Quadratische Reste und das Legendre Symbol

Definition Quadratischer Rest

Sei p prim. Ein Element $a \in \mathbb{Z}_p$ heißt *quadratischer Rest* in $\mathbb{Z}_p^*$, falls es ein $b \in \mathbb{Z}_p^*$ gibt mit $b^2 = a \bmod n$. Wir definieren

$$QR_p = \{a \in \mathbb{Z}_p^* \mid a \text{ ist ein quadratischer Rest } \} \text{ und } QNR_p = \mathbb{Z}_p^* \setminus QR.$$

Definition Legendre Symbol

Sei $p > 2$ prim und $a \in \mathbb{N}$. Das *Legendre Symbol* ist definiert als

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{falls } p|a \\ 1 & \text{falls } (a \bmod p) \in QR_p \\ -1 & \text{falls } (a \bmod p) \in QNR_p. \end{cases}$$

Berechnung von $\mathrm{dlog}_\alpha(\beta) \bmod 2$

Satz Berechnung des niederwertigsten Bits

Sei p prim, α Generator von $\mathbb{Z}_p^*$ und $\beta = \alpha^a \bmod p$. Dann gilt

$$\left(\frac{\beta}{p}\right) = \beta^{\frac{p-1}{2}} \bmod p = \begin{cases} 1 & \text{falls } a = 0 \bmod 2 \\ -1 & \text{falls } a = 1 \bmod 2 \end{cases}.$$

Beweis:

- Es gilt $\mathbb{Z}_p^* = \{\alpha, \alpha^2, \ldots, \alpha^{p-1}\}$. Damit folgt

$$QR_p = \{\alpha^2, \alpha^4, \ldots, \alpha^{2\cdot\frac{p-1}{2}}, \underbrace{\alpha^{2\cdot\frac{p+1}{2}}}_{\alpha^2}, \underbrace{\alpha^{2\cdot\frac{p+3}{2}}}_{\alpha^4}, \ldots, \underbrace{\alpha^{2(p-1)}}_{\alpha^{p-1}}\}$$

- D.h. β ist ein quadratischer Rest gdw a gerade ist.
- Es gilt $\beta^{\frac{p-1}{2}} = \pm 1$, da die 1 in $\mathbb{Z}_p^*$ Quadratwurzeln ± 1 besitzt.
- Ferner ist $\beta^{\frac{p-1}{2}} = \alpha^{\frac{a(p-1)}{2}} = 1$ gdw $\frac{a(p-1)}{2}$ Vielfaches von $p-1$.
- D.h. $\beta^{\frac{p-1}{2}} = 1$ gdw a gerade ist.

Korollar: Wir können $\mathrm{dlog}_\alpha(\beta) \bmod 2$ in Zeit $\mathcal{O}(\log^3 p)$ berechnen.

Lernen von $\mathrm{dlog}_\alpha(\beta)$ modulo Teiler von $p-1$

Idee des Pohlig Hellman Algorithmus:

- Wir nehmen an, dass die Zerlegung $p-1=\prod_{i=1}^{k} p_i^{e_i}$ bekannt ist.
- Bestimmen $a = a_i \bmod p_i^{e_i}$ für alle i. Wir ermitteln a mittels CRT.
- Zur Bestimmung von a_i verwenden wir die p_i-adische Zerlegung

  $$a_i = a_{i0} + a_{i1}p_i + a_{i2}p_i^2 + \ldots + a_{ie_i-1}p_i^{e_i-1} \text{ mit } 0 \leq a_{ij} < p_i.$$
- Die a_{ij} werden sukzessive für $j = 0, \ldots, e_i - 1$ berechnet.

Elemente in der p_i-adischen Entwicklung

Bestimmung von a_{i0}:

- Es gilt

$$\begin{aligned}\beta^{\frac{p-1}{p_i}} &= \alpha^{a\cdot\frac{p-1}{p_i}} = \alpha^{(a \bmod p_i)\cdot\frac{p-1}{p_i}} \cdot \underbrace{\alpha^{\lfloor\frac{a}{p_i}\rfloor\cdot p_i\cdot\frac{p-1}{p_i}}}_{1} \\ &= \alpha^{(a \bmod p_i)\cdot\frac{p-1}{p_i}} = \alpha^{(a_i \bmod p_i)\cdot\frac{p-1}{p_i}} = \alpha^{a_{i0}\cdot\frac{p-1}{p_i}}.\end{aligned}$$

- Wir berechnen $\alpha^{\ell\cdot\frac{p-1}{p_i}}$ für $\ell = 0, \ldots, p_i - 1$ und vergleichen mit $\beta^{\frac{p-1}{p_i}}$.

Bestimmung von a_{ij}:

- Angenommen, wir haben bereits $a_{i0}, \ldots, a_{ij-1}$ bestimmt.
- Setze $r = a_0 + \ldots + a_{ij-1}p^{j-1}$ und $\beta' := \beta \cdot \alpha^{-r}$.
- Analog zum obigen Fall berechnen wir

$$\beta'^{\frac{p-1}{p_i^{j+1}}} = \alpha^{(a-r)\cdot\frac{p-1}{p_i^{j+1}}} = \alpha^{(a-r \bmod p_i^{j+1})\cdot\frac{p-1}{p_i^{j+1}}} = \alpha^{(a_i-r \bmod p_i^{j+1})\cdot\frac{p-1}{p_i^{j+1}}} = \alpha^{a_{ij}\cdot\frac{p-1}{p_i}}.$$

- Durch Vergleich mit $\alpha^{\ell\cdot\frac{p-1}{p_i}}$, $\ell = 0, \ldots, p_i - 1$ bestimmen wir a_{ij}.

Pohlig-Hellman Algorithmus

Algorithmus Pohlig-Hellmann

EINGABE: p, α, $\beta = \alpha^a$ und $p-1 = \prod_{i=1}^{k} p_i^{e_i}$

1. FOR $i = 1, \ldots, k$ und $\ell = 0, \ldots, p_i - 1$ berechne $c_{i\ell} = \alpha^{\ell \cdot \frac{p-1}{p_i}}$.
2. FOR $i = 1, \ldots, k$ und $j = 0, \ldots, e_i - 1$
   1. Bestimme $c_{i\ell}$ mit $c_{i\ell} = \beta^{\frac{p-1}{p_i^{j+1}}}$. Setze $a_{ij} = \ell$ und $\beta := \beta \cdot \alpha^{-a_{ij} p_i^j}$.
3. Für $i = 1, \ldots, k$ berechne $a_i = a_{i0} + a_{i1} p_i + \ldots + a_{ie_i-1} p_i^{e_i-1}$.
4. Bestimme $a = CRT(a_1, \ldots, a_k) \bmod p - 1$.

AUSGABE: $a = \mathrm{dlog}_\alpha \beta$

Laufzeit:

- Schritt 1: $(p_1 + \ldots + p_k) \cdot \mathcal{O}(\log^3 p)$.
- Schritt 2,3,4: $(e_1 + \ldots + e_k) \cdot \mathcal{O}(\log^3 p) = \mathcal{O}(\log^4 p)$.
- D.h. wir erhalten Gesamtlaufzeit $\mathcal{O}((p_1 + \ldots + p_k) \cdot (\log^4 p))$.
- Damit ist unsere Laufzeit polynomiell falls $p_i = \mathcal{O}(\log p)$ für alle i.

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:

- Sei p' ungerade. Dann ist $(p', q') \in M$ 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.

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 mindestens 43% 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 $X = X_1 + \ldots\ldots X_{2t}$. Dann gilt

1. $\mathrm{Ws}[X \geq 2t(p+\gamma)] \leq e^{-4t\gamma^2}$,
2. $\mathrm{Ws}[X \leq 2t(p+\gamma)] \leq e^{-4t\gamma^2}$.

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

Under der Annahme, dass sich fehlerhafte Lösungen zufällig verhalten, werden für $t = \frac{\ln n}{4\epsilon^2}$, $d = 2t(\delta + \epsilon)$ alle inkorrekte 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 Bitposition.
- 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