Zusammenfassung

Beweisbare Sicherheit und Skalierbarkeit sind zwei wünschenswerte Eigenschaften einer Blockchiffre. Die erste garantiert, dass die Chiffre unsere Erwartung der Sicherheit verschlüsselter Daten erfüllt. Die Skalierbarkeit macht die Nutzung der Chiffre einfacher und ermöglicht Anpassung des Sicherheitsniveaus an die gegenwärtigen Anforderungen durch Änderung gewisser Parameter. In dieser Dissertation untersuchen wir die beweisbare Sicherheit von drei skalierbaren Blockchiffren (Feistel-Chiffre, TST und IDEA) im Random Oracle Model.

Die Dissertation besteht aus zwei Teilen. Der erste Teil ist eine Einführung in die Theorie der beweisbaren Sicherheit. Bis jetzt existieren in der Literatur nur wenige Artikel, welche sich mit der Theorie der beweisbaren Sicherheit von Verschlüsselungsverfahren befassen. Zusätzlich verwenden sie unterschiedliche Sicherheitsmodelle und Begriffe der Ununterscheidbarkeit. Im ersten Teil der Dissertation wird die Theorie der beweisbaren Sicherheit vereinheitlicht und vervollständigt. Dabei werden das uniforme Modell und Vaudenays Begriff von Ununterscheidbarkeit verwendet. Wir illustrieren die Methoden am Beispiel der Analyse des asymmetrischen Feistel-Netzwerks. Im zweiten Teil wird diese Theorie angewandt, um die Sicherheit von zwei anderen skalierbaren Blockchiffren, nämlich TST und IDEA, zu analysieren.

Das erste Kapitel des ersten Teils (Kapitel 2) beschreibt die grundlegenden Begriffe der beweisbaren Sicherheit und führt das Sicherheitsmodell sowie die mathematischen Grundlagen ein. Das darauf folgende Kapitel diskutiert allgemeine Angriffe, nämlich die Known-Plaintext-Attack, die (Adaptive-)Chosen-Plaintext-Attack, die (Adaptive-)Chosen-Ciphertext-Attack und die (Adaptive-)Chosen-Plaintext-Ciphertext-Attack. Die Matrixnormen, die mit den individuellen Angriffen im Zusammenhang stehen, und die, die zu den oberen Grenzwerten der "Advantage" der Angriffe führen, werden hergeleitet. Die Beweise der Sicherheit für einige der Angriffe werden am Beispiel des asymmetrischen Feistel-Netzwerks illustriert.

Es wird oft versucht, einen iterativen Angriff durchzuführen, indem eine einfache Angriffsmethode auf eine Blockchiffre mehrfach angewandt wird. Ein iterativer Angriff ist offensichtlich stärker als ein Einfacher. Eine andere Möglichkeit, einen stärkeren Angriff zu erreichen, ist, mehrere einfache Angriffe nacheinander durchzuführen. Dabei ist die natürliche Frage, welcher Anteil der Advantage in dieser Weise erhöht werden könnte. In Kapitel 4 überprüfen wir die kombinierten Angriffe und leiten die oberen Schranken ihrer Advantage her. Die bekanntesten iterativen Angriffe sind differentielle und lineare Kryptoanalyse. Aufgrund ihrer großen Bedeutung werden sie getrennt behandelt.

Da die Blockgröße der Blockchiffre viel kürzer als die zu verschlüsselnden Nachrichten ist, werden Methoden benötigt, welche lange Daten zu verarbeiten ermöglichen. Einige solche Methoden wurden im NIST-FIPS 81 Standard vorgeschlagen. Das letzte Kapitel des ersten Teils analysiert diese Methoden, sowie eine modifizierte Methode von Diffie, und evaluiert deren Sicherheit.

Im zweiten Teil der Dissertation wird die Sicherheit der skalierbaren Blockchiffren behandelt. Es werden zwei Methoden der Skalierbarkeit — Skalierbarkeit der Chiffre durch Anpassung der Primitive und Skalierbarkeit durch Anpassung der Struktur — eingehend untersucht, und dabei wird die Sicherheit von zwei skalierbaren Verfahren, TST und IDEA, hergeleitet.

Das erste skalierbare Verfahren TST wurde in [8] eingeführt. Es basiert im wesentlichen auf einem modifizierten asymmetrischen Feistel-Netzwerk. Da die Sicherheit des asymmetrischen Feistel-Netzwerkes im ersten Teil bereits behandelt wurde, besprechen wir hier kurz die Auswirkung von Änderungen der Struktur auf die Sicherheit des gesamten TST-Verfahrens und fokussieren uns dann auf die Sicherheit seiner Primitiven und auf deren Beitrag zur Sicherheit der Chiffre. Genauer zeigen wir, dass eine in TST verwendete Hashfunktion schwach ist, und dass das Hinzufügen einer anderen Funktion in das Feistel-Netzwerk nicht den genügenden Ausgleich für die Schwäche liefert. Weiter zeigen wir, dass wenn eine gute Hashfunktion verwendet wird, die P-Box in TST nicht erheblich zur Sicherheit beiträgt, und damit entfernt werden kann. In dieser Weise wird das Schema vereinfacht. Anschließend analysieren wir andere Hashfunktionen und deren Anwendung im Verfahren. Wir zeigen, wie die beste Hashfunktion im Hinblick auf die Sicherheit des gesamten Verfahrens gewählt werden kann.

Die IDEA-Chiffre ist eine der bekanntesten Chiffren, die nicht auf einem Feistel-Netzwerk basieren. Jedoch ist die Skalierbarkeit ihrer Primitiven begrenzt, so dass die Blockgröße der Chiffre nicht 64 Bits übersteigen kann, was gegenwärtigen Anforderungen nicht gerecht wird. In Kapitel 8 untersuchen wir zuerst die Sicherheit des IDEA-Verfahrens, dann zeigen wir, wie aus der IDEA-Chiffre neue skalierbare Chiffren konstruiert werden können. Wir stellen zwei skalierbare Verfahren vor: das erste hat eine parallele Struktur unter Verwendung des zugrundeliegenden IDEA-Verfahrens im größtmöglichen Umfang, das zweite ist seriell und verwendet das IDEA-Verfahren nur einmal pro Runde. Wir evaluieren die Zahl der Runden, die notwendig sind, um Pseudorandomness und Super-Pseudorandomness sicherzustellen.

Die Dissertation schließt mit vier Anhängen. Die ersten Zwei listen die verwendeten Symbole und die Akronyme, der Dritte gibt Eigenschaften der verwendeten Matrixnormen an, und der Letzte enthält eine Anzahl von Lemmas, die in mehreren Beweisen eingesetzt werden.