Quasigroups and Related Systems **12** (2004), 61 – 73

Spurious multiplicative group of GF(p^m): a new tool for cryptography

Czesław Kościelny

Abstract

An unconventional approach to cryptography, consisting in application of an algebraic structure, called spurious multiplication group of $GF(p^m)$ and denoted as $SMG(p^m)$, the operation table of which is not, in general, a Latin square, has been presented. This algebraic system is a natural generalization of the multiplicative group of $GF(p^m)$, so, one can operate on elements of these two structures using the same routine or the same hardware. On the basis of $SMG(p^m)$ many strong symmetric-key ciphers, and at least, as it is shown in the paper, one public-key cipher, can be built.

1. Introduction

At the beginning of the silicon era technological applications of semiconductors in the form of pure crystalline germanium or silicon were very limited. The meaningful development of semiconductor electronics has begun only when the trace amounts of dopants, causing defects of the crystal's structure, to the silicon or germanium crystals have been added. It is possible to perceive some analogy between contemporary cryptography and the pre-semiconductor era in electronics: generally in all currently proposed and used cryptographic systems encrypting/decrypting procedures compute cryptograms corresponding to given plaintexts, and vice versa, using pure algebraic structures such as groups, rings and fields. Doubtlessly, applying in cryptographic operations algebraic structures with small "defects" can

2000 Mathematics Subject Classification: 05B15, 20N05, 94B05
Keywords: cryptography, symmetric-key and public-key ciphers, non-associative algebraic structure.

have positive influence on the properties of ciphers, because it makes cryptanalysis more difficult and may not change the complexity of cryptographic algorithms. As it turned out, this guess was correct, thus, one of many possible "defected" algebraic systems, a spurious multiplicative group of $GF(p^m)$ is described in the paper. This system can deliver many strong and useful ciphers.

The present work is mainly addressed to application researches. Then it is assumed that the books [2, 5, 7, 8] are known to the reader, who also ought to have an adequate mathematical knowledge. There would be no harm if the reader is well-informed about the new trends in modern conventional cryptology [1, 6].

2. Definition of SMG($\mathbf{p^m}$)

For all prime p, for any positive integer $m \geq 2$ and for any polynomial $f(x)$ of degree m over $GF(p)$ there exists an algebraic system denoted as $SMG(p^m)$

$$SMG(p^m) = \langle Gx, \bullet \rangle, \tag{1}$$

consisting of the set Gx of all $p^m - 1$ non-zero polynomials of degree dg over $GF(p)$, $0 \leq dg \leq m-1$, and of an operation of multiplication of these polynomials modulo polynomial $f(x)$. Such an algebraic system is a generalization of the multiplicative group of $GF(p^m)$, therefore, it will be called the spurious multiplicative group of $GF(p^m)$.

The spurious multiplicative group of $GF(p^m)$, more convenient for applications

$$SMG(p^m) = \langle G, \circ \rangle, \tag{2}$$

is obtained using the isomorphic mapping

$$\sigma : Gx \to G, \tag{3}$$

defined by function $\sigma(v(x)) = v(p)$, converting a polynomial $v(x) \in Gx$ to a number from the set $G = \{1, \ldots, p^m - 1\}$. Therefore

$$\forall\, a, b \in G \;\; a \circ b \;\; = \;\; \sigma(\sigma^{-1}(a) \bullet \sigma^{-1}(b) \pmod{f(x)}). \tag{4}$$

Evidently, the inverse mapping σ^{-1} is described by means of the following two-step algorithm:

Step 1:

convert a base 10 number $a \in G$ to base p, namely,

$$a = a_{m-1} \cdots a_1 a_0,\ a_i \in \{0,\ 1,\ \ldots,\ p-1\},$$

Step 2:

$$\sigma^{-1}(a) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} \in Gx.$$

In principle, $SMG(p^m)$ is a commutative quasigroupoid* in which the operation may not neither be closed, nor be fully associative. The operation in G may be implemented in any programming language or by means of an appropriate hardware. However, it is not a trivial task to construct such software or hardware. It requires, for serious applications, very efficient arithmetic operations in the domain of univariate polynomials over the integers modulo p. Since $SMG(p^m)$ is a natural generalization of the multiplicative group of $GF(p^m)$, the multiplication, rising to a power and inversion in $SMG(p^m)$ can be performed by the same routines or by the same hardware as in the multiplicative group of $GF(p^m)$.

3. Known properties of SMG(p^m)

Spurious multiplicative group of p^m-element Galois field is rather a simple algebraic structure, but it has many very interesting properties. From the cryptographic point of view, the most important attribute of $SMG(p^m)$ is the relationship between the number of its reversible elements and a polynomial of degree m over $GF(p)$, defining multiplication of its elements.

The following properties of $SMG(p^m)$ are already known:

P01: The number of $SMG(p^m)$ equals to p^m.

P02: The $p^m - 1$ elements of $SMG(p^m)$ belong to two disjoint sets - a set of reversible elements $SR = \{r_1,\ r_2,\ \ldots,\ r_{N_r}\}$ and a set of irreversible elements $SI = \{i_1,\ i_2,\ \ldots,\ i_{N_i}\}$, where

$$N_r = |SR|,\ N_i = |SI| \text{ and } N_r + N_i = p^m - 1.$$

* The groupoid is an algebraic structure on a set with a binary operator. The only restriction on the operator is closure. It is assumed here that for the quasigroupoid a closure is not required.

P03: Any reversible element of $SMG(p^m)$ is a generator of cyclic group, being a subgroup of $SMG(p^m)$.

P04: If $f(x)$ is irreducible, $SMG(p^m)$ becomes a multiplicative group of $GF(p^m)$.

P05: In a "truly spurious" $SMG(p^m)$ (when $f(x)$ is not irreducible) the maximum order of reversible elements is, in most cases, less than N_r.

P06: In a "truly spurious" $SMG(p^m)$ the system $\langle SR, \circ \rangle$ in most cases forms non-cyclic abelian group.

P07: In a "truly spurious" $SMG(p^m)$ the operation $\circ$ is not closed, since for some $a,\ b\ \in SMG(p^m)$ the case $a \circ b = 0$ occurs.

P08: The multiplication table of a "truly spurious" $SMG(p^m)$ has the form shown in Table 1,

Table 1: Multiplication table in a "truly spurious" $SMG(p^m)$

$\circ$	r_1 r_2 $\cdots$ r_{N_r}	i_1 i_2 $\cdots$ i_{N_i}
r_1 r_2 $\vdots$ r_{N_r}	A	B^T
i_1 i_2 $\vdots$ i_{N_i}	B	C

where $A = SR \times SR$, $B = SI \times SR$, $C = SI \times SI$, and only A is a Latin square.

P09: CONJECTURE: The polynomial $f(x) = x^m$ generates an $SMG(2^m)$ with $N_r = 2^{m-1}$.

P10: CONJECTURE: If $p > 2$ then the polynomial $f(x) = a\,x^2$, where $a \in \{1, 2, \ldots, p-1\}$, generates $SMG(p^m)$ in which all reversible elements form a cyclic group of order $p^2 - p$.

P11: CONJECTURE: In $SMG(p^m)$ with $p > 2$:

if $m = 2$ then there are only three values of N_r such that

N_r	$N_{f(x)}$
$(p-1)^2$	$p\,(p-1)/2$
$p\,(p-1)$	p
p^2-1	$p\,(p-1)/2$

if $m = 3$ then there are only five values of N_r such that

N_r	$N_{f(x)}$
$(p-1)^3$	$p\,(p-1)(p-2)/6$
$p\,(p-1)^2$	$p\,(p-1)$
$(p+1)\,(p-1)^2$	$p^2\,(p-1)/2$
$p^2\,(p-1)$	p
p^3-1	$p\,(p^2-1)/3$

where $N_{f(x)}$ denotes the number of polynomials generating $SMG(p^m)$ with the number of reversible elements equal to N_r.

All reversible elements of $SMG(p^m)$ behave as usual: any such element $a_r \in SMG(p^m)$ has its proper multiplicative order t_r (t_r is the least positive integer such that $a_r^{t_r} = 1$). As regards irreversible elements $a_i \in SMG(p^m)$, each a_i may be characterized by means of so-called multiplicative quasi order t_i, e. g. the least positive integer such that the set $\{a_i^k,\ k = 1, 2, \ldots, t_i\}$ contains all distinct powers of an element a_i.

Although all properties of $SMG(p^m)$ are not yet known, the existence of such quasigroupoids seems to be important for application in cryptography, therefore, some Maple routines aiding the reader in examining the properties of $SMG(p^m)$ in [4] are presented.

4. Examples of SMG($\mathbf{p^m}$)

First example concerns $SMG(3^2) = \langle Gx, \bullet \rangle$, generated by means of a polynomial $f(x) = x^2$, where

$$Gx = \{1,\, 2,\, 1+x,\, 2+x,\, 1+2\,x,\, 2+2\,x,\, x,\, 2\,x\}.$$

In the above set of elements of the spurious multiplicative group of order 8 first six elements have their multiplicative inverses, while the last two ones are irreversible.

It is easy to verify that the multiplication table for considered $SMG(3^2)$ in Table 2 is presented.

Table 2: Multiplication table of $SMG(3^2) = \langle Gx, \bullet \rangle$ generated using $f(x) = x^2$

$\bullet$	1	2	$1+x$	$2+x$	$1+2\,x$	$2+2\,x$	x	$2\,x$
1	1	2	$1+x$	$2+x$	$1+2\,x$	$2+2\,x$	x	$2\,x$
2	2	1	$2+2\,x$	$1+2\,x$	$2+x$	$1+x$	$2\,x$	x
$1+x$	$1+x$	$2+2\,x$	$1+2\,x$	2	1	$2+x$	x	$2\,x$
$2+x$	$2+x$	$1+2\,x$	2	$1+x$	$2+2\,x$	1	$2\,x$	x
$1+2\,x$	$1+2\,x$	$2+x$	1	$2+2\,x$	$1+x$	2	x	$2\,x$
$2+2\,x$	$2+2\,x$	$1+x$	$2+x$	1	2	$1+2\,x$	$2\,x$	x
x	x	$2\,x$	x	$2\,x$	x	$2\,x$	0	0
$2\,x$	$2\,x$	x	$2\,x$	x	$2\,x$	x	0	0

Using the mapping (1.3) we obtain $SMG(3^2) = \langle G, \circ \rangle$, where

$$G = \{1,\, 2,\, 4,\, 5,\, 7,\, 8,\, 3,\, 6,\, 7,\, 8\},$$

with the following operation table:

Table 3: Multiplication table in $SMG(3^2) = \langle G, \circ \rangle$ generated using $f(x) = x^2$

$\circ$	1	2	4	5	7	8	3	6
1	1	2	4	5	7	8	3	6
2	2	1	8	7	5	4	6	3
4	4	8	7	2	1	5	3	6
5	5	7	2	4	8	1	6	3
7	7	5	1	8	4	2	3	6
8	8	4	5	1	2	7	6	3
3	3	6	3	6	3	6	0	0
6	6	3	6	3	6	3	0	0

We may notice that operation tables have the form defined by the property **P09**.

In the second example the polynomial $f(x) = x^4+x^2+1 = (x^2+x+1)^2$ over $GF(2)$ is used to construct $SMG(2^4) = \langle G, \circ \rangle$, where

$$G = \{1, 2, 3, 4, 5, 6, 8, 10, 11, 12, 13, 15, 7, 9, 14\}.$$

Similarly, as in the previous example, we take reversible elements as the first 12 elements of the set G, this way the last 3 elements are irreversible.

Table 4: Multiplication table in $SMG(2^4) = \langle G, \circ \rangle$ generated using $f(x) = x^4 + x^2 + 1$

$\circ$	1	2	3	4	5	6	8	10	11	12	13	15	7	9	14
1	1	2	3	4	5	6	8	10	11	12	13	15	7	9	14
2	2	4	6	8	10	12	5	1	3	13	15	11	14	7	9
3	3	6	5	12	15	10	13	11	8	1	2	4	9	14	7
4	4	8	12	5	1	13	10	2	6	15	11	3	9	14	7
5	5	10	15	1	4	11	2	8	13	3	6	12	14	7	9
6	6	12	10	13	11	1	15	3	5	2	4	8	7	9	14
8	8	5	13	10	2	15	1	4	12	11	3	6	7	9	14
10	10	1	11	2	8	3	4	5	15	6	12	13	9	14	7
11	11	3	8	6	13	5	12	15	4	10	1	2	14	7	9
12	12	13	1	15	3	2	11	6	10	4	8	5	14	7	9
13	13	15	2	11	6	4	3	12	1	8	5	10	9	14	7
15	15	11	4	3	12	8	6	13	2	5	10	1	7	9	14
7	7	14	9	9	14	7	7	9	14	14	9	7	0	0	0
9	9	7	14	14	7	9	9	14	7	7	14	9	0	0	0
14	14	9	7	7	9	14	14	7	9	9	7	14	0	0	0

The multiplication table of the considered $SMG(2^4)$ is presented in Table 4. Using this table we can examine multiplicative orders of all reversible elements and multiplicative quasi-order of any irreversible elements as well. This task is a little laborious, but to make it easier the multiplicative orders of all 12 reversible elements as well as multiplicative quasi-orders of 3 irreversible elements of the examined $SMG(2^4)$, together with the sets of distinct successive powers of any element, have been computed and presented below.

reversible element	multiplicative order	set of distinct successive powers of the element
1	1	{1}
2	6	{1, 2, 4, 5, 8, 10}
3	6	{1, 3, 4, 5, 12, 15}
4	3	{1, 4, 5}
5	3	{1, 4, 5}
6	2	{1, 6}
8	2	{1, 8}
10	6	{1, 2, 4, 5, 8, 10}
11	6	{1, 4, 5, 6, 11, 13}
12	6	{1, 3, 4, 5, 12, 15}
13	6	{1, 4, 5, 6, 11, 13}
15	2	{1, 15}
irreversible element	**multiplicative quasi-order**	**set of distinct successive powers of the element**
7	2	{0, 7}
9	2	{0, 9}
14	2	{0, 14}

The next example concerns $SMG(5^2)$ with 16 reversible elements. According to the property **P11** in this case $N_{f(x)} = 10$ and the polynomials x^2+1, x^2+4, x^2+x, x^2+x+3, x^2+2x, x^2+2x+2, x^2+3x, x^2+3x+2, x^2+4x, x^2+4x+3 for constructing such spurious multiplicative group of $GF(5^2)$ may be used. Using the polynomial $f(x) = x^2+1$ we obtain the following elements of the interior of the multiplication table:

$$A = \begin{bmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 9 & 10 & 12 & 13 & 15 & 17 & 18 & 20 & 21 & 24 \\
2 & 4 & 1 & 3 & 10 & 12 & 13 & 20 & 24 & 21 & 5 & 9 & 6 & 15 & 17 & 18 \\
3 & 1 & 4 & 2 & 15 & 18 & 17 & 5 & 6 & 9 & 20 & 21 & 24 & 10 & 13 & 12 \\
4 & 3 & 2 & 1 & 20 & 24 & 21 & 15 & 18 & 17 & 10 & 13 & 12 & 5 & 9 & 6 \\
5 & 10 & 15 & 20 & 4 & 9 & 24 & 3 & 13 & 18 & 2 & 12 & 17 & 1 & 6 & 21 \\
6 & 12 & 18 & 24 & 9 & 10 & 3 & 13 & 20 & 1 & 17 & 4 & 5 & 21 & 2 & 15 \\
9 & 13 & 17 & 21 & 24 & 3 & 15 & 18 & 1 & 5 & 12 & 20 & 4 & 6 & 10 & 2 \\
10 & 20 & 5 & 15 & 3 & 13 & 18 & 1 & 21 & 6 & 4 & 24 & 9 & 2 & 12 & 17 \\
12 & 24 & 6 & 18 & 13 & 20 & 1 & 21 & 15 & 2 & 9 & 3 & 10 & 17 & 4 & 5 \\
13 & 21 & 9 & 17 & 18 & 1 & 5 & 6 & 2 & 10 & 24 & 15 & 3 & 12 & 20 & 4 \\
15 & 5 & 20 & 10 & 2 & 17 & 12 & 4 & 9 & 24 & 1 & 6 & 21 & 3 & 18 & 13 \\
17 & 9 & 21 & 13 & 12 & 4 & 20 & 24 & 3 & 15 & 6 & 10 & 2 & 18 & 5 & 1 \\
18 & 6 & 24 & 12 & 17 & 5 & 4 & 9 & 10 & 3 & 21 & 2 & 15 & 13 & 1 & 20 \\
20 & 15 & 10 & 5 & 1 & 21 & 6 & 2 & 17 & 12 & 3 & 18 & 13 & 4 & 24 & 9 \\
21 & 17 & 13 & 9 & 6 & 2 & 10 & 12 & 4 & 20 & 18 & 5 & 1 & 24 & 15 & 3 \\
24 & 18 & 12 & 6 & 21 & 15 & 2 & 17 & 5 & 4 & 13 & 1 & 20 & 9 & 3 & 10
\end{bmatrix}$$

$$B = \begin{bmatrix} 7 & 14 & 16 & 23 & 14 & 16 & 7 & 23 & 7 & 14 & 7 & 16 & 23 & 16 & 23 & 14 \\ 8 & 11 & 19 & 22 & 19 & 22 & 11 & 8 & 19 & 22 & 22 & 8 & 11 & 11 & 19 & 8 \\ 11 & 22 & 8 & 19 & 8 & 19 & 22 & 11 & 8 & 19 & 19 & 11 & 22 & 22 & 8 & 11 \\ 14 & 23 & 7 & 16 & 23 & 7 & 14 & 16 & 14 & 23 & 14 & 7 & 16 & 7 & 16 & 23 \\ 16 & 7 & 23 & 14 & 7 & 23 & 16 & 14 & 16 & 7 & 16 & 23 & 14 & 23 & 14 & 7 \\ 19 & 8 & 22 & 11 & 22 & 11 & 8 & 19 & 22 & 11 & 11 & 19 & 8 & 8 & 22 & 19 \\ 22 & 19 & 11 & 8 & 11 & 8 & 19 & 22 & 11 & 8 & 8 & 22 & 19 & 19 & 11 & 22 \\ 23 & 16 & 14 & 7 & 16 & 14 & 23 & 7 & 23 & 16 & 23 & 14 & 7 & 14 & 7 & 16 \end{bmatrix}$$

$$C = \begin{bmatrix} 23 & 0 & 0 & 16 & 14 & 0 & 0 & 7 \\ 0 & 8 & 11 & 0 & 0 & 19 & 22 & 0 \\ 0 & 11 & 22 & 0 & 0 & 8 & 19 & 0 \\ 16 & 0 & 0 & 7 & 23 & 0 & 0 & 14 \\ 14 & 0 & 0 & 23 & 7 & 0 & 0 & 16 \\ 0 & 19 & 8 & 0 & 0 & 22 & 11 & 0 \\ 0 & 22 & 19 & 0 & 0 & 11 & 8 & 0 \\ 7 & 0 & 0 & 14 & 16 & 0 & 0 & 23 \end{bmatrix}$$

If we use the polynomial $f(x) = x^2 + 4\,x + 3$ we get correspondingly:

$$A' = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 7 & 9 & 10 & 13 & 14 & 15 & 16 & 17 & 20 & 21 & 23 \\ 2 & 4 & 1 & 3 & 10 & 14 & 13 & 20 & 21 & 23 & 5 & 7 & 9 & 15 & 17 & 16 \\ 3 & 1 & 4 & 2 & 15 & 16 & 17 & 5 & 9 & 7 & 20 & 23 & 21 & 10 & 13 & 14 \\ 4 & 3 & 2 & 1 & 20 & 23 & 21 & 15 & 17 & 16 & 10 & 14 & 13 & 5 & 9 & 7 \\ 5 & 10 & 15 & 20 & 7 & 17 & 2 & 14 & 4 & 9 & 16 & 21 & 1 & 23 & 3 & 13 \\ 7 & 14 & 16 & 23 & 17 & 1 & 10 & 9 & 20 & 2 & 21 & 3 & 5 & 13 & 15 & 4 \\ 9 & 13 & 17 & 21 & 2 & 10 & 23 & 4 & 16 & 20 & 1 & 5 & 14 & 3 & 7 & 15 \\ 10 & 20 & 5 & 15 & 14 & 9 & 4 & 23 & 3 & 13 & 7 & 17 & 2 & 16 & 1 & 21 \\ 13 & 21 & 9 & 17 & 4 & 20 & 16 & 3 & 7 & 15 & 2 & 10 & 23 & 1 & 14 & 5 \\ 14 & 23 & 7 & 16 & 9 & 2 & 20 & 13 & 15 & 4 & 17 & 1 & 10 & 21 & 5 & 3 \\ 15 & 5 & 20 & 10 & 16 & 21 & 1 & 7 & 2 & 17 & 23 & 13 & 3 & 14 & 4 & 9 \\ 16 & 7 & 23 & 14 & 21 & 3 & 5 & 17 & 10 & 1 & 13 & 4 & 15 & 9 & 20 & 2 \\ 17 & 9 & 21 & 13 & 1 & 5 & 14 & 2 & 23 & 10 & 3 & 15 & 7 & 4 & 16 & 20 \\ 20 & 15 & 10 & 5 & 23 & 13 & 3 & 16 & 1 & 21 & 14 & 9 & 4 & 7 & 2 & 17 \\ 21 & 17 & 13 & 9 & 3 & 15 & 7 & 1 & 14 & 5 & 4 & 20 & 16 & 2 & 23 & 10 \\ 23 & 16 & 14 & 7 & 13 & 4 & 15 & 21 & 5 & 3 & 9 & 2 & 20 & 17 & 10 & 1 \end{bmatrix}$$

$$B' = \begin{bmatrix} 6 & 12 & 18 & 24 & 12 & 24 & 6 & 24 & 12 & 18 & 6 & 12 & 18 & 18 & 24 & 6 \\ 8 & 11 & 19 & 22 & 22 & 8 & 19 & 19 & 8 & 11 & 11 & 19 & 22 & 8 & 11 & 22 \\ 11 & 22 & 8 & 19 & 19 & 11 & 8 & 8 & 11 & 22 & 22 & 8 & 19 & 11 & 22 & 19 \\ 12 & 24 & 6 & 18 & 24 & 18 & 12 & 18 & 24 & 6 & 12 & 24 & 6 & 6 & 18 & 12 \\ 18 & 6 & 24 & 12 & 6 & 12 & 18 & 12 & 6 & 24 & 18 & 6 & 24 & 24 & 12 & 18 \\ 19 & 8 & 22 & 11 & 11 & 19 & 22 & 22 & 19 & 8 & 8 & 22 & 11 & 19 & 8 & 11 \\ 22 & 19 & 11 & 8 & 8 & 22 & 11 & 11 & 22 & 19 & 19 & 11 & 8 & 22 & 19 & 8 \\ 24 & 18 & 12 & 6 & 18 & 6 & 24 & 6 & 18 & 12 & 24 & 18 & 12 & 12 & 6 & 24 \end{bmatrix}$$

$$C' = \begin{bmatrix} 18 & 0 & 0 & 6 & 24 & 0 & 0 & 12 \\ 0 & 11 & 22 & 0 & 0 & 8 & 19 & 0 \\ 0 & 22 & 19 & 0 & 0 & 11 & 8 & 0 \\ 6 & 0 & 0 & 12 & 18 & 0 & 0 & 24 \\ 24 & 0 & 0 & 18 & 12 & 0 & 0 & 6 \\ 0 & 8 & 11 & 0 & 0 & 19 & 22 & 0 \\ 0 & 19 & 8 & 0 & 0 & 22 & 11 & 0 \\ 12 & 0 & 0 & 24 & 6 & 0 & 0 & 18 \end{bmatrix}$$

Finally, Table 5 contains the multiplication table in the multiplicative group of $GF(2^4)$. Comparing it with Table 4 we may notice that $SMG(2^4)$ clumsily imitates the multiplicative group of $GF(2^4)$, since these tables are coincident only in 48 places (about 21,3 %).

Table 5: Multiplication table in $SMG(2^4)$, being the multiplicative group of $GF(2^4)$, generated using $f(x) = x^4 + x^3 + x^2 + x + 1$ (irreducible polynomial)

$\circ$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	2	4	6	8	10	12	14	15	13	11	9	7	5	3	1
3	3	6	5	12	15	10	9	7	4	1	2	11	8	13	14
4	4	8	12	15	11	7	3	1	5	9	13	14	10	6	2
5	5	10	15	11	14	1	4	9	12	3	6	2	7	8	13
6	6	12	10	7	1	11	13	14	8	2	4	9	15	5	3
7	7	14	9	3	4	13	10	6	1	8	15	5	2	11	12
8	8	15	7	1	9	14	6	2	10	13	5	3	11	12	4
9	9	13	4	5	12	8	1	10	3	7	14	15	6	2	11
10	10	11	1	9	3	2	8	13	7	6	12	4	14	15	5
11	11	9	2	13	6	4	15	5	14	12	7	8	3	1	10
12	12	7	11	14	2	9	5	3	15	4	8	13	1	10	6
13	13	5	8	10	7	15	2	11	6	14	3	1	12	4	9
14	14	3	13	6	8	5	11	12	2	15	1	10	4	9	7
15	15	1	14	2	13	3	12	4	11	5	10	6	9	7	8

The examples presented concern very small $SMG(p^m)$, whereas, in practice, strong cryptographic system are built using $SMG(p^m)$ having, say, 10^{3000} and more elements.

5. SMG(p^m)-based public key cryptosystem

On the basis of $SMG(p^m)$ one can construct many strong symmetric-key block ciphers with a really huge key space. The author intend to publish this problem in the next article, presenting now more difficult task of constructing $SMG(p^m)$-based public-key cryptosystem.

Public-key cryptographic algorithms are designed to resist chosen plain text attacks and their security is based both on the difficulty of finding the secret key from the public key and the difficulty of determining the plaintext from the cryptogram. At present, the most common public-key cryptosystem is the RSA algorithm. It is guessed that the security of RSA depends on the problem of factoring large numbers. It has never been mathematically proven that one needs to factor the modulus n to calculate a plaintext knowing a cryptogram and a public key. It is conceivable that an entirely different way to break RSA can be discovered (perhaps this way is already known to some cryptanalysts). Therefore, cryptographers attempt to activate alternative public-key encryption algorithms, e.g. the basic ElGamal encryption scheme. It is well known that the progress in the discrete logarithm problem forces the users of the basic ElGamal public-key cryptosystem, working in a multiplicative group of $GF(p)$, to permanently increase a prime modulus p in order to ensure the desired security. For long-term security, at least 2000-bit moduli should be used at present. Common system-wide parameters need even larger key sizes, since computing the database of discrete logarithms for one particular p will discredit the secrecy of all private keys computed using this value of p. But the task of finding a generator of a multiplicative group of $GF(p)$ is infeasible for an ordinary user if $p > 2^{2000} \approx 0.11510^{603}$. As shown in the sequel, it is possible to overcome this inconvenience by forming an ElGamal public-key cryptosystem which works in a spurious multiplicative group of $GF(p^m)$. In this case an infeasible task of determining a generator of the multiplicative group of $GF(p)$ is eliminated and the use of 10000-bit modulus, and even more, is possible.

A concise description of slightly modified algorithms for ElGamal public-key encryption scheme [3, 4, 5], working in $SMG(p^m)$, is given below.
Key generation: Each entity creates its public key and the corresponding private key. So each entity $\mathcal{A}$ ought to do the following:

- Choose an arbitrary polynomial $f(x)$ of the degree m over $GF(p)$ and construct a spurious multiplicative group of $GF(p^m)$ that is $SMG(p^m)$, consisting of the set $G = \{1, \ldots, p^m - 1\}$ and of the operation of mul-

tiplication of elements from this set, which is performed by means of a function **mult**(x, y), $x, y \in G$. The function **pow**(x, k), carrying out the operation of rising any element x from G to a k^{th} power, $p^m - 1 \leq k \leq -p^m + 1$, is also defined.

- Select a random reversible element $\alpha \in SMG(p^m)$, $\alpha \neq 1$.
- Choose a random integer $a \in G$, $2 \leq a \leq p^m - 2$, and compute the element $\beta =$ **pow**(α, a).
- $\mathcal{A}$'s public key is α and β, together with $f(x)$ and the functions **mult** and **pow**, if these last three parameters are not common to all the entities.
- $\mathcal{A}$'s private key is a.

Encryption: Entity $\mathcal{B}$ encrypts a message m for $\mathcal{A}$, which $\mathcal{A}$ decrypts. Thus $\mathcal{B}$ should make the following steps:

- Obtain $\mathcal{A}$'s authentic public key α, β, and $f(x)$ together with the functions **mult** and **pow** if these parameters are not common.
- Represent the message m as a number from the set G.
- Choose a random integer $k \in G$.
- Determine numbers $c_1 =$**pow**(α, k) and $c_2 =$**mult**$(m,$ **pow**$(\beta, k))$.
- send the ciphertext $c = (c_1,\ c_2)$ to $\mathcal{A}$.

Decryption: To find plaintext m from the ciphertext $c = (c_1,\ c_2)$, $\mathcal{A}$ should perform the following operations:

- Use the private key a to compute $g =$ **pow**$(c_1,\ a)$ and then compute $g^{-1} =$ **pow**$(g,\ -1)$.
- Retrieve the plaintext by computing $m =$ **mult**$(g^{-1},\ c_2)$.

If $f(x)$ is irreducible, then ElGamal cryptosystem works in a subgroup of the multiplicative group of $GF(p^m)$. In this case $SMG(p^m)$ becomes a multiplicative group of $GF(p^m)$ and all its elements are reversible. If, in addition, $f(x)$ is primitive, then we can easily compute a set of cryptographic keys for public-key cryptosystem, working in a multiplicative group of $GF(p^m)$ choosing $\alpha = p$ in the second step of a key generation algorithm.

5. Conclusions

A new simple algebraic structure very useful in cryptography, which was named $SMG(p^m)$, being the generalization of the multiplicative group of $GF(p^m)$, has been presented. The structure described, apart from immediate application in cryptography, may be interesting to mathematicians, because all its properties are not known yet. Furthermore, all reversible elements of any $SMG(p^m)$ form an interesting group, which was earlier not noticed.

Acknowledgment

The author wishes to thank A. D. Keedwell for very valuable suggestions.

References

[1] **A. Biryukov**: *Block Ciphers and Stream Ciphers: the State of the Art*, `http://www.esat.kuleuven.ac.be/abiryukov/lecturenotes.pdf`, 2003.

[2] **N. Ferguson, B. Schneier**: *Practical Cryptography*, John Wiley & Sons, 2003.

[3] **C. Kościelny**: *A New Approach to the ElGamal Encryption Scheme*, Int. J. Appl. Math. Comput. Sci. **14** (2004), 101 – 103.

[4] **C. Kościelny**: *User-Friendly ElGamal Public-Key Encryption Scheme*, `http://www.mapleapps.com`, 2003.

[5] **A. J. Menezes, P. C. van Oorschot, S. A. Vanstone**: *Handbook of Applied Cryptography*, CRC Press, 1998.

[6] **B. Preneel et. al.**: *New Trends in Cryptology*, `http://www.stork.eu.org/documents/ENS-D4-1-4.pdf`, 2003.

[7] **B. Schneier**: *Applied Cryptography*, (Second Edition): Protocols, Algorithms, and Cource Code in C, John Wiley & Sons, 1996.

[8] **D. R. Stinson**: *Cryptography – Theory and Practice*, CRC Press, 1995.

Received August 31, 2004

Academy of Management in Legnica
Faculty of Computer Science
ul. Reymonta 21
59-220 Legnica
Poland
e-mail: c.koscielny@wsm.edu.pl