THE ROUND FUNCTIONS OF CRYPTOSYSTEM PGM GENERATE THE SYMMETRIC GROUP

A. CARANTI AND F. DALLA VOLTA

Abstract. S. S. Magliveras et al. have described symmetric and public key cryptosystems based on *logarithmic signatures* (also known as *group bases*) for finite permutation groups. In this paper we show that if G is a nontrivial finite group which is not cyclic of order a prime, or the square of a prime, then the round (or encryption) functions of these systems, that are the permutations of G induced by the *exact-transversal logarithmic signatures* (also known as *transversal group bases*), generate the full symmetric group on G. This answers a question of S. S. Magliveras, D.R. Stinson and Tran van Trung.

1. Introduction

S. S. Magliveras has described in [7] a symmetric key cryptosystem, called PGM (for Permutation Group Mappings), which is based on *logarithmic signatures* (also known as *group bases*) for finite permutation groups. In [8], S. S. Magliveras, D.R. Stinson and Tran van Trung have described two public key cryptosystems MST_1 and MST_2, which are based on logarithmic signatures. An implementation of a symmetric block cipher TST based on these ideas is described in [4, 3].

These cryptosystems are based on certain round (or encryption) functions, the PGM transformations, which are the permutations on the set $\{ 1, 2, \dots, \lvert G \rvert \}$, where G is a finite group, induced by *exact-transversal logarithmic signatures* on G (these are also known as *transversal group bases*; see Section 2 for the relevant definitions). In [9], S. S. Magliveras and N. D. Memon studied the algebraic properties of the group generated by the set $\hat{\mathcal{E}}$ of PGM transformations, in particular investigating its size. This is because a small group here would make the cryptosystem weak, and indeed questions about the size of the corresponding groups have been asked (and answered) for DES [6, 2, 11], AES [12], and other cryptosystems.

S. S. Magliveras and N. D. Memon have proved in [9] that the group is as big as possible, subject to some restrictions.

Theorem 1.1 (Magliveras-Memon). *Let G be a finite non-Hamiltonian group. Suppose the order of G is different from*

$$q, 1+q^2, 1+q^3, \frac{q^k-1}{q-1}, 2^{k-1}(2^k \pm 1), 11, 12, 15, 22, 23, 24, 176, 276,$$

where q is a prime power and k is a positive integer.

Then the group $\langle \hat{\mathcal{E}} \rangle$ generated by $\hat{\mathcal{E}}$ is the full symmetric group $\mathrm{Sym}(\lvert G \rvert)$.

Date: 17 September 2003.

Key words and phrases. Permutation group mappings (PGM), exact-transversal logarithmic signatures, group bases, primitive permutation groups, symmetric group.

(Here a group is said to be *Hamiltonian* when all of its subgroups are normal.)

S. S. Magliveras, D.R. Stinson and Tran van Trung suggest in [8] that the above Theorem may in fact hold in more general circumstances. The goal of this short note is to show that this is indeed the case. We prove

Theorem 1.2. *Let G be a nontrivial finite group. Suppose G is not cyclic of order a prime, or the square of a prime.*

Then the group $\langle \hat{\mathcal{E}} \rangle$ generated by $\hat{\mathcal{E}}$ is the full symmetric group $\mathrm{Sym}(|G|)$.

In a cyclic group of prime order we have $\hat{\mathcal{E}} = \emptyset$, so the result does not hold. We deal with the case of cyclic groups of order the square of a prime in Section 5.

The key to our approach is an analysis of some PGM transformations from the point of view of imprimitive group actions (Section 3). We are then able to avoid a call to the classification of 2-transitive groups (which is where the list of exceptions in Theorem 1.1 comes in), obtaining an elementary proof of Theorem 1.2 (Section 4).

We are grateful to Andrea Lucchini for a useful reference.

2. Preliminaries

In this section we recall briefly the definitions we need from [9, 8], and set up some notation for the rest of the paper. Two convenient references for the theory of (permutation) groups we use are [10, 1]. For a positive integer n, we write

$$\mathbf{I}_n = \{ 0, 1, \dots, n-1 \}$$

Let G be a finite group. Let

$$\{ 1 \} = G_0 < G_1 < \dots < G_{s-1} < G_s = G \tag{2.1}$$

be a chain of subgroups of G, with $s \geq 2$. (So there is no such chain if G is trivial, or if it has prime order.) An *exact-transversal logarithmic signature* (ETLS) for G with respect to (2.1) is an s-tuple $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_s)$, where each α_i is a bijection between $\mathbf{I}_{|G_i : G_{i-1}|}$ and a complete set of right coset representatives of G_{i-1} in G_i, for $i = 1, \dots s$. (These are called *transversal group bases* in [4, 3].) In this paper we will only need the case when $s = 2$, so that (2.1) becomes a chain

$$\{ 1 \} < H < G.$$

Writing $\mu = |H|$ and $\lambda = |G : H|$ (so that $\lambda\mu = |G|$), we have that $\alpha_1 : \mathbf{I}_\mu \to H$ is a bijection, and α_2 is a bijection between $\mathbf{I}_\lambda$ and a complete set of right coset representatives of H in G.

Writing $n = |G|$, an ETLS α with respect to $\{ 1 \} < H < G$ establishes a bijection between $\mathbf{I}_n$ and G, given by

$$\begin{aligned} \breve{\alpha} : \ & \mathbf{I}_n \to G \\ & x \mapsto \alpha_1(x_1) \cdot \alpha_2(x_2), \end{aligned} \tag{2.2}$$

where x is written uniquely as $x = x_2 + \lambda x_1$, with $x_2 \in \mathbf{I}_\lambda$, and $x_1 \in \mathbf{I}_\mu$.

The map $\mathbf{I}_n \to \mathbf{I}_\mu \times \mathbf{I}_\lambda$, that maps x to the pair (x_1, x_2), is known as a *knapsack transformation* [4, Def. 2.19]. A proof in Section 4 would be slightly smoother using the (equivalent) knapsack transformation in which the roles of x_1 and x_2 are reversed. We prefer to stick to the conventions of [8, 9], though.

Once an ETLS α is fixed (see the comments in Subsection 4.3), one may consider the set of permutations of $\mathbf{I}_n$ given by

$$\hat{\mathcal{E}} = \hat{\mathcal{E}}_\alpha = \left\{ \breve{\alpha} \circ \breve{\beta}^{-1} : \mathbf{I}_n \to \mathbf{I}_n \mid \beta \text{ an ETLS for } G \right\}. \tag{2.3}$$

(Here and in the following, we compose maps left-to-right.) This is the set of PGM transformations mentioned in the statements of Theorems 1.1 and 1.2. Note that if γ is a further ETLS, we have

$$(\breve{\alpha} \circ \breve{\gamma}^{-1})^{-1} \circ (\breve{\alpha} \circ \breve{\beta}^{-1}) = \breve{\gamma} \circ \breve{\beta}^{-1}.$$

It follows, as in [8], that the group generated by $\hat{\mathcal{E}}$ also contains all permutations

$$\breve{\gamma} \circ \breve{\beta}^{-1} : \mathbf{I}_n \to \mathbf{I}_n,$$

where β, γ are ETLS for G.

We write $\mathrm{Sym}(X)$ (resp. $\mathrm{Alt}(X)$) for the symmetric (resp. alternating) group on a set X; we write $\mathrm{Sym}(n) = \mathrm{Sym}(\mathbf{I}_n)$, and similarly for Alt. In particular, $\hat{\mathcal{E}} \subseteq \mathrm{Sym}(n)$.

3. Imprimitivity

In this section we analyze the permutations $\breve{\alpha} \circ \breve{\beta}^{-1} \in \mathrm{Sym}(n)$, where α and β are ETLS of a certain form, from the point of view of *imprimitive group actions*. Our arguments apply to the case when α is a fixed ETLS with respect to $\{ 1 \} < H < G$, and β is another ETLS with respect to $\{ 1 \} < H < G$, obtained from α via certain transformations, which we now describe.

We consider the partition of G in the right cosets of H, and certain transformation on G that move cosets to cosets. The first such transformation is obtained by reordering the coset representatives in α. That is, given a permutation $\tau \in \mathrm{Sym}(\lambda)$, we obtain a new ETLS β by setting $\beta_1 = \alpha_1$, and then $\beta_2(x_2) = \alpha_2(x_2\tau)$, for $x_2 \in \mathbf{I}_\lambda$. From (2.2) we have $x\breve{\beta} = \beta_1(x_1) \cdot \beta_2(x_2) = \alpha_1(x_1) \cdot \alpha_2(x_2\tau)$. In other words $x\breve{\beta} = (x\breve{\tau})\breve{\alpha}$, where $x\breve{\tau} = (x_2 + \lambda x_1)\breve{\tau} = x_2\tau + \lambda x_1$; that is, $\breve{\beta} = \breve{\tau} \circ \breve{\alpha}$.

All these transformations $\breve{\tau}$ act *imprimitively* on $\mathbf{I}_n$. We recall that if a group S acts transitively on a set X, then we say that S acts *imprimitively* on X (or simply that S is *imprimitive*) if there is a partition $\mathcal{P}$ of X, called a *block system*, whose elements, called *blocks*, satisfy the following properties:

(1) S maps an element of $\mathcal{P}$ onto another element of $\mathcal{P}$ (it follows in particular that all elements of $\mathcal{P}$ have the same order);
(2) the elements of $\mathcal{P}$ are proper subsets of X, containing at least two elements.

One says that S *respects* the block system $\mathcal{P}$ on X. (See for instance [1, Sect. 1.9] or [10, Sect. 7.2], for further details. We regret that we are using the term *block* in a sense that is different by that of [9, 8], but the terminology we use is well established in the context of permutation groups.)

The transitive group S is said to be *primitive* if it is not imprimitive. It is an easy fact that a 2-transitive group is primitive (see [10, 7.2.4] or [1, Theorem 1.7]).

In our context, the $\breve{\tau}$ act on $\mathbf{I}_n$, respecting the block system on $\mathbf{I}_n$ given by the blocks

$$B_{x_2} = \{\, x_2 + \lambda x_1 : x_1 \in \mathbf{I}_\mu \,\}, \tag{3.1}$$

for $x_2 \in \mathbf{I}_\lambda$. Now note that $\breve{\alpha} \circ \breve{\beta}^{-1} = \breve{\alpha} \circ \breve{\alpha}^{-1} \circ \breve{\tau}^{-1} = \breve{\tau}^{-1}$. We can then forget about α and β, and consider only the $\breve{\tau}^{-1}$. We call these transformations $\breve{\tau}^{-1}$ (or the $\breve{\tau}$, which is the same) the *blockwise permutations* of the block system B_i.

The second type of transformations arise from permutations within a single coset. Choose a fixed coset representative $\alpha_2(z_0)$, for some $z_0 \in \mathbf{I}_\lambda$, and a fixed element $h \in H$, and consider the β that coincides with α, but for $\beta_2(z_0) = h \cdot \alpha_2(z_0)$. We have $x\breve{\beta} = x\breve{\alpha}$, except when $x = z_0 + \lambda x_1$, when we have

$$x\breve{\beta} = \beta_1(x_1) \cdot \beta_2(z_0) = \alpha_1(x_1) \cdot (h \cdot \alpha_2(z_0)) = (\alpha_1(x_1) \cdot h) \cdot \alpha_2(z_0).$$

Now, given a group H, the group homomorphism $H \to \mathrm{Sym}(H)$ given by $h \mapsto (k \mapsto k \cdot h)$ is called the *regular representation* of H. We write τ_h for the permutation of $\mathbf{I}_\mu$ induced by the image of h under the regular representation, via the bijection $\alpha_1 : \mathbf{I}_\mu \to H$. In other words, for $x_1 \in \mathbf{I}_\mu$ we write $\alpha_1(x_1) \cdot h = \alpha_1(x_1 \tau_h)$. In this setting, we have $\breve{\beta} = \breve{\tau}_{z_0,h} \circ \breve{\alpha}$, where $\breve{\tau}_{z_0,h} = \breve{\alpha} \circ \breve{\beta}^{-1}$ is the identity on all blocks, except that on the block B_{z_0} it will act as $(z_0 + \lambda x_1)\breve{\tau}_{z_0,h} = z_0 + \lambda(x_1 \tau_h)$. We call these transformations the *regular permutations* of the block B_{z_0}. Clearly, they also respect the block system (3.1).

Note that the combination of the two classes of transformations we have described go under the name of *monomial transformations* in [9]. Monomial transformations alone would yield 1-transitivity; however, we will be proving a stronger statement in Section 4.

The third class of transformations occurs when we obtain β from α by permuting the elements of H, that is, by taking $\beta_2 = \alpha_2$, and then $\beta_1(x_1) = \alpha_1(x_1 \tau)$, where $\tau \in \mathrm{Sym}(\mu)$. This yields, proceeding as above, transformations of the form $x\breve{\tau} = (x_2 + \lambda x_1)\breve{\tau} = x_2 + \lambda(x_1 \tau)$. In other words, these *diagonal permutations* act with the same permutation at the same time on all the blocks. (Here we regard elements in different blocks to be the same if they have the same x_1 coordinate.) Again, these transformations respect the block system (3.1).

4. Proof of Theorem 1.2

4.1. **2-transitivity.** We begin with showing that $\langle\, \hat{\mathcal{E}} \,\rangle$ acts 2-transitively on G.

Fix a nontrivial, proper subgroup H of G, and consider the setting of Section 3. If $x, x' \in \mathbf{I}_n$ are in different blocks, and $y, y' \in \mathbf{I}_n$ are also in different blocks, there is a composition of blockwise and regular permutations that carries x onto y and x' onto y'. In fact, first use a blockwise permutation to carry x within the block to which y belongs, and x' within the block to which y' belongs. (To avoid complicating notation unnecessarily, we keep the names x and x' for the images of x and x' under this permutation.) Then use regular permutations within the two blocks to carry x onto y and x' onto y'.

If x and x' are in the same block B, and y and y' are in the same block C, first apply a blockwise permutation to carry B onto C, and then use a diagonal permutation (which induces the full symmetric group on each block) to carry x onto y and x' onto y'.

We are left with the case when x and x' are in the same block B, while y and y' are in different blocks. Clearly the transformations of Section 3 are not enough here, as a 2-transitive group is primitive.

Given the above, however, it will be enough to find an element of $\hat{\mathcal{E}}$ that fixes x', and moves x out of B. By applying a blockwise permutation, and a diagonal one, we may assume that $B = B_0$, the zeroth block of α, and $x' = 0$. Suppose thus α is an ETLS with respect to $\{1\} < H < G$, with $\alpha_1(0) = \alpha_2(0) = 1$, so that the coset $H\alpha_2(0)$ is H, and $x'\breve{\alpha} = 0\breve{\alpha} = 1$. Write $x\breve{\alpha} = h \in H$. We also consider another nontrivial, proper subgroup K, and an ETLS β with respect to $\{1\} < K < G$, with $\beta_1(0) = \beta_2(0) = 1$. Let B'_i be the blocks relative to β. We will make more precise choices of H, K and β later, according to the properties of G.

We note first that since G is nontrivial, and it is not cyclic of order a prime or the square of a prime, it has at least two distinct nontrivial, proper subgroups. Moreover, if all the nontrivial, proper subgroups have the same order p, then p is a prime number, and so G is a (non-cyclic) elementary abelian p-group of order p^2.

Accordingly, we distinguish two cases. Suppose first that G has two nontrivial, proper subgroups H and K, with $|H| < |K|$. We have thus $|B'_i| = |K| > |B_0| = |H|$ for all i. If $h \in K$, so that $h\breve{\beta}^{-1} \in B'_0$, we may modify β by a diagonal permutation, so that $0\breve{\beta} = 1$ still holds, but $h\breve{\beta}^{-1} \notin B_0$, as $|B_0| < |B'_0|$. We have thus $0(\breve{\alpha} \circ \breve{\beta}^{-1}) = 0$ and $x(\breve{\alpha} \circ \breve{\beta}^{-1}) \notin B_0$, as requested. If $h \notin K$, so that $h\breve{\beta}^{-1} \in B'_i$, for some $i \neq 0$, we may modify β by a regular permutation on B'_i, so that $h\breve{\beta}^{-1} \notin B_0$, as $|B_0| < |B'_i|$. Here, too, we have $0(\breve{\alpha} \circ \breve{\beta}^{-1}) = 0$ and $x(\breve{\alpha} \circ \breve{\beta}^{-1}) \notin B_0$.

If G is elementary abelian, of order p^2, let H and K be any two nontrivial, proper subgroups. Here we have $B_i = B'_i$ for all i. As $H \cap K = 1$, and $h \neq 1$, we have $h \notin K$, so that $h\breve{\beta}^{-1} \notin B_0$.

We have thus proved $\langle \hat{\mathcal{E}} \rangle$ to be 2-transitive in all cases.

4.2. **Completion of the proof.** Suppose first that the order n of G is even, and let H be a subgroup of G of order 2. With respect to $\{1\} < H < G$, a nontrivial regular permutation on a given block will be a transposition. Since $\langle \hat{\mathcal{E}} \rangle$ is 2-transitive, it follows that $\langle \hat{\mathcal{E}} \rangle$ contains all transpositions, and thus $\langle \hat{\mathcal{E}} \rangle = \mathrm{Sym}(n)$.

Note that in this case, and with this choice of H, the permutations of Section 3 clearly generate the wreath product $\mathrm{Sym}(2) \operatorname{wr} \mathrm{Sym}(n/2)$. This is well-known to be a maximal subgroup of $\mathrm{Sym}(n)$. We have not used this fact here, but our proof of 2-transitivity could be read to mean that $\langle \hat{\mathcal{E}} \rangle$ contains properly this wreath product.

When n is odd, we begin with showing that $\langle \hat{\mathcal{E}} \rangle$ contains a 3-cycle.

Start with a diagonal permutation σ which is the transposition (ab) on each block (see the observation at the end of Section 3). Fix any block B. The regular permutation on the block B induced by a suitable element of H will be a p-cycle of the form $\pi = (abc\dots)$, for some c. Conjugate σ by π to get a permutation $\sigma^\pi = \pi^{-1}\sigma\pi$ which is the transposition (ab) on all blocks, except that on block B it will be $(ab)^{(abc\dots)} = (bc)$. We obtain that the product $\sigma^\pi \cdot \sigma$ is the identity on all blocks, except on block B, where it is the 3-cycle $(bc)(ab) = (abc)$.

We might now appeal to an observation of C. Jordan ([5], [1, Section 5.1, Fact 1]) to the effect that a primitive group that contains a 3-cycle is either the alternating or the symmetric group. We then conclude by observing that $\hat{\mathcal{E}}$ contains an odd permutation, and thus $\hat{\mathcal{E}} = \mathrm{Sym}(n)$. This follows from [9, Theorem 5.4]: a blockwise permutation that exchanges just two blocks will be the product of an odd number p of transpositions.

For completeness, however, we give the short argument (for the case of 2-transitive groups) that shows that $\hat{\mathcal{E}}$ contains all 3-cycles, and thus contains $\mathrm{Alt}(n)$. Let a, b, c be any three distinct elements of $\hat{\mathcal{E}}$. Since $\hat{\mathcal{E}}$ contains a 3-cycle, and it is 2-transitive, there are $d, e \in \mathbf{I}_n \setminus \{ a, b, c \}$ such that $(bad), (bce) \in \hat{\mathcal{E}}$. If $d = e$, then $(bcd)(bad)^{-1} = (abc) \in \hat{\mathcal{E}}$. If $d \neq e$, then $(bad)^{(bce)} = (cad) \in \hat{\mathcal{E}}$, and we argue as in the previous case.

4.3. **A remark on the choice of α.** Concerning the definition of $\hat{\mathcal{E}} = \hat{\mathcal{E}}_\alpha$ given in (2.3), we may note that all the transformations $\breve{\alpha} \circ \breve{\beta}^{-1}$, that we have considered in this Section and the previous one, can be taken with respect to a fixed ETLS α, chosen once and for all with respect to $\{ 1 \} < H < G$, where the choice of H depends on the properties of the group, as we have just seen, and we take (just for simplicity) $\alpha_1(0) = \alpha_2(0) = 1$.

5. The case of the cyclic group of order p^2

If $G = \langle a \rangle$ is a cyclic group of order p^2, where p is a prime, the second part of the argument of Subsection 4.1 does not work, as G has a unique nontrivial, proper subgroup $H = \langle a^p \rangle$. In fact, since $\hat{\mathcal{E}}$ consists of the (imprimitive) permutations of Section 3, $\langle \hat{\mathcal{E}} \rangle$ is not 2-transitive here.

In this case we have the following

Proposition 5.1. *Let G be a cyclic group of order p^2, where p is a prime. Then:*

(1) *the group $\langle \hat{\mathcal{E}} \rangle$ is a proper, imprimitive subgroup of* $\mathrm{Sym}(p^2)$*;*
(2) *given an* ETLS *α, there exists a logarithmic signature γ such that*

$$\langle \hat{\mathcal{E}} \cup \{ \breve{\alpha} \circ \breve{\gamma}^{-1} \} \rangle = \mathrm{Sym}(p^2).$$

(The ETLS α is taken with respect to the only possible choice $\{ 1 \} < H < G$.) We refer to [8] for the general definition of *logarithmic signatures*. (These are called *group bases* in [4, 3].) In the special case of the cyclic group G of order p^2 we are considering here, a logarithmic signature is a pair of (injective) maps $\gamma_1, \gamma_2 : \mathbf{I}_p \to G$, so that each element of G can be written (uniquely) as $\gamma_1(x_1) \cdot \gamma_2(x_2)$, for $x_1, x_2 \in \mathbf{I}_p$. As in the case of an ETLS, we obtain a bijection $\breve{\gamma} : \mathbf{I}_{p^2} \to G$ as $(x_2 + px_1)\breve{\gamma} = \gamma_1(x_1) \cdot \gamma_2(x_2)$.

We choose $\alpha_1(x_1) = a^{px_1}$ and $\alpha_1(x_2) = a^{x_2}$, so that $x\breve{\alpha} = a^x$. Here B_0 is the set of multiples of p in $\mathbf{I}_{p^2}$. Then we take the logarithmic signature γ defined by $\gamma_1(x_1) = a^{x_1}$ and $\gamma_1(x_2) = a^{px_2}$. One sees that $0(\breve{\alpha} \circ \breve{\gamma}^{-1}) = 0$, and $p(\breve{\alpha} \circ \breve{\gamma}^{-1}) = 1$, so that $\breve{\alpha} \circ \breve{\gamma}^{-1}$ fixes 0, and takes $p \in B_0$ to an element $1 \notin B_0$, as requested.

This yields that the group $\langle\, \hat{\mathcal{E}} \cup \{\, \breve{\alpha} \circ \breve{\gamma}^{-1} \,\}\,\rangle$ is 2-transitive; the rest of the proof follows as in Section 4.

References

1. Peter J. Cameron, *Permutation groups*, London Mathematical Society Student Texts, vol. 45, Cambridge University Press, Cambridge, 1999. MR **2001c:**20008
2. K. W. Campbell and M. J. Wiener, *DES is not a group*, Advances in Cryptology - Crypto '92 (Santa Barbara, 1992) (Heidelberg) (E.F. Brickell, ed.), Lecture Notes in Computer Science, vol. 740, Springer, 1993, pp. 512–520.
3. Valér Čanda, Tran van Trung, Spyros Magliveras, and Tamás Horváth, *Symmetric block ciphers based on group bases*, Selected areas in cryptography (Waterloo, ON, 2000) (Doug Stinson and Stafford Tavares, eds.), Lecture Notes in Comput. Sci., vol. 2012, Springer, Berlin, 2001, pp. 89–105. MR 1 895 584
4. Tamás Horváth, *Das TST-kryptosystem*, Ph.D. thesis, Fachbereich Maschinentechnik der Universität GH Essen, December 1998.
5. C. Jordan, *Théorèmes sur les groupes primitifs*, J. Math. Pures Appl. (1871), 383–408.
6. Burton S. Kaliski, Jr., Ronald L. Rivest, and Alan T. Sherman, *Is the data encryption standard a group? (Results of cycling experiments on DES)*, J. Cryptology **1** (1988), no. 1, 3–36. MR **89f:**94017
7. S. S. Magliveras, *A cryptosystem from logarithmic signatures of finite groups*, Proceedings of the 29th Midwest Symposium on Circuits and Systems (Mohammed Ismail, ed.), Elsevier Science Ltd, 1986, pp. 972–975.
8. S. S. Magliveras, D. R. Stinson, and Tran van Trung, *New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups*, J. Cryptology **15** (2002), no. 4, 285–297. MR 1 944 653
9. Spyros S. Magliveras and Nasir D. Memon, *Algebraic properties of cryptosystem PGM*, J. Cryptology **5** (1992), no. 3, 167–183. MR **93h:**94017
10. Derek J. S. Robinson, *A course in the theory of groups*, second ed., Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996. MR **96f:**20001
11. Ralph Wernsdorf, *The one-round functions of the DES generate the alternating group*, Advances in cryptology—EUROCRYPT '92 (Balatonfüred, 1992), Lecture Notes in Comput. Sci., vol. 658, Springer, Berlin, 1993, pp. 99–112. MR **94g:**94031
12. Ralph Wernsdorf, *The round functions of RIJNDAEL generate the alternating group*, Proceedings of the 9th International Workshop on Fast Software Encryption, Lecture Notes in Computer Science, vol. 2365, Springer-Verlag, Heidelberg, 2002, FSE2002, Leuven, Belgium, February 2002, pp. 143–148.

(A. Caranti) Dipartimento di Matematica, Università degli Studi di Trento, via Sommarive 14, I-38050 Povo (Trento), Italy

E-mail address: `caranti@science.unitn.it`

URL: `http://www-math.science.unitn.it/~caranti/`

(F. Dalla Volta) Dipartimento di Matematica e Applicazioni, Edificio U7, Università degli Studi di Milano–Bicocca, via Bicocca degli Arcimboldi 8, I-20126 Milano, Italy

E-mail address: `dallavolta@matapp.unimib.it`

URL: `http://www.matapp.unimib.it/~dallavolta/`