Lineare Codes und Kryptosysteme

Wir gehen hier so kurz wie möglich auf lineare, fehlerkorrigierende Codes und ihre Anwendung in der Kryptographie ein. Die Situation ist relativ analog zur gitterbasierten Kryptographie.

Lineare, fehlerkorrigierende Codes

Ein linearer Code ist ein Vektorunterraum C von $\mathbb{F}_q^n$. Die Dimension k von C ist die Dimension von C als $\mathbb{F}_q$-Vektorraum. Die Elemente von C heißen Codeworte von C. Sind $v = (v_i)$ und $w = (w_i)$ zwei Codeworte, dann ist der Abstand von v und w durch $\mathrm{dist}(v, w) = \#\{i \mid v_i \neq w_i\}$ definiert. Der Minimumabstand d von C wird als $d = \min\{\mathrm{dist}(v, 0) \mid v \in C\backslash\{0\}\}$ definiert. Man sagt dann, C sei ein (n, k, d)-Code. Der Minimumabstand entspricht dem ersten sukzessiven Minimum $\lambda_1(\Lambda)$ eines Gitters Λ.

Bei der Übertragung eines Codeworts v über eine rauschende Leitung kann es vorkommen, daß gewisse Koordinaten von v gestört werden und der Empfänger ein von v verschiedenes Element $a \in \mathbb{F}_q^n$ erhält. Werden maximal $e = \lfloor (d-1)/2 \rfloor$ Koordinaten gestört, so ist v als zu a nächstes Codewort aus C eindeutig definiert. Die Berechnung von v nennt sich auch Decodierung. Das Problem der Decodierung ist analog zum CVP in Gittern Λ und ist im allgemeinen ebenfalls NP-hart. In der Nachrichtenübertragung verwendet man allerdings gerade solche speziellen Codes, für welche die Decodierung leicht ist. Zu diesen Codes zählen die Goppa Codes, welche mit Hilfe von algebraischen Kurven über $\mathbb{F}_q$ definiert werden.

Will man eine Nachricht m über eine rauschende Leitung übertragen, so codiert man die Nachricht m als Codeworte und schickt die Codeworte anstelle der Nachricht. Ist $b_i \in C$ eine Basis von C und $m = (m_i) \in \mathbb{F}_q^k$, so kann man m in das Codewort $v = \sum_{i=1}^k m_i v_i$ codieren. Die Matrix $(b_1, \ldots, b_k)$ heißt Generatormatrix von C. Eine Nachricht der Länge k über $\mathbb{F}_q$ wird also in Codeworte der Länge n über $\mathbb{F}_q$ expandiert. Um eine möglichst hohe

Übertragungsrate und Fehlerkorrektur zu erzielen, will man sowohl k also auch d maximieren. Dies sind allerdings offenbar gegenläufige Prozesse, es gilt beispielsweise die Singleton-Schranke $d + k \leq n + 1$.

Das McEliece Kryptosystem

Dieses Public-Key Kryptosystem ist im wesentlichen analog zum GGH Kryptosystem. Man verwendet einen linearen Code C. Der geheime Schlüssel besteht aus einer Generatormatrix, für welche das Decodierungsproblem leicht ist. Der öffentliche Schlüssel besteht aus einer Generatormatrix, für welche das Decodierungsproblem schwer ist.

Genauer werden die Parameter q, n, k, d vorgegeben. Zur Schlüsselerzeugung wählt A eine Generatormatrix G, welche einen (n, k, d)-Code über $\mathbb{F}_q$ definiert und für welche das Decodierungsproblem leicht ist. A wählt weiter zufällige Matrizen S, P und definert $G' = PGS$. Der geheime Schlüssel ist G, der öffentliche G'.

Zur Verschlüsselung schreibt B die Nachricht als $m \in \mathbb{F}_q^k$ und wählt einen zufälligen Fehlervektor $e \in \mathbb{F}_q^n$ mit $\mathrm{dist}(e, 0) \leq d$. Der Chiffretext ist $c = G'm + e$.

Zur Entschlüsselung geht A wie folgt vor: Berechne $c' = P^{-1}c$, decodiere c' zu m' unter Verwendung von G, berechne $m = S^{-1}m'$. Die Entschlüsselung ist korrekt, da die durch e eingeführten Fehler wegen $\mathrm{dist}(e, 0) \leq d$ decodiert werden können.

Übliche Parametergrößen sind $q = 2$, $n = 1024$, $d = 38$ und $k \geq 644$. Das Verfahren gilt bzw. erscheint für diese Parametergrößen (und unter Verwendung von Goppa Codes) als sicher und Verschlüsselung und Entschlüsselung sind effizient. Ein Problem ist jedoch die große Schlüsselgröße (2^{19} Bits) und die Nachrichtenexpansion von n/k (hier ≥ 1.59). Daher findet das McEliece Kryptosystem in der Praxis wenig Beachtung.

Es ist ebenfalls möglich, ein Signaturverfahren ähnlich dem GGH Verfahren anzugeben. Die Sicherheit ist hier fraglicher, da durch die Unterschriften Informationen über G preisgegeben werden. Das resultierende Verfahren ist jedenfalls ziemlich uneffizient.

Das McEliece Verfahren wurde 1978 erfunden, das erwähnte Signaturverfahren erst kürzlich, so um 2000.