Beschleunigung RSA-Entschlüsselung

$n = p \cdot q$, $\varphi(n) = (p-1)\cdot(q-1)$

Schlüssel: n, e öff., p, q, d geheim

$m' \equiv m^e \bmod n$ als verschlüsselte Nachricht

Berechnung $m'^d \bmod n$ — $\bmod p$, $\bmod q$

$d \bmod p-1$

$m' \bmod p$ $\bmod p$, ebenso $\bmod q$

vorher Zeit $\mathcal{O}(\log^3 n)$

jetzt $\mathcal{O}(\log^3 p + \log^3 q)$

Bitlänge von p, q?

$p \cdot q = n$, $\log p \approx \log q \approx \frac{\log n}{2}$

$$\left(\frac{\log n}{2}\right)^3 + \left(\frac{\log n}{2}\right)^3 = \frac{1}{4}\log^3 n$$