Seitenkanal-Analysen: Stand der Forschung in der Methodik

Kerstin Lemke · Christof Paar

Horst Görtz Institut für IT Sicherheit
Ruhr Universität Bochum
44780 Bochum, Deutschland
{lemke,cpaar}@crypto.rub.de

Zusammenfassung

Seit nunmehr 10 Jahren sind Seitenkanal-Analysen in der angewandten Kryptographie etablierte Angriffsszenarien. Seitenkanal-Analysen basieren auf der Verwendung von physikalischen Messgrößen bei der kryptographischen Analyse einer Implementierung. Die Vielzahl von Veröffentlichungen zu diesem Themenbereich zeugt von einem andauernden Forschungsinteresse sowie von einer Vielfältigkeit der bereits publizierten Methoden und Ergebnisse. Ziel dieses Beitrages ist eine systematische Darstellung der aktuell einsetzbaren Methoden bei Seitenkanal-Analysen. Wir betrachten sowohl fundamentale Ergebnisse als auch neuere Entwicklungen in der Forschung. Ein Gegenstand von hoher praktischer Relevanz ist insbesondere auch die Frage des Umfangs von adäquaten Tests.

1 Einführung

Seitenkanal-Analytik ist ein neueres Forschungsgebiet der angewandten Kryptographie, das sich mit der Untersuchung von physikalischen Eigenschaften realer Implementierungen eines kryptographischen Algorithmus beschäftigt. Seitenkanal-Analysen zeichnen physikalische Messgrößen während der Ausführung der kryptographischen Operation auf und extrahieren hieraus zusätzliche Informationen für die Krypto-Analyse. Die grundlegende Arbeitshypothese basiert darauf, dass sich bei einer realen Implementierung Daten, die während der Bearbeitung der kryptographischen Operation auftreten, auf Messgrößen auswirken. Der funktionale Zusammenhang hierfür ist implementierungsspezifisch und stellt den *Seitenkanal* dar. Ein Angreifer hat Erfolg, wenn aufgrund von Seitenkanal-Analysen ein Informationsverlust eines geheimen kryptographischen Schlüssels eintritt. Analysen beziehen sich daher stets auf eine konkrete Implementierung und können erst nach erfolgten Messungen erfolgen. Seitenkanal-Analysen sind passive Implementierungsangriffe, d.h. sie sind zerstörungsfrei und hinterlassen keine offensichtlichen Spuren nach erfolgtem Angriff.

Ziel dieses Beitrags ist es, die wesentlichen Methoden von Seitenkanal-Analysen zusammenzustellen. Wir streben dabei eine Gesamtdarstellung im Rahmen eines einführenden Beitrags an. Bei der Auswahl der vorgestellten Methoden haben wir sowohl etablierte Verfahren als auch relevante, neuere Forschungsergebnisse berücksichtigt. Eine vollständi-

ge Betrachtung aller bereits publizierten Methoden ist in diesem Rahmen jedoch nicht möglich. In Abschnitt 2 behandeln wir das Seitenkanal-Analysen zugrundeliegende Angreifermodell. Abschnitt 3 beinhaltet die systematische Zusammenstellung der Methodik für Seitenkanal-Analysen. Für die Praxis sind insbesondere angemessene Prüfkriterien für Seitenkanal-Analysen wichtig. Hierfür wird in Abschnitt 4 ein Rahmenwerk bereitgestellt.

2 Angreifermodell

Bei Seitenkanal-Analysen wird vorausgesetzt, dass der Angreifer physikalische Messungen an dem anzugreifenden Krypto-Modul vornehmen kann. Der kryptographische Algorithmus wird als bekannt angenommen, der geheime kryptographische Schlüssel ist dagegen unbekannt und stellt das Angriffsziel dar. Der Angreifer kann durch ein Kommando an das Krypto-Modul die Berechnung des Kryptoalgorithmus wiederholt anstoßen. Die Annahme über die Kenntnis der Eingangs- und Ausgangsdaten des Kryptoalgorithmus kann bei konkreten Szenarien sehr unterschiedlich sein, d.h. von keiner Information bis zu adaptiv wählbaren Daten. Der Angreifer verfügt über eine Mess-Apparatur, die während der kryptographischen Operation physikalische Messgrößen aufzeichnet. Der Angriff ist mit N Ausführungen des Kryptoalgorithmus erfolgreich, wenn ein kritischer Informationsverlust des geheimen Schlüssels nachgewiesen werden kann.

2.1 Physikalische Messgrößen

Als physikalische Messgrößen (Observablen) kommen

- die Ausführungszeit [Koc96],
- die Leistungsaufnahme [KJJ99], sowie
- die Leistungsabstrahlung [GMO01]

einer kryptographischen Implementierung in Frage.

Die Ausführungszeit ist ein kumulierter Messwert pro kryptographischer Operation, der aus der Aufsummierung von Zeitdifferenzen in Teilabschnitten der kryptographischen Implementierung resultiert. Messungen der Leistungsaufnahme und Leistungsabstrahlung erlauben dagegen instantane Beobachtungen der Vorgänge im Krypto-Modul und sind, wenn möglich, der Messung der reinen Ausführungszeit vorzuziehen. Insbesondere sind Zeitinformationen in den Messungen der Leistungsaufnahme und Leistungsabstrahlung direkt enthalten, d.h. es können insbesondere Zeitdifferenzen in Teilabschnitten direkt festgestellt werden.

2.2 Konstruktion des Krypto-Moduls

Gekapselte Krypto-Module oder Krypto-Module in sicheren eingebetteten Systemen (*secure embedded systems*) wie beispielsweise *Smart Cards* unterscheiden sich beim Angreifermodell von kryptographischen Implementierungen in Software, die auf PCs und Workstations zur Anwendung kommen.

2.2.1 Krypto-Module in sicheren, eingebetteten Systemen

Eine Einführung in die Sicherheit von eingebetteten Systemen findet sich beispielsweise in [PPS+04]. Kurz zusammengefaßt sind, abgesehen von Computern, praktisch alle

Geräte, die mit einem Mikroprozessor ausgestattet sind, als eingebettete Systeme zu betrachten. Hierunter fallen gekapselte *Single-Chip* oder *Multi-Chip* Krypto-Module und eingebettete Krypto-Module, die Teil eines größeren Computer-Systems sind. Bei einem sicheren Krypto-Modul setzen wir voraus, dass die Implementierung physisch und logisch gekapselt ist, so dass es keine physische oder logische Schnittstelle zum Auslesen des kryptographischen Schlüssels gibt. Es wird davon ausgegangen, dass der Angreifer physischen Zugang zum Krypto-Modul hat, beispielsweise im Besitz einer Chipkarte ist, die von einem Serivce-Anbieter herausgegeben wird. Die Observablen können somit direkt am Krypto-Modul an den externen Schnittstellen oder im Nahfeld mit einer Sonde aufgezeichnet werden. Für die Messung instantaner Observablen wird üblicherweise ein digitales Speicheroszilloskop eingesetzt (s. Abb. 1).

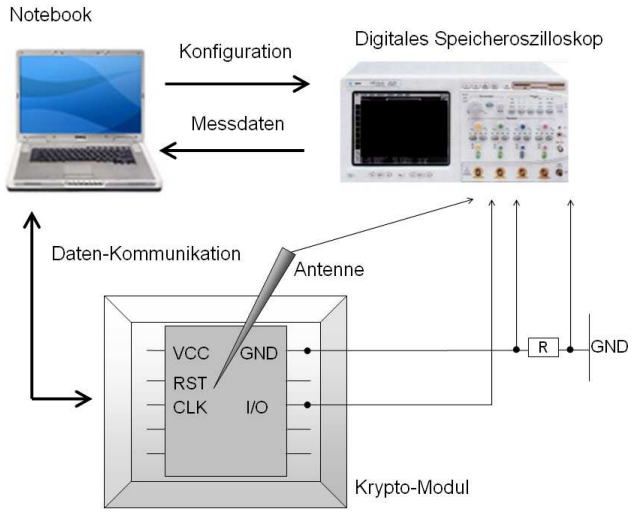

Abb. 1: Messung der Leistungsaufnahme und Leistungsabstrahlung direkt am Krypto-Modul

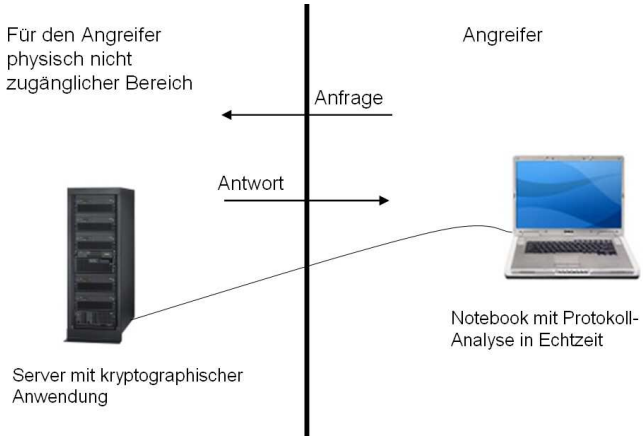

Abb. 2: Messung der Zeitdauer über eine Netzwerkverbindung

2.2.2 Software basierte Krypto-Module zum Einsatz auf universalen Plattformen

Eine andere Situation liegt vor im Falle von Software basierten Krypto-Modulen zum Einsatz auf PCs und Workstations. Ein Angreifer mit physischem Zugang zu der Plattform hat einfachere Möglichkeiten, einen kryptographischen Schlüssel auszulesen, z.B.

durch Ausbau der Festplatte. Seitenkanal-Analysen betrachten hier deshalb einen räumlich entfernten Angreifer, der über das Netzwerk mit der kryptographischen Implementierung agieren kann, jedoch nicht direkt Messgrößen an der Plattform abgreifen kann (s. Abb. 2). Als Seitenkanal kommt bei Netzwerk-Angriffen praktisch nur die Antwortzeit der kryptographischen Anwendung in Frage.

3 Methodik

Das Ziel dieses Abschnittes ist eine Gesamtdarstellung der Methodik bei Seitenkanal-Analysen. Wir differenzieren in einstufige (Abschnitt 3.1) und zweistufige Methoden (Abschnitt 3.2). Bei Abschnitt 3.1 und 3.2 setzen wir zunächst voraus, dass keine algorithmischen Gegenmaßnahmen implementiert sind. Die Anpassung der Methoden bei Vorliegen von algorithmischen Gegenmaßnahmen wird in Abschnitt 3.3 betrachtet. Die hier vorgestellten Methoden für instantane Observablen werden sowohl für Messdaten der Leistungsaufnahme als auch der Leistungsabstrahlung eingesetzt; für die Wahl der Methode spielt die physikalische Herkunft der Messdaten keine Rolle.

3.1 Einstufige Seitenkanal-Analysen: Schlüsselextraktion

Einstufige Seitenkanal-Analysen beinhalten Methoden, die bei Vorliegen von instantanen Observablen einer Implementierung zur direkten Anwendung geeignet sind. Eine erste Klassifizierung von Methoden führt auf

- einfache Seitenkanal-Analysen (z.B. *Simple Power Analysis (SPA)* [KJJ99] und *Simple Electromagnetic Analysis (SEMA)* [GMO01]) und
- differentielle Seitenkanal-Analysen (z.B. *Differential Power Analysis (DPA)* [KJJ99], *Differential Electromagnetic Analysis (DEMA)* [GMO01] oder auch die Detektion von partiellen Kollisionen im Krypto-Algorithmus [SWP03]).

3.1.1 Einfache Seitenkanal-Analysen

Einfache Seitenkanal-Analysen nutzen direkte Schlüsselabhängigkeiten aus, die in den Observablen nachweisbar sind, und sind besonders bei Implementierungen von asymmetrischen Krypto-Algorithmen relevant. Beispielsweise kann in Abhängigkeit eines Bits des geheimen Schlüssels eine zusätzliche Operation implementiert sein. Bei derart offensichtlichen Schwachstellen reicht unter Umständen eine einzige Messung aus, um den geheimen Schlüssel zu kompromittieren. Ein klassisches Beispiel hierfür ist eine ungeschützte Implementierung der (modularen) Exponentiation (Abb. 3).

Falls die Multiplikation in Schritt 2.2 in Abb. 3 von der Quadrierung in Schritt 2.1 anhand einer Messung unterscheidbar ist (z.B. durch die zeitliche Dauer oder durch Mustererkennung), so ist der Exponent e direkt ablesbar. Handelt es sich beispielsweise um einen geheimen Exponenten bei einer RSA basierten digitalen Signatur, so ist hierdurch der private Schlüssel bereits kompromittiert. In dem Fall, dass Rauschen in den Messdaten eine Analyse anhand *einer* Messung unterbindet, kann durch Erhöhung der Anzahl der Messungen N und Mittelwertbildung das relevante Signal trotzdem extrahiert werden. Dies ist möglich, da für das arithmetische Mittel $\overline{I_t}$ von N unabhängigen identisch verteilten Messwerten I_{t_i} einer Stichprobe mit Mittelwert μ_t und Varianz σ_t^2 sich der Erwartungswert $E(\overline{I_t}) = \mu_t$ und die Varianz $V(\overline{I_t}) = \frac{\sigma_t^2}{N}$ ergibt.

INPUT: $g \in G$ (G: endliche abelsche Gruppe mit 1 als neutralem Element) und eine positive Zahl $e = (e_t e_{t-1} \cdots e_1 e_0)_2$.
OUTPUT: g^e.
1. $A \leftarrow 1$.
For i from t downto 0 do the following:
    2.1 $A \leftarrow A \cdot A$.
    2.2 If $e_i = 1$, then $A \leftarrow A \cdot g$.
3. Return(A).

Abb. 3: : Ein Algorithmus zur Exponentiation

3.1.2 Differentielle Seitenkanal-Analysen

Differentielle Seitenkanal-Analysen werden häufig für die Analyse von Implementierungen von Blockchiffren eingesetzt. Sie erfordern Messungen mit variablen Eingangs- oder Ausgangsdaten, die als bekannt vorausgesetzt werden. In der Regel ist der Anteil des Seitenkanals in den Messgrößen klein und zudem durch Rauschen überlagert. Der Angreifer hat typischerweise kein Vorwissen über die Art und die Zeitpunkte von Seitenkanälen. Die Auswertung erfolgt daher mittels statistischer Signifikanztests, die auf statistische Unabhängigkeit zwischen den Messdaten im vermuteten Bereich der kryptographischen Operation und dem Ergebnis einer Auswahlfunktion prüfen. Auswahlfunktionen (*selection functions* oder auch *partitioning functions*) beziehen sich auf ein Zwischenergebnis im Krypto-Algorithmus, das sowohl eine Funktion der bekannten Eingangs- oder Ausgangsdaten als auch eines Teilschlüssels ist. Die Wahl der Teilschlüssel und der Auswahlfunktion ist stets spezifisch für den Krypto-Algorithmus und wird im folgenden näher erläutert am Beispiel des *Advanced Encryption Standard* (AES).

Teilschlüssel: Bei Blockchiffren mit einer wiederholt angewendeten Rundenfunktion werden für jede Iteration Rundenschlüssel verwendet. Beim AES handelt es sich um 128-bit Rundenschlüssel. Der Schlüsselraum eines Teilschlüssels wird bei differentiellen Seitenkanal-Analysen vollständig geprüft, so dass in der Praxis hierdurch eine Begrenzung des Schlüsselraums auf etwa 2^{16} eintritt. Zur Definition von Teilschlüsseln eignen sich insbesondere die Bearbeitungsschritte in der ersten oder letzten Iteration der Rundenfunktion, in denen der Rundenschlüssel mit den bekannten Daten verknüpft wird. Beim AES setzt sich der 8-bit Eingang einer S-Box aus der XOR-Verknüpfung von bekannten Bits des Klartextes (oder des Chiffrates) und unbekannten Rundenschlüsselbits zusammen. Es sind somit sechzehn disjunkte Unterräume mit je 8 Bit Teilschlüssel naheliegend. Aus den Teilschlüsseln kann der gesamte Rundenschlüssel zusammengesetzt werden. Die Kompromittierung eines Rundenschlüssels hat eine weitreichende Kompromittierung des gesamten Schlüssels zur Folge. Beim AES-128 ist der gesamte Schlüssel direkt kompromittiert; beim AES-192 und AES-256 bleiben 64 bzw. 128 Bit unbekannt, die durch Anwendung der differentiellen Seitenkanal-Analyse auf die nächste Iteration bestimmt werden können.

Auswahlfunktionen: Oft beinhalten Auswahlfunktionen nichtlineare Funktionen der Rundenfunktion; z.B. wird ein Bit am Ausgang einer S-Box beim AES als Auswahlfunktion definiert. Die AES S-Box bildet 8-Bit Eingangsdaten auf 8-Bit Ausgangsdaten ab. Hier

ergeben sich pro S-Box acht 1-Bit Auswahlfunktionen am S-Box Ausgang. Nichtlineare Boolesche Funktionen sind für Seitenkanal-Analysen günstig, da die Ergebnisse der Auswahlfunktion dann für falsche Hypothesen des Teilschlüssels wenig mit den Ergebnissen für den richtigen Teilschlüssel korrelieren. Für den richtigen Teilschlüssel ist das vorhergesagte Teilergebnis jedoch stets auch während der dazugehörigen Messung aufgetreten, sofern keine algorithmischen Gegenmaßnahmen implementiert sind (s. Abschnitt 3.3). Eine möglichst optimale Wahl von geeigneten Auswahlfunktionen berücksichtigt auch die Architektur der Implementierung. Hierbei kann als Auswahlfunktion das Hamminggewicht am S-Box Ausgang (die Anzahl der Ausgangsbits der S-Box mit Wert '1') günstig sein. Das Hamminggewicht-Modell ist von Vorteil, wenn sich die bitweisen Seitenkanäle "ähnlich verhalten" und sich die simultane Seitenkanal-Information einzelner Datenbits verstärkt (und nicht etwa gegenseitig vermindert). Mit einem Hamminggewicht-Modell sind auch lineare Funktionen der Rundenfunktion als Auswahlfunktion verwendbar [LSP04].

Statistische Signifikanztests: Wenn die Implementierung bezüglich der Auswahlfunktion einen Seitenkanal erzeugt, so kann dies anhand statistischer Signifikanztests nachgewiesen werden. Statistische Signifikanztests verwenden die Messdaten $I_t(x_m, k)$ eines diskretisierten Zeitintervalls $t \in [t_0, \cdots, t_s]$ basierend auf den bekannten Eingangs- oder Ausgangsdaten x_m ($m \in \{1, \cdots, N\}$) und dem verwendeten Schlüssel k sowie das Ergebnis der Auswahlfunktion $d(x_m, i)$ mit allen Hypothesen i für einen $n - Bit$ Teilschlüssel mit $0 \leq i < 2^n$. Gängige statistische Tests sind hierbei der T-Test sowie die Korrelationsmethode (siehe auch [AO]).

Bei dem T-Test wird auf Unterschiede im Erwartungswert in Abhängigkeit von $d(x_m, i)$ geprüft. Handelt es sich um eine 1-Bit Auswahlfunktion, so gibt es zwei mögliche Werte von $d(x_m, i)$: '0' und '1'. Für jede Hypothese i werden die N Einzelmessungen entsprechend $d(x_m, i)$ in zwei Stichproben der Mächtigkeit $N_{i,0}$ und $N_{i,1}$ mit $N = N_{i,0} + N_{i,1}$ sortiert. Es sei $\overline{I_{t,i,0}}$ der empirische Mittelwert und $S^2_{t,i,0}$ die empirische Varianz für die Stichprobe mit $d(x_m, i) = 0$, $\overline{I_{t,i,1}}$ der empirische Mittelwert und $S^2_{t,i,1}$ die empirische Varianz für die Stichprobe mit $d(x_m, i) = 1$. Die Prüfgröße beim T-Test (bei gleichen Varianzen) ist

$$T_{t,i} = \frac{|\overline{I_{t,i,0}} - \overline{I_{t,i,1}}|}{S_D} \text{ mit } S_D = \sqrt{\frac{(N_{i,0}-1)S^2_{t,i,0} + (N_{i,1}-1)S^2_{t,i,1}}{N_{i,0}+N_{i,1}-2}} \sqrt{\frac{N_{i,0}+N_{i,1}}{N_{i,0}\cdot N_{i,1}}} \quad (1)$$

für alle Zeitpunkte t bei Annahme einer Normalverteilung der Messwerte. Bei $N > 200$ kann approximativ die Standard-Normalverteilung μ_P zur Bestimmung des Signifikanzniveaus α herangezogen werden. Der Ablehnbereich des Signifikanzniveaus α beim Test auf Gleichheit der Mittelwerte liegt im Intervall $(\mu_{1-\alpha/2}; \infty)$ [Rin03].

Die Korrelationsmethode berechnet den empirischen Korrelationskoeffizienten

$$R_{t,i} = \frac{\sum_m (d(x_m, i) - \overline{d(i)})\ (I_t(x_m, k) - \overline{I_t(k)})}{\sqrt{\sum_m (d(x_m, i) - \overline{d(i)})^2} \sqrt{\sum_m (I_t(x_m, k) - \overline{I_t(k)})^2}} \quad (2)$$

zwischen dem Ergebnis der Auswahlfunktion $d(x_m, i)$ und den Einzelmessungen $I_t(x_m, k)$ an allen Zeitpunkten t. Es ist $\overline{d(i)} = N^{-1} \sum_m d(x_m, i)$ und $\overline{I_t(k)} = N^{-1} \sum_m I_t(x_m, k)$. Da $d(x_m, i)$ i.d.R. nicht normalverteilt sind, ist eine Prüfgröße für statistische Signifikanz analog zum T-Test nicht direkt angebbar.

Das Ergebnis der differentiellen Seitenkanal-Analyse beinhaltet

- für jede Schlüsselhypothese die Prüfgröße an allen untersuchten Zeitpunkten, sowie
- eine Rangliste der Schlüsselhypothesen, sortiert nach dem maximalen Wert der Prüfgröße, der in dem gesamten Zeitbereich erreicht worden ist. Die Schlüsselhypothese, die den maximalen Wert erreicht hat, ist der wahrscheinlichste Kandidat der differentiellen Seitenkanal-Analyse.

Eine differentielle Seitenkanal-Analyse ist erfolgreich, wenn für den korrekten Teilschlüssel — verglichen mit allen anderen Schlüsselhypothesen — signifikant größere Werte für die Prüfgröße erreicht worden sind. Als Ergebnis erhält der Angreifer auch die Zeitpunkte der ausnutzbaren Seitenkanäle und kann weitere Optimierungen (z. B. der Auswahlfunktion) durchführen.

3.2 Zweisstufige Analysen: Profilierung und Schlüsselextraktion

Die effizientesten Methoden in der Schlüsselextraktion verwenden ein zweistufiges Angriffsmodell unter Verwendung derselben Implementierung, aber in unterschiedlicher Konfigurationen:

- eine Implementierung zur *Profilierung*, bei der der verwendete kryptographische Schlüssel (sowie Maskierungswerte im Fall von algorithmischen Gegenmaßnahmen) dem Angreifer bekannt ist, und
- eine Implementierung zur *Extraktion des Schlüssels*, bei der der kryptographische Schlüssel (sowie Maskierungswerte im Fall von algorithmischen Gegenmaßnahmen) unbekannt ist.

Die Phase der Profilierung stellt einen zusätzlichen Schritt gegenüber einstufigen differentiellen Methoden dar. Die Phase der Extraktion des Schlüssels entspricht in ihren Voraussetzungen dem Angreifermodell der einstufigen Methoden, abgesehen davon, dass der Angreifer aus der Profilierungsphase jetzt Vorwissen über die Seitenkanäle mitbringt.

3.2.1 Kumulierte Observablen: Zeit-Analysen

Die erste Veröffentlichung im Jahr 1996 [Koc96] bezog sich auf Zeitanalysen (*Timing Analysis*) einer modularen Exponentiation (Abb. 3), wie sie für die Implementierung vieler asymmetrischer Krypto-Algorithmen verwendet wird. Bei diesem Angriff wird der Exponent ausgehend vom signifikantesten Bit sukzessiv kompromittiert. Eine notwendige Voraussetzung für die Anwendung ist, dass die Implementierung variable Ausführungszeiten in Abhängigkeit von A in Abb. 3 erzeugt. Der Angreifer mißt die Ausführungszeit von N modularen Exponentiationen bei Kenntnis von g und G aus Abb. 3. Das Angriffsziel ist der Exponent e. Ferner wird vorausgesetzt, dass der Angreifer ein identisches Krypto-Modul oder einen Simulator für die Profilierung zur Verfügung hat, womit sich Laufzeiten beliebig gewählter Werte für g, e und G bestimmen lassen. Sind bereits n Bits des Exponenten e bekannt, gibt es zwei Hypothesen für das nächste Bit des Exponenten: '0' oder '1'. Der Test an dem Krypto-Modul zur Profilierung ist folgendermaßen: Für beide Hypothesen wird der Exponent geladen, der sich aus der Konkatenation der bisher bekannten n Bits des Exponenten und der jeweiligen Hypothese zusammensetzt. Für die Laufzeitbestimmung werden für beide Exponenten jeweils dieselben Werte für g und G wie bei der Implementierung zur Schlüsselextraktion verwendet. Die untersuchte Meßgröße ist

die Differenz zwischen der Laufzeit der Implementierung zur Schlüsselextraktion und der Laufzeit der Implementierung zur Profilierung. Der Angreifer entscheidet sich zugunsten der Hypothese, bei der die Varianz dieser Meßgröße minimal wird. Diese Strategie wird dadurch verständlich, dass es im korrekten Fall eine längere Übereinstimmung der Werte von A in Abb. 3 gibt und die Laufzeiten der einzelnen Operationen in Schritt 2.1 und 2.2 von Abb. 3 statistisch unabhängig sind.

Zu Beginn des Jahres 2005 gab es einen viel beachteten Angriff, der Zeitunterschiede bei Cache-Zugriffen einer OpenSSL AES-Implementierung ausnutzt [Ber]. Cache-Speicher ermöglichen schnellere Zugriffszeiten auf Dateninhalte, dagegen können konstante Zugriffszeiten nicht garantiert werden, sofern keine Kontrolle der Cache-Strategie durch den Anwendungsentwickler möglich ist. Die Variation der Zugriffszeiten auf Adressen der AES S-Box ist der Grundgedanke für dieses Angriffsszenario. Konkreter, im Rahmen der Profilierung werden die Ausführungszeiten des AES in Abhängigkeit der 2^8 möglichen Eingangswerte einer S-Box in der ersten Runde empirisch festgestellt. In der Extraktionsphase wird diese Zeitverteilung ebenfalls empirisch gewonnen und durch Vergleich mit der Zeitverteilung aus der Profilierungsphase kann der AES-Schlüssel byteweise zugeordnet werden. Dies ist möglich, da der S-Box Eingang sich aus der XOR-Verknüpfung eines dem Angreifer bekannten Bytes des Klartextes und eines Schlüsselbytes ergibt.

3.2.2 Instantane Observablen: Templates und das stochastische Modell

Bei instantan messbaren Observablen ist die Verwendung von *Templates* [CRR02] die theoretisch effizienteste Methode in der Extraktionsphase. In der Profilierungsphase wird für jeden Teilschlüssel i (bzw. für jede Operation i) eine multivariate, normalverteilte Wahrscheinlichkeitsdichte der Observablen empirisch bestimmt. Diese multivariate Wahrscheinlichkeitsdichte bezieht M ausgewählte Zeitpunkte ein, an denen signifikante Unterschiede im Erwartungswert für verschiedene Teilschlüssel (z. B. mit dem T-Test) nachzuweisen sind. Als Schablone (*Template*) für den Teilschlüssel i wird hierbei die Kombination aus dem M-dimensionalen Vektor der empirischen Mittelwerte $\vec{I_{t,i}}$ und der Kovarianzmatrix C_i des Rauschvektors $\vec{z_m} = \vec{I_{t,i,m}} - \vec{I_{t,i}}$ mit $m \in 1, \cdots, N$ bezeichnet. Die multivariate Wahrscheinlichkeitsdichte eines Rauschvektors $\vec{z}$ für die Schlüsselhypothese i ist

$$f_{C_i}(\vec{z}) = \frac{1}{\sqrt{(2\pi)^M \det C_i}} e^{-\frac{1}{2}\vec{z}^T C_i^{-1} \vec{z}} \quad . \tag{3}$$

Die Entscheidungsstrategie bei der Schlüsselextraktion erfolgt mit Hilfe der Templates. Es wird zugunsten derjenigen Schlüsselhypothese entschieden, für die die multivariate Wahrscheinlichkeitsverteilung den Maximalwert erreicht (*Maximum-Likelihood* Schätzer). Templates sind besonders relevant zur Anwendung bei Stromchiffren, bei denen u.U. eine einzige Messung für die Bestimmung des Schlüssels ausreichen muß.

Das stochastische Modell [SLP05] stellt eine alternative Methode zu Templates dar. Eine Observable I_t wird hier als stochastische Variable aufgefasst, die sich aus einem deterministischen Anteil $h_t(x, k)$ als Funktion eines Teilschlüssels k und der bekannten Eingangs- oder Ausgangsdaten x und Rauschen R_t zusammensetzt: $I_t = h_t(x, k) + R_t$. Die Profilierung des Seitenkanals findet hier in einem ausgewählten Untervektorraum statt, der z.B. durch einzelne Bits von Auswahlfunktionen aufgespannt wird. Hierdurch wird erreicht, dass nicht alle Teilschlüssel in die Profilierung einbezogen werden müssen, sondern ein bis

zwei Teilschlüssel ausreichend sein können, was gegenüber der Template-Methode in der Anwendung bei Blockchiffren von Vorteil ist, wenn beispielsweise nur ein Testschlüssel in der Profilierungsphase verfügbar ist und die Anzahl der Messungen N eher gering ist. Der deterministische Anteil $h_t(x, k)$ wird approximiert durch das Lösen des überbestimmten linearen Gleichungssystems in dem ausgewählten Untervektorraum unter Verwendung der N Einzelmessungen.

Die Schlüsselextraktion beim stochastischen Modell erfolgt entweder mit einem Minimum-Prinzip, das nur den deterministischen Anteil des Seitenkanals berücksichtigt, oder, analog zu den Templates, mittels des *Maximum-Likelihood* Prinzips unter Verwendung der approximierten multivariaten Wahrscheinlichkeitsdichte. Für das Maximum-Likelihood Prinzip wird eine weitere disjunkte Stichprobe von Einzelmessungen in der Profilierungsphase für das Schätzen der Kovarianzmatrix benötigt. Während das stochastische Modell eine Approximierung in einem niedrig dimensionierten Untervektorraum vornimmt, arbeitet das Template-Modell mit der empirisch bestimmten Wahrscheinlichkeitsdichte. In der Extraktionsphase ist die Effizienz des stochastischen Modells somit durch das Template-Modell begrenzt.

3.3 Analysen bei Gegenmaßnahmen

Gegenmaßnahmen können algorithmischer und nicht-algorithmischer Natur sein. Algorithmische Gegenmaßnahmen zielen darauf ab, die Vorhersagbarkeit von Zwischenergebnissen in einem Krypto-Algorithmus durch den Einsatz von (pseudo-)zufälligen Maskierungswerten zu unterbinden. Algorithmische Gegenmaßnahmen können somit eine einstufige differentielle Analyse erschweren oder sogar verhindern. Nicht-algorithmische Gegenmaßnahmen bewirken primär eine Unterdrückung der Seitenkanäle in den Observablen. Es handelt sich hierbei um interne zeitliche De-Synchronisation von Ereignissen, spezielle Abschirmung der kritischen Bauteile des Krypto-Moduls oder Ersetzen der Standard-CMOS Logik durch Gatter, die auf einen datenunabhängigen Stromverbrauch optimiert sind. Die Entwicklung und Analyse der Wirksamkeit von Gegenmaßnahmen ist weiterhin ein hochaktuelles Forschungsgebiet.

Differentielle Analyse zweiter Ordnung (*Second-Order DPA*) [Mes00, WW04] ist als eine Methode vorgeschlagen worden, um trotz Verwendung von Maskierungswerten differentielle Methoden speziell bei Blockchiffren wieder anwenden zu können. Differentielle Methoden zweiter Ordnung verknüpfen zwei Zeitpunkte, an denen Maskierungswerte in die Berechnung eingehen, bevor diese mit differentieller Seitenkanal-Analyse bearbeitet werden. Als Verknüpfungsoperation ist die Multiplikation oder Subtraktion der Messdaten an den zwei Zeitpunkten vorgeschlagen worden. Ohne Kenntnis der Implementierung sind die relevanten Zeitpunkte dem Angreifer nicht bekannt. In diesem Fall hat das für einen systematischen Test zur Folge, dass eine differentielle Seitenkanal-Analyse für alle möglichen Zeitdifferenzen durchzuführen ist.

Durch die Reduktion von zwei Messwerten auf einen Messwert verlieren differentielle Methoden zweiter Ordnung Information. Templates und das stochastische Modell sind hier überlegen, da sie stets mehrere Zeitpunkte berücksichtigen. Bei algorithmischen Gegenmaßnahmen ergibt sich jedoch auch bei Templates und dem stochastischen Modell ein stark erhöhter Aufwand, da die Anzahl der zu jetzt zu profilierenden Zwischenergebnisse

sich als Produkt der Anzahl möglicher Teilschlüssel und der Anzahl möglicher Maskierungswerte ergibt.

4 Prüfkriterien

Bei der Vielzahl der bekannten Methoden wird es immer wichtiger, anerkannte, geeignete Testverfahren für Seitenkanal-Analysen zu finden, die auch effizient durchführbar sind. In diesem Abschnitt möchten wir eine Diskussion über Prüfkriterien von Seitenkanal-Analysen initiieren. Auch wenn in vielen Krypto-Modulen bereits Gegenmaßnahmen implementiert sind und in der öffentlichen Literatur Seitenkanal-Angriffe zumeist nur unter Laborbedingungen demonstriert sind, stellen Seitenkanal-Analysen doch weiterhin eine reale Bedrohung für kryptographische Implementierungen dar. Diese Relevanz ist auch daran zu erkennen, dass Informationsverlust durch Seitenkanäle im Rahmen von Evaluierungsschemata wie Common Criteria bei Krypto-Modulen als eine potentielle Schwachstelle angesehen wird. Bei höheren Prüftiefen sind für den Nachweis der Resistenz gegen Seitenkanal-Angriffe auch praktische Tests erforderlich.

Tests bezüglich Seitenkanälen sollten Aussagen über die Mess-Apparatur, die Informationsbasis, die eingesetzte Methodik, die Anzahl der Messungen und die Signifikanz der Ergebnisse bezogen auf den konkreten Einsatzbereich des Krypto-Moduls liefern. Diese Punkte werden anschließend einzeln näher erläutert.

Mess-Apparatur: Die Mess-Apparatur ist entscheidend für die Qualität der Messung der Observablen und für die Effizienz der Seitenkanal-Analyse. Rauschen kann in externes Rauschen, intrinsisches Rauschen, Quantisierungsrauschen, und algorithmisches Rauschen differenziert werden [MDS99]. Intrinsisches Rauschen und algorithmisches Rauschen wird von dem Messobjekt selbst erzeugt und kann durch die Mess-Apparatur praktisch nicht reduziert werden. Dagegen wird externes Rauschen von externen Quellen, eventuell auch von der Mess-Apparatur, eingestreut, und Quantisierungsrauschen wird hervorgerufen durch den Analog-Digital Wandler der Mess-Apparatur. Eine störungsarme Signaltechnik und Abschirmung des Mess-Prozesses gegenüber externen Störquellen trägt zur Reduzierung des externen Rauschens bei.

Informationsbasis: Hierunter fällt das konkrete Angriffsmodell. Der Test kann in Form einer *White-Box* Analyse durchgeführt werden, bei der alle Konstruktionsdetails bekannt sind, oder in Form einer *Black-Box* Analyse, bei der Internas der Implementierung unbekannt sind. Die Abstufungen dazwischen können fließend sein. Die Bedeutung von offenen Testbedingungen wird dadurch unterstrichen, dass durch privilegierte Testmethoden Schwachstellen nachgewiesen werden können (z. B. [ARRS05, MPO05]), welche in einem nicht-privilegierten Testmodell nicht detektierbar sind. Bei den Testbedingungen ist auch sicherzustellen, dass der relevante Zeitbereich bei instantanen Observablen zweifelsfrei identifiziert wird. Dies ist bei *White-Box* Analysen relativ einfach möglich; bei *Black-Box* Analysen kann es jedoch zu einem erheblichen Mehraufwand führen.

Methodik: Erste Aussagen über eine mögliche Anfälligkeit gegenüber Informationsverlust durch Seitenkanäle sind schon im Rahmen des Entwurfs möglich, z.B. anhand der Beschreibung der Implementierung eines Krypto-Algorithmus. Aussagen aufgrund der Spezifikation betreffen zunächst die Zeitdauer der Implementierung, wenn beispielsweise die Anzahl der Elementaroperationen direkt eine Funktion von Schlüsselbits ist.

Daneben kann zu diesem Zeitpunkt auch schon eine Schwachstellenanalyse erfolgen, die in nachfolgenden Tests geprüft werden kann. Bei *White-Box* Testbedingungen kann ausgehend von einer Schwachstellenanalyse der Implementierung der Einsatz von geeigneten Analysemethoden getroffen werden. Gerade bei *Black-Box* Analysen ist es jedoch wichtig, einen umfassenden Test mit bekannten Angriffsszenarien durchzuführen. Hierfür ist eine geeignete Zusammenstellung von publizierten Angriffsszenarien für verschiedene Krypto-Algorithmen erforderlich, wie sie beispielsweise unter [SCC] zu finden ist. Wir plädieren für offene Testbedingungen, da sie eine höhere Verläßlichkeit für den Testumfang und die Testergebnisse geben und sie zudem den Testaufwand beträchtlich reduzieren können.

Anzahl der Messungen: Die Anzahl der Messungen N ist ein wichtiger Sicherheitsparameter bei Seitenkanal-Analysen. Praktische Analysen mit einer Million Messungen sind bereits durchgeführt worden [MPO05]. Bei zweistufigen Analysen bezeichnet N die Summe der Anzahl der Messungen in beiden Phasen. Die Anzahl der Messungen in der Profilierungsphase ist jedoch weitaus höher als in der Extraktionsphase, so dass in guter Approximation hier N als die Anzahl der Messungen in der Profilierungsphase verwendet werden kann. Die Anzahl der Messungen geht als Parameter in die Signifikanz der Prüfgrößen ein. Die Prüfgröße beim T-Test ist asymptotisch proportional zu $\sqrt{N}$ (vgl. (1)); somit wird bei Erhöhung von N der Nachweis schwächerer Seitenkanäle ermöglicht.

Signifikanz der Ergebnisse: Die Resultate der Seitenkanal-Analysen sind bezüglich ihrer Signifikanz zu bewerten. Im Fall von signifikanten Ergebnissen kann im Hinblick auf die konkrete Einsatzumgebung des Krypto-Moduls auch die Betrachtung von Abstufungen im Angreifermodell relevant sein.

5 Zusammenfassung

In diesem Beitrag geben wir einen Überblick über aktuell einsetzbare Methoden bei Seitenkanal-Analysen. Es ist abschließend festzustellen, daß offenen Testbedingungen heute eine stärkere Bedeutung zukommt als noch vor einigen Jahren.

Literatur

[AO] Manfred Aigner and Elisabeth Oswald. Power Analysis Tutorial, available at http://www.iaik.tugraz.at/aboutus/people/oswald/papers/dpa_tutorial.pdf. Technical report, TU Graz.

[ARRS05] Dakshi Agrawal, Josyula R. Rao, Pankaj Rohatgi, and Kai Schramm. Templates as Master Keys. In Josyula R. Rao and Berk Sunar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2005*, volume 3659 of *LNCS*, pages 15–29. Springer-Verlag, 2005.

[Ber] Daniel J. Bernstein. Cache-timing attacks on AES, available at http://cr.yp.to/antiforgery/cachetiming-20050414.pdf. Technical report.

[CRR02] Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi. Template attacks. In B. S. Kaliski, Ç Koç, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2002*, volume 2523 of *LNCS*, pages 13–28. Springer-Verlag, 2002.

[GMO01] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic analysis: Concrete results. In Ç Koç, D. Naccache, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2001*, volume 2162 of *LNCS*, pages 251–261. Springer-Verlag, 2001.

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In M. Wiener, editor, *Advances in Cryptology – CRYPTO '99*, volume 1666 of *LNCS*, pages 388–397. Springer-Verlag, 1999.

[Koc96] Paul C. Kocher. Timing Attacks on Implementations of Diffie–Hellman, RSA, DSS, and Other Systems. In N. Koblitz, editor, *Advances in Cryptology – CRYPTO '96*, volume 1109 of *LNCS*, pages 104–113. Springer-Verlag, 1996.

[LSP04] Kerstin Lemke, Kai Schramm, and Christof Paar. DPA on n-Bit Sized Boolean and Arithmetic Operations and Its Application to IDEA, RC6, and the HMAC-Construction. In M. Joye and J.-J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, volume 3156 of *LNCS*, pages 205–219. Springer-Verlag, 2004.

[MDS99] Thomas S. Messerges, Ezzy A. Dabbish, and Robert H. Sloan. Investigations of power analysis attacks on smartcards. In *Proceedings of USENIX Workshop on Smartcard Technology*, pages 151–162, 1999.

[Mes00] Thomas S. Messerges. Using Second-Order Power Analysis to Attack DPA Resistant Software. In Ç.K. Koç and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2000*, volume 1965 of *LNCS*, pages 238–251. Springer-Verlag, 2000.

[MPO05] Stefan Mangard, Norbert Pramstaller, and Elisabeth Oswald. Successfully Attacking Masked AES Hardware Implementations. In Josyula R. Rao and Berk Sunar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2005*, volume 3659 of *LNCS*, pages 157–171. Springer-Verlag, 2005.

[PPS+04] Christof Paar, Jan Pelzl, Kai Schramm, André Weimerskirch, and Thomas Wollinger. Eingebettete Sicherheit: State-of-the-art. In Patrick Horster, editor, *D.A.CH Security 2004*, 2004.

[Rin03] Horst Rinne. *Taschenbuch der Statistik*. Verlag Harri Deutsch, 2003.

[SCC] Side Channel Cryptanalysis Lounge, available at http://www.crypto.rub.de/en_sclounge.html.

[SLP05] Werner Schindler, Kerstin Lemke, and Christof Paar. A Stochastic Model for Differential Side Channel Cryptanalysis. In Josyula R. Rao and Berk Sunar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2005*, volume 3659 of *LNCS*, pages 30–46. Springer-Verlag, 2005.

[SWP03] Kai Schramm, Thomas Wollinger, and Christof Paar. A New Class of Collision Attacks and Its Application to DES. In Thomas Johansson, editor, *Fast Software Encryption — FSE 2003*, volume 2887 of *LNCS*, pages 206–222. Springer-Verlag, 2003.

[WW04] Jason Waddle and David Wagner. Towards Efficient Second-Order Power Analysis. In M. Joye and J.-J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, volume 3156 of *LNCS*, pages 1–15. Springer-Verlag, 2004.