

Modified Matrix Modular Cryptosystems

Abstract

The Basic Matrix Modular Cryptosystem (BMMC) is a public-key cryptosystem, which uses some matrix modular exponentiations. The aim of this article is to decrease the number of these exponentiations and consequently to accelerate the execution of encryption algorithm. There are two ways to reach this aim. First way is to determine the large abelian subgroup in general linear group over the large residue ring and to choose the session keys in this subgroup, what will be to give the encryption without exponentiations. Other way is to use random integral exponent of the given matrix in the public key as session key and this will be the only exponentiation in encryption algorithm. A discussion about the security of built modifications made in the article shows that the level of security is high enough for an appropriate choice of parameters of the cryptosystems.

Key words: public key cryptosystem, matrix modular ring, general linear group, residue ring, automorphism.

1. Introduction

The Basic Matrix Modular Cryptosystem (BMMC) is a public key cryptosystem, which was developed in [1]. Its realization needs three matrix modular exponentiations for key generation, three exponentiations under encryption and one exponentiation under decryption for every data block. One may to accelerate encryption by decreasing the number of exponentiations. To reach this aim it is necessary to explore the centralizer of random matrix in the general linear group over residue ring. The structure of this centralizer is unknown in general case. There are two ways for the choice of the random element of centralizer. One way is to use a fixed large abelian subgroup G in a such manner that one may easily to choose the random element x in G , then other random element y in G will be an element of centralizer of x . Other way is to compute the random integral exponent y of the fixed element x in the general linear group over residue ring, then y will be in a centralizer of x and that is only exponentiation needs for encryption. Two different modifications of BMMC are based on these two approaches, namely, Modified Matrix Modular Cryptosystem One (MMMC1) and Modified Matrix Modular Cryptosystem Two (MMMC2). Both cryptosystems provide faster encryption than BMMC but their security have to be explored. On the other hand, the mathematical basis of these cryptosystems security is the same hard computational problem.

In the case of MMC1 and in the case of MMC2 it is a “random salt” conjugation problem. Classical conjugation problem is the following: for the given elements A, B in the group G to find element X in the same group such that

$$X^{-1}AX = B.$$

The “random salt” conjugation problem is the following: for the given matrices A, B in the matrix modular ring $M_2(\mathbb{Z}_n)$ over the residue ring $\mathbb{Z}_n$ to find invertible matrix X in the same ring and random fixed unit α in the residue ring $\mathbb{Z}_n$ by modulo n such that

$$X^{-1}AX = \alpha B.$$

The random fixed “salt” α can be found only under brute force attack and for large enough modulus n this problem is becoming intractable.

45 **2. Subgroup G of the group $GL_2(\mathbf{Z}_n)$**

46 Let G be the following set of 2×2 – matrices:

47
$$G = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a, b \in \mathbf{Z}_n \text{ and } (a^2 - b^2) \in \mathbf{Z}_n^* \right\},$$

48 $\mathbf{Z}_n^*$ is an unit group of the residue ring $\mathbf{Z}_n$.

49 It is easy to verify that G is an abelian subgroup of the group $GL_2(\mathbf{Z}_n)$:

50 1) for $K = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in G$ and $L = \begin{pmatrix} c & d \\ d & c \end{pmatrix} \in G$ we have that

51
$$M = KL \in G,$$

52 because

53
$$KL = \begin{pmatrix} ac + bd & ad + bc \\ ad + bc & ac + bd \end{pmatrix}$$

54 and determinant of KL is

55
$$\det(KL) = (\det K)(\det L) \in \mathbf{Z}_n^*;$$

56 2) for $K = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in G$, $\det K = \gamma \in \mathbf{Z}_n^*$ we have that $K^{-1} \in G$, because

57
$$K^{-1} = \begin{pmatrix} \gamma^{-1}a & -\gamma^{-1}b \\ -\gamma^{-1}b & \gamma^{-1}a \end{pmatrix}, \det K^{-1} = \gamma^{-1} \in \mathbf{Z}_n^*;$$

58 3) for $K = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in G$ and $L = \begin{pmatrix} c & d \\ d & c \end{pmatrix} \in G$ we have that $KL = LK$, because

59
$$KL = \begin{pmatrix} ac + bd & ad + bc \\ ad + bc & ac + bd \end{pmatrix}, LK = \begin{pmatrix} ca + db & cb + da \\ cb + da & ca + db \end{pmatrix}.$$

60 Let a, b be the random elements of the ring $\mathbf{Z}_n$ and let

61
$$M = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

62 be the corresponding element in the ring $M_2(\mathbf{Z}_n)$. What is the probability of the case that M is not
63 in the group G ? In two partial cases of n we may to give answer on this question.

64 Let us suppose that there are or

65 1) $n = p^r$, p is a prime number, $2 \leq r$ is an integer

66 or

67 2) $n = pq$, p and q are primes.

68 The cardinality of the residue ring and its unit group in both cases is the following:

69 1) $|\mathbf{Z}_n| = p^r, |\mathbf{Z}_n^*| = \phi(n) = p^{r-1}(p-1)$

70 or

71 2) $|\mathbf{Z}_n| = pq, |\mathbf{Z}_n^*| = \phi(n) = (p-1)(q-1),$

72 $\phi(n)$ is an Euler function.

73 Then the probability P of the case that matrix M is not in the group G is the following:

74 1) $1 - \frac{\varphi(n)}{n} = 1 - \frac{p^{r-1}(p-1)}{p^r} = \frac{1}{p}$

75 or

76 2) $1 - \frac{\varphi(n)}{n} = 1 - \frac{(p-1)(q-1)}{pq} = \frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$.

77 If bit length of the primes p and q will be 80 bits or bigger, then we have:

78 1) $P \leq 2^{-80}$

79 or

80 2) $P \leq 2^{-79}$.

81 In both cases probability P becomes negligible small and therefore one may suppose that in these
82 two cases random matrix M over $\mathbf{Z}_n$

83
$$M = \begin{pmatrix} a & b \\ b & a \end{pmatrix}, a, b \in \mathbf{Z}_n$$

84 with overwhelming probability is in the group G .

85 *Note.* In the case if modulus n is 64 bit integer one needs to verify that random matrix

86
$$M = \begin{pmatrix} a & b \\ b & a \end{pmatrix}, a, b \in \mathbf{Z}_n$$

87 belongs to the group G .

88 3. Modified Matrix Modular Cryptosystem One (MMMC1) description

89 I. Key generation

90 Alice doing the following:

91 1) picks a random prime number p ;

92 2) makes a choice between

93 2.1) picks an integer $2 \leq r$

94 or

95 2.2) picks a random prime number q ;

96 3) computes $n = p^r$

97 or

98 $n = pq$;

99 4) picks four random integers $a, b, c, d \in \mathbf{Z}_n$;

100 5) composes two random matrices

101
$$V = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \text{ and } W = \begin{pmatrix} c & d \\ d & c \end{pmatrix};$$

102 6) verifies the membership of these matrices to the group G ;

103 7) if at least one of these matrices not belongs to G , then return to 4);

104 *Note 1.* If modulus n is 160 bit integer or bigger, then with overwhelming probability the member-
105 ship of these matrices to the group G is accepted without verification.

106 8) Alice defines two commuting inner automorphisms of the ring $M_2(\mathbf{Z}_n)$:

107
$$\alpha: D \rightarrow V^{-1}DV, \beta: D \rightarrow W^{-1}DW$$

108 for every matrix $D \in M_2(\mathbf{Z}_n)$.

Note 2. Matrices $V, W \in G$ and therefore automorphisms α, β commute. Of course this may be checked directly.

9) Alice computes the following automorphisms of the ring $M_2(\mathbf{Z}_n)$:

$$\varphi = \alpha^2 \beta, \quad \psi = \alpha \beta^2,$$

$$\varphi: D \rightarrow (V^2 W)^{-1} D (V^2 W), \quad \psi: D \rightarrow (V W^2)^{-1} D (V W^2)$$

for every matrix $D \in M_2(\mathbf{Z}_n)$.

Note 3. Automorphisms φ, ψ commute and

$$\varphi = \alpha \beta^{-1} \psi, \quad \psi = \alpha^{-1} \beta \varphi.$$

10) Alice picks a random invertible matrix

$$L \in GL_2(\mathbf{Z}_n),$$

such that L does not belong to the subgroup G ;

11) computes matrices:

$$L^{-1}, \quad \varphi(L), \quad \psi(L^{-1});$$

12) Alice public key is

$$(n, \varphi(L), \psi(L^{-1})),$$

private key is

$$(V, W).$$

II. Encryption

Bob doing the following:

1) presents the plaintext m as a sequence of 2×2 - matrices over residue ring $\mathbf{Z}_n$:

$$m^{(1)}, m^{(2)}, \dots, m^{(N)};$$

2) for every $m^{(i)}, i = 1, 2, \dots, N$ chooses a random matrix $Y^{(i)} \in G$;

3) defines for every $i = 1, 2, \dots, N$ the automorphisms

$$\xi^{(i)}: D \rightarrow (Y^{(i)})^{-1} D Y^{(i)}$$

for every $D \in M_2(\mathbf{Z}_n)$;

4) computes for every $i = 1, 2, \dots, N$ matrices $\xi^{(i)}(\varphi(L)), \xi^{(i)}(\psi(L^{-1})), m^{(i)} \xi^{(i)}(\varphi(L))$;

5) picks for every $i = 1, 2, \dots, N$ random units $\gamma_i \in \mathbf{Z}_n$ ("salt") and computes the ciphertext:

$$C = (C^{(1)} \parallel C^{(2)} \parallel \dots \parallel C^{(N)}), \quad C^{(i)} = (C_1^{(i)}, C_2^{(i)}),$$

$$C_1^{(i)} = \gamma_i^{-1} \xi^{(i)}(\psi(L^{-1})), \quad C_2^{(i)} = \gamma_i m^{(i)} \xi^{(i)}(\varphi(L)), \quad i = 1, 2, \dots, N.$$

III. Decryption

Alice doing the following:

1) computes for every $i = 1, 2, \dots, N$ using her private key:

$$z^{(i)} = \alpha^{-1} \beta(C_1^{(i)}) = \alpha^{-1} \beta(\gamma_i^{-1} \xi^{(i)}(\psi(L^{-1})));$$

2) computes for every $i = 1, 2, \dots, N$ matrices:

$$C_2^{(i)} z^{(i)} = (\gamma_i m^{(i)} \xi^{(i)}(\varphi(L))) z^{(i)} = m^{(i)};$$

3) restores the plaintext m from the matrix sequence $m^{(1)}, m^{(2)}, \dots, m^{(N)}$.

Note 4. Decryption correctness proof will be given later for two modifications.

4. Example 1 (MMMC1)

I. Key generation

Alice doing the following:

1) picks the primes $p = 5$, $q = 7$ and computes $n = pq = 35$;

2) chooses four random integers in the residue ring $\mathbf{Z}_{35}$:

7, 4, 6, 2;

3) composes the random matrices

$$V = \begin{pmatrix} 7 & 4 \\ 4 & 7 \end{pmatrix}, W = \begin{pmatrix} 6 & 2 \\ 2 & 6 \end{pmatrix};$$

4) computes $\det V = 33$, $\det W = 32$ and then computes

$$(\det V)^{-1} = 17, (\det W)^{-1} = 23,$$

therefore V and W are units in the matrix ring $M_2(\mathbf{Z}_{35})$;

5) defines two automorphisms of the ring $M_2(\mathbf{Z}_{35})$:

$$\alpha: D \rightarrow V^{-1}DV, \beta: D \rightarrow W^{-1}DW$$

for every matrix $D \in M_2(\mathbf{Z}_{35})$;

6) computes the following automorphisms:

$$\psi = \alpha^2\beta, \varphi = \alpha\beta^2;$$

7) chooses the random matrix $L \in GL_2(\mathbf{Z}_{35})$:

$$L = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$$

and computes matrix

$$L^{-1} = \begin{pmatrix} 30 & 2 \\ 3 & 34 \end{pmatrix};$$

8) computes matrices:

$$\varphi(L) = (VW^2)^{-1}L(VW^2) = \begin{pmatrix} 34 & 34 \\ 6 & 7 \end{pmatrix},$$

$$\psi(L^{-1}) = (V^2W)^{-1}L^{-1}(V^2W) = \begin{pmatrix} 23 & 24 \\ 16 & 6 \end{pmatrix}.$$

9) Alice public key is

$$\left(n = 35, \varphi(L) = \begin{pmatrix} 34 & 34 \\ 6 & 7 \end{pmatrix}, \psi(L^{-1}) = \begin{pmatrix} 23 & 24 \\ 16 & 6 \end{pmatrix} \right),$$

private key is

$$\left(V = \begin{pmatrix} 7 & 4 \\ 4 & 7 \end{pmatrix}, W = \begin{pmatrix} 6 & 2 \\ 2 & 6 \end{pmatrix} \right).$$

II. Encryption

Bob doing the following:

1) presents the plaintext as a matrix $m \in M_2(\mathbf{Z}_{35})$:

- 177
$$m = \begin{pmatrix} 11 & 2 \\ 9 & 3 \end{pmatrix};$$
- 178 2) picks the random matrix $Y = \begin{pmatrix} 3 & 5 \\ 5 & 3 \end{pmatrix} \in G$ and computes $Y^{-1} = \begin{pmatrix} 2 & 20 \\ 20 & 2 \end{pmatrix};$
- 179 3) defines automorphism ξ of the ring $M_2(\mathbf{Z}_{35})$:
- 180
$$\xi: D \rightarrow Y^{-1}DY$$
- 181 for every matrix $D \in M_2(\mathbf{Z}_{35})$;
- 182 4) computes matrices:
- 183
$$\xi(\varphi(L)) = Y^{-1}\varphi(L)Y = \begin{pmatrix} 29 & 24 \\ 16 & 12 \end{pmatrix},$$
- 184
$$\xi(\psi(L^{-1})) = Y^{-1}\psi(L^{-1})Y = \begin{pmatrix} 13 & 24 \\ 16 & 16 \end{pmatrix};$$
- 185 5) picks random unit $\gamma \in \mathbf{Z}_{35}$:
- 186
$$\gamma = 9, \gamma^{-1} = 4;$$
- 187 6) computes the ciphertext $C = (C_1, C_2)$:
- 188
$$C_1 = \gamma^{-1}\xi(\psi(L^{-1})) = \begin{pmatrix} 17 & 26 \\ 29 & 29 \end{pmatrix}, \quad C_2 = \gamma m \xi(\varphi(L)) = \begin{pmatrix} 9 & 2 \\ 16 & 28 \end{pmatrix}.$$

189 III. Decryption

190 Alice doing the following:

- 191 1) computes matrix z , using her private key:

192
$$z = \alpha^{-1}\beta(C_1) = (V^{-1}W)^{-1}C_1(V^{-1}W) = \begin{pmatrix} 22 & 26 \\ 29 & 24 \end{pmatrix};$$

- 193 2) computes then

194
$$C_2 z = \begin{pmatrix} 11 & 2 \\ 9 & 3 \end{pmatrix} = m.$$

195 5. Modified Matrix Modular Cryptosystem Two (MMMC2) description

196 I. Key generation

197 Alice doing the following:

- 198 1) picks a random prime number p ;
- 199 2) chooses one of the following two cases:
- 200 2.1) picks a random integer $2 \leq r$ and computes $n = p^r$;
- 201 2.2) picks a random prime number $q \neq p$ and computes $n = pq$;
- 202 3) picks a random matrix $W \in GL_2(\mathbf{Z}_n)$;
- 203 4) computes matrices

204
$$F = W^2, \quad H = W^3$$

205 and

206
$$F^2H, \quad FH^2;$$

207 5) picks a random matrix $L \in GL_2(\mathbf{Z}_n)$;

208 6) defines the automorphisms:

$$209 \quad \alpha: D \rightarrow F^{-1}DF, \quad \beta: D \rightarrow H^{-1}DH$$

210 and then computes the automorphisms:

$$211 \quad \varphi = \alpha^2\beta, \quad \psi = \alpha\beta^2,$$

$$\varphi: D \rightarrow (F^2H)^{-1}D(F^2H), \quad \psi: D \rightarrow (FH^2)^{-1}D(FH^2)$$

212 for every matrix $D \in M_2(\mathbf{Z}_n)$.

213 *Note 1.* Automorphisms $\alpha, \beta, \varphi, \psi$ commute each with other because the corresponding matrices

214 F, H, F^2H, FH^2 are some integral exponents of matrix W .

215 7) Alice computes matrices:

$$216 \quad FH, \quad \varphi(L), \quad \psi(L^{-1});$$

217 8) Alice public key is

$$218 \quad (n, \varphi(L), \psi(L^{-1}), FH),$$

219 private key is

$$220 \quad (F, H).$$

221 *Note 2.* The following relations can be easily verified:

$$222 \quad \varphi = \alpha\beta^{-1}\psi, \quad \psi = \alpha^{-1}\beta\varphi.$$

223 II. Encryption

224 Bob doing the following:

225 1) presents the plaintext as a sequence of 2×2 - matrices over the residue ring $\mathbf{Z}_n$:

$$226 \quad m^{(1)}, \dots, m^{(N)};$$

227 2) for every matrix $m^{(i)}, i = 1, \dots, N$ picks random integer k_i and computes matrix

$$228 \quad Y^{(i)} = (FH)^{k_i};$$

229 3) defines automorphisms:

$$230 \quad \xi^{(i)}: D \rightarrow (Y^{(i)})^{-1}DY^{(i)}$$

231 for every matrix $D \in M_2(\mathbf{Z}_n)$, $i = 1, \dots, N$;

232 4) computes matrices for every $i = 1, \dots, N$:

$$233 \quad \xi^{(i)}(\varphi(L)), \quad \xi^{(i)}(\psi(L^{-1})), \quad m^{(i)}\xi^{(i)}(\varphi(L));$$

234 5) picks random units $\gamma_i \in \mathbf{Z}_n^*$, $i = 1, \dots, N$ and computes ciphertext:

$$235 \quad C = C^{(1)} \parallel \dots \parallel C^{(N)},$$

$$236 \quad C^{(i)} = (C_1^{(i)}, C_2^{(i)}), i = 1, \dots, N,$$

$$237 \quad C_1^{(i)} = \gamma_i^{-1} \xi^{(i)}(\psi(L^{-1})), \quad C_2^{(i)} = \gamma_i m^{(i)} \xi^{(i)}(\varphi(L)).$$

238 III. Decryption

239 Alice doing the following:

240 1) using her private key computes for every $i = 1, \dots, N$:

$$241 \quad z^{(i)} = \alpha\beta^{-1}(C_1^{(i)}) = \alpha\beta^{-1}(\gamma_i^{-1}\xi^{(i)}(\psi(L^{-1})));$$

242 2) computes matrices for every $i = 1, \dots, N$:

$$C_2^{(i)} z^{(i)} = m^{(i)};$$

3) restores the plaintext m from the matrix sequence

$$m^{(1)}, \dots, m^{(N)}.$$

Note 3. Automorphisms $\xi^{(i)}$, $i = 1, \dots, N$ commute with automorphisms $\alpha, \beta, \varphi, \psi$.

247

Theorem. The decryption in cryptosystems MMMC1 and MMMC2 is correct.

Proof. Automorphisms $\xi^{(i)}$, $i = 1, \dots, N$ commute with automorphisms α and β in both cryptosystems, besides of definitions of one-named automorphisms are quite different in them. Therefore proof deals with both cryptosystems.

Under computations we have the following:

$$\begin{aligned} (\gamma_i m^{(i)} \xi^{(i)}(\varphi(L))) z^{(i)} &= (\gamma_i m^{(i)} \xi^{(i)}(\varphi(L))) (\alpha \beta^{-1} (\gamma_i^{-1} \xi^{(i)}(\psi(L^{-1})))) = \\ &= (\gamma_i \gamma_i^{-1} m^{(i)} \xi^{(i)}(\varphi(L))) (\xi^{(i)}(\alpha \beta^{-1}(\psi(L^{-1})))) = \\ &= m^{(i)} (\xi^{(i)}(\varphi(L))) (\xi^{(i)}(\varphi(L^{-1}))) = m^{(i)} (\xi^{(i)}(\varphi(L) \varphi(L^{-1}))) = \\ &= m^{(i)} \xi^{(i)} \varphi(LL^{-1}) = m^{(i)} \xi^{(i)} \varphi(I) = m^{(i)} I = m^{(i)}. \end{aligned}$$

257

6. Example 2 (MMMC2)

I. Key generation

Alice doing the following:

1) picks prime number $p = 5$ and computes $n = p^2 = 25$;

2) picks the random matrix

$$W = \begin{pmatrix} 7 & 3 \\ 5 & 2 \end{pmatrix} \in GL_2(\mathbf{Z}_{25});$$

3) computes matrices

$$F = W^2 = \begin{pmatrix} 14 & 2 \\ 20 & 19 \end{pmatrix}, \quad H = W^3 = \begin{pmatrix} 8 & 21 \\ 10 & 23 \end{pmatrix}$$

and also matrices

$$F^2 H = \begin{pmatrix} 23 & 24 \\ 15 & 8 \end{pmatrix}, \quad FH^2 = \begin{pmatrix} 6 & 17 \\ 20 & 11 \end{pmatrix};$$

4) chooses the random matrix

$$L = \begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix} \in GL_2(\mathbf{Z}_{25});$$

5) defines automorphisms

$$\alpha, \beta, \varphi, \psi;$$

6) computes matrices

$$FH = \begin{pmatrix} 7 & 15 \\ 0 & 7 \end{pmatrix}, \quad \varphi(L) = \begin{pmatrix} 8 & 24 \\ 17 & 4 \end{pmatrix}, \quad \psi(L^{-1}) = \begin{pmatrix} 3 & 8 \\ 7 & 10 \end{pmatrix};$$

274

275

276 7) Alice public key is:

$$277 \quad \left(n = 25, \varphi(L) = \begin{pmatrix} 8 & 24 \\ 17 & 4 \end{pmatrix}, \psi(L^{-1}) = \begin{pmatrix} 3 & 8 \\ 7 & 10 \end{pmatrix}, FH = \begin{pmatrix} 7 & 15 \\ 0 & 7 \end{pmatrix} \right),$$

278 her private key is

$$279 \quad \left(F = \begin{pmatrix} 14 & 2 \\ 20 & 19 \end{pmatrix}, H = \begin{pmatrix} 8 & 21 \\ 10 & 23 \end{pmatrix} \right).$$

280 II. Encryption

281 Bob doing the following:

282 1) presents the plaintext as matrix

$$283 \quad m = \begin{pmatrix} 9 & 16 \\ 10 & 5 \end{pmatrix} \in M_2(\mathbf{Z}_{25});$$

284 2) picks random k , for example, $k = 3$ and computes matrix

$$285 \quad Y = (FH)^3 = \begin{pmatrix} 18 & 5 \\ 0 & 18 \end{pmatrix};$$

286 3) defines automorphism

$$287 \quad \xi: D \rightarrow Y^{-1}DY$$

288 for every matrix $D \in M_2(\mathbf{Z}_{25})$;

289 4) computes matrices

$$290 \quad \xi(\varphi(L)) = \begin{pmatrix} 13 & 14 \\ 17 & 24 \end{pmatrix}, \quad \xi(\psi(L^{-1})) = \begin{pmatrix} 8 & 13 \\ 7 & 5 \end{pmatrix},$$

$$291 \quad m\xi(\varphi(L)) = \begin{pmatrix} 8 & 10 \\ 15 & 10 \end{pmatrix};$$

292 5) picks $\gamma = 7$, then computes

$$293 \quad C_1 = \gamma^{-1}\xi(\psi(L^{-1})) = \begin{pmatrix} 19 & 9 \\ 1 & 15 \end{pmatrix}, C_2 = \gamma m\xi(\varphi(L)) = \begin{pmatrix} 23 & 20 \\ 5 & 20 \end{pmatrix},$$

$$294 \quad C = (C_1, C_2).$$

295 III. Decryption

296 Alice doing the following:

297 1) computes matrix z using her private key:

$$298 \quad z = \alpha\beta^{-1}(C_1) = (FH^{-1})^{-1}C_1(FH^{-1}) = \begin{pmatrix} 18 & 2 \\ 6 & 16 \end{pmatrix};$$

299 2) computes

$$300 \quad C_2 z = \begin{pmatrix} 9 & 16 \\ 10 & 5 \end{pmatrix} = m.$$

301 7. Security of MMMC1 and MMMC2

302 Look at some of the attacks on the cryptosystems MMMC1 and MMMC2.

7.1 A ciphertext only attack

Let $C = (C_1, C_2)$ be a ciphertext for plaintext m , then

$$C_1 = \gamma^{-1} \xi(\psi(L^{-1})), \quad C_2 = \gamma m \xi(\phi(L))$$

and therefore we come to the equation system with unknowns matrices m , Y and unknown unit $\gamma \in \mathbf{Z}_n^*$:

$$\begin{cases} C_1 = \gamma^{-1} Y^{-1} \psi(L^{-1}) Y, \\ C_2 = \gamma m Y^{-1} \phi(L) Y. \end{cases} \quad (*)$$

For random unit γ cryptanalyst has not another way to solve this equation system as to suppose concrete value $\gamma = \gamma_0$ and to solve the conjugation problem: to find unknown matrix Y from the equation:

$$\gamma_0 C_1 = Y^{-1} \psi(L^{-1}) Y.$$

Rewriting this matrix equation as system of four linear equations with four unknowns cryptanalyst finds the set of solutions, depending on one or more parameters, each of which runs $\mathbf{Z}_n$. Then he inserts each solution $Y = Y_0$ in the second equation of system (*) :

$$C_2 = \gamma_0 m Y_0^{-1} \phi(L) Y_0$$

and finds corresponding solution $m = m_0$. Thus, for each fixed γ_0 cryptanalyst receives at least n pairs of the form (Y_0, m_0) . Because γ_0 accepts $\phi(n)$ values, the cryptanalyst gets $n\phi(n)$ triples of the form (γ_0, Y_0, m_0) . Consequently, if n is not less than 64 bit integer, then check which of these non less approximately 2^{125} triplets is a true solution becomes infeasible.

7.2. A known-plaintext attack

Let $(m^{(1)}, C^{(1)}), \dots, (m^{(k)}, C^{(k)})$ be the pairs of the form plaintext-ciphertext. Cryptanalyst needs to find unknown plaintext $m^{(k+1)}$ from the corresponding ciphertext $C^{(k+1)}$.

In our case for the cryptosystems MMMC1 and MMMC2 encryption uses the new random one-time key Y for the new plaintext. Therefore knowledge of previous pairs of the form plaintext-ciphertext gives no information to find the unknown plaintext from the corresponding ciphertext for a new pair.

7.3. A chosen-plaintext attack

There are the same arguments as for a known-plaintext attack.

7.4. An adaptive chosen-plaintext attack

There are the same arguments as before.

7.5. A chosen-ciphertext attack

Let m^* be a random matrix in the group $GL_2(\mathbf{Z}_n)$, $C = (C_1, C_2)$ be a ciphertext for unknown plaintext m . Cryptanalyst Connor computes $m^* C_2$ and offers Alice to decrypt the ciphertext $C^* = (C_1, m^* C_2)$. Then Alice finds corresponding plaintext $m^* m$ and sends it to Connor. Finally Connor computes the initial plaintext as the following:

$$(m^*)^{-1} (m^* m) = m.$$

7.6. Protection from a chosen ciphertext attack

To prevent this attack one has to replace one-sided ciphertext with two-sided ciphertext. Namely, one-sided ciphertext:

$$C = (C_1, C_2), C_1 = \gamma^{-1}Y^{-1}\psi(L^{-1})Y, C_2 = \gamma mY^{-1}\phi(L)Y$$

is replaced with two-sided ciphertext

$$C = (C_1, C_2), C_1 = \gamma^{-1}Y^{-1}\psi(L^{-1})Y, C_2 = \gamma^2Y^{-1}\phi(L)YmY^{-1}\phi(L)Y.$$

In this case decryption becomes the following:

a) Alice computes

$$z = \alpha\beta^{-1}(C_1);$$

b) then computes

$$zC_2z = m.$$

The chosen ciphertext attack in this case will not be successful, since the matrices Y and m in general do not commute. These variants of the MMMC1 and MMMC2 will be called closed cryptosystem variants.

Note. An attack with a chosen ciphertext breaks cryptosystems RSA, ElGamal and Rabin, but attempts to build their modifications resistant to this attack, still resulted in a very inefficient cryptosystems. As we can see, for the matrix modular cryptosystems situation is different, since the closed variant differs from the usual only a few number of matrix multiplications.

8. Conclusions

In paper two modifications of Basic Matrix Modular Cryptosystem (BMMC) are developed. Both cryptosystems are faster than the BMMC and balanced with respect to a pair of security-efficiency. In the most important case for the use of public-key cryptosystems, namely, key exchange protocols for symmetric ciphers, such as AES, the key length is usually equal to 256 bits. Protocol using BMMC was developed for the key exchange in [2]. Replacing this cryptosystem on the one of the modified matrix cryptosystems, we obtain plaintext (key) as a 2×2 matrix over the residue ring $\mathbf{Z}_n$ with 64 bit modulus n . As shown in the article, for such modulus n modified matrix modular cryptosystems are fast and secure, they can be used in various applications.

References

- [1]. Rososhek S.K. New Practical Algebraic Public-Key Cryptosystem and Some Related Algebraic and Computational Aspects. Applied Mathematics. 2013, 4(7): 1043–1049.
- [2]. Rososhek S.K., Gorbunov E.S. Non commutative analogue of Diffie-Hellman protocol in matrix ring over the residue ring. International Journal of Computers and Technology. 2013, 11(10): 3051-3059.