Cold boot attacks

Szenario: Halderman et al 2008

- Computer wird inkorrekt runtergefahren, z.B. durch AUS-Schalter.
- DRAM erhält seinen Speicherinhalt für wenige Sekunden.
- Insbesondere stehen geheime Schlüssel im DRAM.
- Massives Kühlen erhält die Speicherinhalte stundenlang.
- Prozess induziert Ausfälle und Fehler bei einzelnen Bits.
- D.h. wir benötigen einen Algorithmus zur Ausfall-/Fehlerkorrektur.
- **Ziel:** Korrekturalgorithmen für Faktorisierung (p, q).

2-adische Faktorisierung

Algorithmus 2-adische Faktorisierung

EINGABE: $N = pq$ mit Bitlänge $2n$

- FOR $i = 1$ to n bestimme $M = \{(p', q') \mid p'q' = N \bmod 2^n\}$.
- Für alle $(p', q') \in M$ mit Bitlänge jeweils n: Teste ob $p'q' = N$.

AUSGABE: p, q

Laufzeit:

- Für ungerades p' existiert $(p', q') \in M$ mit $q' = (p')^{-1}N \bmod 2^n$.
- Damit ist $|M| \geq 2^{n-1} = \Omega(\sqrt{N})$.
- D.h. 2-adische Faktorisierung ist nicht besser als triviales Raten.

Bsp: Berechne M für $165 = 11 \cdot 15$.

Heninger-Shacham Algorithmus

Szenario:

- Erhalten $\tilde{p}$ mit Bits von p und Ausfällen, z.B. $\tilde{p} = 1?0??1$.

Algorithmus Heninger-Shacham

EINGABE: $N = pq$ mit Bitlänge $2n$, Bitmaterial $\tilde{p}, \tilde{q}$.

- FOR $i = 1$ to n bestimme $M = \{(p', q') \mid p'q' = N \bmod 2^n\}$. Verwerfe solche (p', q'), die inkonsistent mit dem Bitmaterial $\tilde{p}, \tilde{q}$ sind.
- Für alle $(p', q') \in M$ mit Bitlänge jeweils n: Teste ob $p'q' = N$.

AUSGABE: p, q

Bsp: Faktorisiere $N = 10100101$ mittels $\tilde{p} = 101?$ und $\tilde{q} = 1??1$.

Satz Heninger-Shacham 2009

Sei $N = pq$ und $\tilde{p}, \tilde{q}$ beinhalten jeweils mindestens 57% der Bits, gleichverteilt über den Bitvektor. Dann kann N mit großer Ws in polynomieller Zeit faktorisiert werden.

Fehlerkorrektur

Szenario: (Henecka, May, Meurer 2010)

- Physikalische Messung liefert $\tilde{p}, \tilde{q}$ mit fehlerhaften Bits.
- Jedes Bit flippt mit bekannter Fehlerrate $\delta < \frac{1}{2}$.
- Man beachte: Für $\delta = \frac{1}{2}$ liefern $\tilde{p}, \tilde{q}$ keine Information.

Algorithmus FEHLERKORREKTUR

EINGABE: $N = pq$ mit Bitlänge $2n$, fehlerhaftes Bitmaterial $\tilde{p}, \tilde{q}$

1. Wähle t und Hamming Distanz d geeignet.
2. FOR i=1 to $\frac{n}{t}$
   1. Berechne $M = \{(p', q') \mid p'q' = N \bmod 2^{it}\}$. Verwerfe (p', q') mit Hamming-Distanz $H((p', q'), (\tilde{p}, \tilde{q})) > d$ im letzten t-Bit Fenster.
3. Für alle $(p', q') \in M$ mit Bitlänge jeweils n: Teste ob $p'q' = N$.

AUSGABE: p, q

Bsp: Faktorisiere $10100101 = 1011 \cdot 1111$ mittels $\tilde{p} = 10\mathbf{0}1$, $\tilde{q} = \mathbf{0}111$. $(t = 2, d = 1)$

Hoeffding Schranke

Wahl von t und d:

- $|M|$ soll polynomiell beschränkt sein, d.h. $t = \mathcal{O}(\log n)$.
- Korrekte Lösung p, q darf nicht verworfen werden: t und d groß.
- Wenige inkorrekte Lösungen sollen in M verbleiben: d klein.

Satz Hoeffding

Seien $X_1, \ldots, X_{2t}$ unabhängige 0,1-wertige Zufallsvariablen mit $\mathrm{Ws}[X_i = 1] = p$. Sei $X = X_1 + \ldots + X_{2t}$. Dann gilt

$$\mathrm{Ws}[|X - 2tp| \leq 2t\gamma] \leq e^{-4t\gamma^2}.$$

Erhalt der korrekten Lösung

Lemma Erhalt der korrekten Lösung

Sei $t = \frac{\ln n}{4\epsilon^2}$ für ein konstantes $\epsilon > 0$ und $d = 2t(\delta + \epsilon)$. Dann bleibt die korrekte Lösung in FEHLERKORREKTUR mit Ws $\geq 1 - \frac{1}{t}$ erhalten.

Beweis:

- Sei $p, q \bmod 2^{it}$ die korrekte partielle Lösung in Iteration i.
- In jeder Iteration vergleichen wir $2t$ Bits von p, q mit $\tilde{p}, \tilde{q}$.
- Definiere X_i als XOR der Bits in Position i für $i = 1, \ldots, 2t$.
- D.h. $X = X_1 + \ldots + X_{2t}$ bezeichnet die Anzahl verschiedener Bits.
- Jedes Bit kippt mit Ws δ, d.h. $E[X] = 2t \cdot E[X_i = 1] = 2t\delta$.
- Wir verwerfen (p, q) falls die Distanz zu $(\tilde{p}, \tilde{q})$ größer d ist.
- Nach Hoeffding Schranke geschieht dies pro Runde mit Ws

$$\text{Ws}[X > d] = \text{Ws}[X > 2t(\delta + \epsilon)] \leq e^{-4t\epsilon^2} = e^{-\ln n} = \frac{1}{n}.$$

- D.h. FEHLERKORREKTUR verwirft (p, q) nicht in $\frac{n}{t}$ Runden mit

$$\text{Ws}[\text{Erfolg}] \geq (1 - \tfrac{1}{n})^{\frac{n}{t}} \geq 1 - \tfrac{1}{t}.$$

Inkorrekte Lösungen werden eliminiert

Lemma Elimination inkorrekter Lösungen

Unter der Annahme, dass sich fehlerhafte Lösungen zufällig verhalten, werden für $t = \frac{\ln n}{4\epsilon^2}$, $d = 2t(\delta + \epsilon)$ alle inkorrekten Lösungen mit großer Ws eliminiert, sofern $\delta < \frac{1}{2}(1 - \sqrt{\ln(2)}) - \epsilon \approx 0.084 - \epsilon$.

Beweis:

- Sei (p', q') inkorrekt. Wir vergleichen $2t$ Bits von p', q' und $\tilde{p}, \tilde{q}$.
- Sei X_i eine Zufallsvariable für das XOR der Bits an Position i.
- D.h. $X = X_1 + \ldots + X_{2t}$ ist die Anzahl der verschiedenen Bits.
- Unter unserer Annahme für (p', q') gilt $E[X] = 2t \cdot E[X_i = 1] = t$.
- Wir eliminieren (p', q') nicht, falls $X \leq d$. D.h. mit

$$\text{Ws}[X \leq d] = \text{Ws}[X \leq 2t(\delta + \epsilon)] = \text{Ws}[X \leq 2t(\tfrac{1}{2} - \underbrace{(\frac{1}{2} - \delta - \epsilon)}_{\gamma})] \leq e^{-4t\gamma^2}.$$

- Falls $\gamma^2 > \frac{\ln 2}{4}$, so erhalten wir $\text{Ws}[X \leq d] < 2^{-t}$.
- D.h. alle 2^t inkorrekten Lösungen werden mit großer Ws eliminiert.
- Wir benötigen $(\frac{1}{2} - \delta - \epsilon)^2 > \frac{\ln 2}{4}$ bzw $\delta < \frac{1}{2}(1 - \sqrt{\ln(2)}) - \epsilon$.

Fehlerkorrektur bei Faktorisierung

Satz Henecka, May, Meurer 2010

Sei $N = pq$ und $\tilde{p}, \tilde{q}$ mit Fehlerrate $\delta < 0.084 - \epsilon$ behaftet. Dann faktorisiert FEHLERKORREKTUR N mit großer Ws in Zeit $\mathcal{O}(\log^{2+\mathcal{O}(\frac{1}{\epsilon^2})} N)$.

Resultate für RSA-Schlüssel mit mehr Information:

Schlüssel	Fehlerrate δ
(p, q)	0.084
(p, q, d)	0.160
(p, q, d, d_p)	0.206
(p, q, d, d_p, d_q)	0.237