ENCIPHERING-MAPS WITH PSEUDO-INVERSES AND PSEUDO-TABULATIONS

RICHARD GABRIEL

Communicated by Marius Iosifescu

Using a special Pseudo-Inverse, a linear cryptographic method is developed by continuing the paper [8]. Both papers complement each other.

AMS 2010 Subject Classification: 94A60, 15A09.

Key words: cryptography, enciphering-maps, pseudo-inverses, pseudo-tabulations, λG-matrices, λ-symmetry.

1. THE REGULAR SPECTRAL PSEUDO-INVERSES $C^{(p)}$

Let F be an algebraic field with involution $\lambda : a \to \overline{a}$ For any matrix $C \in F_{nn}$, let

$$C = T \begin{bmatrix} U & 0 \\ 0 & J \end{bmatrix} T^{-1}, \ \det U \neq 0, \quad J^k = 0 \tag{1}$$

be the Jordan-decomposition. Further let

$$C^d = T \begin{bmatrix} U^{-1} & 0 \\ 0 & 0 \end{bmatrix} T^{-1} \tag{2}$$

be the Drazin-Inverse and

$$C^{(p)} = T \begin{bmatrix} U^{-1} & 0 \\ 0 & E \end{bmatrix} T^{-1} \tag{3}$$

the regular spectral Pseudo-Inverse introduced in [4–8]. This nomenclature is justified, because of the following relations

$$C^{(p)} = C^{-1} \ \text{ for } \ \det C \neq 0;$$

$$C^{(p)} = E \ \text{ for } \ C^k = 0;$$

$$0^{(p)} = E;$$

$$(SCS^{-1})^{(p)} = SC^{(p)}S^{-1};$$

$$\begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix}^{(p)} = \begin{bmatrix} C_1^{(p)} & 0 \\ 0 & C_2^{(p)} \end{bmatrix}.$$

Also, the following relations apply:

$$CC^{(p)} = T \begin{bmatrix} E & 0 \\ 0 & J \end{bmatrix} T^{-1} = C^{(p)}C,$$

and therefore

$$[CC^{(p)}]^{(p)} = E = [C^{(p)}C]^{(p)}.$$

In the formulas above 0 describes a fitting square or rectangular zero matrix.

THEOREM 1. *For any matrix $C \in F_{nn}$ we have*

$$[C^{(p)}CC^{(p)}]^{(p)}C^{(p)} = E.$$

Proof. This relation applies to the Jordan-Form (1).
In addition, the following relations hold true:

$$C^{(p)} = E + C^d - CC^d;$$
$$C^d = C^k[C^{(p)}]^{k+1};$$
$$[C^{(p)}]^* = [C^*]^{(p)};$$
$$(C^T)^{(p)} = [C^{(p)}]^T.$$

Because $C^{(p)}$ is regular, it can be used to define enciphering-maps.

In order to get $C^{(p)}$ numerically, we express C with its complete factors:

$$C = G_1G_2...G_k\Delta^{-1}H_k...H_2H_1.$$

From this we got in [5]

$$C^{(p)} = E + G_1G_2...G_k(\Delta^{-k-1} - \Delta^{-k})H_k...H_2H_1,$$

and in [2]

$$C^d = G_1G_2...G_k\Delta^{-k}H_k...H_2H_1. \quad \square$$

2. ENCIPHERING-MAPS WITH PSEUDO-INVERSES

We consider the enciphering-map

(4) $$Y = (X\Sigma X^*)^{(p)}X \quad (X, Y) \in F_{mn}$$

which is recursive (or also involutive), if the relation

(5) $$X = (Y\Sigma Y^*)^{(p)}Y$$

is satisfied identically. Introducing (4) in (5), it follows

$$X = \left\{(X\Sigma X^*)^{(p)}(X\Sigma X^*)\left[(X\Sigma X^*)^{(p)}\right]^*\right\}^{(p)}(X\Sigma X^*)^{(p)}X. \tag{6}$$

If X has a maximal rank at $m < n$, it follows

$$E = \left\{(X\Sigma X^*)^{(p)}(X\Sigma X^*)[(X\Sigma X^*)^{(p)}]^*\right\}^{(p)}(X\Sigma X^*)^{(p)} \tag{7}$$

for all $X \in F_{mn}$. A matrix Σ fulfilling (7) was called a λG-matrix in [8].

The following STATEMENTS were shown to hold true:

a) A λ-symmetrical matrix Σ is also λG.
b) A regular λG-matrix is also λ-symmetrical for $F \neq GF(3)$.
c) For $n = 2$ a λG-matrix is always λ-symmetrical.

THEOREM 2. *If Σ is a λG-matrix, so is $\Sigma_1 = S\Sigma S^*$ for any $S \in F_{kn}$.*

Proof. We have, with $X_1 = XS$

$$\left\{(X\Sigma_1X^*)^{(p)}X\Sigma_1X^*[(X\Sigma_1X^*)^{(p)}]^*\right\}^{(p)}(X\Sigma_1X^*)^{(p)} =$$

$$\left\{[(XS)\Sigma(XS)^*]^{(p)}[(XS)\Sigma(XS)^*]\left[[(XS)\Sigma(XS)^*]^{(p)}\right]^*\right\}^{(p)}[(XS)\Sigma(XS)^*]^{(p)} =$$

$$\left\{(X_1\Sigma X_1^*)^{(p)}X_1\Sigma X_1^*[(X_1\Sigma X_1^*)^{(p)}]^*\right\}^{(p)}(X_1\Sigma X_1^*)^{(p)} = E \quad \square$$

The following theorem was already formulated in [8], but not proven completely. This will be done here.

THEOREM 3. *For $F \neq GF(3)$ a λG-matrix Σ is always λ-symmetrical: $\Sigma^* = \Sigma$.*

Proof. We consider in Theorem 2

$$S = S(2,n) = \begin{array}{c} \\ \\ \end{array}\begin{array}{cc} \begin{array}{ccccccccc} & & k & & & j & & & \end{array} & \\ \left[\begin{array}{ccccccccc} 0 & \dots & 0 & 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & \dots & 1 & 0 & \dots & 0 & 0 & \dots & 0 \end{array}\right] & \begin{array}{c} k \\ j \end{array} \end{array}$$

Then we obtain:

$$S\Sigma S^* = \left[\begin{array}{cc} \sigma_{kk} & \sigma_{kj} \\ \sigma_{jk} & \sigma_{jj} \end{array}\right],$$

which is λG according to Theorem 2. According to Preposition 3 in [8] this matrix is λ-symmetrical:

$$\overline{\sigma}_{kk} = \sigma_{kk},\ \overline{\sigma}_{kj} = \sigma_{jk},\ \overline{\sigma}_{jj} = \sigma_{jj}$$

for all (k,j). This proofs Theorem 3. $\square$

3. CIPHERING OF A PSEUDO-TABLE WITH COMBINATORIAL KEYS

Consider two combinatorial keys

$$\alpha = (1 \le \alpha_1 < \alpha_2 < ... < \alpha_r \le m),$$

$$\beta = (1 \le \beta_1 < \beta_2 < ... < \beta_s \le n).$$

To these keys we associate, respectively, two diagonal matrices

$$D(\alpha) = diag\begin{pmatrix} & & \alpha_1 & & & \alpha_2 & & & \alpha_r & & & \\ 0 & ... & 1 & 0 & ... & 1 & 0 & ... & 1 & 0 & ... & 0 \end{pmatrix},$$

$$D(\beta) = diag\begin{pmatrix} & & \beta_1 & & & \beta_2 & & & \beta_r & & & \\ 0 & ... & 1 & 0 & ... & 1 & 0 & ... & 1 & 0 & ... & 0 \end{pmatrix}.$$

With them we define the pseudo-table

$$A\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = D(\alpha) \cdot A \cdot D(\beta).$$

The non-zero part of $A\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ is the intersection of rows $(\alpha_1, \alpha_2, ...\alpha_r)$ and columns $(\beta_1, \beta_2, ...\beta_s)$ of the matrix A.

Now, suppose the key matrices

$$D(\alpha) \cdot \Sigma_L \cdot D(\alpha) \textit{ and } D(\beta) \cdot \Sigma_R \cdot D(\beta)$$

are computed from the parametric matrix repository key (shortly, SMPD)

$$\{\Sigma_L(n, n), A(m, n), \Sigma_R(m, m)\}.$$

If we apply a left ciphering to the pseudo-table $D(\alpha) \cdot A \cdot D(\beta)$, this will be replaced by

$$K \cdot D(\alpha) \cdot A \cdot D(\beta),$$

where

$$K = \{D(\alpha) \cdot A \cdot D(\beta) \cdot \Sigma_L \cdot D(\beta) \cdot [D(\alpha) \cdot A \cdot D(\beta)]^*\}^{(p)}$$
$$= \{D(\alpha) \cdot A \cdot D(\beta) \cdot \Sigma_L \cdot D(\beta) \cdot A^* \cdot D(\alpha)\}^{(p)}.$$

THEOREM 4. *The encoding matrix of a pseudo-table has the form*

$$\tilde{A}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = A - D(\alpha) \cdot A \cdot D(\beta) + K \cdot D(\alpha) \cdot A \cdot D(\beta)$$
$$= A + (K - E) \cdot D(\alpha) \cdot A \cdot D(\beta).$$

Decoding can be done with the same formula.

4. FOUR-TABULATIONS

Let us examine pseudo-tabulations which are of practical interest. They must satisfy three criteria:

1. They have to cover the matrix $A(m,n)$
2. They have to exhibit a cardinal number which is big enough.
3. Coding and decoding have to be done with the same formula.

The first criteria is already met by *four-tabulations*, described by the pattern

B(r,s)	C(r,n-s)
F(m-r,s)	G(m-r,n-s)

Ciphering leads to

$K_1 \cdot B(r,s)$	$K_2 \cdot C(r,n-s)$
$K_3 \cdot F(m-r,s)$	$K_4 \cdot G(m-r,n-s)$

where

$$K_1 = (B \cdot \Sigma(r,r) \cdot B^*)^{(p)},$$
$$K_2 = (C \cdot \Sigma(r,r) \cdot C^*)^{(p)},$$
$$K_3 = (F \cdot \Sigma(n-r,n-r) \cdot F^*)^{(p)},$$
$$K_4 = (G \cdot \Sigma(n-r,n-r) \cdot G^*)^{(p)}.$$

Since $\Sigma(r,r)$ and $\Sigma(n-r,n-r)$ are supposed to be λ-symmetrical, coding and decoding work with the same formula.

5. COMBINED CIPHERINGS

The three criteria, that must fulfill a unified ciphering strategy, can be reached in three steps:

I. An input-ciphering, possible through a fore-ciphering.
II. A combinatorial ciphering, mediated through one or more combinatorial keys.
III. An output-ciphering, possible through a fore-ciphering.

Decoding is done with the same formulas as encoding in opposite direction.

The cardinal number of such an enciphering can be given as

$$k = m^2 n^2 2^{m+n} \sigma.$$

Here $m^2 n^2$ come from four-tabulations I and III, whereas 2^{m+n} indicates the combinatorial keys in step II. The factor σ indicates the cardinal number of the key-matrices Σ_L and Σ_R. If m and n are relatively small, it could be of interest to apply step II q times with q different combinatorial keys and to apply Theorem 4 for each key. Then the cardinal number will be

$$k = m^2 n^2 2^{q(m+n)}\sigma.$$

REFERENCES

[1] R.E. Cline, *An Application of Representation 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.* Linear Algebra Appl. **40** (1981), 19–23.

[3] M.P. Drazin, *Pseudo-inverses in associative rings and semigroups.* Amer. Math. Monthly **65**, (1958), 506–514.

[4] R. Gabriel, *Das verallgemeinerte Inverse einer Matrix, deren Elemente einem beliebigen Körper angehören.* J. Reine Angew. Math. **234** (1969), 107–122 and **244** (1970), 83–93.

[5] R. Gabriel, *Das verallgemeinerte Inverse einer Matrix über einem beliebigen Körper-mit Skelettzerlegungen berechnet.* Rev. Roumaine Math. Pures Appl. **XX** (1975), *2*, 213–225.

[6] R. Gabriel, *Pseudoinversen mit Schlüssel und ein System der algebraischen Kryptographie.* Rev. Roumaine Math. Pures Appl. **XXII** (1977), *8*, 1077–1099.

[7] R. Gabriel, *Verschlüsselungsabbildungen mit Pseudo-Inversen, Zufallsgeneratoren und Täfelungen.* Kybernetika **18** (1982), *6*, 485–504, Academia Praha.

[8] R. Gabriel, *The symmetry of some recursive ciphering maps with pseudoinverse and pseudotabulation.* Rev. Roumaine Math. Pures Appl. **56** (2011) *3*, 185–194.

[9] R.E. Hartwig, *Drazin and Gabriel inverses in cryptography.* Preprint, North Carolina State University, 2014.

[10] L.S. Hill, *Cryptography in an algebraic alphabet.* Amer. Math. Monthly **36** (1929), 306–312.

[11] J. Levine and J.V. Brawley, *Involutory commutants with some applications to algebraic cryptography.* I. J. Reine Angew. Math. **224** (1966), 20–43 and **227** (1967), 1–27.

[12] R. Penrose, *A generalized inverse for matrices.* Proc. Cambridge Philos. Soc. **51**, Cambridge Univ. Press, 1958, pp. 406–413.

Received 16 April 2014

Member of
The New York Academy of Sciences
Wilhelmshavener Str. 67,
D-10551 Berlin
Germany