



- Institut
- Forschung
- Lehre
- Mitarbeiter
- Archiv
- Presse und Jobs
- Intranet
- Sitemap

- Fakultät IEF
- Institute der Elektrotechnik
- Projekte

Startseite » Mitarbeiter » Archiv » Mathias Schmalisch

### Mathias Schmalisch

Dipl.-Ing. Mathias Schmalisch

### Forschungsgebiete

- Kryptographieprozessoren

### Projekte

- SECOM - Secure Communication over ISDN

### Publikationen

Die Anzahl von Veröffentlichungen: 15

Schmalisch, M.; Timmermann, D.  
 Comparison of Algorithms for Elliptic Curve Cryptography over Finite Fields of GF(2<sup>m</sup>) ( Folien )  
 Proceedings of the IASTED International Conference on Communication, Network and Information Security, S. 136-140, ISBN: 0-89896-402-0, New York, USA, Dezember 2003

Schmalisch, M.; Timmermann, D.  
 A Reconfigurable Arithmetic Logic Unit for Elliptic Curve Cryptosystems over GF(2<sup>m</sup>) ( Folien )  
 The 46th IEEE Midwest Symposium on Circuits and Systems (MWSCAS), Kairo, Ägypten, Dezember 2003

Schmalisch, M.; Fiedler, M.; Timmermann, D.  
 Eine ALU für die schnelle Berechnung der Kryptographie auf Basis elliptischer Kurven ( Folien )  
 4. IuK-Tage Mecklenburg-Vorpommern, Rostock, Deutschland, Juni 2003

Schmalisch, M.; Ploog, H.; Timmermann, D.  
 Kriterien zur optimalen Auswahl von Elliptic Curve Cryptography als Hard- oder Softwarelösung ( Folien )  
 Embedded Intelligence 2002, Band 1, S. 489-498, Nürnberg, Deutschland, Februar 2002

Schmalisch, M.; Ploog, H.; Timmermann, D.  
 Laufzeitoptimierte VHDL Bibliothek zur Verifikation und Simulation kryptographischer Prozessoren ( Folien )  
 GI/ITG/GMM Workshop - Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen, S. 154 - 162, ISBN: 3-8265-9859-8, Tübingen, Deutschland, Februar 2002

Ploog, H.; Schmalisch, M.; Timmermann, D.  
 Anwendung einer Library-optimierten VHDL-Kodierung für mobile ISDN-Verschlüsselung  
 14. Mikroelektroniktagung 2001, OVE-Schriftenreihe Nr. 26, S. 185-190, ISBN: 3-85133-022-6, Wien, Österreich, Oktober 2001

Schmalisch, M.; Timmermann, D.  
 Grundlagen der Elliptic Curve Cryptography ( Folien )  
 3. IuK-Tage Mecklenburg-Vorpommern, Rostock, Deutschland, Juni 2001

Schmalisch, M.; Timmermann, D.  
 Einführung in die Elliptic Curve Cryptography ( Folien )  
 10. Symposium Maritime Elektronik, S. 125-128, Rostock, Deutschland, Juni 2001

Schmalisch, M.; Ploog, H.; Grassert, F.; Timmermann, D.  
 Kryptographieprozessor zur Verschlüsselung von ISDN-Daten ( Folien )  
 Embedded Intelligence 2001, S. 267-276, Nürnberg, Deutschland, Februar 2001

Schmalisch, M.; Timmermann, D.  
 Entwicklung von Hardwarekryptographie für hohe Datenraten  
 Berichtskolloquium des Graduiertenkollegs, Rostock, Deutschland, November 2000

Schmalisch, M.; Ploog, H.; Timmermann, D.  
 Sicherheitsversteigerung eines ISDN-Gerätes durch rekonfigurierbare Logik  
 Herbstworkshop des Graduiertenkollegs, Göhren, erschienen in: Rostocker Informatik-Berichte, S. 89-96, Göhren, Deutschland, November 2000

Schmalisch, M.; Ploog, H.; Timmermann, D.  
 SECOM: Sichere Online Verschlüsselung für ISDN-Geräte  
 35. Sitzung des Arbeitskreises Technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Rostock, Deutschland, September 2000

Ploog, H.; Schmalisch, M.; Timmermann, D.  
 Security Upgrade of Existing ISDN Devices by Using Reconfigurable Logic  
 FPL 2000, 10th Int'l Conf. on Field-Programmable Logic and Applications, erschienen in: Lecture Notes in Computer Science #1896, Field-Programmable Logic and Applications, Springer Verlag, Heidelberg., ISBN: 3-540-67899-9, Villach, Schweiz, August 2000

Schmalisch, M.; Ploog, H.; Timmermann, D.  
 SECOM: Mobiles Gerät zur Verschlüsselung von ISDN-Datenströmen  
 Exponat auf der Cebit 2000, Hannover, Deutschland, Februar 2000

Ploog, H.; Schmalisch, M.; Timmermann, D.  
 Kryptomodul für schnelle DES basierende Verschlüsselungssysteme ( Folien )  
 2. IuK Tage M-V, Rostock, Deutschland, Juni 1999

Suchbegriff...



Mitarbeitersuche...



### Kontakt

Besucher:  
 Fakultät für Informatik und Elektrotechnik  
 Institut für Angewandte Mikroelektronik und Datentechnik  
 Haus 1, Raum 1207 (Sekretariat)  
 Richard Wagner Str. 31  
 18 119 Rostock-Warnemünde  
 Tel.: +49 381 498 7251  
 Fax: +49 381 498 118 7251  
 Email  
 Postanschrift:  
 Universität Rostock  
 Institut für Angewandte Mikroelektronik und Datentechnik  
 18051 Rostock

### Schnelleinstieg

- [Publikationen](#)
- [Anfahrt](#)
- [Kontakt](#)
- [Laborpraktikum](#)
- [Lehrangebot](#)
- [Highlights](#)
- [Projekte](#)