Martin Otto: Fault Attacks and Countermeasures

Dissertation, 2005, in der Arbeitsgruppe „Codes und Kryptographie“
betreut von Prof. Dr. Johannes Blömer
Institut für Informatik
Fakultät für Informatik, Elektrotechnik und Mathematik
Universität Paderborn

Zusammenfassung

Das Ergebnis dieser Arbeit sind neue Resultate für Fehlerangriffe auf Implementierungen von Kryptosystemen, sowie passende neue Gegenmaßnahmen. Der Schwerpunkt liegt dabei auf digitalen Unterschriften.
Kryptosysteme, die auf mobilen Geräten wie Smartcards implementiert werden, bieten durch die physikalischen Eigenschaften dieser Geräte einem Beobachter neue Informationsquellen (Seitenkanäle, wie Dauer der Berechnung oder Energieverbrauch). Mit Hilfe dieser Seitenkanäle können einige Kryptosysteme gebrochen werden, die im klassischen Sinne beweisbar sicher sind.
Grundlage dieser Arbeit ist dabei der Seitenkanal der fehlerhaften Ausgaben, die durch induzierte Fehler erzeugt werden. Die beiden Hauptziele sind dabei die Herleitung neuer Fehlerangriffe, sowie die Entwicklung neuer Algorithmen, die immun gegen Fehlerangriffe sind.
Die Arbeit beinhaltet neue Angriffe für die beiden populärsten Public-Key Verfahren, RSA und Systeme basierend auf elliptischen Kurven. Für RSA wird gezeigt, dass ein bekannter Angriff auf eine Variante des wiederholten Quadrierens auch auf die andere anwendbar ist, beide also gleichermaßen anfällig sind. Für elliptische Kurven zeigen wir, dass anders als bisher angenommen auch hier Fehlerangriffe einfach möglich sind. Dazu entwickeln wir einen neuen Fehlertyp und zeigen seine Anwendbarkeit für viele Varianten des wiederholten Verdoppelns.
Wir präsentieren auch Algorithmen, die gegen bekannte Fehlerangriffe immun sind. Für RSA stellen wir einen neuen Algorithmus für CRT-RSA vor, einer schnellen und daher sehr beliebten Variante von RSA. Für elliptische Kurven geben wir einen neuen Algorithmus an, der das wiederholte Verdoppeln gegen alle bekannten Fehlerangriffe schützt.