New RSA Vulnerabilities Using Lattice Reduction Methods

Alexander May

Zusammenfassung

Die vorliegende Dissertationsschrift beschäftigt sich mit dem heutzutage bekanntesten und meistverwendeten Public-Key Kryptosystem; dem 1978 von Rivest, Shamir und Adleman vorgeschlagenen RSA-Kryptosystem. Es wird gezeigt, dass spezielle Parameterwahlen bei diesem Kryptosystem zu Polynomialzeit-Angriffen führen.

Betrachten wir dazu die Generierung der RSA-Parameter genauer: Man wählt zwei große Primzahlen p und q und berechnet deren Produkt $N = pq$. Der sogenannte RSA-Modul N ist öffentlich, wohingegen die Faktorisierung von N in p und q geheim ist. Weiterhin wählt man ein Schlüsselpaar (e, d) mit der Eigenschaft $ed = 1 \bmod (p-1)(q-1)$. Hierbei ist der Parameter e bei RSA öffentlich bekannt, und der Parameter d ist geheim.

Der geheime Schlüssel d kann leicht aus (N, e) berechnet werden, falls man die Faktorisierung von N kennt. Daher kann ein Angreifer versuchen, die Faktorisierung von N zu bestimmen. Es ist aber bisher kein Algorithmus bekannt, der die Faktorisierung von N in polynomieller Zeit in der Bitlänge von N berechnet.

Die vorliegende Arbeit zeigt, dass ein Angreifer die Faktorisierung in polynomieller Zeit finden kann, falls e eine spezielle Form hat oder der Angreifer in den Besitz eines Bruchteils der Bits des geheimen Schlüssels d gelangt. Als Methode wird in der Arbeit ein von Coppersmith 1996 vorgestellter Algorithmus zum Bestimmen kleiner Nullstellen modularer Polynomgleichungen verwendet und weiterentwickelt. Die Dissertationsschrift umfasst unter anderem die folgenden Resultate:

- Verallgemeinerung der Coppersmith-Methode für univariate Polynome. Weiterhin wird ein Ansatz zur Konstruktion optimaler Gitterbasen entwickelt. Diese Gitterbasen werden in der Coppersmith-Methode benötigt.

- Faktorisierung von N mit Hilfe von (N, e) in Polynomialzeit, falls das zugehörige d von der Form $d = \frac{d_1}{d_2} \bmod (p-1)(q-1)$ für kleine d_1, d_2 ist.

  Dieses Resultat führt zur Kryptanalyse einer 2001 vorgeschlagenen RSA-Variante.

- Faktorisierung des RSA-Moduls N in Polynomialzeit, falls der Wert $d_p = d \bmod p-1$ klein ist und gleichzeitig $q \leq N^{0.382}$. Kleine Werte von d_p sind praxisrelevant, da sie den Dekodiervorgang in RSA beschleunigen.

- Verschiedene Polynomialzeit-Angriffe auf RSA, falls man Teile der Bits des geheimen Schlüssels d oder des Parameters d_p kennt. Die Angriffe werden zusätzlich auf RSA-Moduln der Form $N = p^r q$ für $r > 1$ erweitert.