Kurzfassung der Dissertation

Design und Analyse von Blockhiffrenkonstruktionen

Design and Analysis of Block Cipher Constructions

Dipl.-Inf. Andrey Bogdanov
Lehrstuhl für eingebettete Sicherheit
Ruhr-Universität Bochum

Die vorliegende Dissertation beschäftigt sich mit symmetrischen kryptographischen Algorithmen. Den Schwerpunkt bilden Blockchiffren sowie Hashfunktionen und Message Authentication Codes (MAC), welche auf Blockchiffren basieren. Diese Arbeit umfasst drei Themenkomplexe — verschiedenen Ansätzen der symmetirscher Kryptoanalyse entsprechend: Erstens werden mehrere Blockchiffrenkonstruktionen in Bezug auf statistische Kryptoanalyse evaluiert. Zweitens werden praktische Angriffe auf weit eingesetzte symmetrische Kryptosysteme vorgeschlagen, teilweise mit Beschleunigung in Hardware. Drittens werden neuartige kryptoanalytische seitenkanalbasierte Techniken entwickelt und auf Blockchiffrenkonstruktionen angewendet.

Differentielle und lineare Kryptoanalysen sind bekannte statistische Angriffe auf Blockchiffren. In dieser Dissertation wird die Sicherheit von Unbalanced Feistel Networks (UFN) mit komprimierender MDS-Diffusion in Bezug auf differentielle Kryptoanalyse untersucht. Obere Schranken für die Wahrscheinlichkeiten der differentiellen Charakteristiken solcher Konstruktionen werden bewiesen. Es wird demonstriert, dass die Effizienz solcher UFNs mit der von Balanced Feistel Networks vergleichbar sein kann. Des Weiteren werden einige kryptographische Lightweight-Konstruktionen designt, welche Substitution-Permutation Networks mit Bitpermutationen verwenden. Als Ergebnis werden Lightweight-Blockchiffren und blockchiffrenbasierte Kompressionsfunktionen für Lightweight-Hashfunktionen entworfen und analysiert. Diese Konstruktionen erfordern nur geringe Chipfläche und lassen sich auf den meisten RFID-Tags effizient implementieren.

In dieser Arbeit werden auch praktische Angriffe auf symmetrische Kryptosysteme betrachtet, am Beispiel der KeeLoq-Blockchiffre und KeeLoq-Authentifizierungssysteme, welche bei der Zutrittskontorolle im Automotive-Bereich weiten Einsatz findet, sowie am Beispiel der A5/2-Stromchiffre, welche weltweit zum Schutz von GSM-Verbindungen benutzt wird. Lineare Slide-Angriffe auf KeeLoq werden vorgeschlagen, was zum schnellsten bekannten für alle Schlüssel funktionierenden Angriff führt. Ernsthafte Schwächen der KeeLoq-Schlüsselverwaltung werden indentifiziert. Die KeeLoq-Authentifizierungsprotokolle sind analysiert. Eine dedizierte Hardwarearchitektur zum Angreifen von A5/2 wird entwickelt, welche Schlüsselbestimmung innerhalb einer Sekunde in Echtzeit für verschiedene GSM-Kommunikationskanäle erlaubt. Dieser Hardware-Baustein basiert auf einem optimierten Hardwarealgorithmus zur schnellen Gauss-Elimination über binären endlichen Körpern.

Der letzte Themenkomplex dieser Dissertation ist die Seitenkanalanalyse von Blockchiffrenkonstruktionen. Wie einfache und differentielle Seitenkanalanalysen, benutzen die Kollisionsangriffe ebenfalls Seitenkanalinformationen, z.B. Messkurven des Stromverbrauchs oder der elektromagnetischen Abstrahlung der Implementierungen anzugreifender kryptographischer Algorithmen. Bezeichnend für Kollisionsangriffe ist allerdings, dass diese die kryptoanalytischen Eigenschaften der Kryptoalgorithmen wesentlich benutzen. Zusätzlich zur Anwendung von Kollisionsangriffen auf AES-basierte MACs, werden in dieser Arbeit auch zahlreiche Methoden zum Optimieren von Kollisionsangriffen vorgeschlagen. Die Verbesserungen schließen den Begriff der verallgemeinerten Kollisionen, lineare und algebraische kollisionsbasierte Schlüsselbestimmung sowie neue statistische Methoden zur Kollisionsdetektierung ein. Im Falle von AES bringen diese Techniken wesentliche Vorteile und machen Kollisionsangriffe auf vielen Plattformen effizienter als solche etablierte Angriffsmethoden wie stochastische Angriffe und Template-Angriffe.