

GRÖBNER BASEN UND DAS KRYPTOVERFAHREN POLLY TWO

LE VAN LY

Vorläufige Version, 27 Februar 2003

ABSTRACT. Ausgehend von einem von Fellows und Koblitz vorgestellten Public-Key-Kryptoverfahren namens *Polly Cracker* habe ich ein Kryptoverfahren *Polly Two* entwickelt, das im Gegensatz zu *Polly Cracker* gegen alle bekannten Angriffe sicher ist. Bei *Polly Two* ist dabei sowohl die Ausführbarkeit, als auch die Sicherheit stark mit der Komplexität von Gröbner Basis-Berechnungen verknüpft.

1. POLLY CRACKER

Das von Fellows und Koblitz [2] 1993 entwickelte Public-Key-Kryptoverfahren *Polly Cracker* basiert auf NP-harten Problemen und funktioniert wie folgt:

Gegeben sind ein endlicher Körper \mathbb{F} und ein Polynomring $P = \mathbb{F}[x_1, \dots, x_n]$. Als öffentlicher Schlüssel verwendet eine der Parteien, genannt *Alice*, ein Ideal $\mathfrak{a} \subseteq P$, dargestellt durch Erzeugende f_1, \dots, f_s . Alices öffentlicher Schlüssel ist dann eine Nullstelle $\xi \in \mathbb{F}^n$ von \mathfrak{a} . Um eine Nachricht $m \in \mathbb{F}$ zu verschlüsseln, generiert eine zweite Partei *Bob* ein zufälliges Polynom $h \in \mathfrak{a}$ und verschlüsselt m durch $c := m + h$. Die Entschlüsselung besteht dann für Alice darin, das Polynom c in der Nullstelle ξ auszuwerten und so $c(\xi) = m + h(\xi) = m$ zu erhalten.

Ein generischer Angriff auf das Verfahren wäre der Versuch der Berechnung einer Nullstelle von \mathfrak{a} , z.B. indem man eine Gröbner Basis von \mathfrak{a} bezüglich einer lexikographischen Ordnung bestimmt. Wählt man jedoch die Anzahl der Variablen oder den Grad der erzeugenden Polynome genügend groß, ist diese Berechnung nicht in angemessener Zeit möglich.

Dagegen ist aber ein Angriff auf mit *Polly Cracker* verschlüsselte Nachrichten durch Methoden der Linearen Algebra in vielen Fällen erfolgreich [1], [3]. Gegen diese Art von Angriffen gab es bislang keine effizienten Gegenmaßnahmen.

2. POLLY TWO

Das neue Verfahren *Polly Two* wird wie folgt durchgeführt: Gegeben ist wie bei *Polly Cracker* ein endlicher Körper \mathbb{F} und ein Polynomring $\mathbb{F}[x_1, \dots, x_n]$. Zusätzlich betrachtet man einen zweiten Polynomring $Q = \mathbb{F}[y_1, \dots, y_t]$ und Polynome $g_1, \dots, g_t \in P$, die auf natürliche Weise eine Abbildung φ von Q nach P vermöge der Zuordnung $y_i \mapsto g_i$ definieren. Der Bildring $\mathbb{F}[g_1, \dots, g_t]$ werde mit R bezeichnet.

1. Schlüsselerzeugung:

Alices öffentlicher Schlüssel besteht aus einem Ideal $\mathfrak{b} \subseteq Q$, dargestellt durch dünn

besetzte Polynome $F_1, \dots, F_s \in Q$. Ein geheimer Schlüssel ist dann eine Nullstelle $\xi \in \mathbb{F}^n$ von dem zu \mathfrak{b} zugehörigen Bildideal $\mathfrak{a} := \varphi(\mathfrak{b})P$, die jedoch keine Nullstelle der Polynome g_1, \dots, g_t sein darf.

2. Verschlüsselung:

Um eine Nachricht $m \in \mathbb{F}$ zu verschlüsseln, generiert Bob zufällige, dünn besetzte Polynome $h \in Q$ und $h' \in \text{Kern } \varphi$ und ein Monom $y^\kappa := y_1^{\kappa_1} \dots y_t^{\kappa_t}$ und addiert bzw. multipliziert diese zu der Nachricht m zu einem Geheimtext

$$(c = my^\kappa + h + h', \kappa).$$

3. Entschlüsselung

Alice entschlüsselt die Nachricht (c, κ) , indem sie $\varphi(c)(\xi)/\varphi(y^\kappa)(\xi) = m$ berechnet. Sie erhält den korrekten Klartext, weil $\varphi(h) \in \mathfrak{a}$ und $\varphi(h') = 0$ gelten.

3. GRÖBNER BASEN UND POLLY TWO

Ich führe hier einige Punkte auf, die die starke Verknüpfung von Gröbner Basen mit der Sicherheit und der Durchführbarkeit des Kryptoverfahrens Polly Two verdeutlichen:

- Die Parameter und das Ideal \mathfrak{b} müssen so gewählt werden, daß keine Nullstellen von $\mathfrak{a} = \varphi(\mathfrak{b})P$ berechenbar sind. Das heißt insbesondere, daß keine Gröbner Basis von \mathfrak{a} berechenbar sein darf.
- Durch die Berechnung von Gröbner Basen von Eliminationsidealen lassen sich Erzeugendensysteme von Kern φ berechnen (Implizitation). Dabei verschiedene Fragen bezüglich der Eigenschaften diese Ideals auf. Darf zum Beispiel eine Gröbner Basis von Kern φ aus Sicherheitsgründen überhaupt berechenbar sein?
- Ein Angriff kann durchgeführt werden, wenn sowohl die \mathbb{F} -Vektorraum-Dimension von $Q/\text{Kern } \varphi \cong R$ klein, als auch die Reduktion von Polynomen zu Normalformen mit einer Gröbner Basis in kurzer Zeit möglich ist.
- Um zu verschlüsseln, benötigt man dünn besetzte Polynome aus Kern φ . Dabei darf die Auswahl nicht zu gering sein, um einen Angriff durch vollständiges Durchsuchen zu vermeiden. Dies kann man durch Einsatz von Gröbner Basis-Techniken erreichen?

Insgesamt erhält man so ein Public-Key-Kryptoverfahren Polly Two, das gegen alle bekannten Angriffe sicher und gleichzeitig mit Hilfe von Gröbner Basis-Techniken und Computer-Algebra-Programmen algorithmisch durchführbar ist.

REFERENCES

- [1] Boo Barkee, Deh Cac Can, Julia Ecks, Theo Moriarty, R. F. Ree: Why you cannot even hope to use Gröbner Bases in Public Key Cryptography: An open letter to a Scientist Who failed and a Challenge to Those Who Have not yet failed. In: Journal of Symbolic Computation no.18, 1994, 497–501.
- [2] M. Fellows, N. Koblitz: Algebraic cryptosystems galore!. In: Finite fields: theory, applications, and algorithms (Las Vegas, NV, 1993), 51–61, Contemp. Math. 168.
- [3] N. Koblitz: Algebraic Aspects of Cryptography. Algorithms and Computation in Mathematics 3. Springer-Verlag, Berlin, 1998.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, POSTFACH 200363, 53133 BONN
E-mail address: levan.ly@bsi.bund.de