



Der ECC-Brainpool veranstaltet am 12.12.2001 einen Workshop zu dem Thema

## Side-Channel-Attacks auf Kryptoalgorithmen

Alle Mitglieder des ECC-Brainpool sind herzlich eingeladen, daran teilzunehmen. Der Ort der Veranstaltung ist:

**Bundesamt für Sicherheit in der Informationstechnik (BSI)**  
**Godesberger Allee 183**  
**53133 Bonn**

Geplantes Programm:

- 10:00 Uhr: Begrüßung
- 10:10 Uhr: Einführung – Schutzmaßnahmen gegen Side-Channel-Attacks (*K. Nguyen, Philips Semiconductors*)
- 10:50 Uhr: DPA-Tests als Bestandteil der Evaluationsstandards im Bereich der Kreditwirtschaft (*D. Feldhusen, SRC*)
- 11:30 Uhr: Kaffeepause
- 11:50 Uhr: A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks (*T. Takagi, TU Darmstadt*)
- 12:30 Uhr: Eine Möglichkeit der Analyse der SPA-Resistenz von Punktmultiplikationsverfahren (*E. Oswald, IAIK, TU Graz*)
- 13:10 Uhr: Mittagspause
- 14:10 Uhr: Kollisionsattacken beim Comp128 auf Smartcards (*A. Wiemers, BSI*)
- 14:50 Uhr: Maßnahmen gegen DPA-Attacken aus algorithmischer Sicht (*R. Blümel, cryptovision*)
- 15:30 Uhr: Kaffeepause
- 15:50 Uhr: DPA-Gegenmaßnahmen bei einer ECDSA-Implementierung auf Chipkarten (*M. Seysen, G&D*)
- 16:30 Uhr: Secure, fast and parallel scalar multiplication on general elliptic curves over  $F_p$  (*W. Fischer, Infineon*)
- 17:10 Uhr: Abschließende Diskussion

Um Anmeldung möglichst bis zum 7.12. wird gebeten. Anmeldungen gehen bitte per Email an [info@ecc-brainpool.org](mailto:info@ecc-brainpool.org). Wegen der Räumlichkeiten ist die Anzahl der Teilnehmer auf maximal 50 beschränkt.