J. Cryptology (1992) 5: 167–183

Journal of Cryptology

Algebraic Properties of Cryptosystem PGM

Spyros S. Magliveras* and Nasir D. Memon
Department of Computer Science and Engineering, University of Nebraska–Lincoln, Lincoln, NE 68588-0115, U.S.A

Communicated by Ernest F. Brickell

Received 30 March 1989 and revised 9 June 1991

Abstract. In the late 1970s Magliveras invented a private-key cryptographic system called *Permutation Group Mappings* (PGM). PGM is based on the prolific existence of certain kinds of factorization sets, called *logarithmic signatures*, for finite permutation groups. PGM is an endomorphic system with message space $\mathbb{Z}_{|G|}$ for a given finite permutation group G. In this paper we prove several algebraic properties of PGM. We show that the set of PGM transformations $\mathcal{T}_G$ is not closed under functional composition and hence not a group. This set is 2-transitive on $\mathbb{Z}_{|G|}$ if the underlying group G is not hamiltonian and not abelian. Moreover, if the order of G is not a power of 2, then the set of transformations contains an odd permutation. An important consequence of these results is that the group generated by the set of transformations is nearly always the symmetric group $\mathcal{S}_{|G|}$. Thus, allowing multiple encryption, any permutation of the message space is attainable. This property is one of the strongest security conditions that can be offered by a private-key encryption system.

Key words. Cryptography, Cryptology, Finite permutation group, Permutation group mappings (PGM), Multiple encryption, Logarithmic signatures.

1. Introduction

Permutation Group Mappings (PGM) is a private-key cryptosystem invented by Magliveras in the late 1970s. The cryptosystem is based on a space-efficient data structure for permutation groups called a *logarithmic signature*. In our earlier papers [9], [13], [10] we described the relationship of logarithmic signatures to the pioneering work of Sims [17] and to that of other researchers. Various statistical tests have been conducted which show that PGM is statistically robust [11]–[13]. Preliminary software implementations of PGM variants show that the system is fast (well over 6 Mbits/s on a SUN Sparcstation 2) [14]. Since composition of two

* S. S. Magliveras was supported in part by NSF/NSA Grant Number MDA904-82-H0001, by U.S. West Communications, and by the Center for Communication and Information Science of the University of Nebraska.

permutations can be done in one machine cycle on a specially designed fine-grain parallel machine, PGM is intrinsically fast. The system is suitable for parallel implementation both in software and hardware.

This paper investigates the algebraic structure of the transformations induced by PGM. We show that the set of PGM transformations is not closed under functional composition and hence not a group. The above property implies that multiple encryption strengthens the system. We also show that the set generated by these transformations is almost always the full symmetric group. This implies that, assuming multiple encryption, a given sequence of k distinct ciphertexts can arise from any sequence of k distinct plaintexts, by an appropriate PGM multiple encryption. Thus, the cryptanalyst gets no information about the sequence of k distinct plaintexts which actually produce the corresponding sequence of k distinct ciphertexts. The afformentioned property is a strong security condition.

In Section 3 we give a classification of logarithmic signatures and show their existence. In Section 4 we describe the PGM cryptosystem. An example illustrating the basic system is provided. In Section 5 we identify various transformations that can be performed on a logarithmic signature to yield a different logarithmic signature. We describe some of these transformations by means of appropriate group actions. We define *equivalence* among logarithmic signatures and show that the number of inequivalent logarithmic signatures for a moderate-sized permutation group is astronomical. Since, in PGM, pairs of logarithmic signatures serve as keys, it follows that the key space of PGM is large. In Section 6 we briefly discuss the security of PGM under a chosen-plaintext attack. We then proceed to derive the main result of the paper that the set of PGM transformations generates the symmetric group on the message space.

2. Preliminaries

In this section we introduce some notation and terminology used in later sections. We assume that the reader is familiar with the elementary concepts of group theory. For a proper introduction to the theory of groups and finite permutation groups the reader is referred to [5] and [18]. Here we introduce some of the notation and concepts relevant to this paper.

Let $\mathscr{S}_X$ be the symmetric group on a set X, If $X = \{1, \ldots, n\}$ we write $\mathscr{S}_n$ for $\mathscr{S}_X$. A *permutation group* is a pair (X, G) where X is a finite set and G is a subgroup of $\mathscr{S}_X$. Moreover, (X, G) is said to have *degree* $|X|$. A *group action* is a triple (X, G, π) where X is a set, G is a group, and π is a mapping $\pi: X \times G \to X$, where $\pi(x, g)$ is denoted by x^g and subject to the following two conditions:

1. $(x^g)^h = x^{gh}$ for all $x \in X$ and for all $g, h \in G$.
2. $x^1 = x$ for all $x \in X$.

To simplify notation we denote a group action (X, G, π) by $G|X$. A group action $G|X$ induces an equivalence relation $\sim$ on X as follows: for $x, y \in X$, $x \sim y$ if and only if $x^g = y$ for some $g \in G$. The $\sim$ equivalence classes are called the *G-orbits* of X. If $y \in Y \subseteq X$ and $H \subseteq G$, then $y^H = \{y^h | h \in H\}$ and $Y^H = \{y^h | y \in Y \text{ and } h \in H\}$.

It is easily seen that the G-orbit of X containing y is the set y^G. If $G|X$ is a group action, then $Y \subseteq X$ is called a *fixed block* of G if and only if $Y^G = Y$. Similarly, any $x \in X$ is called a *fixed point* of G if and only if $x^G = x$. For any $x \in X$, the set $G_x = \{g \in G | x^g = x\}$ is called the *stabilizer of* x *in* G. It is easy to show that G_x is a subgroup of G. A permutation group (X, G) is called *transitive* if there is just one orbit in the action of G on X. A permutation group (X, G) is called *k-transitive* $(k \geq 1)$ if, given any two ordered k-tuples $(x_1, \ldots, x_k), (y_1, \ldots, y_k)$ of distinct elements of X, there is some g in G such that $x_i^g = y_i$ for all i such that $1 \leq i \leq k$. A nonabelian group G is said to be *hamiltonian* if every subgroup of G is normal.

A *cryptosystem* is an ordered four-tuple $\Pi = (\mathscr{M}, \mathscr{K}, \mathscr{C}, \mathscr{T})$. where $\mathscr{M}$, $\mathscr{K}$, and $\mathscr{C}$ are finite sets called the *message space*, the *key space*, and *ciphertext space*, respectively, and $\mathscr{T}$ is a family of transformations $\{E_k\}_{k \in \mathscr{K}}$ mapping $\mathscr{M}$ to $\mathscr{C}$ such that, for each $k \in \mathscr{K}$, E_k is invertible. We denote the inverse of E_k by D_k. Implicit in a cryptosystem $(\mathscr{M}, \mathscr{K}, \mathscr{C}, \mathscr{T})$ is the mapping $E: k \to E_k$ that associates to each key $k \in \mathscr{K}$ the transformation E_k induced by k. The cryptosystem is said to be *faithful* if E is injective.

If the message space and ciphertext space are the same, then the cryptosystem is called *endomorphic*, and in this case, for every key k, $E_k: \mathscr{M} \to \mathscr{C}$ is a permutation on $\mathscr{M}$. An endomorphic cryptosystem Π is said to be *closed* if and only if $\mathscr{T}$ is closed under functional composition. In other words, Π is *closed*[1] if and only if, for every two keys $i, j \in \mathscr{K}$, there exists a key $k \in \mathscr{K}$ such that $E_i E_j = E_k$. Since $\mathscr{T}$ forms a finite cancellation semigroup under composition, it follows that Π is closed if and only if $\mathscr{T}$ forms a group under composition. Let $\mathscr{G}_\Pi = \langle \mathscr{T} \rangle$ be the group generated by $\mathscr{T}$, then $\mathscr{G}_\Pi$ is a subgroup of $\mathscr{S}_\mathscr{M}$.

Although the terminology that follows is not standard, it is natural and extends the terminology used in [7]. For a positive integer t, a cryptosystem Π is said to be *t-transitive* if given any ordered t-tuple of distinct messages $(m_1, \ldots, m_t) \in \mathscr{M}^t$ and any ordered t-tuple of distinct ciphertexts $(c_1, \ldots, c_t) \in \mathscr{C}^t$, there is some $k \in \mathscr{K}$ such that $E_k(m_i) = c_i$ for all i such that $1 \leq i \leq t$. Here we also write $E_k(m_1, \ldots, m_t) = (c_1, \ldots, c_t)$. Note that we speak of a t-transitive system whether or not $\mathscr{T}$ is a group. It is clear that a t-transitive system is $(t-1)$-transitive.

3. Logarithmic Signatures

Let G be a finite permutation group of degree n. A *logarithmic signature* for G is an ordered collection $\alpha = \{B_i: i = 1, \ldots, s\}$ of ordered sets $B_i = \{u(i, 1), \ldots, u(i, r_i)\}$, such that:

1. $u(i, j) \in \mathscr{S}_n$ for all $1 \leq j \leq r_i$ and $1 \leq i \leq s$.
2. Each element g of G can be expressed uniquely as a product of the form

$$g = q_s \cdot q_{s-1} \cdots q_2 \cdot q_1 \tag{1}$$

for some $q_i \in B_i$.

[1] We wish to remark that the term *closed* had been used by Shannon [15] to mean something different. Our usage follows the terminology of Kaliski *et al.* [7].

Intuitively, we view a logarithmic signature for a group G as a kind of basis for G, in the sense that each group element has a unique representation as described above. Each such "basis" induces a total order on G, and therefore a bijection from $\mathbb{Z}_{|G|}$ onto G.

Note that the elements q_i in (1) are not necessarily elements of G, but could belong to a much larger group in which G is embedded. The B_i are called the *blocks* of α and the vector of block lengths $\mathbf{r} = (r_1, \ldots, r_s)$ is called the *type* of α. We define the *length* of a logarithmic signature α to be the number $\sum_{i=1}^{s} r_i$. The logarithmic signature is called *nontrivial* if $s \geq 2$ and $r_i \geq 2$ for $1 \leq i \leq s$; otherwise it is called *trivial*. A logarithmic signature is called *tame* if the factorization in (1) can be achieved in time polynomial in the degree n of G; it is called *supertame* if the factorization can be achieved in time $O(n^2)$. A logarithmic signature is called *wild* if it is not tame. We denote by Λ the collection of all logarithmic signatures of G.

Let $\gamma: G = G_0 > G_1 > \cdots > G_s = 1$ be a chain of subgroups of G, and let $\{B_i: i = 1, \ldots, s\}$ be an ordered collection of subsets of G, where each $B_i = \{u(i, j): j = 1, \ldots, r_i\}$ is a complete set of right coset representatives of G_i in G_{i-1}. It can be seen that $\{B_i\}_i$ forms a logarithmic signature for G. Such a logarithmic signature is called a *transversal* with respect to γ. Here the type $\mathbf{r} = (r_1, \ldots, r_s)$ has $r_i = [G_i : G_{i-1}]$. In view of the fact that membership in a permutation group can be tested in time polynomial in the degree and the number of generators [3], a transversal logarithmic signature α of length polynomial in n is tame. We denote the set of all transversal logarithmic signatures of G with respect to a chain γ by $\Lambda(\gamma)$. In Section 5 we indicate how $\Lambda(\gamma)$ is a single regular orbit under the action of a certain monomial group. Existence of supertame logarithmic signatures is established in the following lemma.

Lemma 3.1. *If G is a permutation group, then there exists a supertame logarithmic signature for G.*

Proof. Suppose G acts on the letters of $X = \{1, 2, \ldots, n\}$. Let $G = G_0 > G_1 > \cdots > G_s = 1$ be a chain of nested stabilizers in G. Thus, $G_0 = G$ and, for any $i \geq 1$, G_i fixes pointwise the letters $1, 2, \ldots, i$ of X. Suppose now that the orbit of $i \in X$ under G_{i-1} is $B = \{\delta_1 = i, \delta_2, \ldots, \delta_{r_i}\}$ and that $u(i, j) \in G_{i-1}$ moves δ_1 to δ_j, then $G_{i-1} = G_i u(i, 1) + G_i u(i, 2) + \cdots + G_i u(i, r_i)$. Consider the logarithmic signature

$$\alpha = [u(1, 1), \ldots, u(1, r_1); u(2, 1), \ldots, u(2, r_2); \ldots; u(s, 1), \ldots, u(s, r_s)].$$

Now, note that an element h in G_{i-1} belongs to the coset $G_i u(i, j)$ if and only if h moves $\delta_1 = i$ to δ_j. Thus determining the right G_i coset in G_{i-1} to which h belongs can be done in $O(1)$ operations. Now, the element $h \cdot u(i, j)^{-1}$ fixes $1, 2, \ldots, i-1, i$ and therefore belongs to G_i. Computing $h \cdot u(i, j)^{-1}$ can be done in $O(n)$ operations. Recursively, given any element $g \in G$, we descend in at most n steps and have $g \cdot u(1, j_1)^{-1} \cdot u(2, j_2)^{-1} \cdots u(s, j_s)^{-1} = 1$. Inverting yields the unique factorization $g = u(s, j_s) \cdots u(2, j_2) \cdot u(1, j_1)$. □

For the rest of the paper it is more convenient to write $\{u(i, j): 0 \leq j \leq r_i - 1; 1 \leq i \leq s\}$ rather than $\{u(i, j): 1 \leq j \leq r_i; 1 \leq i \leq s\}$ for a logarithmic signature of

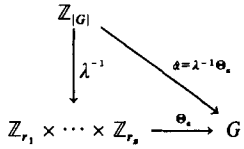

Fig. 1. Definition of mapping $\hat{\alpha}$.

a group. Before we describe PGM we introduce some notation. By $\alpha[i; j]$ we mean the jth element of the ith block of α. Also, if $\mathbf{r} = (r_1, \ldots, r_s)$ and $(p_1, \ldots, p_s) \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$, then $\alpha(p_1, \ldots, p_s) = \alpha[s; p_s] \cdots \alpha[2; p_2]\alpha[1; p_1]$.

We now define the bijection induced by a logarithmic $\alpha \in \Lambda$ in a precise manner. If $\mathbf{r} = (r_1, \ldots, r_s)$ is the type of a logarithmic signature α, define the integers m_i, $i = 1, 2, \ldots, s$, by

$$m_1 = 1, \qquad m_i = \prod_{j=1}^{i-1} r_j, \qquad i = 2, \ldots, s. \tag{2}$$

Let λ be the bijection from $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$ onto $\mathbb{Z}_{|G|}$, defined by

$$\lambda(p_1, \ldots, p_s) = \sum_{i=1}^{s} p_i m_i \qquad \text{for any} \quad p_i \in \mathbb{Z}_{r_i}. \tag{3}$$

For any $x \in \mathbb{Z}_{|G|}$, $\lambda^{-1}(x)$ is efficiently computable by successive subtractions (representation of x with respect to mixed base $(r_1, \ldots, r_s)$). For a group G and a logarithmic signature $\alpha = \{\alpha[i; j]: j = 0, \ldots, r_i - 1; i = 1, \ldots, s\}$ define the bijection $\Theta_\alpha: \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s} \to G$ by

$$\Theta_\alpha(p_1, \ldots, p_s) = \alpha(p_1, p_2, \ldots, p_s). \tag{4}$$

Next, for any $\alpha \in \Lambda$, define a map $\hat{\alpha}: \mathbb{Z}_{|G|} \to G$ by composing λ^{-1} with Θ_α, thus $\hat{\alpha} = \lambda^{-1}\Theta_\alpha$. We illustrate the definition of $\hat{\alpha}$ in Fig. 1. The function $\hat{\alpha}$ is always efficiently computable, but $\hat{\alpha}^{-1}$ is not unless α is tame. We denote by $\hat{\Lambda}$ the collection $\{\hat{\alpha}: \alpha \in \Lambda\}$.

4. Cryptosystem PGM

Having defined the mappings $\hat{\alpha}$, for $\alpha \in \Lambda$, the basic cryptographic system PGM is defined as follows: for a given pair of logarithmic signatures, α, β with β tame, the encryption transformation $E_{\alpha,\beta}: \mathbb{Z}_{|G|} \to \mathbb{Z}_{|G|}$ is the mapping

$$E_{\alpha,\beta} = \hat{\alpha} \cdot \hat{\beta}^{-1}. \tag{5}$$

The corresponding decryption transformation is obtained by reversing the order of the pair of logarithmic signatures, that is

$$D_{\alpha,\beta} = E_{\alpha,\beta}^{-1} = E_{\beta,\alpha} = \hat{\beta} \cdot \hat{\alpha}^{-1}. \tag{6}$$

In the case of PGM we see that the message space and the cipher space is $\mathbb{Z}_{|G|}$ where G is the underlying group, hence PGM is endomorphic. The key space is $\Lambda \times \Lambda$, the collection of all ordered pairs of logarithmic signatures of G. We denote

by $\mathscr{T}_G$ the set of transformations defined by the key space and by $\mathscr{G}_G$ the group generated by $\mathscr{T}_G$ under functional composition.

To clarify the ideas presented above, we illustrate PGM by means of an example. The group used here is the alternating group on five points, $\mathscr{A}_5$, of order 60. This implies that the message space $\mathscr{M}$ and the ciphertext space $\mathscr{C}$ are the set $\{0, 1, \ldots, 59\}$. A supertame logarithmic signature α, with respect to a chain of stabilizer subgroups is obtained by Knuth's algorithm [8] using the generators (1 2 3 4 5) and (1 2 3)(4)(5). Another supertame logarithmic signature β is obtained by applying the procedure *shuffle* to α. The blocks of α consist of right coset representatives in a chain of subgroups in G. Procedure shuffle consists of changing the coset representatives and their relative order within each block. We say more about shuffle in the next section. The number of blocks is $s = 3$, and the vector of block lengths is $\mathbf{r} = (5, 4, 3)$. The integers m_i are computed to be 1, 5, and 20, respectively. The two logarithmic signatures, along with the appropriate knapsack $\mathbf{v}$ needed to compute λ and λ^{-1} efficiently, are shown in Table 1.

Although it is simpler to illustrate PGM by means of this example, we wish to warn the reader that whenever the logarithmic signatures α and β are transversals with respect to the same chain of subgroups, some unwelcome regularities arise. We wish to thank one of the referees for pointing out that in such a case we have, for $x, y \in \mathscr{M}$, $x \equiv y \pmod{m_i}$ if and only if $E_{\alpha,\beta}(x) \equiv E_{\alpha,\beta}(y) \pmod{m_i}$. In actual practice we avoid this problem by selecting α and β to be of different types.

Let us now demonstrate the operation of enciphering. If, for example, the message is 49, then it can be decomposed uniquely with respect to $\mathbf{v}$ as $49 = 4 + 5 + 40$. This process determines the vector of row-indices $\lambda^{-1}(49) = (4, 1, 2)$. We next compute $\pi = \Theta_\alpha(4, 1, 2) = \alpha[3; 2] \cdot \alpha[2; 1] \cdot \alpha[1; 4] = (1\ 5\ 4)(2)(3)$. We then compute $\Theta_\beta^{-1}(\pi)$, the representation of π with respect to β. Since β is supertame and $\pi(1) = 5$, we locate the element in block 1 of β that sends 1 to 5. This element is $\beta[1; 4]$. So $\pi = h_1 \cdot \beta[1; 4]$ for some $h_1 \in G_1$. Solving for h_1 yields $h_1 = \pi \cdot \beta[1; 4]^{-1} =$

Table 1. The two logarithmic signatures and the knapsack.

α	$\mathbf{v}$	β
(1)(2)(3)(4)(5)	0	(1 4 2 3 5)
(1 2 3 4 5)	1	(1)(2)(3 5 4)
(1 3 5 2 4)	2	(1 2 5 4 3)
(1 4 2 5 3)	3	(1 3)(2 4)(5)
(1 5 4 3 2)	4	(1 5 3 4 2)
(1)(2)(3)(4)(5)	0	(1)(2 3)(4 5)
(1)(2 3)(4 5)	5	(1)(2 5 3)(4)
(1)(2 4 3)(5)	10	(1)(2 4 3)(5)
(1)(2 5 3)(4)	15	(1)(2)(3)(4)(5)
(1)(2)(3)(4)(5)	0	(1)(2)(3)(4)(5)
(1)(2)(3 4 5)	20	(1)(2)(3 5 4)
(1)(2)(3 5 4)	40	(1)(2)(3 4 5)

(1)(2 4)(3 5). Now h_1 fixes 1 and sends 2 to 4. Again, we locate the element of the second block of β which sends 2 to 4, namely $\beta[2; 2]$. Hence,$h_1 = h_2 \cdot \beta[2; 2]$, which yields $h_2 = (1)(2)(3\ 5\ 4)$. Continuing in this manner we completely factor π with respect to β and get $\pi = \beta[3; 1] \cdot \beta[2; 2] \cdot \beta[1; 4]$. This determines the vector of row pointers for β to be $(4, 2, 1) \in \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_3$ and $\lambda(4, 2, 1)$ is $4 + 10 + 20 = 34$. Thus, we have $E_{\alpha,\beta}(49) = 34$. The reader can easily verify that $D_{\alpha,\beta}(34) = E_{\beta,\alpha}(34) = 49$.

5. Transformations on Logarithmic Signatures

In this section we define and study transformations on the family of logarithmic signatures of a given group G. In particular, by applying these transformations we are able to generate new logarithmic signatures from a given one, and establish lower bounds on the total number of logarithmic signatures for G. Moreover, we characterize equivalence among logarithmic signatures in terms of certain transformations. Finally we deal with some questions about properties of logarithmic signatures that are preserved by these transformations.

Suppose that $\beta = \{B_i: i = 1, \ldots, s\}$ is a transversal logarithmic signature of a group G with respect to the chain of subgroups $\gamma : G = G_0 > G_1 \cdots > G_s = 1$. Note that while $\beta = \{B_i: i = 1, \ldots, s\}$ is a logarithmic signature for $G = G_0$, the set of blocks $\beta(k) = \{B_{k+1}, \ldots, B_s\}$ is a logarithmic signature for G_k. If the element $u(i, j) \in B_i$ of $\beta(k)$ is replaced by $h \cdot u(i, j)$, where $h \in G_i$, the resulting collection $\beta(k)^*$ forms a new logarithmic signature for G_k. Moreover, any rearrangement of the elements of a block $B_i \in \beta(k)$ yields a new logarithmic signature for G_k. Procedure *shuffle* consists of applying the operations described above to a logarithmic signature.

Procedure *shuffle* for generating new logarithmic signatures from a given one can be concisely described by considering a certain group action. If $\beta = \{B_i: i = 1, \ldots, s\}$, $B_i = \{u(i, j): j = 0, \ldots, r_i - 1\}$, is a transversal logarithmic signature of G with respect to the chain $\gamma : G = G_0 > G_1 > \cdots > G_s = 1$ of subgroups, let $\mathbf{M}$ be the group of all matrices of the form

$$M = \begin{bmatrix} H_1 & 0 & \cdots & 0 \\ 0 & H_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & H_s \end{bmatrix},$$

where H_i is an $r_i \times r_i$ monomial matrix with entries in G_i. Thus, H_i can be thought of as an $r_i \times r_i$ permutation matrix whose unity entries have been replaced by arbitrary elements of G_i. The procedure shuffle described above for obtaining new logarithmic signatures of G corresponds to acting on

$$(u(1, 0), \ldots, u(1, r_1 - 1); \ldots; u(s, 0), \ldots, u(s, r_s - 1)) \tag{7}$$

on the left by some $M \in \mathbf{M}$, that is,

$$(v(1, 0), \ldots, v(s, r_s))^T = M \cdot (u(1, 0), \ldots, u(s, r_s))^T. \tag{8}$$

Thus, the totality $\Lambda(\gamma)$ of logarithmic signatures with respect to γ is an **M**-orbit. We observe that since only the identity of **M** fixes a logarithmic signature in $\Lambda(\gamma)$, **M** acts regularly on $\Lambda(\gamma)$. This implies that

$$|\Lambda(\gamma)| = |\mathbf{M}| = \prod_{i=1}^{s} |G_i|^{r_i} r_i! = \prod_{i=1}^{s} \left(\prod_{j=i+1}^{s} r_j \right)^{r_i} r_i! \tag{9}$$

Now we define another group action on Λ. Let

$$\mathbf{T} = G \times \mathscr{S}_n \times \mathscr{S}_n \times \cdots \times \mathscr{S}_n \times G \tag{10}$$

be a direct product, where n is the degree of G and the symmetric group $\mathscr{S}_n$ occurs $s-1$ times. For $q = (g_0, g_1, \ldots, g_s) \in \mathbf{T}$ and

$$\alpha = (\alpha[1;0], \ldots, \alpha[1; r_1 - 1]; \ldots; \alpha[s;0], \ldots, \alpha[s; r_s - 1]) \in \Lambda. \tag{11}$$

Let q act on α by $(q, \alpha) \to \alpha^q$, where

$$\alpha^q = (g_1^{-1}, \ldots, g_1^{-1}; \ldots; g_s^{-1}, \ldots, g_s^{-1}) \cdot \alpha \cdot (g_0, \ldots, g_0; \ldots; g_{s-1}, \ldots, g_{s-1}). \tag{12}$$

This means that all the elements of the first block are multiplied by g_1^{-1} on the left and by g_0 on the right. The elements of the second block are multiplied by g_2^{-1} on the left and by g_1 on the right, and so on. Finally, the elements in block s are multiplied by g_s^{-1} on the left and by g_{s-1} on the right. It is seen that $\alpha^1 = \alpha$ and $(\alpha^q)^t = \alpha^{qt}$; hence **T** acts on the collection of logarithmic signatures in Λ having s blocks. If $g_0 = g_s = 1$, we say that α^q is a *sandwich* of α. If $g_1 = g_2 = \cdots = g_s = 1$, then we effectively multiply only the elements of the first block on the right by g_0. We call this transformation a *right translation* of α. On the other hand, if $g_0 = g_1 = \cdots = g_{s-1} = 1$, then we call the transformed logarithmic signature a *left translate* of α. Let **S** be the subgroup of **T** that consists of the elements of the form $(1, g_1, \ldots, g_{s-1}, 1)$ of **T**, and let **H** be the subgroup of **S** that consists of all elements $(1, g_1, \ldots, g_{s-1}, 1)$ with $g_i \in G_i$.

Suppose that α is a logarithmic signature for a group G of type $\mathbf{r} = (r_1, \ldots, r_i, r_{i+1}, \ldots, r_s)$. We can create a new logarithmic signature β by *fusing* two consecutive blocks of α, say B_i and B_{i+1} of lengths r_i and r_{i+1} to a single block of length $r_i \cdot r_{i+1}$. Thus, if $g = q_s \ldots q_{i+1} \cdot q_i \ldots q_2 \cdot q_1$ is the factorization of g with respect to α, then the factorization of g with respect to β will be $g = q_s \ldots q_{i+2} \cdot t \cdot q_{i-1} \ldots q_2 \cdot q_1$, where $t = q_{i+1} \cdot q_i$. In this case we say that α is a *refinement* of β. The refinement relation defines a partial order on Λ and we write $\alpha < \beta$ to denote that α is a refinement of β.

Finally, observe that if $g = q_s \cdot q_{s-1} \ldots q_2 \cdot q_1$, then we have $g^{-1} = q_1^{-1} \cdot q_2^{-1} \ldots q_s^{-1}$. This implies that if

$$\alpha = \{\alpha[i;j] : j = 0, \ldots, r_i - 1; i = 1, \ldots, s\} \tag{13}$$

is a logarithmic signature, then

$$\alpha' = \{\alpha[i;j]^{-1} : j = 0, \ldots, r_i - 1; i = s, \ldots, 1\} \tag{14}$$

is also a logarithmic signature. We call α' the *inversion* of α. Inversion induces a duality on Λ. For example, a system of right coset representatives in a chain γ of subgroups (*right transversal* logarithmic signature), is transformed into a system of

left coset representatives (*left transversal* logarithmic signature). In this paper we do not study properties of inversion.

Definition 5.1. Two logarithmic signatures α, β of a group G are said to be *equivalent* if and only if $\hat{\alpha} = \hat{\beta}$.

We denote the equivalence of two logarithmic signatures α and β by $\alpha \sim \beta$. If α, β, and γ are logarithmic signatures of a group G, then it follows from the definition that $E_{\alpha,\gamma} = E_{\beta,\gamma}$ if and only if $\alpha \sim \beta$. Also, we see that if α is a refinement of β, then $\alpha \sim \beta$. Hence if two logarithmic signatures are equivalent, then they need not have the same type. The concept of equivalence is very important from a cryptanalytic point of view. For a cryptanalyst to break PGM, he only needs to construct logarithmic signatures that are equivalent to the ones specified by the key. The following result was shown by Magliveras and Kreher, but its proof has not appeared in print. The theorem establishes necessary and sufficient conditions for equivalence of two logarithmic signatures of the same type in terms of sandwich transformations. Since sandwiching produces equivalent logarithmic signatures we see that PGM is not faithful.

Theorem 5.1. *Let α and β be two logarithmic signatures of a group G, such that they have the same type $\mathbf{r} = (r_1, \ldots, r_s)$. Then α and β are equivalent if and only if they are in the same sandwich* S*-orbit.*

Proof. If α and β are in the same sandwich S-orbit, then they are equivalent. For the converse, let $\alpha = \{B_1, B_2, \ldots, B_s\}$ and $\beta = \{B'_1, B'_2, \ldots, B'_s\}$, where $B_i = \{u_{i,0}, u_{i,1}, \ldots, u_{i,r_i-1}\}$ and $B'_i = \{u'_{i,0}, u'_{i,1}, \ldots, u'_{i,r_i-1}\}$. Now since $\alpha \sim \beta$, we have

$$\alpha(j_1, \ldots, j_s) = \beta(j_1, \ldots, j_s), \qquad 0 \le j_i \le r_i - 1. \tag{15}$$

Specifically, we have $\alpha(0, 0, \ldots, 0, j) = \beta(0, 0, \ldots, 0, j)$ for $0 \le j \le r_s - 1$. That is, $u_{s,j} \cdot u_{s-1,0} \cdots u_{1,0} = u'_{s,j} \cdot u'_{s-1,0} \cdots u'_{1,0}$. Let $t_{s-1} = u'_{s-1,0} \cdots u'_{1,0} \cdot u_{1,0}^{-1} \cdots u_{s-1,0}^{-1}$, then, $u_{s,j} = u'_{s,j} \cdot t_{s-1}$, and consequently $B_s = B'_s \cdot t_{s-1}$. In particular, note that

$$u_{s,0}^{-1} \cdot u'_{s,0} = t_{s-1}^{-1}. \tag{16}$$

Next, from (15) we have $\alpha(0, 0, \ldots, 0, j, 0) = \beta(0, 0, \ldots, 0, j, 0)$ for $0 \le j \le r_{s-1} - 1$. This means that $u_{s,0} \cdot u_{s-1,j} \cdot u_{s-2,0} \cdots u_{1,0} = u'_{s,0} \cdot u'_{s-1,j} \cdot u'_{s-2,0} \cdots u'_{1,0}$. Therefore, $u_{s,0} \cdot u_{s-1,j} = u'_{s,0} \cdot u'_{s-1,j} \cdot (u'_{s-2,0} \cdots u'_{1,0} \cdot u_{1,0}^{-1} \cdots u_{s-2,0}^{-1})$. Letting $t_{s-2} = u'_{s-2,0} \cdots u'_{1,0} \cdot u_{1,0}^{-1} \cdots u_{s-2,0}^{-1}$ and using (16) we get $u_{s-1,j} = t_{s-1}^{-1} \cdot u'_{s-1,j} \cdot t_{s-2}$. Hence $B_{s-1} = t_{s-1}^{-1} \cdot B'_{s-1} \cdot t_{s-2}$. Continuing in this manner we get $\alpha = (t_1^{-1}, \ldots, t_{s-1}^{-1}, 1) \cdot \beta \cdot (1, t_1, \ldots, t_{s-1})$. □

It is not hard to verify that the monomial shuffle and inversion of a transversal logarithmic signature remain transversal. Also, a subgroup involved in a transversal logarithmic signature can be refined in a "nontransversal" way. For example, suppose that the alternating group $\mathscr{A}_5$ is a subgroup of G and the elements of $\mathscr{A}_5$ form the last block of a logarithmic signature. Then we can replace this block by a

Input: A logarithmic signature $\alpha = \{B_1, \ldots, B_s\}$
that is the sandwich of a transversal.
Output: A transversal β that is equivalent to α.

Begin

$x \leftarrow \alpha[s; 0]$;
$xinv \leftarrow x^{-1}$;
For $j = 0$ to $r_s - 1$ do
$\beta[s; j] \leftarrow \alpha[s; j] \cdot xinv$;
For $i = s - 1$ to 2 do
begin
For $j = 0$ to $r_i - 1$ do
$\beta[i; j] \leftarrow x \cdot \alpha[i; j]$;
$x \leftarrow \beta[i; 0]$;
$xinv \leftarrow x^{-1}$;
For $j = 0$ to $r_i - 1$ do
$\beta[i; j] \leftarrow \beta[i; j] \cdot xinv$;
end;
For $j = 0$ to $r_1 - 1$ do
$\beta[1; j] \leftarrow x \cdot \alpha[1; j]$;
End.

Fig. 2. Algorithm to construct an equivalent transversal.

nontransversal logarithmic signature for $\mathscr{A}_5$. Therefore refinement does not preserve the transversal property. In the cases of sandwiching and left and right translations, although the resulting logarithmic signatures are not transversals, in Fig. 2 we give a polynomial-time algorithm for constructing a transversal equivalent to the transformed logarithmic signature.

In view of this fact we broaden the use of the term transversal to include logarithmic signatures for which there exists a polynomial-time algorithm to compute an equivalent transversal. The algorithm starts with the last block B_s and *standardizes* it by multiplying on the right by the inverse of the first element $\alpha[s; 0]^{-1}$. The resulting block B_s' is the subgroup G_{s-1} with the identity as its first element. We then proceed upward, standardizing the jth block by multiplying on the left by $\alpha[j + 1; 0]$ and on the right by the new $\alpha[j; 0]^{-1}$. The procedure terminates after the first block has been standardized. It is easily seen that the resulting logarithmic signature β is a transversal. Since β is a sandwich of α, we have $\alpha \sim \beta$. Note that we could have used any element of a block for standardization, rather than the first one.

An interesting question is whether there exist new types of transformations that would map a tame logarithmic signature to an equivalent wild one. An affirmative answer would lead to a public-key cryptosystem based on PGM. Suppose, for example, that α and β are logarithmic signatures of G, with α wild and β tame. Then $\hat{\alpha}\hat{\beta}^{-1}$ is computable in polynomial time, while $\hat{\beta}\hat{\alpha}^{-1}$ is not. So, indeed, the existence of wild logarithmic signatures would give rise to one-way functions. Moreover, if there exist transformations which map wild logarithmic signatures to tame ones, we would have the trap doors required to build a public-key system.

The logarithmic signatures we have mentioned so far have all been transversals

Table 2. A logarithmic signature of $\mathcal{A}_5$ that is not a transversal.

Block 1
(1)(2)(3)(4)(5)
(1 5 2)(3)(4)
(1 3)(2 4)(5)
(1)(2 3 4)(5)
(1)(2 5 4)(3)
(1 3 5 2 4)
(1)(2 3)(4 5)
(1 5 4 3 2)
(1 5 3 4 2)
(1)(2)(3 4 5)
(1)(2 5 3)(4)
(1)(2)(3 5 4)
(1)(2 5)(3 4)
(1)(2 3 5)(4)
(1 3 2 4 5)
Block 2
(1 3)(2)(4 5)
(1 4)(2)(3 5)
(1)(2)(3)(4)(5)
(1 3 5)(2)(4)

and hence tame. We conjecture that wild logarithmic signatures will occur in profusion for arbitrary groups. We have constructed many nontransversal logarithmic signatures for the cyclic group $\mathbb{Z}_8$ and the alternating group $\mathcal{A}_5$. In fact the cyclic group $\mathbb{Z}_8$ turns out to be the smallest group for which there exist nontransversal logarithmic signatures. We exhibit one such logarithmic signature for $\mathcal{A}_5$ in Table 2. The logarithmic signature has two blocks of size 15 and 4, respectively. The first block cannot be a subgroup or the translate of a subgroup since $\mathcal{A}_5$ has no subgroups of order 15. The fact that the second block is not a translate of a subgroup was established by multiplying it on the left and right in all possible ways and then checking for closure.

The above process is not feasible for larger groups. However, we note that the algorithm in Fig. 2 can be modified to yield an efficient algorithm to determine whether a given logarithmic signature is a transversal. At every stage, after standardizing the current block B_i, we check the order of the group generated by $\langle B_i, B_{i+1}, \ldots, B_s \rangle$. This can be done in polynomial time from [3] and the fact that the number of generators is polynomial in n. If the order equals $r_i \cdot r_{i+1} \ldots r_s$, we continue; otherwise the logarithmic signature is not a transversal.

A consequence of (9) is that the number of logarithmic signatures arising just from a single chain of subgroups is astronomical. Even after considering equivalence induced by sandwiching, we arrive at an extremely large lower bound for the size of $\hat{\Lambda}$. In Table 3 we tabulate some facts about logarithmic signatures of small groups. These results have been obtained by an exhaustive computation. It is amazing that

Table 3. Logarithmic signatures of small groups.

G	$\hat{\Lambda}$	$\lvert\mathscr{T}_G\rvert$	$\mathscr{G}_G$	All transversal?
$\mathbb{Z}_4$	16	24	$\mathscr{S}_4$	Yes
$\mathscr{V}_4$	24	24	$\mathscr{S}_4$	Yes
$\mathbb{Z}_6$	132	500	$\mathscr{S}_6$	Yes
$\mathscr{S}_3$	288	702	$\mathscr{S}_6$	Yes
$\mathbb{Z}_8$	1,152	5,568	$\mathscr{S}_8$	No
$\mathbb{Z}_4 \times \mathbb{Z}_2$	2,304	17,088	$\mathscr{S}_8$	Yes
$\mathscr{V}_8$	4,032	10,432	$\mathscr{S}_8$	Yes
$\mathscr{Q}_8$	1,344	5,280	$\mathscr{S}_8$	Yes
$\mathscr{D}_8$	3,328	32,640	$\mathscr{S}_8$	Yes
$\mathbb{Z}_9$	648	1,224	$\mathscr{S}_9$	Yes
$\mathscr{V}_9$	2,160	8,208	$\mathscr{S}_9$	Yes
$\mathscr{A}_4$	304,128	?	$\mathscr{S}_{12}$	Yes

the number of inequivalent logarithmic signatures for $\mathscr{A}_4$ is 304,128. We have been unable to compute the order of $\mathscr{T}_G$ in this case.

6. Security of PGM

In this section we examine the security of PGM. To begin with we address the security of the cryptosystem under a chosen-plaintext attack. We then proceed to investigate algebraic properties of PGM, showing that, in general, PGM is 2-transitive.

One of the strongest possible security conditions that can be offered by a private key cryptosystem is that it provides $|\mathscr{M}|$-transitivity. We show that allowing multiple encryption, PGM offers $|\mathscr{M}|$-transitivity.

Consider the PGM transformation $E_{\alpha,\beta}$ defined by logarithmic signatures α and β. It can be shown that if α is known up to equivalence, then a chosen-plaintext attack will yield β up to equivalence. The number of required plaintext-ciphertext correspondences is of the order of $\Omega(\sum_{i=1}^{s} r_i)$ where $(r_1, \ldots, r_s)$ is the type of β. We leave it to the reader to verify this statement. Of course the cryptanalyst is still faced with the uncertainty of the type of β. However, if we assume that both α and β are kept secret, we know of no attack other than running through the set of all possible inequivalent α's, each time conducting the above chosen-plaintext attack to determine an appropriate β. In view of the extremely large number of equivalence classes of logarithmic signatures, such an attack is hopeless even for groups of relatively small degree ($n \simeq 20$).

We now proceed to investigate the algebraic properties of the cryptosystem.

Lemma 6.1. *Given a group G that is not cyclic of prime order, let $x \in \mathbb{Z}_{|G|}$ and $g \in G$. Then there exists a nontrivial logarithmic signature $\alpha \in \Lambda$ such that $\hat{\alpha}(x) = g$.*

Proof. Let $|G| = mp$ where p is a prime and $m \neq 1$, then there exists a subgroup $P \leq G$ with $|P| = p$. Let γ be a transversal logarithmic signature for G with respect

to the chain $G = G_0 > G_1 = P > G_2 = 1$. Clearly, γ has two blocks B_1 and B_2, and is of type $\mathbf{r} = (m, p)$. If $g \in G$, then $g \in Pu$ for some $u \in B_1$, hence $g = qu$ for some $q \in P$. On the other hand, given $x \in \mathbb{Z}_{|G|}$, we have $\lambda^{-1}(x) = (i, j)$ with respect to the type $\mathbf{r}$, where $0 \leq i \leq m-1$ and $0 \leq j \leq p-1$. Let α be a logarithmic signature that arises from γ by rearranging its elements so that u appears in the ith position of the first block and q in the jth position of the second block. Then we have $\hat{\alpha}(x) = g$. □

Theorem 6.1. *Given any group G, and any $x, y \in \mathbb{Z}_{|G|}$, there exist $\alpha, \beta \in \Lambda$ such that $E_{\alpha,\beta}(x) = y$. In other words, $\mathscr{T}_G$ is 1-transitive.*

Proof. Let g be an arbitrary element of G. From Lemma 6.1 there exist $\alpha, \beta \in \Lambda$ such that $\hat{\alpha}(x) = g$ and $\hat{\beta}(y) = g$. This implies that $E_{\alpha,\beta}(x) = \hat{\alpha}\hat{\beta}^{-1}(x) = y$. □

Theorem 6.2. *If a group G has a proper subgroup H that is not normal in G, then $\mathscr{T}_G$ is 2-transitive.*

Proof. Although $\mathscr{T}_G$ is not a group, without loss of generality, it will suffice to show that given any $x, y \in \mathbb{Z}_{|G|} - \{0\}$, there exist $\alpha, \beta \in \Lambda$ such that $E_{\alpha,\beta}(0, x) = (0, y)$. Let α be a logarithmic signature for G with respect to the chain $G = G_0 > H = G_1 > 1$. Then α has two blocks B_1 and B_2, and type $\mathbf{r} = (k, h)$ where $h = |H|$ and $k = [G : H]$. Given $x, y \in \mathbb{Z}_{|G|} - \{0\}$, let $\lambda^{-1}(x) = (i_x, j_x)$ and $\lambda^{-1}(y) = (i_y, j_y)$ with respect to $\mathbf{r}$, where $0 \leq i_x, i_y < k$ and $0 \leq j_x, j_y < h$. There are altogether nine cases for the values of i_x, i_y, j_x, j_y to be considered. In each case we construct a logarithmic signature β with type $\mathbf{r}$ such that $E_{\alpha,\beta}(0, x) = (0, y)$.

Case 1: $i_x, i_y, j_x, j_y > 0$. Let β be the same as α except that we exchange the elements in positions i_x and i_y of the first block and the elements in positions j_x and j_y in the second block. So we have $\beta[1; i_y] = \alpha[1; i_x]$ and $\beta[2; j_y] = \alpha[2; j_x]$. It follows that $E_{\alpha,\beta}(0, x) = (0, y)$.

Case 2: $i_x = i_y = 0$ *and* $j_x, j_y > 0$. This can be dealt with in a similar manner as Case 1. Here we need to exchange the elements in the second block only.

Case 3: $i_x, i_y > 0$ *and* $j_x = j_y = 0$. Again this is similar to Cases 1 and 2. This time we only need to exchange the elements in position i_x and i_y of the first block.

Case 4: $i_x = 0$ *and* $i_y, j_x, j_y > 0$. Since H is not normal there exist $u \in H$ and $t \in G$ such that $tut^{-1} \notin H$. Rearrange, if necessary, the second block of α so that $\alpha[2; j_x] = u$, and place the identity $1 \in G$ in position $\alpha[1; 0]$ as the coset representative of H. Also place 1 in position $\alpha[2; 0]$. We have $\hat{\alpha}(x) = \alpha[2; j_x] \cdot \alpha[1; 0] = u \cdot 1 = u \in H$. Since $v = u^{-1}tut^{-1} \notin H$, v lies in some coset of H, the coset representative of that is $\alpha[1; i]$ for some $i \neq 0$. Let γ be a logarithmic signature that is obtained from α by

(i) replacing $\alpha[1; i]$ by $u^{-1}tut^{-1}$;
(ii) exchanging the elements in $\alpha[1; i]$ and $\alpha[1; i_y]$;
(iii) exchanging $\alpha[2; j_x]$ and $\alpha[2; j_y]$.

Right translate γ by t and left translate it by t^{-1} to obtain a new logarithmic signature β. The resulting β has $\beta[1; 0] = t$, $\beta[1; i_y] = u^{-1}tu$ and $\beta[2; 0] = t^{-1}$, $\beta[2; j_y] = t^{-1}u$. It follows that $\hat{\beta}(0) = 1$ and $\hat{\beta}(y) = u$. Hence $E_{\alpha,\beta}(0, x) = (0, y)$.

Case 5: $i_y = 0$ *and* $i_x, j_x, j_y > 0$. By Case 4, there exist two logarithmic signatures α and β such that $E_{\alpha,\beta}(0, y) = (0, x)$, but then we have $E_{\beta,\alpha}(0, x) = (0, y)$.

Case 6: $i_x, j_y = 0$ *and* $i_y, j_x > 0$. Again as in Case 4 we assume that $\alpha[1; 0] = \alpha[2; 0] = 1 \in G$ and $\alpha[2; j_x] = u$ where $t^{-1}ut \notin H$. We have $\hat{\alpha}(x) = \alpha[2; j_x] \cdot \alpha[1; 0] = u \cdot 1 = u$. Since $v = t^{-1}ut \notin H$, v belongs to some coset of H, with coset representative $\alpha[1; i]$ for some $i \neq 0$. Let γ be the same as α except that we replace $\alpha[1; i]$ by $t^{-1}ut$ and exchange the elements $\alpha[1; i]$ and $\alpha[1; i_y]$. Right translate γ by t^{-1} and left translate by t to get β. The resulting β has $\beta[1; 0] = t^{-1}$, $\beta[1; i_y] = t^{-1}u$ and $\beta[2; 0] = t$. It follows that $E_{\alpha,\beta}(0, x) = (0, y)$.

Case 7: $i_y, j_x = 0$ *and* $i_x, j_y > 0$. This is symmetric to Case 6 and follows in the same way as Case 5 was obtained from Case 4.

Case 8: $j_x = 0$ *and* $i_x, i_y, j_y > 0$. Again we begin with $\alpha[1; 0] = \alpha[2; 0] = 1 \in G$. Let $\hat{\alpha}(x) = \alpha[2; 0] \cdot \alpha[1; i_x] = v$ where $v \notin H$. Construct β from α by:

(i) Exchanging the elements $\alpha[1; i_x]$ and $\alpha[1; i_y]$.
(ii) For $\alpha[2; j_y] = u \in H$ replacing $\alpha[1; 0]$ by u^{-1}; this is possible because $u^{-1} \in H$ and $1, u^{-1}$ represent the same right H coset.
(iii) Finally exchanging the elements $\alpha[2; 0]$ with $\alpha[2; j_y]$.

We now have $\beta[1; 0] = u^{-1}$, $\beta[1; i_y] = v$, $\beta[2; 0] = u$, and $\beta[2; j_y] = 1$. It follows that $E_{\alpha,\beta}(0, x) = (0, y)$.

Case 9: $j_y = 0$ *and* $i_x, i_y, j_x > 0$. This is symmetric to the previous case. □

Theorem 6.3. *There exists a group G for which* $\mathscr{T}_G$ *is not closed.*

Proof. Table 3 shows that $\mathscr{T}_G \neq \mathscr{G}_G$ for several small groups. □

In fact we conjecture that $\mathscr{T}_G$ is almost never closed, and when it is closed, $\mathscr{T}_G = \mathscr{S}_G$.

Theorem 6.4. *If a group G has a proper subgroup H of odd order, then* $\mathscr{T}_G$ *has a transformation that is an odd permutation in* $\mathscr{S}_{|G|}$.

Proof. Consider a transversal logarithmic signature α with respect to the chain $G = G_0 > G_1 = H > G_2 = 1$. The signature α has two blocks and type $\mathbf{r} = (k, h)$, where $h = |H|$ and $k = [G : H]$. Now let β be a second logarithmic signature that is identical to α, except that the first two elements in the first block are interchanged. It is clear that $\hat{\alpha}\hat{\beta}^{-1}$ will be an element of order two and have a factorization as a product of h transpositions. More precisely, we have

$$\hat{\alpha}\hat{\beta}^{-1} = (0, 1)(k, k + 1)(2k, 2k + 1) \ldots ((h - 1)k, (h - 1)k + 1). \quad \square \qquad (17)$$

In view of the fact that every finite 2-transitive group contains a unique minimal normal subgroup that is elementary abelian or simple [1], [16], the recent classification of finite simple groups yields a classification of finite 2-transitive groups. This in turn leads to the following interesting consequence.

Theorem 6.5. *If G is a finite nonabelian, nonhamiltonian group with $|G|$ different from $q, (1+q^2), (1+q^3), (q^n-1)/(q-1), 2^{n-1}(2^n \pm 1), 11, 12, 15, 22, 23, 24, 28, 176, 276$, where q is the power of a prime and n is a positive integer, then $\mathcal{T}_G$ is 2-transitive and $\mathcal{G}_G \cong \mathcal{S}_{|G|}$.*

Proof. The finite doubly transitive groups of degree m are known [6] and consist of the class of alternating groups $\mathcal{A}_m$, the class of symmetric groups $\mathcal{S}_m$, certain infinite classes of groups of degrees q, $(1+q^2)$, $(1+q^3)$, $(q^n-1)/(q-1)$, $2^{n-1}(2^n \pm 1)$, where q is a power of a prime and n a positive integer, together with a finite set of certain sporadic groups of degrees 11, 12, 15, 22, 23, 24, 28, 176, and 276. Since the degree of $\mathcal{G}_G$ is $|G|$, it follows from the hypothesis that $\mathcal{G}_G$ must be isomorphic to $\mathcal{A}_{|G|}$ or $\mathcal{S}_{|G|}$. However, since $|G| \neq 2^a$, by Theorem 6.4 there is an odd permutation in $\mathcal{G}_G$. Hence $\mathcal{G}_G \cong \mathcal{S}_{|G|}$. □

Although the above results suggest that PGM is secure, we wish to make it explicit to the reader that the status of security for PGM is still unsettled. PGM without multiple encryption is 2-transitive as we have shown, but it would be stronger to show that the number of transformations carrying a pair (m_1, m_2) of distinct messages to a pair (c_1, c_2) of distinct ciphers is independent of the particular pairs. This would correspond to the condition of PGM offering *Ordered Perfect 2-fold secrecy* ($O(2)$-*secrecy*) [4]. A similar comment can be made about PGM with multiple encryption as it relates to $O(|\mathcal{M}|)$-secrecy. On the other hand, we would like to point out that DES is not even known to be 1-transitive.

7. Conclusions

In this paper we have studied the algebraic structure of the PGM cryptosystem. PGM is a private key cryptosystem based on logarithmic signatures of finite permutation groups. The cryptosystem possesses desirable algebraic properties from a cryptographic point of view. The set of PGM transformations is not closed under functional composition and hence not a group. This set is 2-transitive if the underlying group is not hamiltonian and not abelian. Moreover, if $|G| \neq 2^a$, then the set of transformations contains an odd permutation. The consequence of these results is that the group generated by the set of transformations is nearly always the full symmetric group.

PGM promises to be a fast cryptosystem. In the fastest modes of its current implementation PGM attains a speed of well over 6 Mbits/s on a SUN4/Sparcstation 2 computer. PGM is more flexible than DES because of the versatility offered by changing the carrier group. Moreover, DES is not known to be 1-transitive.

Many questions still remain unanswered. We have asked earlier whether there exist transformations that convert a tame logarithmic signature to a wild one. Such

a transformation would lead to a public-key cryptosystem. In addition, the question whether nontransversal logarithmic signatures are wild needs to be adressed.

Evidence from Table 3 suggests that the condition that G possess a nonnormal subgroup may be unnecessary for the 2-transitivity of $\mathscr{T}_G$. It would be interesting to investigate whether this condition can be removed.

There is evidence to suggest that multiple encryptions using the composition of at most two PGM transformations may be sufficient to cover the symmetric group $\mathscr{S}_{|G|}$. Is it the case that $\mathscr{T}_G\mathscr{T}_G = \mathscr{S}_{|G|}$? This would be a desirable property for the cryptosystem. We pose this question to the reader.

For encryption, being able to factor all of G is not a requirement. For example, for a given $\varepsilon > 0$, it may be possible to find subsets $X_1, \ldots, X_s, Z \subset G$ with $|Z|/|G| < \varepsilon$ such that each element $g \in G - Z$ has a unique factorization $g = x_s \ldots x_2 \cdot x_1$, where $x_i \in X_i$. Such *near-factorizations* have been studied in [2] for $Z = \{1\}$, but not much is known for nonabelian G and $Z \neq \{1\}$.

Acknowledgments

The authors wish to thank the referees for their substantive and helpful remarks.

References

[1] P. Cameron, Finite permutation groups and finite simple groups, *Bulletin of the London Mathematical Society*, **13** (1981), 1–22.

[2] I. D. de Caen, D. A. Gregory, and D. L. Kreher, Near-factors of finite groups, Preprint (1989).

[3] M. Furst, J. E. Hopcroft, and E. Luks, Polynomial-time algorithms for permutation groups, in *Proceedings of the 21st IEEE Symposium on Foundations of Computation of Computer Science* (1980), pp. 36–41.

[4] P. Godlewski and C. Mitchell, Key-minimal cryptosystems for unconditional secrecy, *Journal of Cryptology*, **3** (1991), 1–25.

[5] M. Hall Jr., *The Theory of Groups*, 2nd edn., Chelsea, New York (1976).

[6] T. B. D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge (1986), pp. 255–256.

[7] B. S. Kaliski Jr., R. L. Rivest, and A. T. Sherman, Is the data encryption standard a group? (Results of cycling experiments on DES), *Journal of Cryptology*, **1** (1988), 3–36.

[8] D. E. Knuth, Notes on efficient representation of permutation groups, Correspondence with M. Furst (1981).

[9] S. S. Magliveras, A cryptosystem from logarithmic signatures of finite groups, in *Proceedings of the 29th Midwest Symposium on Circuits and Systems* (1986), pp. 972–975.

[10] S. S. Magliveras and N. D. Memon, Properties of cryptosystem PGM, in *Advances in Cryptology —Crypto '89*, Lecture Notes in Computer Science, Vol. 435, Springer-Verlag, Berlin (1989), pp. 447–460.

[11] S. S. Magliveras and N. D. Memon, Linear complexity profile analysis of the PGM cryptosystem, *Congressus Numerantium*, **72** (1989), 51–60.

[12] S. S. Magliveras and N. D. Memon, Complexity tests for cryptosystem PGM, *Congressus Numerantium*, **79** (1990), 61–68.

[13] S. S. Magliveras, B. A. Oberg, and A. J. Surkan, A new random number generator from permutation groups, *Rendiconti del Seminario Matematico di Milano*, **54** (1985), 203–223.

[14] S. S. Magliveras and P. Petersen, Software implementation of the PGM encryption system, CCIS Report, Center for Communication and Information Science, University of Nebraska–Lincoln, (1991).

[15] C. E. Shannon, The mathematical theory of communication, *Bell Systems Technical Journal*, **28** (1949), 379–423.
[16] E. Shult, Permutation groups with few fixed points: in P. Plaumann and K. Strambach, editors, *Geometry–Von Staudt's Point of View*, Reidel, Dordrecht (1981), pp. 275–311.
[17] C. C. Sims, Some group-theoretic algorithms: in M. F. Newman, editor, *Topics in Algebra*, Lecture Notes in Mathematics, Vol. 697, Springer-Verlag, Berlin (1978), pp. 108–124.
[18] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York (1964).