

Vorlesung Sicherheit

Dennis Hofheinz

ITI, KIT

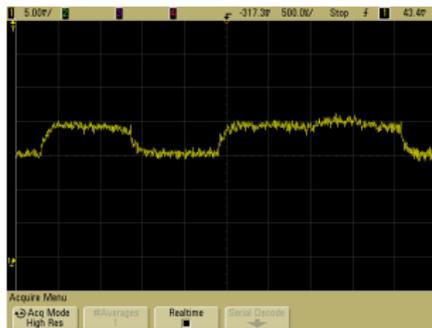
13.07.2017

- 1 **Einschub: Seitenkanalangriffe**
 - Simple Power Attacks (SPAs)
 - Demonstration
 - Gegenmaßnahmen gegen SPA
 - Differential Power Analysis (DPA)
 - (Weitere) Beispiele für Seitenkanäle
 - Aktive Seitenkanalangriffe
 - Theoretische Modelle
 - Zusammenfassung

- 1 **Einschub: Seitenkanalangriffe**
 - Simple Power Attacks (SPAs)
 - Demonstration
 - Gegenmaßnahmen gegen SPA
 - Differential Power Analysis (DPA)
 - (Weitere) Beispiele für Seitenkanäle
 - Aktive Seitenkanalangriffe
 - Theoretische Modelle
 - Zusammenfassung

Simple Power Attacks (SPAs)

- **Ziel:** Geheime Information, die auf Chip verarbeitet wird
 - Gespeicherter/verarbeiteter Schlüssel (DES- K , RSA- sk , ...)
 - Erzeugter Zufall (RSA-OAEP-/ElGamal-Verschlüsselung)
- **Vorgehen:** Stromverbrauchsmessung \rightarrow Trace \rightarrow Geheimnis
 - Wenn K in Algorithmus bitweise verarbeitet, dann könnte...



(Quelle: wikipedia.org)

im einfachsten Fall $K_1 = 1, K_2 = 0, K_3 = K_4 = 1, \dots$ bedeuten

- **Szenario:** RSA-Entschlüsselung (ggf. mit gepaddetem M)

$$M = C^d \bmod N$$

- Gängige Implementierung mit Square-and-Multiply:

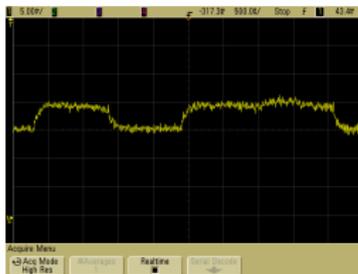
- 1 write $d = \sum_{i=0}^{n-1} 2^i d_i$ (d.h. d_i i -tes Bit von d)
- 2 let $x := C, z := 1$ (x Hilfsvariable, z Zwischenergebnis)
- 3 for i from 0 to $n - 1$
 - 1 if $d_i = 1$ then
$$z := z \cdot x \bmod N$$
 - 2 $x := x^2 \bmod N$ ($x = C^{2^i} \bmod N$ vor diesem Schritt)
- 4 return $M := z = C^d \bmod N$

Beispiel einer SPA

- **Szenario:** RSA-Entschlüsselung mit Square-and-Multiply

$$M = C^d \bmod N$$

- Beobachtungen:
 - d wird bitweise abgearbeitet
 - Im i -ten Schleifendurchlauf $1 + d_i$ modulare Multiplikationen
- Deshalb:



bedeutet hier $d_0 = 0$, $d_1 = 1$ (wenn dies der Anfang ist)

1 Einschub: Seitenkanalangriffe

- Simple Power Attacks (SPAs)
- **Demonstration**
- Gegenmaßnahmen gegen SPA
- Differential Power Analysis (DPA)
- (Weitere) Beispiele für Seitenkanäle
- Aktive Seitenkanalangriffe
- Theoretische Modelle
- Zusammenfassung

- **Demonstration:** Messung der Abstrahlung eines FPGA bei Zufallserzeugung

1 Einschub: Seitenkanalangriffe

- Simple Power Attacks (SPAs)
- Demonstration
- **Gegenmaßnahmen gegen SPA**
- Differential Power Analysis (DPA)
- (Weitere) Beispiele für Seitenkanäle
- Aktive Seitenkanalangriffe
- Theoretische Modelle
- Zusammenfassung

Gegenmaßnahmen gegen SPA

- Hardware-Gegenmaßnahmen:
 - Elektromagnetische/akustische Abschirmung
 - Stromverbrauch/Laufzeit konstant halten
- Algorithmische Gegenmaßnahmen:
 - Konkreten Ablauf (bis auf Ausgabe) unabhängig von Geheimnis gestalten
 - Zufällige Störungen/Operationen einbauen
- Leider viele unveröffentlichte und ad-hoc-Methoden
- **Aber:** aktuelle Chipkarten gegen SPA unanfällig

1 Einschub: Seitenkanalangriffe

- Simple Power Attacks (SPAs)
- Demonstration
- Gegenmaßnahmen gegen SPA
- **Differential Power Analysis (DPA)**
- (Weitere) Beispiele für Seitenkanäle
- Aktive Seitenkanalangriffe
- Theoretische Modelle
- Zusammenfassung

Differential Power Analysis (DPA)

- DPA: Verbesserung von/Alternative zu SPA
- DPA hat höhere Anforderungen als SPA:
 - Implementierung muss (bis auf Schlüssel) bekannt sein
 - Viele Traces benötigt
- DPA hat einige Vorteile gegenüber SPA:
 - Geheimnis muss nicht bitweise abgearbeitet werden
 - (Fast) beliebige Korrelationen zwischen Geheimnis und Seitenkanal nutzbar
 - Auch „gröbere“ Seitenkanäle wie Laufzeit nutzbar

- Annahme: viele Traces T_X (für Eingaben X) gegeben, dann:
 - 1 Rate ersten Teil s von Geheimnis S , der benutzt wird
 - 2 Verifiziere Korrektheit von s wie folgt:
 - 1 Simuliere (mit geratenem s) System für alle X , soweit möglich
 - 2 Gruppiere Eingaben X nach *simuliertem* Stromverbrauch

$\mathcal{L} := \{X \mid \text{Simulation mit } X \text{ hat niedrigen Stromverbrauch}\}$

$\mathcal{H} := \{X \mid \text{Simulation mit } X \text{ hat hohen Stromverbrauch}\}$

- 3 Betrachte durchschnittlichen *realen* Stromverbrauch:

$$T_{\mathcal{L}} := \mathbf{E}_{X \in \mathcal{L}}(T_X) \qquad T_{\mathcal{H}} := \mathbf{E}_{X \in \mathcal{H}}(T_X)$$

- 4 Wenn $T_{\Delta} := T_{\mathcal{H}} - T_{\mathcal{L}}$ „groß“, dann richtiges s gefunden

- Naive Implementierungen von DES, RSA, ... angreifbar
 - Laufzeitbetrachtung (ein Wert pro Eingabe) reicht aus
- Gegenmaßnahmen wie bei SPA, und mehr:
 - „Blinding“: wähle zufälliges R und berechne M als

$$M = C^d = (R \cdot C)^d / R^d \text{ mod } N$$

- Gängige Chipkarten berücksichtigen DPA

- 1** **Einschub: Seitenkanalangriffe**
 - Simple Power Attacks (SPAs)
 - Demonstration
 - Gegenmaßnahmen gegen SPA
 - Differential Power Analysis (DPA)
 - (Weitere) Beispiele für Seitenkanäle**
 - Aktive Seitenkanalangriffe
 - Theoretische Modelle
 - Zusammenfassung

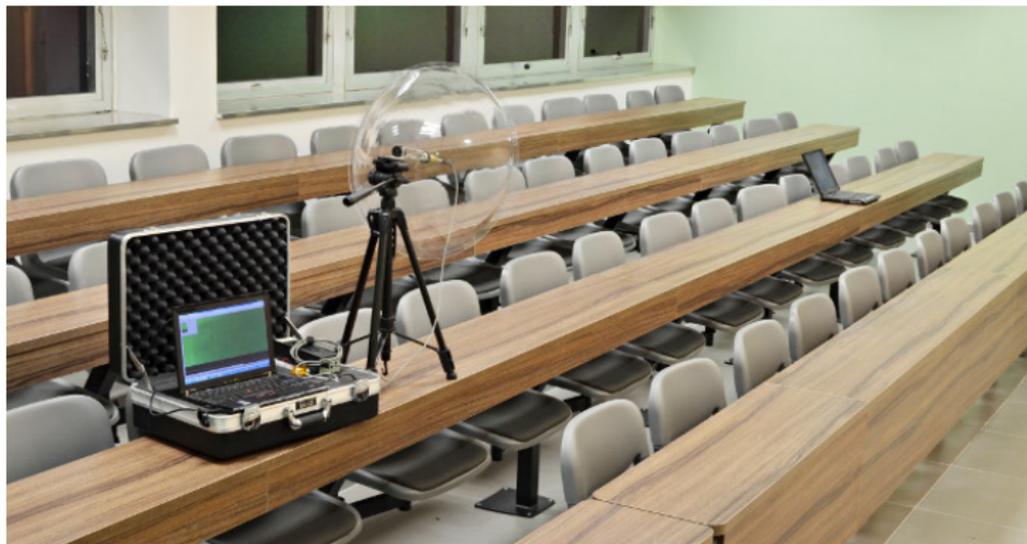
(Weitere) Beispiele für Seitenkanäle

- Stromverbrauch (abgelesen über andere Wege, z.B. Berührung, Messung des elektrischen Potentials)
- Elektromagnetische Abstrahlung
- Gesamtlaufzeit eines Algorithmus („Timing-Attack“)
- Temperatur (möglicherweise. . .)
- ...

Demonstration: Radio & Bildschirm(kabel-)abstrahlung
Quelle: <http://www.erikyyy.de/tempest/>

- Akustische Abstrahlung
- Extrahiere RSA-Schlüssel durch Rechnergeräusche (Ultraschall)
- Quelle der folgenden Bilder:
<http://tau.ac.il/~tromer/acoustic/>
 - Daniel Genkin, Adi Shamir (bekannt von RSA), Eran Tromer et al.

Akustische Abstrahlung



Akustische Abstrahlung

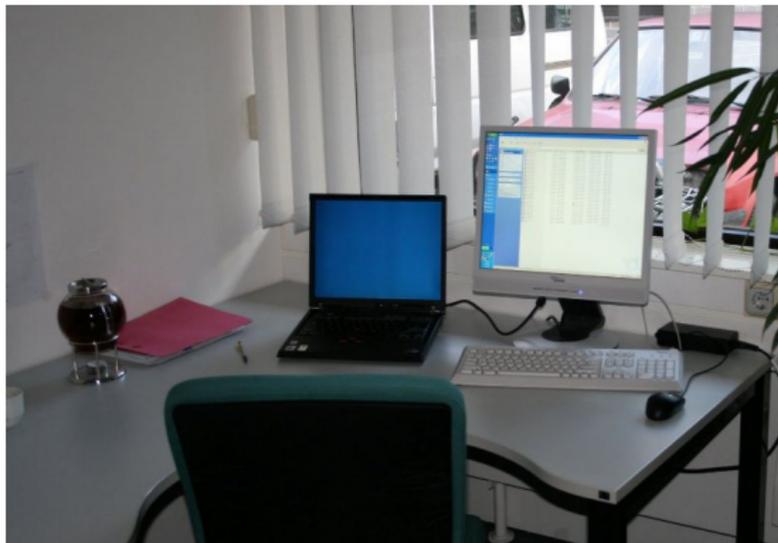
- Geht auch ohne Richtmikro:



Demonstration: Wie klingt das? (für uns eigentlich nicht hörbar, heruntermoduliert)

Ein exotischer Seitenkanal

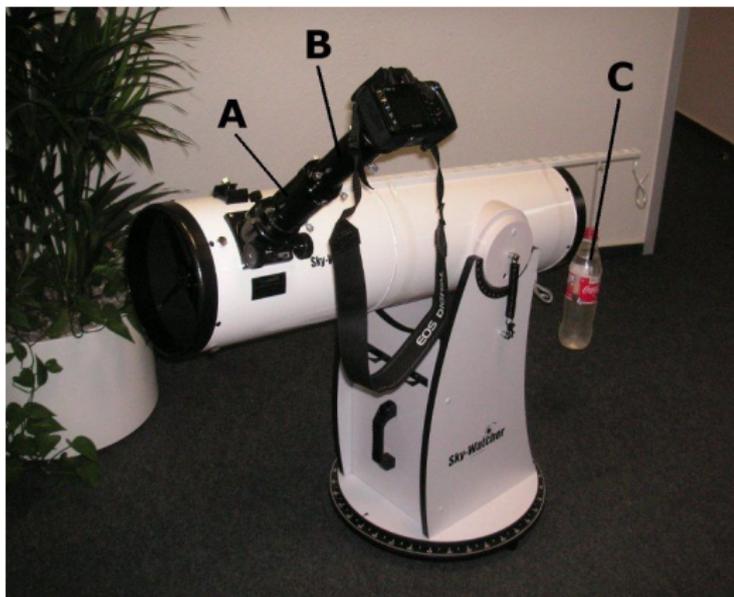
- **Idee:** nutze Lichtreflektionen aus



(Quelle der folgenden Bilder: Backes, Dürmuth, Unruh: „Compromising Reflections – or – How to Read LCD Monitors Around the Corner“)

Ein exotischer Seitenkanal

- Angriffswerkzeug:



Ein exotischer Seitenkanal

- **Angriffsbeispiele:**



Ein exotischer Seitenkanal

- **Angriffsbeispiele:**



- **Angriffsbeispiele:**



Ein exotischer Seitenkanal

- Angriffsbeispiele:



Eine exotische Gegenmaßnahme



Aber: Snowden...? (Dokumentation „Citizen Four“)

1 Einschub: Seitenkanalangriffe

- Simple Power Attacks (SPAs)
- Demonstration
- Gegenmaßnahmen gegen SPA
- Differential Power Analysis (DPA)
- (Weitere) Beispiele für Seitenkanäle
- **Aktive Seitenkanalangriffe**
- Theoretische Modelle
- Zusammenfassung

- **Idee:** manipulierte System auf physikalischem Weg
 - Gewinne dadurch Information über Geheimnis in System
- **Beispiel 1:** Angriff auf CRT-RSA
- **Beispiel 2:** Cold Boot Attacks

(Aktiver) Angriff auf CRT-RSA

- System berechnet $M_P = C^d \bmod P$ und $M_Q = C^d \bmod Q$, setzt $M \bmod N$ mit Chinesischem Restsatz zusammen
- Realistisch, weil viel effizienter als direkte Rechnung $\bmod N$
- **Angriff:** störe *nur* Berechnung von M_P (nicht aber von M_Q)
- Für gestörtes \widetilde{M} gilt $\widetilde{M} \neq C^d \bmod P$ und $\widetilde{M} = C^d \bmod Q$
- Zusammen mit echtem (ungestörtem) M gilt

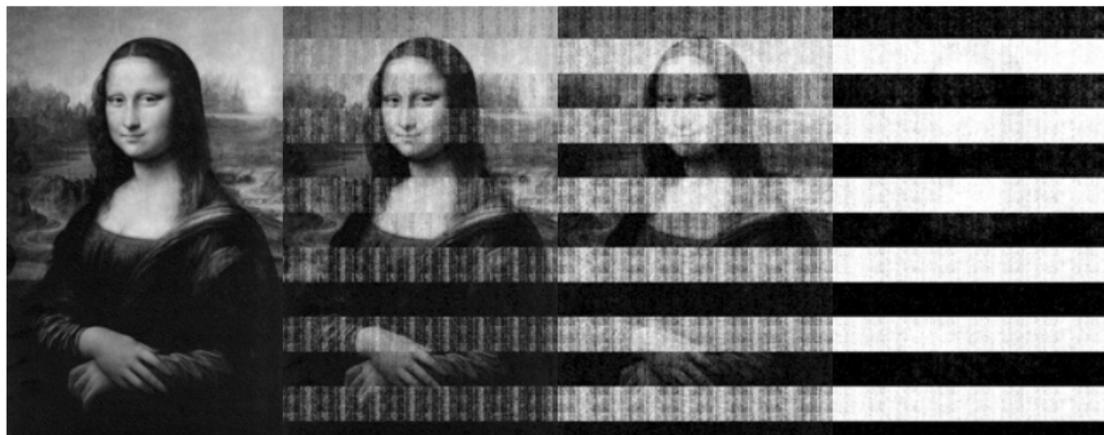
$$\widetilde{M} - M \neq 0 \bmod P \quad \text{und} \quad \widetilde{M} - M = 0 \bmod Q$$

- Also nur Q Teiler von $\widetilde{M} - M$, deshalb $\gcd(\widetilde{M} - M, N) = Q$

- **Ziel:** Festplattenverschlüsselung brechen
- **Überblick Festplattenverschlüsselung:** (vereinfacht)
 - Gesamte Festplatte (symmetrisch) verschlüsselt
 - Bei Start/Aufwachen Frage nach Schlüssel K
 - Während Betrieb K im Hauptspeicher
- **Grobe Idee des Angriffs:**
 - 1 Festplatten-verschlüsseltes Notebook stehlen
 - 2 Notebook ausschalten (Akku raus, kein Herunterfahren)
 - 3 Hauptspeicher ausbauen und auslesen $\rightarrow K$
(Alternativ: extern booten, und Hauptspeicher auslesen)

Cold Boot Attacks

- **Problem:** ausgebauter Hauptspeicher verliert Information



(Quelle: Princeton University)

- **Frage:** Wie schnell geht das?

Cold Boot Attacks

- Lösung:



(Quelle: Princeton University)

- Demonstration für BitLocker verfügbar, weitere angreifbar

1 Einschub: Seitenkanalangriffe

- Simple Power Attacks (SPAs)
- Demonstration
- Gegenmaßnahmen gegen SPA
- Differential Power Analysis (DPA)
- (Weitere) Beispiele für Seitenkanäle
- Aktive Seitenkanalangriffe
- **Theoretische Modelle**
- Zusammenfassung

- **Sind wir also physikalischen Angriffen ausgeliefert?**
- Nicht ganz:
 - Seit ≈ 2004 theoretische Modelle für Seitenkanalangriffe
 - Ziel: theoretisches Modell \Rightarrow sichere Schemata
 - Schwierigkeit: handhabbare *und* realistische Modelle finden
- Aktueller Stand:
 - Es existieren handhabbare (d.h. erfüllbare) Modelle
 - Insbesondere: symmetrische/asymmetrische Verschlüsselung
 - Es existieren realistische (von Praktikern begrüßte) Modelle
 - Allerdings sind diese nur schwer handhabbar
- Forschung: effiziente Verfahren für realistische Modelle

Beispiel für theoretisches Modell

- IND-CPA (für PKE) mit Leakage-Resilience:
 - 1 \mathcal{A} erhält pk
 - 2 \mathcal{A} wählt L , erhält $L(sk)$
 - 3 \mathcal{A} wählt $M^{(1)}, M^{(2)}$, erhält $C^* = \text{Enc}(pk, M^{(b)})$
 - 4 \mathcal{A} rät b (und gewinnt, wenn richtig geraten)
- L sollte nicht *nach* Erhalt von C^* gewählt werden
- L sollte nicht erlauben, sk zu berechnen
- Vorgesprochen: L beliebig, aber $L(sk)$ (deutlich) kürzer als sk
 - Beispiel für erlaubtes L : $L(sk) =$ „erste Hälfte von sk “
 - Schwierigkeit: Verfahren muss von L unabhängig sein
 - Für dieses Modell existieren effiziente sichere Verfahren
- Realistischer/schwieriger: L beliebig, aber *one-way*

Beispiel für theoretisches Ergebnis

- **Ziel:** „Immunisierung“ von Schaltkreisen
- **Idee:** Schaltkreis $C \rightarrow$ immunisierter Schaltkreis C'
- Passive Sicherheit möglich:
 - Sei $t \in \mathbb{N}$ vorgegeben und fest
 - Dann existiert C' , so dass die Belegung von je t beliebigen interne Bits (=„Drähte“) von C' unabhängig zufällig aussieht
- Auch aktive Sicherheit möglich (Absicherung gegen „Tampering“ von bis zu t Bits)
- Absicherungen erhöhen Größe von Schaltkreis signifikant

1 Einschub: Seitenkanalangriffe

- Simple Power Attacks (SPAs)
- Demonstration
- Gegenmaßnahmen gegen SPA
- Differential Power Analysis (DPA)
- (Weitere) Beispiele für Seitenkanäle
- Aktive Seitenkanalangriffe
- Theoretische Modelle
- Zusammenfassung

- Auf ungesicherte Systeme oft schon SPA anwendbar
- DPA flexibler, benötigt aber mehr Traces
- Vielzahl von passiven/aktiven physikalischen Angriffen möglich
 - Mehr/erweiterte Angriffe aktuell untersucht
- Theoretische Modelle/Konstruktionen aktuell diskutiert
 - Realistische/handhabbare Modelle