Kybernetika

Richard Gabriel

Verschlüsselungsabbildungen mit Pseudo-Inversen, Zufallsgeneratoren und Täfelungen

Kybernetika, Vol. 18 (1982), No. 6, 485--504

Persistent URL: http://dml.cz/dmlcz/124857

KYBERNETIKA — JAHRGANG *18* (1982), HEFT 6

VERSCHLÜSSELUNGSABBILDUNGEN MIT PSEUDO-INVERSEN, ZUFALLSGENERATOREN UND TÄFELUNGEN

RICHARD GABRIEL

Es wird versucht, die vom Autor [10], [11] eingeleitete und von R. E. Hartwig [14], [18] und J. Levine [18] weiterentwickelte Lineare Kryptographie, die sich auf Pseudo-Inversen gründet, allgemein darzustellen, wobei Schlüssel in der Gestalt von Zufallsgeneratoren und Täfelungen in Betracht kommen. Es sind restriktionslose Schlüssel, die das Public-Key Kryptosystem ergänzen können.

1. VERSCHLÜSSELUNGSABBILDUNGEN MIT PSEUDO-INVERSEN

1.1. Algebraische Kryptographie kann man in einer beliebigen endlichen algebraischen Struktur $\boldsymbol{R}$ betrachten. Indem man die Buchstaben eines Alphabets $\mathscr{A}$ durch die Symbole aus $\boldsymbol{R}$, nach einer umkehrbaren Abbildung $\alpha : \mathscr{A} \to \boldsymbol{R}$ ersetzt, entsteht die Voraussetzung, einen im Alphabet $\mathscr{A}$ gegebenen Text $\mathscr{T}$ nach algebraischen Regeln zu verschlüsseln. In [10] und [11], wo auch erstmals das verallgemeinerte Inverse in die Kryptographie eingeführt wurde, war $\boldsymbol{R} = GF(p_1 p_2 \dots p_t)$ die entsprechende algebraische Struktur. In den Verallgemeinerungen von Hartwig und Levine [14], [18] war es für $N = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_t^{\gamma_t}$ entweder ein Produkt von Galois Felder $\boldsymbol{R} = GF(N) = GF(p_1^{\gamma_1}) \oplus GF(p_2^{\gamma_2}) \oplus \dots \oplus GF(p_t^{\gamma_t})$ oder ein Restklassenring $\boldsymbol{R} = \mathbb{Z}/N$, wobei man die Matrizen über diese Strukturen, einheitlich als einen $s\pi r$-Ring untersuchen konnte.

Nun kann, mehreren Autoren nach, ein Primkörper $\boldsymbol{R} = GF(p) \cong \mathbb{Z}/p$ kryptanalytisch eine grössere Sicherheit gewährleisten als die zusammengesetzten Strukturen. Dann interessieren vornehmlich folgende Primkörper: $GF(31)$, $GF(37)$, $GF(41)$, $GF(43)$, $GF(47)$. Ein anderer Grund, weiterhin nur noch Primkörper zu betrachten, ist es, dass in der vorliegenden Arbeit auch Schlüssel in der Gestalt von Zufallszahlen betrachtet werden, die man am besten in $GF(p)$ als Kongruenzzufallsgeneratoren definieren kann.

1.2. Ist $\mathscr{T}$ ein im Alphabet $\mathscr{A}$ gegebener Text und $\mathscr{T}_\alpha$ seine Darstellung im Primkörper $\mathbb{F} = GF(p)$; $\alpha : \mathscr{T} \to \mathscr{T}_\alpha$, so wird in der Linearen Kryptographie zuerst $\mathscr{T}_\alpha$ zerhackt und daraus kanonisch eine rechteckige Matrix $\boldsymbol{P}(m, l)$ gebildet. Klassisch ist dann die Verschlüsselungsmethode, in der ein Schlüssel eine konstante umkehrbare Schlüsselmatrix $\boldsymbol{K} \in \mathbb{F}_{m \times m}$ ist, wobei Verschlüsselung und Entschlüsselung nach den Formeln

$$\boldsymbol{Q} = \boldsymbol{K}\boldsymbol{P}\,; \quad \boldsymbol{P} = \boldsymbol{K}^{-1}\boldsymbol{Q} \tag{1.1}$$

erfolgen. Eine theoretische Entwicklung im Sinne der Kryptananalyse erfährt der Sonderfall

$$\boldsymbol{K} = \boldsymbol{K}^{-1} = \text{involutorisch}$$

in Arbeiten von Levine und Brawley [19] in Verbindung mit den auf Hill zurückgehende Zwei Nachrichten Probleme, sowie auch bei den Drei Nachrichten Probleme in Arbeiten von Gabriel [8], [9].

Ein Modell der Linearen Kryptographie mit variabler Schlüsselmatrix wurde vom Autor [10], [11] definiert. Ist $\boldsymbol{A} = \boldsymbol{A}(m, n)$ ein Teil der Klartextmatrix $\boldsymbol{P}(m, l)$, so berechnet die in [11] eingeführte Formel:

$$\boldsymbol{K} = \Big[\sum_{k=1}^{n} \sigma_k \boldsymbol{a}_k \boldsymbol{a}_k^{\mathrm{T}}\Big]^{(\mathrm{p})}\,; \quad \boldsymbol{a}_k = \text{Spalte } k \text{ in } \boldsymbol{A} \tag{1.2}$$

aus dem gegebenen Text und einem Schlüssel $\sigma = (\sigma_1, \ldots, \sigma_k, \ldots, \sigma_n)$ eine umkehrbare Schlüsselmatrix $\boldsymbol{K}$, so dass zusammen mit der Abbildung

$$\Phi : \{\boldsymbol{A}; \sigma\} \to \boldsymbol{K} \tag{1.3}$$

stets auch, so Satz 8 in [11]:

$$\Phi : \{\boldsymbol{K}\boldsymbol{A}; \sigma\} \to \boldsymbol{K}^{-1} \tag{1.4}$$

gilt. Das heisst, dass man die Matrix der Entschlüsselung $\boldsymbol{K}^{-1}$ nach der gleichen Formel und demselben Schlüssel erhält, wie $\boldsymbol{K}$. Ausserdem ist der Schlüssel σ restriktionslos, ein Prinzip, das in der vorliegenden Arbeit bei allen noch zu definierenden Schlüsseln gültig bleibt.

Die Operation (p) ist ein spektrales Pseudoinverses und hat in [5] folgende konstruktive Definition. Ist

$$\boldsymbol{C} = \boldsymbol{T}\begin{bmatrix} \boldsymbol{U} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{S} \end{bmatrix}\boldsymbol{T}^{-1} \tag{1.5}$$

die Jordan Zerlegung der Matrix $\boldsymbol{C} \in \mathbb{F}_{n \times n}$, wobei $\boldsymbol{U}$ den ganzen regulären Block darstellt und $\boldsymbol{S}$ die Gesamtheit der singulären Jordanzellen, so wird

$$\boldsymbol{C}^{(\mathrm{p})} = \boldsymbol{T}\begin{bmatrix} \boldsymbol{U}^{-1} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{E} \end{bmatrix}\boldsymbol{T}^{-1}\,; \quad \boldsymbol{E} = \text{Einheitsmatrix} \tag{1.6}$$

definiert. Diese Formel wird aber nicht zur numerischen Berechnung von $\boldsymbol{C}^{(p)}$ gebraucht. Dafür verwendet man, so wie in [6], [11], ein vollständiges Skelett

$$\boldsymbol{G}_1, \boldsymbol{G}_2, \ldots, \boldsymbol{G}_{k_0}, \Delta, \boldsymbol{H}_{k_0}, \ldots, \boldsymbol{H}_2, \boldsymbol{H}_1$$

für welches dem Satze 1 in [6] nach

$$\boldsymbol{C}^{(p)} = \boldsymbol{E} + \boldsymbol{G}_1\boldsymbol{G}_2 \ldots \boldsymbol{G}_{k_0}\left(\Delta^{-k_0-1} - \Delta^{-k_0}\right)\boldsymbol{H}_{k_0} \ldots \boldsymbol{H}_2\boldsymbol{H}_1 \tag{1.7}$$

gilt.

1.3. Betrachten wir die Formel (1.2) in der üblicheren Schreibart

$$\boldsymbol{K} = \left[\boldsymbol{A}\Sigma\boldsymbol{A}^{\mathrm{T}}\right]^{(p)}; \quad \Sigma = \operatorname{diag}(\sigma_1, \ldots, \sigma_k, \ldots, \sigma_n) \tag{1.8}$$

so war es Hartwig [14], der, von hier ausgehend, die Klasse aller Schlüssel, in einer möglichst allgemeinen Struktur, erweiterte. Für das vorliegende Studium kommen davon aber nur die restriktionslosen Schlüssel in Betracht. Eine solche Schlüsselerweiterung ist es, dass man in $\mathbb{F} = GF(p)$, Σ als eine beliebige symmetrische Matrix nehmen kann. Wir zeigen diesen Beweis in $GF(p)$ mit einer direkten Methode und als eine nahe Ergänzung zum Satz 8 in [11].

Satz 1. Ist Σ symmetrisch, so berechnet die Formel $\boldsymbol{K} = (\boldsymbol{A}\Sigma\boldsymbol{A}^{\mathrm{T}})^{(p)}$ aus $\boldsymbol{A} \in \mathbb{F}_{m\times n}$ und $\Sigma \in \mathbb{F}_{n\times n}$ eine reguläre Schlüsselmatrix $\boldsymbol{K}$,

$$\Phi : \{\boldsymbol{A}; \Sigma\} \to \boldsymbol{K} \tag{1.9}$$

so dass stets

$$\Phi : \{\boldsymbol{K}\boldsymbol{A}; \Sigma\} \to \boldsymbol{K}^{-1} \tag{1.10}$$

gilt.

Beweis. In der Phase der Verschlüsselung wird $\boldsymbol{B} = (\boldsymbol{A}\Sigma\boldsymbol{A}^{\mathrm{T}})^{(p)}\boldsymbol{A}$ gebildet, während bei der Entschlüsselung

$$\boldsymbol{K}_1 = (\boldsymbol{B}\Sigma\boldsymbol{B}^{\mathrm{T}})^{(p)} \tag{1.11}$$

berechnet wird. Es soll $\boldsymbol{K}_1 = \boldsymbol{K}^{-1}$ sein. Das führt zu

$$\left\{(\boldsymbol{A}\Sigma\boldsymbol{A}^{\mathrm{T}})^{(p)} \cdot \boldsymbol{A}\Sigma\boldsymbol{A}^{\mathrm{T}} \cdot \left[(\boldsymbol{A}\Sigma\boldsymbol{A}^{\mathrm{T}})^{(p)}\right]^{\mathrm{T}}\right\}^{(p)} = \left[(\boldsymbol{A}\Sigma\boldsymbol{A}^{\mathrm{T}})^{(p)}\right]^{-1} \tag{1.12}$$

was eine von $\Sigma = \Sigma^{\mathrm{T}}$ bedingte Identität bezüglich $\boldsymbol{A} \in \mathbb{F}_{m\times n}$ sein soll. Indem wir bemerken, dass sich darin überall $\boldsymbol{C} := \boldsymbol{A}\Sigma\boldsymbol{A}^{\mathrm{T}} \in \mathbb{F}_{m\times m}$ herausgebildet hat, verwandelt sich (1.12) in

$$\left[\boldsymbol{C}^{(p)} \cdot \boldsymbol{C} \cdot (\boldsymbol{C}^{(p)})^{\mathrm{T}}\right]^{(p)} = (\boldsymbol{C}^{(p)})^{-1} \tag{1.13}$$

Einem noch zu beweisenden Lemma nach gilt

$$(\boldsymbol{C}^{\mathrm{T}})^{(p)} = (\boldsymbol{C}^{(p)})^{\mathrm{T}} \tag{1.14}$$

Da Σ symmetrisch ist, so ist es auch $\boldsymbol{C} = \boldsymbol{A}\Sigma\boldsymbol{A}^{\mathrm{T}} : \boldsymbol{C}^{\mathrm{T}} = \boldsymbol{C}$. Dann wird (1.14) zu

$$[\boldsymbol{C}^{(p)} \,.\, \boldsymbol{C} \,.\, \boldsymbol{C}^{(p)}]^{(p)} = [\boldsymbol{C}^{(p)}]^{-1} \tag{1.15}$$

Anhand der Definitionsformel (1.6) kann man nachprüfen, dass dieses eine Identität ist, für alle $\boldsymbol{C} \in \mathbb{F}_{m\times m}$. □

Bemerkung. In [12] haben wir, die bedingte Identität (1.2) analysierend, bewiesen, dass die Bedingung $\Sigma = \Sigma^{\mathrm{T}}$ im Falle $p \neq 2$, $m \geqq 2$ auch notwendig ist im Zusammenhang dieses Satzes. Dann ist die Menge der symmetrischen Schlüsselmatrizen $\boldsymbol{M} = \{\Sigma; \Sigma^{\mathrm{T}} = \Sigma\}$ vollständig.

1.4. Sei

$$\boldsymbol{A} = \boldsymbol{A}_1 + \boldsymbol{A}_2\,; \quad (\boldsymbol{A}, \boldsymbol{A}_1, \boldsymbol{A}_2) \subset \mathbb{F}_{m\times n} \tag{1.16}$$

die in [5] definierte, eindeutige innsere Zerlegung (one line decomposition) einer rechteckigen Matrix in einem Körper $GF(p) = \mathbb{F}$. Dabei ist

$$\boldsymbol{A}_1\boldsymbol{A}_2^{\mathrm{T}} = \boldsymbol{0}\,, \quad \boldsymbol{A}_1^{\mathrm{T}}\boldsymbol{A}_2 = \boldsymbol{0}\,, \quad (\boldsymbol{A}_2\boldsymbol{A}_2^{\mathrm{T}})^k = \boldsymbol{0} \tag{1.17}$$

und für die Matrix $\boldsymbol{A}_1$ hat das System von Penrose

$$\boldsymbol{A}_1\boldsymbol{X}\boldsymbol{A}_1 = \boldsymbol{A}_1;\ \boldsymbol{X}\boldsymbol{A}_1\boldsymbol{X} = \boldsymbol{X}\,; \quad (\boldsymbol{A}_1\boldsymbol{X})^{\mathrm{T}} = \boldsymbol{A}_1\boldsymbol{X}\,; \quad (\boldsymbol{X}\boldsymbol{A}_1)^{\mathrm{T}} = \boldsymbol{X}\boldsymbol{A}_1 \tag{1.18}$$

eine Lösung, die mit $\boldsymbol{A}_1^{\dagger}$ bezeichnet wird. Das in [5] definierte verallgemeinerte Inverse einer Matrix in einem Körper, das jenes von Moore-Penrose verallgemeinert, hat die Form $\boldsymbol{A}^{\dagger} = \boldsymbol{A}_1^{\dagger} + \boldsymbol{A}_2^{\mathrm{T}}$. Da es die für die Lineare Kryptographie bedeutsame Rekursiveigenschaft $(\boldsymbol{A}^{\dagger})^{\dagger} = \boldsymbol{A}$ hat, so befand es sich in [10], [11] im Ursprung der Einführung von Pseudo-Inversen in die Kryptographie. Um damit Verschlüsselungsabbildungen der Form $f : \mathbb{F}_{m\times n} \to \mathbb{F}_{m\times n}$ zu definieren, ist es, da $\boldsymbol{A} \in \mathbb{F}_{m\times n}$, $\boldsymbol{A}^{\dagger} \in \mathbb{F}_{n\times m}$ gilt, zweckmässig, noch die zusätzliche Bezeichnung

$$\boldsymbol{A}^{\mp} := (\boldsymbol{A}^{\dagger})^{\mathrm{T}} \in \mathbb{F}_{m\times n} \tag{1.19}$$

einzuführen. Dann ist

$$f(\boldsymbol{Z}) = \boldsymbol{Z}^{\mp} \tag{1.20}$$

eine vorerst parameterlose Verschlüsselungsabbildung, die mit ihrer Entschlüsselungsabbildung übereinstimmt, zumal $(\boldsymbol{Z}^{\mp})^{\mp} = \boldsymbol{Z}$ gilt. Um darin zusammen mit Hartwig [14] einen Schlüssel der Form $(\xi, \eta) \in \mathbb{F}^2$ einzuführen, sei, von der inneren Zerlegung (1.16) ausgehend, folgendes definiert

$$\boldsymbol{A}^{\mp}(\xi, \eta) = \xi\boldsymbol{A}_1^{\mp} + \eta\boldsymbol{A}_2\,; \quad (\xi \neq 0 \neq \eta) \tag{1.21}$$

Dafür gilt

$$\begin{aligned}[\boldsymbol{A}^{\mp}(\xi, \eta)]^{\mp}(\xi, \eta^{-1}) &= (\xi\boldsymbol{A}_1^{\mp} + \eta\boldsymbol{A}_2^{\mp})^{\mp}(\xi, \eta^{-1}) = \\ &= \xi(\xi\boldsymbol{A}_1^{\mp})^{\mp} + \eta^{-1}(\eta\boldsymbol{A}_2) = \boldsymbol{A}_1 + \boldsymbol{A}_2 = \boldsymbol{A}\end{aligned} \tag{1.22}$$

Demnach hat die Verschlüsselungsabbildung

$$f(\boldsymbol{Z}) = \boldsymbol{Z}^{\mp}(\xi, \eta) \tag{1.23}$$

als Entschlüsselungsabbildung die Funktion

$$f^{-}(\boldsymbol{Z}) = \boldsymbol{Z}^{\mp}(\xi, \eta^{-1}) \tag{1.24}$$

zumal $f^{-}[f(\boldsymbol{Z})] = \boldsymbol{Z}$; $\boldsymbol{Z} \in \mathbb{F}_{m\times n}$ gilt.

Nun erfolgt aber die numerische Berechnung von $\boldsymbol{Z}^{\mp}(\xi, \eta)$ nicht nach der inneren Zerlegung (1.16), sondern entweder nach einem verallgemeinerten Skelett [6], [11]:

$$\boldsymbol{A}^{\mp}(\xi, \eta) = \eta\boldsymbol{A} + \boldsymbol{G}\boldsymbol{G}_1\boldsymbol{G}_2 \ldots \boldsymbol{G}_{k_0}(\xi\Delta^{-k_0-1} - \eta\Delta^{-k_0})\,\boldsymbol{H}_{k_0} \ldots \boldsymbol{H}_1\boldsymbol{H} \tag{1.25}$$

oder mit einem Drazin Inversen.

Von der Jordanform (1.5) ausgehend, hat das Drazin Inverse einer Matrix in einem Körper $\boldsymbol{C} \in \mathbb{F}_{n\times n}$ die Gestalt

$$\boldsymbol{C}^{\mathrm{d}} = \boldsymbol{T}\begin{bmatrix}\boldsymbol{U}^{-1} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{0}\end{bmatrix}\boldsymbol{T}^{-1} \tag{1.26}$$

Es ist die eindeutige Lösung eines multiplikativen Systems

$$\boldsymbol{C}^{k+1}\boldsymbol{X} = \boldsymbol{C}^{k}\boldsymbol{X}, \quad \boldsymbol{X}\boldsymbol{C}\boldsymbol{X} = \boldsymbol{X}, \quad \boldsymbol{X}\boldsymbol{C} = \boldsymbol{C}\boldsymbol{X}; \quad k \geqq k_0 \tag{1.27}$$

und hat deswegen unter den spektralen Pseudo-Inversen eine zentrale Stellung. Eine Eigenschaft von $\boldsymbol{C}^{\mathrm{d}}$, die Hartwig [14] direkt aus diesem System bemerkt hat, ist

$$[\boldsymbol{C}^{*}]^{\mathrm{d}} = [\boldsymbol{C}^{\mathrm{d}}]^{*} \tag{1.28}$$

wobei $(\cdot)^{*}$ ein gerader oder schiefer Morphismus bezüglich der Multiplikation ist, so wie es auch die Transponierung ist. Damit können wir die Formel (1.14) beweisen.

Lemma 1. Für eine Matrix in einem Körper $\boldsymbol{C} \in \mathbb{F}_{n\times n}$ gilt:

$$(\boldsymbol{C}^{\mathrm{T}})^{(\mathrm{p})} = (\boldsymbol{C}^{(\mathrm{p})})^{\mathrm{T}} \tag{1.14}$$

Beweis. Das folgt, wenn man feststellt, dass

$$\boldsymbol{C}^{(\mathrm{p})} = \boldsymbol{E} + \boldsymbol{C}^{\mathrm{d}} - \boldsymbol{C}\boldsymbol{C}^{\mathrm{d}} \tag{1.29}$$

gilt, darin die Transponierung anwendet und die Beziehung (1.28) beachtet. □

Definieren wir

$$\boldsymbol{C}^{(\mathrm{p})}(\xi, \eta) = \xi\boldsymbol{C}^{\mathrm{d}} + \eta(\boldsymbol{E} - \boldsymbol{C}\boldsymbol{C}^{\mathrm{d}}) = \boldsymbol{T}\begin{bmatrix}\xi\boldsymbol{U}^{-1} & \boldsymbol{0}\\ \boldsymbol{0} & \eta\boldsymbol{E}\end{bmatrix}\boldsymbol{T}^{-1} \tag{1.30}$$

so kann man damit als eine Verallgemeinerung des Satzes 3 in [5] die Matrix $\boldsymbol{A}^{\mp}(\xi, \eta)$ wie folgt ausdrücken:

$$\boldsymbol{A}^{\mp}(\xi, \eta) = [(\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}})^{(\mathrm{p})}(\xi, \eta)]\,.\,\boldsymbol{A} = \boldsymbol{A}\,.\,[(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A})^{(\mathrm{p})}(\xi, \eta)] \tag{1.31}$$

Wir führen dann auch noch die Formel von $\boldsymbol{C}^{(p)}(\xi, \eta)$ mit einem vollständigen Skelett der Matrix $\boldsymbol{C}$ an:

$$\boldsymbol{C}^{(p)}(\xi, \eta) = \eta \boldsymbol{E} + \boldsymbol{G}_1 \boldsymbol{G}_2 \ldots \boldsymbol{G}_{k_0}(\xi \Delta^{-k_0-1} - \eta \Delta^{-k_0}) \boldsymbol{H}_{k_0} \ldots \boldsymbol{H}_2 \boldsymbol{H}_1 \tag{1.32}$$

Für $\xi = 1$, $\eta = 0$ ist das Clines Formel [1] für das Drazin Inverse, während für $\xi = 1$, $\eta = 1$ ist es unsere Formel (1.6) für $\boldsymbol{C}^{(p)}$.

1.5. Von den bisher betrachten Verschlüsselungsabbildungen

$$f(\boldsymbol{Z}) = (\boldsymbol{Z}\Sigma\boldsymbol{Z}^{\mathrm{T}})^{(p)}\, \boldsymbol{Z}\,; \quad \Sigma = \Sigma^{\mathrm{T}}$$

und

$$f(\boldsymbol{Z}) = \boldsymbol{Z}^{\mp}(\xi, \eta)\,; \quad \xi \neq 0 \neq \eta$$

stimmt die erste, entsprechend dem Satze 1 mit ihrer Entschlüsselungsabbildung überein $f^{-}(\boldsymbol{Z}) = f(\boldsymbol{Z})$, während für die zweite $f^{-}(\boldsymbol{Z}) = \boldsymbol{Z}^{\mp}(\xi, \eta^{-1})$ gezeigt wurde. Da für $\Sigma = \boldsymbol{E}$ entsprechend dem Satze 3 in [5]

$$f(\boldsymbol{Z}) := (\boldsymbol{Z}\boldsymbol{Z}^{\mathrm{T}})^{(p)}\, \boldsymbol{Z} = \boldsymbol{Z}^{\mp} \tag{1.33}$$

gilt, so kann man für eine Vereinheitlichung der Bezeichnungen übereinkommen

$$\boldsymbol{Z}^{\mp}(\Sigma) := (\boldsymbol{Z}\Sigma\boldsymbol{Z}^{\mathrm{T}})^{(p)}\, \boldsymbol{Z} \tag{1.34}$$

als ein Σ-relatives verallgemeinertes Inverses zu betrachten. Mit dieser Bezeichnung hat Satz 1 die Form

$$[\boldsymbol{Z}^{\mp}(\Sigma)]^{\mp}(\Sigma) = \boldsymbol{Z}\,; \quad \boldsymbol{Z} \in \mathbb{F}_{m \times n} \tag{1.35}$$

eine Identität, die für $GF(p)$, $p \neq 2$, $m \geqq 2$ notwendigerweise von $\Sigma^{\mathrm{T}} = \Sigma$ bedingt ist.

Zusammensetzen der bisher erreichten Verschlüsselungsabbildungen ergibt

$$f(\boldsymbol{Z}) := \boldsymbol{Z}^{\mp}(\xi, \eta, \Sigma) := [(\boldsymbol{Z}\Sigma\boldsymbol{Z})^{(p)}(\xi, \eta)]\, \boldsymbol{Z} \tag{1.36}$$

Eine Verallgemeinerung von Satz 1 ist folgende Aussage.

Satz 2. Ist $\Sigma \in \mathbb{F}_{n \times n}$ eine symmetrische Matrix und $\xi \neq 0 \neq \eta$, so gilt identisch

$$[\boldsymbol{Z}^{\mp}(\xi, \eta, \Sigma)]^{\mp}(\xi, \eta^{-1}, \Sigma) = \boldsymbol{Z}\,; \quad \boldsymbol{Z} \in \mathbb{F}_{m \times n} \tag{1.37}$$

Beweis. In einer zum Satz 1 analogen Beweisart wird man sich diesmal auf

$$[\boldsymbol{C}^{(p)}(\xi, \eta)\,.\,\boldsymbol{C}\,.\,\boldsymbol{C}^{(p)}(\xi, \eta)]^{(p)}(\xi, \eta) = [\boldsymbol{C}^{(p)}(\xi, \eta^{-1})]^{-1} \tag{1.38}$$

stützen, eine Identität, die man auf grund der Definitionsformel (1.30) verifizieren kann. □

Weitere Aussagen dieser Art in allgemeineren Strukturen findet man bei Hartwig [14]. Entsprechend diesem Satz wird die Entschlüsselungsabbildung bezüglich (1.36) folgende Form haben:

$$f^{-}(\boldsymbol{Z}) = \boldsymbol{Z}^{\mp}(\xi, \eta^{-1}, \Sigma) \tag{1.39}$$

Führen wir noch einen additiven Schlüssel $\boldsymbol{\beta} \in \mathbb{F}_{m \times n}$ ein, so kann man auch die Verschlüsselungsabbildung

$$f(\boldsymbol{Z}) = \boldsymbol{Z}^{\mp}(\xi, \eta, \Sigma) + \boldsymbol{\beta} \tag{1.40}$$

schreiben, deren Entschlüsselungsabbildung die Form

$$f^{-}(\boldsymbol{Z}) = (\boldsymbol{Z} - \boldsymbol{\beta})(\xi, \eta^{-1}, \Sigma) \tag{1.41}$$

hat. Dazu kann man auch einige Sonderfälle betrachten, wie zum Beispiel

$$\begin{aligned} &f(\boldsymbol{Z}) = \boldsymbol{Z}^{\mp} + \boldsymbol{\beta}\,; \qquad f^{-}(\boldsymbol{Z}) = (\boldsymbol{Z} - \boldsymbol{\beta})^{\mp} \\ &f(\boldsymbol{Z}) = \boldsymbol{Z}^{\mp}(\xi, \eta) + \boldsymbol{\beta}\,; \quad f^{-}(\boldsymbol{Z}) = (\boldsymbol{Z} - \boldsymbol{\beta})^{\mp}(\xi, \eta^{-1}) \\ &f(\boldsymbol{Z}) = \boldsymbol{Z}^{\mp}(\Sigma) + \boldsymbol{\beta}\,; \qquad f^{-}(\boldsymbol{Z}) = (\boldsymbol{Z} - \boldsymbol{\beta})^{\mp}(\Sigma) \end{aligned} \tag{1.42}$$

Der Schlüssel $\boldsymbol{\beta}$ hat die Rolle, die parameterbezogenen verallgemeinerten Inversen $\boldsymbol{Z}^{\mp}(\xi, \eta, \Sigma)$ zu perturbieren. Andere Schlüssel dieser Art, wie zum Beispiel eine Permutation π von markierten Stellen in der Matrix $\boldsymbol{Z}$ oder ein Tauschalphabet, das eine Permutation μ in $GF(p)$ ist, könnten dem Vergleich mit dem einfacheren additiven Schlüssel $\boldsymbol{\beta}$ nicht standhalten. Um aber eine möglichst allgemeine Verschlüsselungsabbildung zu schreiben, betrachten wir auch

$$f(\boldsymbol{Z}) = \pi\mu\boldsymbol{Z}^{\mp}(\xi, \eta, \Sigma) + \boldsymbol{\beta}\,; \quad \boldsymbol{Z} \in \mathbb{F}_{m \times n} \tag{1.43}$$

mit der Entschlüsselungsabbildung

$$f^{-}(\boldsymbol{Z}) = [\pi^{-1}\mu^{-1}(\boldsymbol{Z} - \boldsymbol{\beta})]^{\mp}(\xi, \eta^{-1}, \Sigma) \tag{1.44}$$

Für einen ausgewogenen Haushalt der Parameter wird aber die Menge der Schlüssel der Form

$$\zeta = (\xi, \eta, \Sigma, \boldsymbol{\beta}) \tag{1.45}$$

vorerst ausreichen.

1.6. Im Falle einer langen Klartextmatrix $\boldsymbol{P}(m, l)$ sei vereinbart, dass diese als eine Folge gleichartig dimensionierter Untermatrizen

$$\boldsymbol{X}_1(m, n), \boldsymbol{X}_2(m, n), \ldots, \boldsymbol{X}_i(m, n), \ldots, \boldsymbol{X}_q(m, n) \tag{1.46}$$

dargestellt wird. Die Dimensionszahlen (m, n) werden einmal festgelegt und als konstant betrachtet. Die Matrizen $\boldsymbol{X}_i(m, n)$ können als Seiten des Textes bezeichnet werden.

Wir werden dann, ohne schon die allgemeinen Täfelungen einzusetzen, sondern nur die bisherigen Formeln verwendend, folgende Verschlüsselungsstrategien betrachten.

a) Alle Seiten $\boldsymbol{X}_i(m, n)$; $(i = 1, \ldots, q)$ werden entsprechend einem festen Schlüssel $\zeta = (\xi, \eta, \Sigma, \boldsymbol{\beta})$ mit den Formeln (1.40) und (1.41) verschlüsselt und entschlüsselt.

b) Mit den Parametern einer markierten Seite $\boldsymbol{X}_{i_0}(m, n)$ und einem gegebenen festen Schlüssel $\zeta = (\xi, \eta, \Sigma, \boldsymbol{\beta})$ wird eine reguläre Schlüsselmatrix berechnet:

$$\boldsymbol{K} = [\boldsymbol{X}_{i_0} \Sigma \boldsymbol{X}_{i_0}^{\mathrm{T}}]^{(\mathrm{p})}(\xi, \eta) \tag{1.47}$$

Damit werden alle Seiten verschlüsselt

$$\boldsymbol{Y}_i = \boldsymbol{K}\boldsymbol{X}_i + \boldsymbol{\beta}\,; \quad (i = 1, \ldots, q) \tag{1.48}$$

Die Entschlüsselung erfolgt offenbar nach

$$\boldsymbol{X}_i = \boldsymbol{K}^{-1}(\boldsymbol{Y}_i - \boldsymbol{\beta})\,; \quad (i = 1, \ldots, q) \tag{1.49}$$

wobei $\boldsymbol{K}^{-1}$ aus dem Kryptogramm $\boldsymbol{Y}_{i_0}$ der markierten Seite $\boldsymbol{X}_{i_0}$ und dem gegebenen Schlüssel ζ, nach folgender Formel berechnet wird

$$\boldsymbol{K}^{-1} = [(\boldsymbol{Y}_{i_0} - \boldsymbol{\beta})\, \Sigma (\boldsymbol{Y}_{i_0} - \boldsymbol{\beta})^{\mathrm{T}}]^{(\mathrm{p})}(\xi, \eta^{-1}) \tag{1.50}$$

c) Da die Schlüssel $\zeta = (\xi, \eta, \Sigma, \boldsymbol{\beta})$, abgesehen von $\xi \neq 0 \neq \eta$, $\Sigma^{\mathrm{T}} = \Sigma$, keinen Restriktionen unterstellt sind, so kann man es einem vereinbarten Zufallsgenerator überlassen, für jede Seite $\boldsymbol{X}_i(m, n)$ einen Schlüssel ζ_i zu erzeugen und damit nach der besprochenen Prozedur zu verschlüsseln und entschlüsseln.

Für jede dieser Strategien kann man auch die verschiedenen Sonderfällen der allgemeinen Formel (1.40) betrachten.

Bezeichnungen.

$\rightarrow$: siehe
p, p_0 : Primzahlen
$\mathbb{Z}$: Ring der ganzen Zahlen
$GF(p) : \cong \mathbb{Z}/p$
$\mathbb{F}_{m \times n}$: $m \times n$ Matrizen über $\mathbb{F}$
$(\cdot)^{\mathrm{T}}$, $(\cdot)^{\dagger}$, $(\cdot)^{\mathrm{d}}$: Transponierung, verallgemeinertes Inverses, Drazin Inverses
$\boldsymbol{A}^{\mp}$, $\boldsymbol{A}^{\mp}(\xi, \eta)$, $\boldsymbol{A}^{\mp}(\xi, \eta, \Sigma) : \rightarrow$ (1.19), (1.21), (1.36)
$\boldsymbol{C}^{(\mathrm{p})}$, $\boldsymbol{C}^{(\mathrm{p})}(\xi, \eta) : \rightarrow$ (1.6), (1.30)
$\square_{k=1 \div s}$: $\rightarrow$ (2.3)
$\boldsymbol{A}^{\mp}(\xi, \eta, \tau) : \rightarrow$ (2.5)

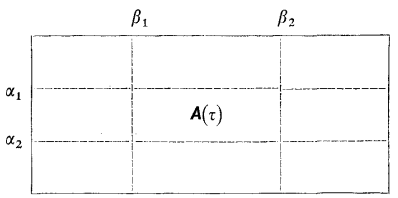
2. VERSCHLUSSELÜNGSSTRATEGIEN MIT TÄFELUNGEN

Zumal die verallgemeinerten Inversen $\boldsymbol{A}^{\dagger}$, $\boldsymbol{A}^{\mp}(\xi, \eta)$, $\boldsymbol{A}^{\mp}(\Sigma)$, $\boldsymbol{A}^{\mp}(\xi, \eta, \Sigma)$ für eine beliebige rechteckige Matrix $\boldsymbol{Z} \in \mathbb{F}_{q \times r}$ definiert wurden, so sind diese Operationen insbesondere auch für eine beliebige Untermatrix von $\boldsymbol{A} = \boldsymbol{A}(m, n)$ definierbar. Ein Täfelchen $\boldsymbol{Z}(\tau)$ von $\boldsymbol{A}$ wird von vier Parametern

$$\tau = (\alpha_1, \alpha_2, \beta_1, \beta_2) \quad \text{mit} \quad 1 \leqq \alpha_1 \leqq \alpha_2 \leqq m\,, \quad 1 \leqq \beta_1, \beta_2 \leqq n \tag{2.1}$$

ausgezeichnet, so wie es im folgenden Schema deutlich ist.

(2.2)



Eine vollständige Zerlegung von $\boldsymbol{A}$ in disjunkte Täfelchen definiert eine echte Täfelung τ, wofür eine geeignete Bezeichnung zweckmässig ist:

$$\boldsymbol{A} := \square_{k=1 \div s} \boldsymbol{A}(\tau_k); \quad \tau = (\tau_1, \tau_2, \ldots, \tau_s) \tag{2.3}$$

Ersetzt man darin jedes Täfelchen mit seinem verallgemeinerten Inversen, so bezeichne

$$\boldsymbol{A}^{\mp}(\tau) = \square_{k=1 \div s} [\boldsymbol{A}(\tau_k)]^{\mp} \tag{2.4}$$

Analog sei

$$\boldsymbol{A}^{\mp}(\xi, \eta, \tau) = \square_{k=1 \div s} [\boldsymbol{A}(\tau_k)]^{\mp}(\xi, \eta); \quad (\xi \neq 0 \neq \eta) \tag{2.5}$$

Zumal die Rekursiveigenschaften gültig bleiben

$$[\boldsymbol{A}^{\mp}(\tau)]^{\mp}(\tau) = \boldsymbol{A}; \qquad \boldsymbol{A} \in \mathbb{F}_{m \times n} \tag{2.6}$$

$$[\boldsymbol{A}^{\mp}(\xi, \eta, \tau)]^{\mp}(\xi, \eta^{-1}, \tau) = \boldsymbol{A}; \quad \boldsymbol{A} \in \mathbb{F}_{m \times n} \tag{2.7}$$

so eignen sich diese Konstruktionen zur Definierung weiterer Verschlüsselungsabbildungen. Dafür kann man drei Strategien betrachten.

a) Zur Verschlüsselung von $\boldsymbol{Z} = \boldsymbol{Z}(m, n)$ sei ein fester Schlüssel

$$\zeta = (\xi, \eta, \Sigma, \boldsymbol{\beta}); \quad (\xi, \eta) \in \mathbb{F}^2, \Sigma \in \mathbb{F}_{n \times n}, \boldsymbol{\beta} \in \mathbb{F}_{m \times n}, \Sigma^{\mathrm{T}} = \Sigma, \quad \xi \neq 0 \neq \eta \tag{2.8}$$

und eine verschlüsselte Täfelung $\tau = (\tau_1, \tau_2, \ldots, \tau_s)$ gegeben. Ist $\tau_k = (\alpha_1, \alpha_2, \beta_1, \beta_2)$, dann bezeichne $\tilde{\tau}_k = (\beta_1, \beta_2, \beta_1, \beta_2)$. Dementsprechend mögen $\boldsymbol{\beta}_k = \boldsymbol{\beta}(\tau_k)$ und $\Sigma_k := \Sigma(\tilde{\tau}_k)$ die ausgezeichneten Täfelchen, dem Schema (2.2) zufolge, bezeichnen. Bezeichnet ausserdem $\boldsymbol{Z}_k := \boldsymbol{Z}(\tau_k)$, so gehört zur Verschlüsselungsabbildung

$$f(\boldsymbol{Z}) = \square_{k=1 \div s} \boldsymbol{Z}_k^{\mp}(\xi, \eta, \Sigma_k) + \boldsymbol{\beta}_k \tag{2.9}$$

die Entschlüsselungsabbildung

$$f^{-}(\boldsymbol{Z}) = \square_{k=1 \div s} (\boldsymbol{Z} - \boldsymbol{\beta})_k^{\mp}(\xi, \eta^{-1}, \Sigma_k) \tag{2.10}$$

Varianten dafür hat man durch Partikularisierung der Schlüssel.

b) Es wird im Abschnitt 3 gezeigt, wie sich eine allgemeine Täfelung mit einem Zufallsgenerator $\mathfrak{z} = \{z(k)\} \subset GF(p)$ erzeugen lässt. Dann sei vereinbart, dass,

sobald der Wert $z(k_0)$ das Täfelchen $\boldsymbol{Z}_k = \boldsymbol{Z}_k(m_k, n_k)$ ausgezeichnet hat, die fortlaufenden Werte des gleichen Zufallsgenerators $z(k_0 + 1), z(k_0 + 2), \ldots, z(k_0 + t)$ einen Schlüssel $\zeta_k = (\xi_k, \eta_k, \Sigma_k, \boldsymbol{\beta}_k)$ erzeugen mögen, mit dem die Transformation von $\boldsymbol{Z}_k(m_k, n_k)$ erfolgen kann. Dann hat man solche Verschlüsselungs- und Entschlüsselungsabbildungen, die von einem Zufallsgenerator abhängen und von gewissen programmspezifischen Anweisungen.

$$f(\boldsymbol{Z}) = \square_{k=1 \div s} \boldsymbol{Z}_k^{\mp}(\xi_k, \eta_k, \Sigma_k) + \boldsymbol{\beta}_k ; \quad \Sigma_k^{\mathrm{T}} = \Sigma_k , \quad \xi_k \neq 0 \neq \eta_k \tag{2.11}$$

$$f^{-}(\boldsymbol{Z}) = \square_{k=1 \div s} (\boldsymbol{Z}_k - \boldsymbol{\beta}_k)^{\mp} (\xi_k, \eta_k^{-1}, \Sigma_k) \tag{2.12}$$

Die Kardinalzahl der dabei verwendeten Schlüsselelemente, die von $\mathfrak{z} = \{z(k)\}$ erzeugt werden, ist in dieser Variante $|\zeta| = \sum_{k=1}^{s} (4 + m_k n_k + n_k^2)$ und hängt von der Täfelung τ ab, die gleichfalls von $\mathfrak{z}$ erzeugt wird.

Für einen ausgewogenen Haushalt der Parameter kann es zu den programmspezifischen Anweisungen auch gehören, dass $\Sigma_k = \Sigma_k(n_k, n_k)$ im Besonderen nur eine allgemeine Diagonalmatrix $\Sigma_k = \mathrm{diag}\,(\sigma_1, \ldots, \sigma_{n_k})$ sein soll, oder eine Diagonalmatrix mit nur wenigen eingestreuten symmetrischen nichtdiagonal Elementen. Bezüglich $\boldsymbol{\beta}_k$ kann man im Besonderen anweisen, dass es nur an einer Stelle nullverschieden ist, das heisst das $\boldsymbol{\beta}_k$ nur eine Stelle in $\boldsymbol{Z}_k^{\mp}(\xi_k, \eta_k, \Sigma_k)$ additiv perturbiert, so wie es zum Beispiel die in §3 erklärte dominante Stelle des Täfelchens $\boldsymbol{Z}_k$ sein kann. Anweisungen dieser Art führen auch zur Definierung von gewissen Startvektoren und Stopzahlen. Schliesslich kann man anweisen, dass eine der Dimensionszahlen der Täfelchen beschränkt sei.

c) In der vorherigen Strategie 2.1.b. verfügte man über einen laufenden Zufallsgenerator und ein Verschlüsselungsprogramm. Es ist dann eine einfache zusätzliche Anweisung, dass man mit demselben Zufallsgenerator und gleichem Programm die Matrix zwei- oder dreimal übertäfelt und programmgemäss iterativ verschlüsselt. Da es jedesmal eine andere Täfelung ist, so kann dadurch der Sicherheitsgrad beliebig steigen. Bei der Entschlüsselung bedarf man dabei noch nicht des inversen Verlaufs des Zufallsgenerators. Setzt man voraus, dass im Falle von drei Täfelungen: $\boldsymbol{Z}_1, \boldsymbol{Z}_2, \boldsymbol{Z}_3$ die Startvektoren des Zufallsgenerators $\mathfrak{z} = \{z(k)\}$ für diese Täfelungen sind, so hat man bei der Entschlüsselung nur die Reihenfolge dieser Vektoren umzukehren: $\boldsymbol{Z}_3, \boldsymbol{Z}_2, \boldsymbol{Z}_1$. Die Stopzahlen ergeben sich in einer echten Täfelung aus dem Programm. Eine sinnvolle Partikularisierung in dieser Variante ist es, wenn man ausser den verschlüsselten Täfelungen keine weiteren Schlüssel der Gestalt $(\xi, \eta, \Sigma, \boldsymbol{\beta})$ hinzunimmt, sondern die Täfelchen nur mit reinen verallgemeinerten Inversen der Form (1.20) transformiert.

2.2. Wir bezeichnen, vom Schema (2.2) ausgehend, mit $\boldsymbol{A}^{\mp}(\xi, \eta, \Sigma(\tilde{\tau}), \tau)$ eine Matrix, die ausserhalb des ausgezeichneten Täfelchens $\boldsymbol{A}(\tau)$ mit $\boldsymbol{A}(m, n)$ übereinstimmt,

und an die Stelle von $\boldsymbol{A}(\tau)$ das transformierte Täfelchen $[\boldsymbol{A}(\tau)]^{\mp}(\xi, \eta, \Sigma(\tilde{\tau}))$ gesetzt wird; $\Sigma(\tilde{\tau})$ wurde bereits erklärt. Ist nun eine von einem Zufallsgenerator $\mathfrak{z} = \{z(k)\} \subset$ $\subset GF(p)$ erzeugte freie Täfelung

$$\tau = (\tau_1, \tau_2, \ldots, \tau_i, \tau_{i+1}, \ldots, \tau_t) \tag{2.13}$$

gegeben, deren Komponenten im allgemeinen nicht disjunkt sein müssen, so kann die Iteration

$$\begin{aligned} \boldsymbol{A}_1 &= \boldsymbol{A}^{\mp}(\xi, \eta, \Sigma(\tilde{\tau}_1), \tau_1) \\ \boldsymbol{A}_j &= \boldsymbol{A}_{j-1}^{\mp}(\xi, \eta, \Sigma(\tilde{\tau}_j), \tau_j)\,; \quad j = 2, \ldots, t \end{aligned} \tag{2.14}$$

eine Verschlüsselungsstrategie ergeben, deren Entschlüsselung nach der inversen Iteration

$$\boldsymbol{A}_{j-1} = \boldsymbol{A}_j^{\mp}(\xi, \eta^{-1}, \Sigma(\tilde{\tau}_j), \tau_j)\,; \quad j = t, \ldots, 2, 1 \tag{2.15}$$

erfolgt, wozu man auch den inversen Ablauf des Zufallsgenerators benötigt. Von Interesse kann dabei eine Variante mit folgenden Merkmalen sein.

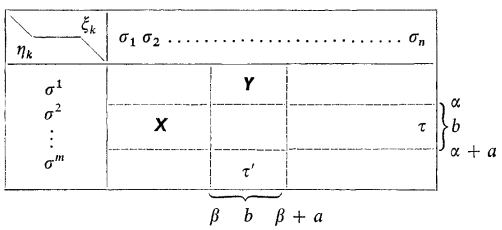
(i) Die Täfelchen τ_j mögen entweder Streifen horizontaler Art $\tau = (\alpha, \alpha + a, 1, n)$ oder vertikaler Art $\tau' = (1, m, \beta, \beta + a)$ sein, wobei für die Breite $b = a + 1$ nur die Werte 1, 2, 3 zugelassen werden. Wenn $\alpha + a$ den Wert m, oder $\beta + a$ den Wert n überschreiten, so ergänzt man den entsprechenden Streifen zyklisch mit Zeilen oder Spalten vom Anfang der Matrix.

(ii) Für einen ausgewogenen Haushalt der Parameter betrachte man an Stelle von $\Sigma = \Sigma(n, n)$ entweder eine feste Diagonalmatrix $\Sigma_1 = \operatorname{diag}(o_1, \ldots, \sigma_n)$, dann wenn der zu transformierende Streifen horizontaler Art ist oder eine zweite feste Diagonalmatrix $\Sigma_2 = \operatorname{diag}(\sigma^1, \ldots, \sigma^m)$ dann, wenn der Streifen vertikaler Art ist. Ausserdem sei die Perturbation $\boldsymbol{\beta} = 0$.

(iii) Ein Zufallsgenerator $\mathfrak{z} = \{z(k)\} \subset GF(p)$ mag entscheiden, wie die Alternierung horizontaler und vertikaler Streifen zu erfolgen hat, und mag ausserdem die Werte $1 \leqq \alpha_i \leqq m$ und $1 \leqq \beta_j \leqq n$ erzeugen sowie auch den Schlüssel (ξ_k, η_k).

Für diese die Matrix $\boldsymbol{A}(m, n)$ stochastisch horizontal und vertikal abtastende Täfelungsstrategie betrachten wir folgendes Schema:

(2.16)



Dabei wird ein Täfelchen horizontaler Art $\tau_i = \tau = (\alpha_i, \alpha_i + a, 1, n)$ nach der Formel

$$\boldsymbol{A}_{i-1}(\tau_i) := \boldsymbol{X} \to (\boldsymbol{X}\Sigma_1\boldsymbol{X}^{\mathrm{T}})^{(\mathrm{p})}(\xi_i, \eta_i)\,.\,\boldsymbol{X} := \boldsymbol{A}_i(\tau_i) \tag{2.17}$$

transformiert, während ein Täfelchen vertikaler Art die Transformationsformel

$$\boldsymbol{A}_{j-1}(\tau_j) := \boldsymbol{Y} \to \boldsymbol{Y}(\boldsymbol{Y}^{\mathrm{T}}\Sigma_2\boldsymbol{Y})^{(\mathrm{p})}(\xi_j, \eta_j) := \boldsymbol{A}_j(\tau_j) \tag{2.18}$$

hat. Die gewählte Länge der Iteration wird von der Qualität des Zufallsgenerators abhängen und, da man auch jenen mit inversem Ablauf benötigt, so betrachtet man $\mathfrak{z} = \{z(k)\} \subset GF(p)$ am besten in der Form

$$z_k = a_1 z_{k-1} + a_2 z_{k-2} + \ldots + a_r z_{k-r} + a_0 \tag{2.19}$$

2.3. Im Falle der one line Nachrichtenübertragung ist es bedeutsam, das Verschlüsselung und Entschlüsselung möglichst schnell erfolgen. In der Berechnung von $\boldsymbol{C}^{(\mathrm{p})}(\xi, \eta)$ und $\boldsymbol{A}^{\mp}(\xi, \eta)$ mit einem vollständigen oder verallgemeinerten Skelett, wie in (1.32), (1.25), gibt es aber eine relative Komplexität, die zur Sicherheit des Systems gehört. Überlegt man, dass auch eine allgemeine, echte oder freie Täfelung einen zusätzlichen nur schwer durchschaubaren Schlüssel darstellt und will man auf ein Programm mit einem vollständigen Skelett verzichten, so kann man anweisen, dass eine der Dimensionszahlen der Täfelchen nicht die Schranke $b = 3$ überschreitet. Dann gibt es für $\boldsymbol{C}^{(\mathrm{p})}(\xi, \eta)$ eine direktere Formel als jene mit einem vollständigen Skelett.

Wir betrachten dafür das charakteristische Polynom einer Matrix dritter Ordnung in der Form

$$\Delta(\lambda) = \det(\boldsymbol{C} - \lambda\boldsymbol{E}) = -\lambda^3 + \mu_1\lambda^2 - \mu_2\lambda + \mu_3 \tag{2.20}$$

so dass

$$\mu_1 = \mathrm{sp}\,\boldsymbol{C}\,, \quad \mu_2 = \sum_{1 \leqq k < j \leqq 3} \begin{vmatrix} c_{kk} & c_{kj} \\ c_{jk} & c_{jj} \end{vmatrix}, \quad \mu_3 = \det \boldsymbol{C} \tag{2.21}$$

gilt. Ausserdem bezeichne $r = \mathrm{Rang}\ \boldsymbol{C}$, $\varrho =$ Ordnung des regulären Blocks $\boldsymbol{U}$ in der Jordanform (1.5).

Lemma 2. Die in (1.30) definierte Konstruktion $\boldsymbol{C}^{(\mathrm{p})}(\xi, \eta)$ kombiniert sich im Falle einer Matrix dritter Ordnung, aus den Matrizen

$$\boldsymbol{E}, \boldsymbol{C}, \boldsymbol{Q} = \mathrm{adj}\,\boldsymbol{C}$$

so wie es in der nachstehenden Tabelle dargestellt ist. Darin sind die Bedingungen der Spalten (r, ϱ) äquivalent mit jenen der Spalten $(\boldsymbol{Q}, \mu)$.

(2.22)

r	ϱ	$\mathbf{C}^{(\mathrm{p})}(\xi, \eta)$	$\mathbf{Q}$	μ
3	3	$\xi\mu_3^{-1}\mathbf{Q}$		$\mu_3 \neq 0$
2	2	$\xi\mu_1\mu_2^{-1}\mathbf{E} - \xi\mu_2^{-1}\mathbf{C} + (\eta\mu_2^{-1} - \xi\mu_1\mu_2^{-1})\,\mathbf{Q}$		$\mu_3 = 0, \mu_2 \neq 0$
2	1	$\eta\mathbf{E} - (\eta\mu_1^{-1} - \xi\mu_1^{-2})\,\mathbf{C} + (\eta\mu_1^{-2} - \xi\mu_1^{-3})\,\mathbf{Q}$	$\mathbf{Q} \neq 0$	$\mu_3 = 0 = \mu_2$
1	1	$\eta\mathbf{E} + (\xi\mu_1^{-2} - \eta\mu_1^{-1})\,\mathbf{C}$	$\mathbf{Q} = 0$	$\mu_3 = 0 = \mu_2$
	0	$\eta\mathbf{E}$		$\mu_1 = \mu_2 = \mu_3 = 0$

Bemerkungen. a) Formeln diesen Typs wurden im allgemeinen Fall $\mathbf{C} \in \mathbb{F}_{n\times n}$ in [5], [13] bewiesen.

b) Für $n = 1$ gilt in einem Körper $\mathbb{F}$ offenbar

$$c^{(\mathrm{p})}(\xi, \eta) = \begin{cases} \xi c^{-1} & \text{für} \quad c \neq 0 \\ \eta & \text{für} \quad c = 0 \end{cases}$$

c) Für $n = 2$ gilt entsprechend

$$\mathbf{C}^{(\mathrm{p})}(\xi, \eta) = \begin{cases} \xi\mu_2^{-1}\mathbf{Q} & \text{für} \quad \mu_2 = \det \mathbf{C} \neq 0 \\ \eta\mathbf{E} + (\xi\mu_1^{-2} - \eta\mu_1^{-1})\,\mathbf{C} & \text{für} \quad \mu_2 = 0\,, \quad \mu_1 = \operatorname{sp} \mathbf{C} \neq 0 \\ \eta\mathbf{E} & \text{für} \quad \mu_1 = \mu_2 = 0 \end{cases}$$

d) In der Streifenstrategie der Variante 2.2 haben in den Formeln (2.17) und (2.18) die Matrizen $\mathbf{C}_1 = \mathbf{X}\Sigma_1\mathbf{X}^{\mathrm{T}}$ und $\mathbf{C}_2 = \mathbf{Y}^{\mathrm{T}}\Sigma_2\mathbf{Y}$ die Ordnung $b \leqq 3$.

3. MIT ZUFALLSGENERATOREN ERZEUGTE TÄFELUNGEN

3.1. Wir behandeln anhand von Beispielen, Möglichkeiten, mit einem Zufallsgenerator echte Täfelungen zu erzeugen. Sei

$$\mathscr{S} = \{(i_1, j_1), (i_2, j_2), \ldots, (i_k, j_k), \ldots, (i_l, j_l)\} \tag{3.1}$$

eine Menge von Stellen in einer Matrix $\mathbf{Z}(m, n)$. Darin kann man nach verschiedenen lexikographischen Kriterien dominante Stellen (i^*, j^*) definieren. So zum Beispiel definiert

$$\begin{aligned} j^* &= \min j\,; \quad (i, j) \in \mathscr{S} \\ i^* &= \min i\,; \quad (i, j^*) \in \mathscr{S} \end{aligned} \tag{3.2}$$

die oberste der am meisten links gelegenen Stellen in $\mathscr{S}$. Analog kann man an Stelle dieses links-oben Kriteriums andere oben-links, rechts-oben, oben-rechts usw. Kriterien betrachten.

Sei ausserdem $\mathfrak{z} = \{z(k)\} \subset GF(p)$ ein von einer Stammfunktion $g(z_r, z_{r-1}, \ldots$ $\ldots, z_1)$ erzeugter Kongruenzzufallsgenerator. Wir können dann in einer Matrix $\boldsymbol{Z}(m, n)$ mit den Daten des betrachteten Zufallsgenerators, einem Startvektor $z_0 = (z_r^0, z_{r-1}^0, \ldots, z_1^0)$ und einem Kriterium der dominanten Stelle folgende Täfelungsprozedur definieren.

a) $\boldsymbol{Z}_1(m_1, n_1)$ sei ein Täfelchen, das die dominante Stelle der Matrix $\boldsymbol{Z}(m, n)$ enthält, und das ist je nach dem Kriterium entweder $(1, 1)$, $(1, n)$, $(m, 1)$ oder (m, n), während die Dimensionszahlen (m_1, n_1) von

$$m_1 = z(1) \bmod (m) + 1 \tag{3.3}$$

$$n_1 = z(2) \bmod (n) + 1$$

gegeben sein mögen.

b) Vorausgesetzt die Täfelung wurde bis zur Stelle $k - 1$ erklärt, so sei $\boldsymbol{Z}_k(m_k, n_k)$ ein Täfelchen, das die dominante Stelle (i_k^*, j_k^*) in

$$\tilde{\boldsymbol{Z}}^k = \boldsymbol{Z} \setminus \bigsqcup_{j=1 \div k-1} \boldsymbol{Z}_j \tag{3.4}$$

enthält, und dessen Dimensionen von den Formeln

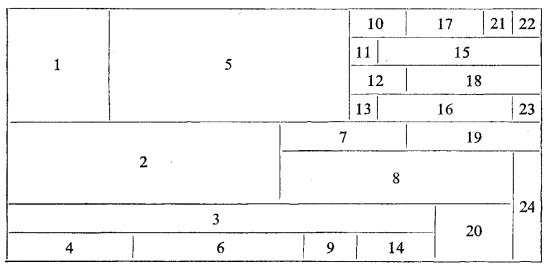
$$m_k = z(2k - 1) \bmod (\tilde{m}_k) + 1 \tag{3.5}$$

$$n_k = z(2k - 1) \bmod (\tilde{n}_k) + 1$$

erklärt sind. Dabei mögen $(\tilde{m}_k, \tilde{n}_k)$ die Dimensionszahlen eines maximalen Täfelchens in $\tilde{\boldsymbol{Z}}^k$ bezeichnen, das darin die dominante Stelle (i_k^*, j_k^*) enthält.

Beispiel 1. Wir betrachten die von der Stammfunktion $g(z) = 11z + 2$ in $GF(31)$ erzeugten Iteration $z_{k+1} = 11z_k + 2$, welche folgenden Zufallsgenerator ergibt: 0, 2, 24, 18, 14, 1, 13, 21, 16, 23, 7, 17, 3, 4, 15, 12, 10, 19, 25, 29, 11, 30, 22, 27, 20, 5, 26, 9, 8, 28, 0.

Mit der Startzahl $z_0 = 3$ und dem links-oben Kriterium ergibt, das der definierten Täfelungsprozedur zufolge, in einer Matrix $\boldsymbol{Z}(10, 24)$ folgende Täfelung:



Bemerkung. Es ist eine allgemeingültige Feststellung, dass die Täfelung ungleichförmig ist, obzwai der Zufallsgenerator es war. Verwendet man eine Verschlüsselungsstrategie der Variante 2.1.c., und übertäfelt man die Matrix zweimal, so kann man, die sich herausgestellte Ungleichförmigkeit beachtend, empfehlen, dass die erste Täfelung etwa nach einem links-oben Kriterium zu vollziehen sei, während die zweite nach einem rechts-unten Kriterium.

3.2. Mit Täfelchen, bei denen eine der Dimensionszahlen klein ist, erfolgt die Verschlüsselung schneller. Zieht man aber eine gleichförmige Täfelung vor, so kann man folgende leicht abgeänderte Täfelungsprozedur verwenden:

– Man wende, im Falle des links-oben Kriteriums, die Täfelungsprozedur (3.5) solange an, bis für die dominante Stelle die Ungleichung

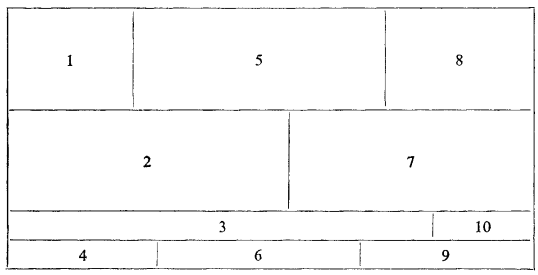
$$j_k^* > \left[\frac{n}{2}\right] + 1 \tag{3.6}$$

eintritt. Danach setze man

$$\boldsymbol{Z}_k = \tilde{\boldsymbol{Z}}_0^k = \text{maximales Täfelchen in } \tilde{\boldsymbol{Z}}^k, \text{ das } (i_k^*, j_k^*) \text{ enthält.} \tag{3.7}$$

In der zweiten Phase wurde der Zufallsgenerator gestoppt. Mit dieser Prozedur ergibt der im Beispliel 1 betrachtete Zufallsgenerator folgende Täfelung.

Beispiel 2.

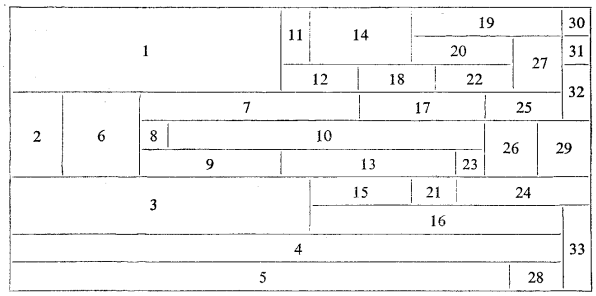


Will man aber, dass eine der Dimensionszahlen aller Täfelchen kleiner als 3 sei, so wird man die Formeln (3.5) etwa wie folgt abändern:

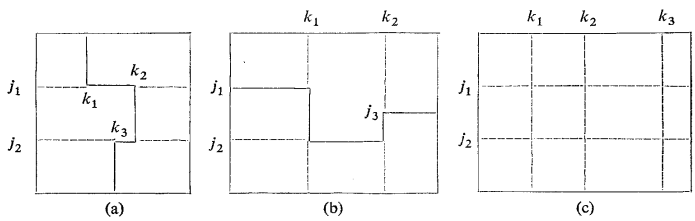
$$\begin{aligned} \bar{m}_k &= z(2k-1) \bmod (\tilde{m}_k) + 1 \\ m_k &= \min(\bar{m}_k, 3) \\ n_k &= z(2k) \bmod (\tilde{n}_k) + 1 \end{aligned} \tag{3.8}$$

Dann ergibt der betrachtete Zufallsgenerator mit der Startzahl $z_0 = 12$ und dem links-oben Kriterium folgende Täfelung:

Beispiel 3.



Im Besonderen kann man auch vertikale und horizontale „Torschlüsseltäfelungen", so wie es partikulär in den Schemen a und b zu sehen ist, definieren, oder so wie bei Levine und Hartwig [18], verschiedene Gittertäfelungen (Schema c), wobei die entsprechenden Parameter gleichfalls von einem Zufallsgenerator erzeugt sein können.



4. EINE ERGÄNZUNG FÜR DAS PUBLIC KEY KRYPTOSYSTEM

4.1. Ist p_0 eine sehr grosse Primzahl, so ist $GF(p_0) \cong \mathbb{Z}/p_0$ der Rahmen, in dem das Public Key Library System operiert. Darin betrachtet man die Exponentialfunktion

$$y = a^x; \quad a = \text{Primelement in } GF(p_0) \tag{4.1}$$

und deren Umkehrfunktion

$$x = \log_a y \tag{4.2}$$

Dabei ist relevant, dass man zur Berechnung der ersten nut etwa 2 log p_0 Operationen beansprucht, während für die zweite bereits etwa $p_0^{1/2}$. Eine Funktion dieser Art nennt man *one way function*.

Einer Darstellung von E. Henze [15] nach, dient das open public key System dazu, um vor dem Austausch geheimer Nachrichten zwischen zwei Teilnehmern eines Netzes, Schlüsseleinstellungen zu verabreden. Besteht das Netz aus den Teilnehmern $(1, 2, \ldots, n)$ so wird vorausgesetzt, das jeder Teilnehmer i einen nur ihm bekannten Schlüssel $x_i \in GF(p_0)$ hat. Ausserdem wird die Existenz einer Schlüsselbibliothek vorausgesetzt, in der die Grössen

$$y_i = a^{x_i} (\mathrm{mod}\ p_0)\,; \quad i = 1, \ldots, n \tag{4.3}$$

enthalten sein mögen und zu der jeder Beteiligte des Netzes freien Zugang hat. Die Schlüsseleinstellung zwischen i und j erfolgt nach der Regel

$$s_{ij} := y_i^{x_j} = a^{x_i x_j} = a^{x_j x_i} = y_j^{x_i} := s_{ji} \tag{4.4}$$

Die Sicherheit dieser Methode beruht auf der Eigenschaft einer one way function, nämlich der unterschiedlichen Komplexität in der Berechnung der Funktionswerte von $y = a^x$ und $x = \log_a y$ in $FG(p_0)$. Siehe [3], [15], [21].

4.2. Nun lässt sich das Public Key Kryptosystem am besten mit solchen kryptographischen Methoden ergänzen, in denen der Schlüssel ein freies Modulelement ist und wo bei der Verschlüsselung und Entschlüsselung derselbe Schlüssel operiert, wie es auch in unserem System der Fall ist. Für eine Ergänzung des Public Key Systems mit der Methode der Linearen Kryptographie ist es zweckmässig, noch folgendes zu vereinbaren:

a) Die Existenz eines linearen Raumes vereinheitlichter Schlüssel

$$\mathfrak{K} = \{\kappa \mid \kappa = (\kappa_1, \kappa_2, \ldots, \kappa_v, \ldots, \kappa_w)\}\,; \quad \kappa_j \in GF(p) \tag{4.5}$$

und einer eindeutigen, nicht unbedingt umkehrbaren Abbildung

$$\psi : GF(p_0) \to \mathfrak{K}' \subset \mathfrak{K} \tag{4.6}$$

b) Die Existenz einer Basis von Funktionen in $[GF(p)]^r$

$$g_1, g_2, \ldots, g_v\,; \quad v \leqq w \tag{4.7}$$

die als Stammfunktionen für einen Zufallsgenerator in Betracht kommen können.

c) Die Existenz eines festen Systems von Formeln und Anweisungen, mit denen man einem Zufallsgenerator $\mathfrak{z} = \{z(k)\} \subset GF(p)$ einen effektiven Schlüssel unseres Systems

$$\varphi(\mathfrak{z}) = \zeta = (\xi, \eta, \Sigma, \beta, \tau) \tag{4.8}$$

zuordnet.

Diese Definierung ergibt den Rahmen des zu erklärenden Zusammenschlusses, der von allen Beteiligten des Netzes bekannt sein mag.

Bemerkung. Es wird nicht untersucht, ob man ψ einfach lexikographisch nehmen soll oder als eine kompliziertere Abbildung. Vorläufig betseht aber keine Veranlassung, die Abbildungen ψ und φ nicht möglichst einfach zu nehmen.

Im erklärten Rahmen kann die Ergänzung des Public Key Systems in zwei Varianten erfolgen, einer reinen und einer hybriden.

(i) Die reine Variante ist von $\mathscr{K}' = \mathscr{K}$ gekennzeichnet. Mit einem Teil der Komponenten $(\kappa_1, \kappa_2, \ldots, \kappa_v)$ von

$$\boldsymbol{\kappa}_{ij} = \psi(s_{ij}) := \boldsymbol{\kappa} = (\kappa_1, \kappa_2, \ldots, \kappa_w) \tag{4.9}$$

wird eine Stammfunktion

$$g = \sum_{j=1}^{v} \kappa_j g_j \tag{4.10}$$

berechnet. Iterativ erzeugt g einen Zufallsgenerator

$$z_k = \mathbf{g}(z_{k-1}, z_{k-2}, \ldots, z_{k-r}) \tag{4.11}$$

Die restlichen Komponenten $(\kappa_{v+1}, \ldots, \kappa_w)$ werden zum Erzeugen von Startvektoren und Stopzahlen sowie für einige andere programmspezifische Anweisungen verwendet. Wir bemerken auch, dass man eine Basis von Zufallsgeneratoren am ehesten linear nehmen soll.

Beachten wir, dass Card $\mathscr{K} = p^w$ und Card $GF(p_0) = p_0$ ist, so wird man eine Dimensionierung von $\mathscr{K}$ so vornehmen, dass man $p^w \sim p_0$ hat, woraus $w \sim \ln p_0 \mid \ln p$ folgt.

(ii) In der hybriden Variante $\mathscr{K}' \subset \mathscr{K}$, $\mathscr{K}' \neq \mathscr{K}$ sei vereinbart, dass

$$\boldsymbol{\kappa} = (\boldsymbol{\kappa}^1, \boldsymbol{\kappa}^2) \in \mathscr{K}\,, \quad \boldsymbol{\kappa}^1 \in \mathscr{K}' \tag{4.12}$$

ist, wobei der grössere Teil davon, $\boldsymbol{\kappa}^1$, aus $\boldsymbol{\kappa}^1 = \psi(s_{ij})$ entstehen mag und daher geheim ist, während der aus nur wenigen Komponenten bestehende Teil $\boldsymbol{\kappa}^2$ nicht als geheim vorausgesetzt sein soll. Es sei vorausgesetzt, dass bei jeder Nachrichtenübertragung zwischen dem Sender i und dem Empfänger j der Sender i den Zusatzschlüssel $\boldsymbol{\kappa}^2$ anders wählt und diesen unverschlüsselt dem Empfänger j mitteilt. Sonst hätte sich die hybride Variante nicht von der reinen zu unterscheiden.

Bemerkung. Zumal ein Schlüssel $\zeta = (\xi, \eta, \Sigma, \boldsymbol{\beta}, \boldsymbol{\tau})$ im Falle der Verschlüsselungsstrategien mit Täfelungen keine festgelegte Dimension hat, so war es eine natürliche Art, diese Ergänzung des Publik Key Systems mit Hilfe von Zufallsgeneratoren zu vollziehen.

4.3. Zusammenfassend können wir in einem vereinheitlichten System von Public Key und Linearer Kryptographie mit Pseudo-Inversen, Zufallsgeneratoren und Täfelungen folgende Stufen von Schlüsseln feststellen:

Schlüssel der Stufe 1 x_i, geheimgehalten vom Teilnehmer i

Schlüssel der Stufe 2 $y_i = a^{x_i}$, in einer offenen Bibliothek enthalten

Schlüssel der Stufe 3 $s_{ij} = a^{x_i x_j}$ nur für die Teilnehmer i und j berechenbar

Schlüssel der Stufe 4 die vereinheitlichten Schlüssel in $\mathscr{K}$ und die dazugehörigen Zufallsgeneratoren

Schlüssel der Stufe 5 verschlüsselte Täfelungen

Schlüssel der Stufe 6 die in ein Pseudo-Inverses eingebauten Schlüssel (ξ, η, Σ)

Schlüssel der Stufe 7 die von den Formeln (1, 2), (1.8), (1.47), (1.50) usw. berechneten Schlüsselmatrizen und die Perturbation β

Diese Stufen stellen die Ordnung dar, in der die verschiedenen Schlüssel operieren. Man kann sagen, dass ein Arsenal von restriktionslosen Schlüsseln und Varianten des Systems vorliegt, Varianten, die sich durch verschiedene sinnvolle Partikularisierungen der Parameter ergeben können. Ausserdem gehört zur Sicherheit des Systems auch die Komplexität der Pseudo-Inversen Operation sowie der Umstand, dass es schwierig ist, eine allgemeine Täfelung anders als algorithmisch zu definieren.

Schlussbemerkungen. 1) Behandelt man die gleiche Problematik in einer allgemeineren Struktur, so wie $\boldsymbol{R} = GF(N)$ oder $\boldsymbol{R} = \mathbb{Z}/N$, so werden sich die entsprechenden Verschlüsselungsabbildungen formell nicht wesentlich von jenen in $GF(p)$ unterscheiden.

2) Kryptanalytische Fragen wurden hier nicht eingehend behandelt. Das Ziel der Arbeit war es, die Möglichkeiten der in [11] eingeleiteten Methode weitgehend zu erforschen, ohne dass der Anlass dazu von einem Erfolg der Kryptanalyse bezüglich der Formel in [11] gegeben war.

3) Die hier betrachteten Verschlüsselungsstrategien entsprechen den Möglichkeiten moderner Geräte und Programmierungstechniken. Man kann auch untersuchen, welche Strategie am besten den spezifischen Anwendungsgebieten der Kryptographie entsprechen. Folgendes scheint sinnvoll zu sein:

a) Verschlüsselungen in einer Bibliothek gesicherter Texte mit der Strategie vom Punkte 1.6.b

b) one line Nachrichtenübertragungen mit der Strategie vom Punkte 2.2.

c) Public Key Library ergänzt mit Strategien von den Punkten 2.1.b, 2.1.c, 2.2.

(Eingegangen am 28. April 1981.)

[1] R. E. Cline: An Application of Representations for the Generalized Inverse of a Matrix. MRC Technical Report 592, 1965.
[2] R. E. Cline: Note on an extension of the Moore-Penrose inverse (submitted for publication).
[3] W. Diffie, M. E. Hellman: New directions in cryptography. IEEE Trans. Inform. Theory *IT-22* (1976), 644—654.
[4] M. P. Drazin: Pseudo-inverses in associate rings and semigroups. Amer. Math. Monthly *65* (1958), 506—514.
[5] R. Gabriel: Das verallgemeinerte Inverse, deren Elemente einem beliebigen Körper angehören. J. reine angew. Math. *234* (1969), 107—122; *244* (1970), 83—93.
[6] R. Gabriel: Das verallgemeinerte Inverse einer Matrix über einem beliebigen Körper — mit Skelettzerlegungen berechnet. Rev. Roumaine Math. Pures Appl. *XX* 1975, 2, 213—225.
[7] R. Gabriel: Eine Kollinearitatsbedingung für Involutionen in Gruppen und Algebren. J. reine angew. Math. *268* (1974), 20—49.
[8] R. Gabriel: Das verallgemeinerte Inverse in Algebren. Rev. Roumaine Math. Pures Appl. *XX* (1975), 3, 311—324.
[9] R. Gabriel: Dreinachrichtenprobleme in verallgemeinerter Definition. J. reine angew. Math. *290* (1977), 199—202.
[10] R. Gabriel: Ein kryptographisches System definiert mit verallgemeinerten Inversen. Vorgetragen Univ. Bukarest, Dezember 1971.
[11] R. Gabriel: Pseudoinversen mit Schlüssel und ein System der algebraischen Kryptographie. Rev. Roumaine Math. Pures Appl. *XXII* (1977), 8, 1077—1099.
[12] R. Gabriel: Über spektrale Pseudo-Inversen, Lineare Kryptographie und umkehrbare Zufallsgeneratoren (in Druck).
[13] R. Gabriel, R. E. Hartwig: The Drazin inverse as a gradient (submitted for publication).
[14] R. E. Hartwig: Drazin inverses in cryptography (submitted for publication).
[15] E. Henze: Kryptographie und Nachrichtenübertragung. Informationsverarbeitung und Kommunikation, Band 8.
[16] L. S. Hill: Cryptography in an algebraic alphabet. Amer. Math. Monthly *36* (1929), 306—312.
[17] B. Jansson: Random Number Generators. Almqvist - Wiksell, Stockholm 1966.
[18] J. Levine, R. E. Hartwig: Application of the Drazin Inverse to the Hill Cryptographic System, I, II, III, IV. Cryptologia (1980).
[19] J. Levine, J. V. Brawley: Involutory commutants with some applications to algebraic cryptography, I. J. reine angew. Math. *224* (1966), 20—43; II. *227* (1967), 1—24.
[20] R. Penrose: A generalized inverse for matrices. Proc. Cambridge Philos. Soc. *51* (1958), 406—413.
[21] R. L. Rives, A. Shamir, L. Adleman: A method for obtaining digital signatures and public-key cryptosystems. Comm. ACM *21* (1978), 120—126.

Dr. Richard Gabriel, Zentrum für Mathematische Statistik, str. Stirbei Voda 174, 77104 Bukarest. R. S. Romania.