

ten Körper nicht übertragen, unter Anderem, da es auch **selbstduale** Codes gibt [vgl. 8, S. 36].

Bemerkung 9

Der zu einem $[n, k, d]_q$ -Code C duale Code C^\perp ist ein $[n, n - k, d']_q$ -Code [vgl. 8, S. 36].

Wird der duale Code zu einem dualen Code eines linearen Codes C gebildet, so ist dieser wieder C , also gilt:

$$C^{\perp\perp} = C$$

Theorem 7

Der duale Code zu einem verallgemeinerten Reed-Solomon-Code ist ebenfalls ein verallgemeinerter Reed-Solomon-Code [vgl. 19, S. 14].

So gilt $GRS_k(u, v)^\perp = GRS_{n-k}(u, v')$, wobei für die Komponenten des Vektors v' gilt:

$$v_i \cdot v'_i \prod_{j=1, j \neq i}^n (u_j - u_i) = 1$$

[vgl. 19, S. 14]

Beweis. Zunächst wird $k = n-1$ angenommen. Dann ist zu zeigen, dass $GRS_{n-1}(u, v)^\perp = GRS_1(u, v')$ gilt. Dafür genügt es, zu beweisen, dass $v'_i \neq 0$ gilt und v' damit ein gültiges Gewichtstupel ist, da für alle u_i bereits bekannt ist, dass sie die Forderungen von GRS-Codes erfüllen. Die Codewortmenge von $GRS_1(u, v')$ ist dadurch, dass zulässige Polynome auf diesem Code nur Skalare sein können, durch alle skalaren Vielfachen von allen v'_i bereits vollständig beschrieben.

Aus Definition 24 ergibt sich nun, dass zu zeigen ist, dass

$$(hG) \cdot (kv') = 0$$

gelten muss, wobei h eine beliebige Nachricht aus \mathbb{F}_q , G die Generatormatrix des $GRS_{n-1}(u, v)$ -Codes und k eine beliebiges Element aus \mathbb{F}_q ist. Da h und k Werte ungleich 0 annehmen können, gilt nach dem Nullproduktsatz bereits, dass $G \cdot v' = 0$ gelten muss. Mit Vorausgriff

auf Bemerkung 10 lässt sich entsprechend das folgende Gleichungssystem konstruieren [vgl. 21, S. 304]:

$$\begin{aligned} v_0 v'_0 + v_1 v'_1 + \dots + v_{n-1} v'_{n-1} &= 0 \\ u_0 v_0 v'_0 + u_1 v_1 v'_0 + \dots + u_{n-1} v_{n-1} v'_{n-1} &= 0 \\ &\vdots \\ u_0^{n-2} v_0 v'_0 + u_1^{n-2} v_1 v'_0 + \dots + u_{n-1}^{n-2} v_{n-1} v'_{n-1} &= 0 \end{aligned}$$

Dies entspricht in Matrixschreibweise

$$\left[\begin{array}{cccc} 1 & 1 & \cdots & 1 \\ u_0 & u_1 & \cdots & u_{n-1} \\ \vdots & & & \vdots \\ u_0^{n-2} & u_1^{n-2} & \cdots & u_{n-1}^{n-2} \end{array} \right] \left[\begin{array}{c} v_0 v'_0 \\ v_1 v'_1 \\ \vdots \\ v_{n-1} v'_{n-1} \end{array} \right] = 0 \quad (3.1)$$

Falls ein $v'_i = 0$ ist, so ergibt sich dadurch, dass keine Komponente der linken *Vandermonde*-Matrix gemäß der Definition von *GRS*-Codes gleich 0 sein kann, dass alle $v_i v'_i = 0$ und in der Folge alle $v'_i = 0$ sein müssten, was jedoch nicht möglich ist, zum Beispiel da die Dualisierung dieses Codes nicht wieder den $GRS_{n-1}(u, v)$ -Code erzeugen kann. Damit ist gezeigt, dass $\forall i \in \{0, \dots, n-1\}: v'_i \neq 0$ gilt und zugleich, dass $GRS_{n-1}(u, v)^\perp$ die Forderungen eines *GRS*-Codes erfüllt. Dass sich dieses Resultat nun auch auf *GRS*-Codes mit beliebigem $k < n-1$ übertragen lässt, ergibt sich nun aus folgender verallgemeinerten Form der obigen Gleichungen [vgl. 21, S. 304]:

$$\sum_{i=0}^{n-1} (u_i^s v_i)(u_i^t v'_i) = \sum_{i=0}^{n-1} (u_i^{s+t} v_i v'_i) = 0 \quad (3.2)$$

Mit der gleichen Argumentation wie für $k = n-1$ ergibt sich unmittelbar, dass auch hier kein v'_i gleich 0 sein kann. Damit ist das Theorem gezeigt. □

3.2.3 Kontroll- und Generatormatrizen

Da lineare Codes wie gezeigt Vektorräume bilden, ist die Angabe von **Basen** möglich. Durch die Definition der Dualität von Codes zueinander, können **Generator-** und **Kontrollmatrizen** angegeben werden.

Algorithmus 5 Entschlüsselungsalgorithmus des NIEDERREITER-Schemas (nach [34])

Require: S, H, P , Geheimtextvektor $x = k_{pub} \cdot y^T$

- 1: $s \leftarrow S^{-1} \cdot x$
 - 2: $t \leftarrow$ Ergebnis eines zum Code C passenden Dekodierverfahrens auf s
 - 3: $y \leftarrow t \cdot (P^T)^{-1}$
 - 4: **return** y
-

4.3.1 Korrektheit des Verfahrens

Theorem 9

Das Produkt $H \cdot P$ ist eine Paritätsprüfmatrix eines linearen Codes.

Beweis. Nach HILL erzeugen die folgenden Operationen auf einer Generatormatrix G eines linearen $[n, k, d]$ -Codes äquivalente Codes [vgl. 47, S. 50]:

- Zeilenumtauschungen
- Multiplikation einer Zeile mit einem Skalar ungleich 0
- Addition eines skalaren Vielfachen einer Zeile auf eine andere
- Vertauschung von Spalten
- Multiplikation einer Spalte mit einem Skalar ungleich 0.

Da die Matrix P eine (gewichtete) Permutationsmatrix ist, besitzt sie pro Zeile und Spalte genau in einer Komponente einen Wert ungleich 0. Da nach Definition 25 die Zeilen einer Generatormatrix eine Basis des durch den Code beschriebenen Vektorraums bilden und die Zeilen einer Paritätsprüfmatrix eine Basis des Kerns der Generatormatrix [vgl. 24, S. 29f.], besteht hinsichtlich der Zeilenumtauschungen und der Multiplikation einer Zeile mit einem Skalar bereits Äquivalenz, da dies aus der Definition einer Basis unmittelbar folgt und die lineare Unabhängigkeit erhalten bleibt. Bei der Multiplikation der Matrix H mit der Matrix P werden aufgrund der obig beschriebenen Beschaffenheit der Matrix P die Spalten der Matrix H mit Skalaren multipliziert und vertauscht. Hierbei bleibt die lineare Unabhängigkeit nicht zwangsläufig erhalten, jedoch erzeugen diese Operationen **äquivalente Codes**, die sich zwar in der Anordnung der Symbole unterscheiden, aber den gleichen Vektorraum aufspannen [vgl. 25, S. 24] [vgl. 48, S. 1193f.]. Somit ist gezeigt, dass die Aussage gilt. \square

Die Multiplikation dieses Produktes HP mit der Matrix S^T zerstört diese Eigenschaft der Äquivalenz nun, wodurch erst möglich wird, den öffentlichen Schlüssel zu veröffentlichen.

Das Produkt SHP ist im Allgemeinen keine Paritätsprüfmatrix eines gültigen linearen Codes mehr, behindert die Dekodierbarkeit der Codeworte jedoch nicht:

Mit Sidelnikov/Shestakov zeigt sich etwas anderes, das passe ich noch an.

Theorem 10

Das Produkt aus $k_{pub} = S \cdot H \cdot P$ und Klartextvektor y lässt sich durch Algorithmus 5 dechiffrieren.

Beweis. Die Aussage folgt unmittelbar:

$$\begin{aligned} x &= H \cdot P \cdot S^T \cdot y^T \\ s &= S^{-1} \cdot x \\ &\Leftrightarrow S^{-1} \cdot H \cdot P \cdot S^T \cdot y^T \\ &\Leftrightarrow H \cdot P \cdot S^T \cdot (S^T)^{-1} \cdot y^T \\ &\Leftrightarrow H \cdot P \cdot y^T \end{aligned}$$

Da aus Theorem 9 folgt, dass HP eine gültige Paritätsprüfmatrix eines linearen Codes und damit zugleich eine Generatormatrix des dazu dualen Codes darstellt, ist durch $H \cdot P \cdot y^T$ ein gültiges Codewort von y beschrieben, das im Folgenden dekodiert werden kann. Sei t das dekodierte Klartextwort zum Code mit Generatormatrix HP . Die Operation

$$y = t \cdot (P^T)^{-1}$$

ist die inverse Anwendung der Permutation und führt zum Klartext y , da hier – wie im Beweis zu Theorem 9 beschrieben – lediglich die Anordnung der Symbole permutiert wurde und nun rückgängig gemacht wird. Damit ist die Korrektheit des Verfahrens gezeigt. 

4.3.2 Wahl geeigneter Codes

Die Sicherheit eines solchen Kryptosystems ist stark an die Wahl eines geeigneten Codes gebunden. NIEDERREITER formuliert daher folgende Anforderungen an Codes [vgl. 34, S. 161f.]:

- Die Fehlerrichtigurkapazität des Codes sollte relativ hoch sein, sodass eine möglichst große Anzahl an Klartextvektoren verwendet werden kann

Eine alternative Formulierung liefert VAN LINT [vgl. 5, S. 66]:

$$\mathcal{A}_q(n, d) \geq \frac{q^n}{V_q(n, d - 1)} \quad (4.6)$$

Die *Gilbert-Varshamov-Schranke* liefert folglich eine Untergrenze für die maximal mögliche Codewortanzahl eines Codes, der die Bedingung erfüllt. In Bezug zur Kryptographie sind solche Codes von besonderer Bedeutung, da es nicht möglich sein soll, ein Kryptosystem durch bloßes Erraten möglicher Code- oder Klartextworte zu brechen. Dass sowohl *Goppa-Codes* als auch verallgemeinerte *Reed-Solomon-Codes* diese Schranke ab $q \geq 49$ erfüllen, stellen VAN LINT UND SPRINGER dar [vgl. 49].

4.4 Vergleich zum McEliece-Kryptosystem

Die Frage, inwieweit sich beide dargestellten Vorschläge von MC ELIECE und NIEDERREITER und insbesondere auch ihre Sicherheit unterscheiden, ist Gegenstand dieses Abschnittes.

Theorem 12

Sei C ein linearer $[n, k, 2t + 1]$ -Code (wobei t die Fehlerrichturschranke bezeichnet). Dann sind die Kryptosysteme von MC ELIECE und NIEDERREITER bezüglich dieses Codes äquivalent zueinander und weisen dieselbe Sicherheit auf.

Beweis. Die Aussage wird durch einen direkten Beweis gezeigt. Sei G' der öffentliche Schlüssel des MC ELIECE-Kryptosystems, bestehend aus den Matrixprodukt SGP , wobei G eine Generatormatrix des betrachteten Codes ist. Gemäß Abschnitt 3.3.2 kann aus G' eine Paritätsprüfmatrix H' abgeleitet werden (hierbei ist unerheblich, dass es sich bei G' nicht um eine Generatormatrix des betrachteten Codes handelt). Die Verschlüsselungsoperation des MC ELIECE-Kryptosystems ist definiert durch

$$x = u \cdot G' + z \quad (4.7)$$

u bezeichnet einen Klartextblock und z einen Fehlervektor mit Länge n und Gewicht $w(z) \leq t$. Wird diese Gleichung nun mit H'^T multipliziert, ergibt sich durch $G'H'^T = 0$:

$$v = x \cdot H'^T = u \cdot G'H'^T + zH'^T \Leftrightarrow zH'^T \quad (4.8)$$

Die Verschlüsselung im NIEDERREITER-Verfahren ist gegeben durch

$$x = y \cdot H'^T, \quad (4.9)$$

wobei $H' = k_{pub} = SHP$. Da z und y strukturidentisch sind, also Vektoren der Länge n mit Gewicht $w \leq t$, ist durch 4.8 auch die Verschlüsselung des NIEDERREITER-Kryptosystems beschrieben [vgl. 50, S. 272]. Sollte es einer angreifenden Person bei bekanntem x und H' aus Gleichung 4.9 möglich sein, y zu finden, gilt das NIEDERREITER-Verfahren als gebrochen. Gleiches trifft jedoch nach 4.8 auch auf das MCELIECE-Verfahren zu, da auch hier das Finden von z bei bekanntem u und H' zum Bruch des Systems führt.

Auch ausgehend von der NIEDERREITER-Verschlüsselungsgleichung 4.9 kann die Äquivalenz zur MCELIECE-Verschlüsselungsoperation gezeigt werden. Sei c ein n -dimensionaler Vektor mit Gewicht $w \geq t$,³ der die Gleichung $x = cH'^T$ erfüllt. Dann kann c analog zum obigen Vorgehen aufgefasst werden als

$$c = mG' + y \quad (4.10)$$

für einen k -dimensionalen Vektor m und y mit Gewicht y , denn

$$\begin{aligned} x &= c \cdot H'^T = (mG' + y) \cdot H'^T \\ &\Leftrightarrow mG'H'^T + yH'^T \\ &\Leftrightarrow yH'^T, \end{aligned}$$

was wiederum genau Gleichung 4.9 entspricht. Kann also das MCELIECE-Kryptosystem gebrochen werden, so kann es das NIEDERREITER-Kryptosystem ebenfalls [vgl. 50, S. 272]. □

³Bei einem Gewicht größer als t ist c nicht mehr durch das NIEDERREITER-Verfahren dechiffrierbar. Hier ist das jedoch auch gar nicht das Ziel.