel attacks

I agree with the publication of my data on the Workshop website!

PLEASE FILL IN THIS FORM UNTIL 22 SEPT. 2006 AND RETURN IT TO:

Internationales Buero des BMBF
s.krummacher@fz-juelich.de;
Christian.schache@dlr.de

TÜBİTAK-Marmara Research Center
Sunullah.Ozbek@mam.gov.tr;
Artac.Turker@mam.gov.tr