Kurzfassung der Dissertation von Andreas Gornik: „Entwurf und Analyse einer Hardware-Schutzmaßnahme gegen Seitenkanalattacken“

Seitenkanalattacken sind gefährlich, weil vor allem kryptographische Geräte, wie z.B. Chipkarten und Funkschlüssel, mit geringem finanziellen Aufwand mit diesen Angriffen gebrochen werden können, was sie sehr beliebt macht. Diese Angriffe zielen nicht direkt auf den mathematischen Algorithmus, sondern auf die unveränderte physikalische Implementierung und sind deshalb erfolgreich.

Damit ein Verständnis für die Logikschaltungen, aus denen kryptographische Geräte aufgebaut sind, entwickelt werden kann, werden drei grundlegende Logikfamilien und deren Arbeitsweise vorgestellt. Diese sind die statische, die dynamische und die adiabatische Logik.

Im Anschluss wird untersucht, auf welche Art und Weise Seitenkanalinformationen in Logikschaltungen entstehen. Dazu werden die Seitenkanäle Stromaufnahme, elektromagnetische Abstrahlung und die Ausführungszeit von Operationen betrachtet. Die Untersuchungen zeigen, dass symmetrische Logikschaltungen eine gleichförmige Stromaufnahme nur besitzen, wenn keine Fertigungsschwankungen berücksichtigt werden. In der Praxis treten lokale relative Fertigungsschwankungen auf, die dazu führen, dass symmetrische Schaltungen leicht unsymmetrisch ausfallen, und dadurch angreifbar werden. Aus diesem Grund stellen symmetrische Schaltungen keinen guten Schutz gegen Seitenkanalattacken dar.

Mit Hilfe der gewonnenen Erkenntnisse über die Entstehung von Seitenkanalinformationen, und den Arbeitsweisen der drei vorher vorgestellten Logikfamilien, werden bekannte Schutzmaßnahmen aus der Literatur kategorisiert und bewertet. Hier stellt sich heraus, dass die am häufigsten vorgestellten Schutzmaßnahmen symmetrisch sind, und als Schutz auf eine gleichförmige Stromaufnahme setzen. Daher wird eine Methode entwickelt, mit der, während des Entwurfs einer Schutzmaßnahme, die Gleichförmigkeit der Stromaufnahme bestimmt werden kann. Bei der Durchführung eines Entwurfsbeispiels zeigt sich, wie bei der Untersuchung der symmetrischen Logikschaltungen, dass das Ziel einer gleichförmigen Stromaufnahme nicht erreicht werden kann. Deswegen wird bei der Neuentwicklung einer Schutzmaßnahme auf ein anderes wirksames Konzept gesetzt.

Bei dem neuen Konzept geht es im Wesentlichen darum, dass die verwendeten Logikgatter von der Versorgungsspannung abgekoppelt werden. Um dies umzusetzen, werden Pufferkapazitäten verwendet, die über ein bestimmtes Schema geladen, entladen oder zur Versorgung der Logikgatter an selbige geschaltet werden. Hierbei wird sichergestellt, dass zu keinem Zeitpunkt die Logikgatter direkt mit der Versorgungsspannung verbunden sind. Zusätzlich wird eine Trennschaltung verwendet, die dafür sorgt, dass mögliche Übersprechpfade gegen Masse geschaltet werden. Dieses Konzept wird in einer ersten Schaltung umgesetzt und mit Hilfe von Seitenkanalangriffen validiert. Diese Angriffe zeigen, dass der erste Schaltungsentwurf einen höheren Schutz bietet als statische CMOS-Logik.

Um die Schutzwirkung weiter zu erhöhen, wird die Schaltung optimiert. Dazu wurde die komplette Schaltung überarbeitet und mittels Kleinsignalanalyse mit dem ersten Entwurf verglichen. Der Neuentwurf zeigt in der Kleinsignalanalyse ein wesentlich besseres Verhalten, was auf eine höhere Schutzklasse schließen lässt. Dies muss aber an Hand einer Implementierung noch verifiziert werden.