

2010 Workshop on Fault Diagnosis and Tolerance in Cryptography

(FDTC 2010)

**Santa Barbara, California, USA
21 August 2010**



**IEEE Catalog Number: CFP1086C-PRT
ISBN: 978-1-4244-7844-6**

2010 Workshop on Fault Diagnosis and Tolerance in Cryptography

FDTC 2010

Table of Contents

| | |
|----------------------------------|------|
| Preface | vii |
| Program Committee | viii |
| Acknowledgments | ix |
| Contact Information | x |

Session 1: Attacks on AES

| | |
|--|----|
| Differential Fault Analysis against AES-192 and AES-256 with Minimal Faults..... | 3 |
| <i>Chong Hee Kim</i> | |
| Passive and Active Combined Attacks on AES—Combining Fault Attacks and Side Channel Analysis..... | 10 |
| <i>Christophe Clavier, Benoit Feix, Georges Gagnerot, and Mylène Roussellet</i> | |

Session 2: Fault Injection

| | |
|---|----|
| Optical Fault Masking Attacks..... | 23 |
| <i>Sergei Skorobogatov</i> | |
| Memory Address Scrambling Revealed Using Fault Attacks..... | 30 |
| <i>Jacques J.A. Fournier and Philippe Loubet-Moundi</i> | |

Invited Paper

| | |
|--|----|
| Generic Analysis of Small Cryptographic Leaks..... | 39 |
| <i>Itai Dinur and Adi Shamir</i> | |

Session 3: Countermeasures

| | |
|---|----|
| Fault Injection Resilience..... | 51 |
| <i>Sylvain Guilley, Laurent Sauvage, Jean-Luc Danger, and Nidhal Selmane</i> | |
| A Continuous Fault Countermeasure for AES Providing a Constant Error Detection Rate..... | 66 |
| <i>Marcel Medwed and Jörn-Marc Schmidt</i> | |

Invited Paper

| | |
|---|----|
| Multi Fault Laser Attacks on Protected CRT-RSA..... | 75 |
| <i>Elena Trichina and Roman Korkikyan</i> | |

Session 4: Public-Key Techniques

| | |
|---|----|
| Fault Attacks and Countermeasures on Vigilant's RSA-CRT Algorithm..... | 89 |
| <i>Jean-Sébastien Coron, Christophe Giraud, Nicolas Morin, Gilles Piret, and David Vigilant</i> | |
| Low Cost Built in Self Test for Public Key Crypto Cores..... | 97 |
| <i>Duško Karaklajic, Miroslav Knežević, and Ingrid Verbauwhede</i> | |

| | |
|---------------------------|-----|
| Author Index | 105 |
|---------------------------|-----|