Attacken auf RSA durch Lösen von univariaten modularen Polynomgleichungen

Anna Perschl

FH Oberösterreich - Campus Hagenberg
Softwarepark 11, 4232 Hagenberg, Österreich

Don Coppersmith stellte in [1] eine Methode vor, die eine univariate Polynomgleichung mit Modul N und Grad δ in polynomialer Zeit löst, wenn die gesuchte Lösung kleiner als $N^{1/\delta}$ ist. Auf diesen Ergebnissen aufbauend, präsentierte Nicholas Howgrave-Graham in [2] eine weitere Methode.

Mit Hilfe dieser Methoden kann RSA kompromittiert werden, z.B. wenn ein Teil der Nachricht bekannt ist, die Nachricht zwei Mal mit gleichem Schlüssel und unterschiedlichem Padding oder die Nachricht mehrmals mit unterschiedlichen Schlüsseln und bekannten Paddings verschlüsselt wird. In diesen Fällen sind Angriffe dann möglich, wenn ein kleiner öffentlicher Exponent e verwendet wird und die Unbekannte kleiner als $N^{1/e}$ ist. Die Methoden ermöglichen auch das Faktorisieren von N, wenn genügend höchstwertige Bits eines Teilers bekannt sind. Eine aktuelle Übersicht der Anwendungen findet sich in [3], ein aktueller Faktorisierungsalgorithmus in [4].

Die beiden Methoden lösen univariate modulare Polynomgleichungen in Zeit polynomiell in $\log N$ und δ. Da dies jedoch keine konkrete Aussage über die tatsächlichen Laufzeiten zulässt, haben wir beide Methoden im Rahmen der Diplomarbeit in Java implementiert und auf ihren Einsatz in drei Attacken getestet.

Eine Gleichung dritten Grades mit einer Lösung von höchstens 256 Bit und einem Modul von 1024 Bit löst die implementierte Coppersmith-Methode in 55 Sekunden, die implementierte Howgrave-Graham-Methode in 22 Sekunden. Bei einem Modul von 2048 Bit benötigen die Methoden 340 bzw. 150 Sekunden. Wird also eine Nachricht mit öffentlichem Exponent 3 und einem 1024-Bit-Modul verschlüsselt, so kann ein Angreifer, der 3/4 der Nachricht kennt, das unbekannte Viertel der Nachricht in 22 Sekunden ermitteln. Dem Angreifer kann theoretisch bis zu 1/3 der Nachricht unbekannt sein, allerdings ist dann der benötigte Zeitaufwand deutlich größer.

Wir präsentieren die Testergebnisse der Methoden im Detail, zeigen theoretische und praktische Grenzen auf und treffen eine Aussage über ihre Relevanz im Bezug auf die Sicherheit von RSA.

Literatur

[1] Don Coppersmith: Finding a Small Root of a Univariate Modular Equation. In *Advances in Cryptology – EUROCRYPT '96*, Bd. 1070 d. Reihe *Lecture Notes in Computer Science*, S. 155–165, Springer-Verlag, 1996.

[2] Nicholas Howgrave-Graham: Finding Small Roots of Univariate Modular Equations Revisited. In *Crytography and Coding – IMA 1997*, Bd. 1355 d. Reihe *Lecture Notes in Computer Science*, S. 131–142, Springer-Verlag, 1997.

[3] Alexander May: Using LLL-Reduction for Solving RSA and Factorization Problems: A Survey. *LLL+25 Conference in honour of the 25th birthday of the LLL algorithm*, 2007.

[4] Mathias Herrmann, Alexander May: On Factoring Arbitrary Integers with Known Bits. In *INFORMATIK 2007 - Informatik trifft Logistik, Band 2*, Bd. P-110 d. Reihe *Lecture Notes in Informatics*, S. 195–199, 2007.