Group Factorizations in Cryptography

by

Charles A. Cusack

A DISSERTATION

Presented to the Faculty of

The Graduate College at the University of Nebraska

In Partial Fulfillment of Requirements

For the Degree of Doctor of Philosophy

Major: Computer Science

Under the Supervision of Professor Spyros Magliveras

Lincoln, Nebraska

November, 2000

Group Factorizations in Cryptography

Charles A. Cusack, Ph.D.

University of Nebraska, 2000

Adviser: Spyros Magliveras

Logarithmic signatures of permutation groups and their applications in private-key cryptography have been studied since the early 1980s. More recently, Magliveras, Stinson, and Trung have done some preliminary work in creating two new public-key cryptosystems, MST1, based on logarithmic signatures, and MST2, based on another type of group coverings called (r, s)-meshes.

In this thesis, we discuss implementation and security issues relating to both cryptosystems. Our discussion of MST2 is rudimentary. We give an elementary proof that factoring with respect to an (s, r)-mesh is at least as hard as the discrete logarithm problem, and discuss what is known about the *subgroup intersection problem* and its relationship to MST2.

The bulk of the thesis is devoted to logarithmic signatures and MST1. In order to implement MST1, we need two distinct types of logarithmic signatures; those for which factorization is easy, and those for which it is hard. In addition, we need

a method of constructing hard-to-factor logarithmic signatures from easy-to-factor logarithmic signatures, so that the former can serve as public keys, and the latter as private keys.

We provide a thorough analysis of several transformations that can be performed on logarithmic signatures. Every logarithmic signature of a group induces a permutation on S_G. Furthermore, a consequence of the analysis of transformations in this thesis is the discovery that the set of permutations resulting from several classes of logarithmic signatures of a group is the union of cosets of several different groups.

We show that a class of logarithmic signatures called *transversal* are easy to factor, and define and discuss the class of *permutably transversal logarithmic signatures*, which may help provide the trap-door needed for MST1.

We define the class of *canonical logarithmic signatures*. We show that the permutations generated by logarithmic signatures are generated by just the canonical logarithmic signatures, and give bounds on the number of logarithmic signatures and induced permutations of certain classes.

Acknowledgments

I would like to start by thanking the faculty of the Department of Computer Science and Engineering and the Department of Mathematics and Statistics at UNL. I have learned much from faculty in both departments. Along with the faculty, I would like to thank the office staff, who have truly been a blessing to me.

I would like to thank the members of my committee, Professors Earl Kramer, Spyros Magliveras, Jamie Radcliffe, Byrav Ramamurthy, and Sharad Seth. In addition, Professor Jean-Camille Birget was very helpful in several ways.

I would like to thank my adviser, Professor Spyros Magliveras. He has put up with me for 6 years, and has helped me gain greater insight into cryptography and related fields. He has encouraged me both professionally and personally, and I know he will continue to do so.

Lastly, I would like to thank my Lord and Savior, Jesus Christ, who has been the constant in my life as a student. He has once again revealed to me a small chapter of His *Big Book of Theorems*. He gives meaning and purpose to my life and work, and has saved me from that which I could not save myself.

To God be the glory!

Contents

List of Figures

Chapter 1

Introduction

1.1 Cryptography

In 1976, the idea of public-key cryptography was introduced by Diffie and Hellman [4, 5]. In the 24 years since, many public-key cryptosystems have been proposed. Most of these have been shown to be insecure. The two best known public-key cryptosystems, **RSA** [25] and **ElGamal** [6], have stood up against attacks and are generally regarded as being secure. Their security is based on the assumption that factoring integers (**RSA**) and solving the discrete logarithm problem (**ElGamal**) are intractable.[1] Although these assertions have not been proven[2], no one has found an efficient algorithm to solve either problem, and it is generally believed that they are indeed intractable.

Cryptography, especially public-key cryptography, is becoming increasingly im-

[1] More precisely, each is intractable in certain cases.

[2] In fact, neither has been shown to be even NP-hard. It is interesting to note that there is no known public-key cryptosystem based on an NP-hard problem that is regarded as secure.

portant as more and more information is being stored and transmitted using a wide variety of media. As we approach the next millennium[3], the Internet is continuing to grow in popularity and importance at an increasing rate. Almost any information one would want to find is now accessible through phone lines, coaxial cable, and the airwaves via cellular phones or satellites. With the increase in ease of access comes an increased need for security of stored and transmitted information. In addition, computers continue to double in speed every 18 months, making problems that were hard to solve a few years ago much easier to solve today.

In light of these facts, the continuing development and analysis of cryptosystems is of paramount importance. In fact, if *quantum computers* ever become a reality, public-key cryptography as we know it will no longer be secure, since both **RSA** and **ELGamal** have been shown to be insecure against a quantum computer [27]. Since it cannot be assumed that everyone will obtain quantum computers at the same time, there will be a need for public-key cryptosystems which can be implemented on classical computers which are secure against attack by quantum computers. It is unknown if this is possible at this time. Unfortunately, quantum cryptography is beyond the scope of this thesis.

[3] Contrary to popular belief, the start of the next millennium will be January 1, 2001.

1.2 Group Factorizations

Logarithmic signatures of permutation groups and their applications in private-key cryptography have been studied since the early 1980s [16, 20, 19, 18, 17, 21]. More recently, Magliveras, Stinson, and Trung [22] have done some preliminary work in creating two public-key cryptosystems, based on logarithmic signatures (MST1), and another type of group coverings, called $[s, r]$-meshes (MST2). One of the advantages of using logarithmic signatures in cryptography is that permutation multiplication can be done very efficiently in hardware [10].

There are several questions which need to be answered before either of these systems can be realized. It is the goal if this thesis to explore these questions.

In order to implement MST1, it is required that two things be true:

- There exist wild logarithmic signatures. That is, logarithmic signatures which are hard to "invert".
- There exists a method of constructing a wild logarithmic signature from tame (polynomial-time factorable) ones, probably in the form of a product.

As a precursor to answering the first question, we would like to know which logarithmic signatures are tame (not wild). A class of logarithmic signatures, called

r-transversal[4], has been known to be tame for a long time. We show that a more general class, transversal logarithmic signatures, is also tame.[5]

We also investigate a newly defined class of logarithmic signatures, called permutably transversal. This class is closely related to transversal logarithmic signatures, and may provide the link to non-transversal logarithmic signatures we need to answer the second question.

Several transformations that can be performed on logarithmic signatures have been defined and studied by Magliveras and Memon [20], however these authors have left many questions unanswered. We significantly fill in this gap by providing a thorough analysis of the transformations. Every logarithmic signature of a group induces a permutation on S_G, and a consequence of the analysis of transformations is the discovery that the set of permutations resulting from logarithmic signatures of a group is the union of cosets of several different groups. In fact, there are several classes of logarithmic signatures for which this is also true. This helps to provide an understanding of the structure of these permutations. For instance, this gives good evidence that the permutations which correspond to a logarithmic signature are not *random* in any reasonable definition of the word.

[4] What we call r-transversal here was previously called *transversal* by Magliveras and others. Following the idea of Qu [24], we adopt new terminology.

[5] Qu [24] states the result, but gives no proof, and does not make his assumptions clear.

We define another new class of logarithmic signatures, called *canonical*, to which we can, in general, restrict our attention. Given this class, we are able to prove several results about the structure of the set of permutations corresponding to logarithmic signatures, including several results relating to the number of certain types of logarithmic signatures of a group.

These results provide new insight into the structures of the various classes of logarithmic signatures, and the sets of corresponding permutations. Since logarithmic signatures are at the center of MST1, an in-depth understanding of them is required not only to implement MST1, but also to ensure its security. Therefore, it is hoped that these results will help lead to a realization of MST1.

1.3 Organization

The remainder of the thesis is organized as follows.

Chapter 2 contains definitions and basic results in group theory (Section 2.1), logarithmic signatures (Section 2.2), group covers (Section 2.3), and logarithmic signature mappings (Section 2.4). The preliminary chapter concludes with a discussion of groups and cryptography (Section 2.5).

In Chapter 3, we take a closer look at logarithmic signatures. In Section 3.1 we define several important classes of logarithmic signatures, and in Section 3.2 we define several transformations that can be performed on logarithmic signatures. Sections 3.3 and 3.8 discuss an important newly defined class, canonical logarithmic signatures. Sections 3.4, 3.5, and 3.7 are devoted to the classes of exact-transversal, transversal, and permutably-transversal logarithmic signatures. The properties of logarithmic signature transformations are discussed in Section 3.6. Section 3.9 finishes the chapter with a few bounds on the number of logarithmic signatures of certain classes.

Chapter 4 focuses on the issues surrounding MST2. In Section 4.1 we discuss security issues of MST2, and in Section 4.2 we give evidence that factoring with respect to an $[s, r]$-mesh is hard in general. Finally, in Section 4.3 we discuss the coset intersection problem as it relates to MST2.

We conclude with a summary of our contributions and further research in Chapter 5.

Chapter 2

Preliminaries

2.1 Group Theory

For basic definitions in group theory, see [26]. In this paper, we assume that all groups and sets are finite, unless otherwise specified. This assumption will be implicit for all theorems.

The set of all permutations on a set X is a group, called the *symmetric group*, under the operation of composition of functions. We denote by $\mathcal{S}_X$ the symmetric group on the set X. When $X = \{1, \ldots, n\}$, we write $\mathcal{S}_n$ for $\mathcal{S}_X$. A *permutation group* is a pair (X, G) where X is a finite set and G is a subgroup of $\mathcal{S}_X$. The *degree* of G is $|X|$.

Let X be a set, G be a group, written multiplicatively, and suppose a formal operation, denoted as exponentiation,

$$X \times G \to X$$

$$(x, g) \mapsto x^g$$

is defined which satisfies the following axioms:

1. $x^1 = x$ for all $x \in X$, where 1 is the identity in G.

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

Then we say that G *acts on* the set X, and write $G|X$. By the *kernel*, $\mathcal{K}(G|X)$, of a given group action $G|X$ we mean the collection

$$\mathcal{K}(G|X) = \{g \in G : x^g = x, \text{ for all } x \in X\}.$$

It is easy to see that the kernel of a group action is always a normal subgroup of G. When $\mathcal{K}(G|X)$ is the identity subgroup, we say that the action $G|X$ is *faithful.* A faithful group action $G|X$ is equivalent to G being a permutation group in $\mathcal{S}_X$.

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 $y = x^g$ for some $g \in G$. The equivalence classes are called G-*orbits* of the group action. Thus, X is partitioned into $G-$orbits under the action of G on X. It is clear that the $G-$orbit containing $x \in X$ is the subset $x^G = \{x^g : g \in G\}$.

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. The following theorem will be relevant.

Theorem 2.1 *Let G act on a set X. Then the number of elements in the orbit of $x \in X$ is the index of G_x in G, i.e.*

$$|x^G| = [G : G_x] = |G|/|G_x|$$

A group action $G|X$ is called *transitive* if X consists of a single G-orbit, i.e. $x^G{=}X$ for any $x \in X$.

Let k be a positive integer. Then the action $G|X$ induces an action $G|\binom{X}{k}$ in the obvious way: If $A = \{a_1, a_2, \ldots, a_k\} \in \binom{X}{k}$ and $g \in G$, then $A^g = \{a_1^g, a_2^g, \ldots, a_k^g\}$. Similarly, G acts on the k-tuples of X in a natural way: If $\vec{x} = (x_1, x_2, \ldots, x_k)$ is a k-tuple of X, then $\vec{x}^g = (x_1^g, x_2^g, \ldots, x_k^g)$.

The group G is said to be *t-transitive* on X if the induced action of G on the ordered t-subsets of X is transitive. That is, if for any pair of t-tuples $\vec{x}$ and $\vec{y}$ of distinct entries of X, there is an element $g \in G$ such that $\vec{x}^g = \vec{y}$.

Let G be a group. We write $H \leq G$ if H is a subgroup of G, and $H < G$ if H is a proper subgroup of G. Similarly, we use the symbols $\trianglelefteq$ and $\triangleleft$ if H is a normal subgroup of G. We say that H is *subnormal* in G, written $H \triangleleft \triangleleft G$, if there exist groups $H_1, \ldots, H_m$ such that $H \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_m \trianglelefteq G$.

Let H be a subgroup of a group G. Recall that a *right coset* of H in G is a subset of G of the form Hg. Similarly, a *left coset* of H in G is a subset of G of the form

gH. When G is not an abelian group, $Hg \neq gH$ in general.

The following theorem is useful.

Lemma 2.1 *Let $L \subset G$. L is a right coset of G if and only if $LL^{-1}l = L$ for some $l \in L$.*

Proof. It is clear that if L is a coset, $LL^{-1}l = L$ for every $l \in L$, so the first direction is clear. For the other, we notice that $LL^{-1}l = L$ implies that $LL^{-1} = LL^{-1}ll^{-1}LL^{-1} = (LL^{-1})(LL^{-1})$. Since G is finite, this shows that LL^{-1} is a subgroup, and since $L = LL^{-1}l$, L is a right coset. □

Let $A \subseteq G$. Then $\langle A \rangle$ denotes the subgroup generated by A, and $A^g = \{a^g \mid a \in A\}$. If $H \leq G$, the *centralizer* of A in H is $C_H(A) = \{h \in H \mid a^h = a, \forall a \in A\}$. If $a \in G$, $C_H(a) = C_H(\{a\})$.

Let $Z(G)$ be the subset of those elements of G that commute with all elements of G. That is, $Z(G) = \{g \in G : gh = hg \text{ for all } h \in G\}$. Then it is not hard to show that $Z(G)$ is a normal subgroup of G. We call $Z(G)$ the *center* of G.

Let G be a group of order n. For each $g \in G$ we define

$$g_r = \begin{pmatrix} 1 & g_1 & g_2 & \cdots & g_n \\ 1 \cdot g & g_1 \cdot g & g_2 \cdot g & \cdots & g_n \cdot g \end{pmatrix}.$$

Thus, g_r is the permutation in $\mathcal{S}_G$ that maps h to hg. Define $R_G = \{g_r : g \in G\}$.

Then R_G is a subgroup of $\mathcal{S}_G$ which is isomorphic to G. R_G is called the *right regular image* of G. We can define g_l and the *left regular image* of G, L_G, similarly.

Let $g, h \in G$. Then it is not hard to see that for any $x \in G$,

$$g_r(h_l(x)) = g_r(hx) = hxg = h_l(xg) = h_l(g_r(x))$$

Thus, L_G and R_G commute element-wise.

Let $g_r = h_l$. Then $g_r(1) = h_l(1)$, i.e. $1 \cdot g = h \cdot 1$, so $g = h$. Also, $xg = gx$ for all $x \in G$, so g commutes with all elements of G. That is, g is in the center of G. Thus, we have that $L_G \cap R_G = Z(L_G) = Z(R_G)$.

From these results it is easy to see that

$$\mathcal{G} = \langle L_G, R_G \rangle = L_G R_G, \text{ and}$$

$$|\mathcal{G}| = \frac{|L_G| \cdot |R_G|}{|L_G \cap R_G|} = \frac{|L_G| \cdot |R_G|}{|Z(R_G)|} = \frac{|G|^2}{|Z(G)|}.$$

For subgroups $H, K \leq G$, the *normalizer* of H in K is $N_K(H) = \{k \in K \mid H^k = H\}$. If $H \leq G$, the *core* of H in G is $\mathrm{Core}_G(H) = \cap_{g \in G} H^g$, the largest subgroup of H that is normalized by G.

A *normal series* for a groups G is a chain of subgroups

$$1 = G_n \subset G_{n-1} \subset \ldots \subset G_1 \subset G_0 = G$$

such that $G_{i+1} \lhd G_i$. The *factor groups* are the groups G_i/G_{i+1} for $i = 0, \ldots, n-1$. A group G is called *solvable* (or *soluble*) if it has a normal series whose factor groups are cyclic of prime order. Equivalently (when G is finite), G is solvable if it has a normal series with abelian factor groups.

A normal series is called a *composition series* if either each G_{i+1} is a maximal normal subgroup of G_i, or $G_{i+1} = G_i$. The factor groups of a composition series are called the *composition factors* of G.

For any fixed integer d, let Γ_d denote the class of groups all of whose non-cyclic composition factors are isomorphic to some subgroup of $\mathcal{S}_d$.

For the remainder of the paper, we make the following assumptions. Let G be a permutation group of degree n. When we use the term "polynomial", we mean polynomial in n, unless stated otherwise. We assume that G is presented by a polynomial number of generators. When we have a chain of subgroups, $\gamma : G = G_0 > G_1 > \ldots > G_s = 1$, we assume that $[G_{i-1} : G_i]$ is bounded by a polynomial, for $i = 1, \ldots, s$.

For more information on group theory, the reader is directed to [26]. For more information on permutation groups and algorithms, see [3].

2.2 Logarithmic Signatures

In this section we will define the basics of logarithmic signatures. For more information on logarithmic signatures, see, for example, [20].

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 $B_i = \{B(i,1), \ldots, B(i,r_i)\}$ such that the following two properties hold:

i) $\ell = \sum_{i=1}^{s} r_i$ is bounded by a polynomial in n,

ii) $B(i,j) \in \mathcal{S}_n$ for all $1 \leq j \leq r_i$ and $1 \leq i \leq s$, and

iii) each element $g \in G$ can be expressed *uniquely* as a product of the form

$$g \;=\; b_1 \cdot b_2 \cdots b_{s-1} \cdot b_s, \tag{2.1}$$

where $b_i \in B_i$.

The sets B_i are called the *blocks* of α. For simplicity and clarity, we will label the elements of α by $\alpha[i;j] = B(i,j)$, where $1 \leq i \leq s$ and $1 \leq j \leq r_i$. That is, $\alpha[i;j]$ denotes the j^{th} element of the i^{th} block of α. We will denote the i^{th} block of α by $\alpha[i]$.

In this thesis we will restrict our attention to logarithmic signatures with $\alpha[i;j] \in G$. We will show in a later section that this restriction has no significant impact.

The vector of block lengths, $r = (r_1, r_2, \ldots, r_s)$ is called the *type* of α, and the *length* of α is $\ell = \sum_{i=1}^{s} r_i$. Notice that $M{=}|G|{=}\prod_{i=1}^{s} r_i$.

A logarithmic signature is called *nontrivial* if $s \geq 2$ and $r_i \geq 2$ for $1 \leq i \leq s$, and *trivial* otherwise.

A logarithmic signature is called *tame* if there is an algorithm by means of which the factorization in (2.1) can be accomplished in time polynomial in the degree n of G. If the factorization can be done in time $O(n^2)$, the logarithmic signature is called *supertame*. A logarithmic signature is called *wild* if it is not tame.

2.3 Group Covers and $[s, r]$-Meshes

In this section, we give a more general framework for studying coverings of a group, of which logarithmic signatures are one case. We start with some notation. The definitions here are taken from [22].

Let $G^{[\mathbb{Z}]}$ be the collection of all finite sequences in G. We can view the elements of $G^{[\mathbb{Z}]}$ as vectors with entries in G. If $X, Y \in G^{[\mathbb{Z}]}$, we define $X \otimes Y$ to be the tensor product of X and Y. For instance, if $X = (a, b, c)$, and $Y = (x, y)$, then

$$X \otimes Y = (ax, ay, bx, by, cx, cy).$$

Let $X = [x_1, x_2, \ldots, x_r] \in G^{[\mathbb{Z}]}$. Then $|X|$ denotes the length r of X, and $\overline{X}$ denotes the element $\sum_{i=1}^{r} x_i$ in the group ring $\mathbb{Z}G$.

Let G be a permutation group, and let $\alpha = [A_1, A_2, \ldots, A_s]$ be a sequence with $A_i \in G^{[\mathbb{Z}]}$ such that $\sum_{i=1}^{s} |A_i|$ is bounded by a polynomial in the degree of G. Let

$$\sum_{g \in G} a_g g = \overline{A_1} \cdot \overline{A_2} \cdots \overline{A_s},$$

where $a_g \in \mathbb{Z}$. Then we say that α is

i) a *pseudo logarithmic signature* for G if $\prod_{i=1}^{s} |A_i| = |G|$.

ii) a *cover* for G if $a_g > 0$ for all $g \in G$.

iii) a *λ-quasi-logarithmic signature* for G if $a_g \in \{\lambda, \lambda + 1\}$ for all $g \in G$.

iv) a *λ-logarithmic signature* for G if $a_g = \lambda$ for all $g \in G$.

v) a *quasi-logarithmic signature* for G if α is a *1-quasi-logarithmic signature* for G.

vi) a *logarithmic signature* for G if α is a *1-logarithmic signature* for G.

Notice that the definition of logarithmic signature above is equivalent to the definition given in the previous section.

In this paper, we are primarily interested in logarithmic signatures (objects of type iv). We are also interested in a special case of covers (objects of type ii), called $[s, r]$-meshes, which we define next.

Let s and r be positive integers, and G a permutation group. A cover $\alpha = [A_1, A_2, \ldots, A_s]$ is called an $[s, r]$-*mesh* if

i) $A_i \in G^{[\mathbb{Z}]}$ and $|A_i| = r$ for each $i \in \{1, \ldots, s\}$, and

ii) In

$$\sum_{g \in G} a_g g = \overline{A_1} \cdot \overline{A_2} \cdots \overline{A_s},$$

the distribution of $\{a_g : g \in G\}$ is approximately uniform. By approximately uniform, we mean with regard to the usual statistical analysis.

We represent an $[s, r]$-mesh by an $s \times r$ matrix $\alpha = (a_{i,j})$, where each $a_{i,j} \in G$.

2.4 Logarithmic Signature Mappings

In this section, we define some maps that will be useful.

Let α be a logarithmic signature of a group G of type $(r_1, r_2, \ldots, r_s)$. Define the bijection $\Theta_\alpha : \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s} \to G$ by

$$\Theta_\alpha(p_1, \ldots, p_s) = \alpha[1, p_1] \cdots \alpha[s, p_s].$$

Recall that $|G| = M = \prod_{j=1}^{s} r_j$. For each $i = 1, 2, \ldots, s$, define

$$m_i = \begin{cases} 1 & \text{if i=1, and} \\ \prod_{j=1}^{i-1} r_j & \text{otherwise.} \end{cases}$$

It is not hard to see that each $x \in \mathbb{Z}_M$ can be written uniquely as $x = \sum_{i=1}^{s} x_i m_i$, where $0 \leq x_i < r_i$. Define the bijection $\lambda : \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s} \to \mathbb{Z}_M$ by

$$\lambda(p_1, \ldots, p_s) = \sum_{i=1}^{s} p_i m_i.$$

Each logarithmic signature α induces a bijection $\breve{\alpha} : \mathbb{Z}_{|G|} \to G$ given by $\breve{\alpha} = \lambda^{-1}\Theta_\alpha$. Two logarithmic signatures α and β are said to be *equivalent* if and only if $\breve{\alpha} = \breve{\beta}$.

Let α and β be logarithmic signatures for a group G. Then the mapping

$$P_{\alpha,\beta} = \breve{\alpha}\breve{\beta}^{-1}$$

is a permutation on $\mathbb{Z}_{|G|}$. Thus, each pair (α, β) of logarithmic signatures of G corresponds to a permutation $P_{\alpha,\beta} = \breve{\alpha}\breve{\beta}^{-1} \in \mathcal{S}_{|G|}$. It is not hard to see that $P_{\alpha,\beta}^{-1} = P_{\beta,\alpha}$. For any subset $F \subseteq \Lambda$, we denote $F_P = \{P_{\alpha,\beta} : \alpha, \beta \in F\}$. We are interested in F_P and $\langle F_P \rangle$ for various subsets F of Λ.

Let η be a fixed tame logarithmic signature. Then each logarithmic signature α corresponds to a permutation $\widehat{\alpha}$=$P_{\alpha,\eta}$=$\breve{\alpha}\breve{\eta}^{-1} \in \mathcal{S}_{|G|}$. It is easy to see that $\widehat{\alpha}$=$\widehat{\beta}$ if and only if α and β are equivalent. Note that equivalence does not depend on the choice of η. We can think of η as an initial ordering of the elements of G. In light of this, we will call η the *ordering logarithmic signature* of G. Whenever we have a fixed η and a subset $F \subseteq \Lambda$, we denote $\widehat{F} = \{\widehat{\alpha} : \alpha \in F\}$

Since fixing one logarithmic signature makes things easier, we would like to fix η and study the sets $\widehat{F}$ instead of F_P. Unfortunately, the following theorem shows that for any subset $F \subseteq \Lambda$, the set $\widehat{F}$ is not necessarily the same for different choices of η.

Theorem 2.2 *Let G be a group, and η, α, and β any logarithmic signatures of G. Then $P_{\alpha,\beta} = P_{\alpha,\eta}P_{\eta,\beta}$.*

Proof. This is easily established by applying the definition:

$$P_{\alpha,\eta}P_{\eta,\beta} = \breve{\alpha}\breve{\eta}^{-1}\breve{\eta}\breve{\beta}^{-1} = \breve{\alpha}\breve{\beta}^{-1} = P_{\alpha,\beta}.$$

□

In light of this, the properties of these sets will change according to the ordering logarithmic signature. In fact, if we are allowed to replace η by any mapping from G to $\mathbb{Z}_{|G|}$, we can get any $P \in \mathcal{S}_{|G|}$ in the set $\widehat{F}$. However, we show next that we can study these sets independent of the ordering permutation. It is straightforward to see that

$$P_{\alpha,\beta} = \breve{\alpha}\breve{\beta}^{-1} = \breve{\alpha}\breve{\eta}^{-1}\breve{\eta}\breve{\beta}^{-1} = \breve{\alpha}\breve{\eta}^{-1}(\breve{\beta}\breve{\eta}^{-1})^{-1} = \widehat{\alpha} \cdot \widehat{\beta}^{-1}.$$

This establishes the following.

Theorem 2.3 *Let G be a group, and $F \subseteq \Lambda$. Then*

$$F_P = \{P_{\alpha,\beta} : \alpha, \beta \in F\} = \{\widehat{\alpha} \cdot \widehat{\beta}^{-1} : \alpha, \beta \in F\} = \widehat{F}\widehat{F}^{-1}.$$

From this it is easy to see that $\langle F_P \rangle = \langle \widehat{F} \rangle$. That is, the subgroups generated in the two cases are the same. What is interesting about this is the fact that it is not necessarily the case (in fact, often it is *not* the case) that $\widehat{F} \subseteq \widehat{F}\widehat{F}^{-1} = F_P$. This may happen, for instance, if the identity permutation is not in $\widehat{F}$.

In summary, if we wish to study the set F_P, we may fix a logarithmic signature η, first consider the set $\widehat{F}$, and then construct $F_P = \widehat{F}\widehat{F}^{-1}$. However, if we are interested in the subgroup $\langle F_P \rangle$, we can restrict our attention to $\langle \widehat{F} \rangle$. In either case, we start by picking *any* fixed logarithmic signature η, and construct $\widehat{F}$.

2.5 Groups and Cryptography

It is assumed the reader is versed in the basics of cryptography. For an excellent introduction, consult the text by Stinson [29].

The structures defined in the previous sections have applications to cryptography. *Permutation Group Mappings* (*PGM*) is a private-key cryptosystem, invented by Magliveras in the 1970s, that uses logarithmic signatures as keys. More recently, Magliveras and others have been attempting to use logarithmic signatures as the basis for a public-key cryptosystem. A new approach using $[s, r]$-meshes is also being investigated.

In this section, I will briefly describe these three cryptosystems. The latter two systems, refered to as *MST1* and *MST2*, will be discussed in more detail in later sections. These systems were proposed by Magliveras, Stinson, and Trung, and details on both of these can be found in [22].

2.5.1 PGM

The idea behind PGM is simple. Having fixed a logarithmic signature η, and given a pair of logarithmic signatures, α and β, with β tame, the encryption function $E_{\alpha,\beta} : \mathbb{Z}_{|G|} \mapsto \mathbb{Z}_{|G|}$ is given by

$$E_{\alpha,\beta} = P_{\alpha,\beta} = \widehat{\alpha} \cdot \widehat{\beta}^{-1}.$$

Decryption is simply the inverse of encryption:

$$D_{\alpha,\beta} = E_{\alpha,\beta}^{-1} = E_{\beta,\alpha} = \widehat{\beta} \cdot \widehat{\alpha}^{-1}.$$

Notice that α must also be tame if decryption is to be performed. PGM is discussed in detail in [16, 19, 20, 21].

2.5.2 MST1

Before we discuss MST1, we need to make a few assumptions about logarithmic signatures:

- **Assumption 1:** Given a wild logarithmic signature β, it is "hard" to compute $\widehat{\beta}^{-1}$.

- **Assumption 2:** Given a wild logarithmic signature β, it is "hard" to find a set of transversal logarithmic signatures $\theta_1, \theta_2, \ldots \theta_k$ such that $\widehat{\beta} = \widehat{\theta_1}\widehat{\theta_2} \ldots \widehat{\theta_k}$.

Notice that Assumption 2 follows from Assumption 1. Although there is no known proof of these assumptions, there is strong evidence that they are valid. In fact, factoring with respect to a logarithmic signature is very closely related to the *discrete logarithm problem* [22]. Now we describe the cryptosystems.

The reason PGM must be a private-key cryptosystem is that the logarithmic signatures α and β are both tame, so that anyone who knows α and β can do both the encryption and decryption. The most obvious way to modify PGM into a public-key system is to require that α be wild. However, in order to facilitate decryption, there must be some way for the user, and only the user, to "invert" α. This is the basis of MST1.

With MST1, a user, say Alice, selects a group G and a pair of logarithmic signatures (α, β), with α wild, and β tame, such that a factorization $\widehat{\alpha}\widehat{\beta}^{-1} = \widehat{\theta_1} \cdots \widehat{\theta_k}$ is known, where the θ_i are tame and $k \geq 2$ is small. Alice publishes the group G and the pair of logarithmic signatures (α, β) as her public key, but keeps the factorization to herself.

Although in practice, there is no known easy way to construct factorizations $\widehat{\alpha}\widehat{\beta}^{-1} = \widehat{\theta_1} \cdots \widehat{\theta_k}$, in the next section we give a result of Magliveras and Memon [20] that essentially shows that for most groups, the factorizations do exist.

The encryption function is $E_{\alpha,\beta} = \widehat{\alpha}\widehat{\beta}^{-1}$, which anyone can compute since β is tame. The decryption funtion is $D_{\alpha,\beta} = E_{\beta,\alpha} = \widehat{\beta}\widehat{\alpha}^{-1} = \widehat{\theta_k}^{-1} \cdots \widehat{\theta_1}^{-1}$, which only Alice can perform by Assumption 2.

There are several important questions that must be answered about MST1:

1. Since one cannot compute a "factorization" $\widehat{\alpha}\widehat{\beta}^{-1} = \widehat{\theta_1} \cdots \widehat{\theta_k}$, how does one build a wild logarithmic signature from a set of tame logarithmic signatures? Without this, one cannot hope to implement MST1.

2. Are Assumptions 1 and 2 valid? If not, MST1 is not secure.

3. Is MST1 secure? What potential attacks are there against MST1, and can they be prevented?

4. Is MST1 practical? In particular, is it "fast" enough for practical use?

2.5.3 MST2

MST2 uses $[s, r]$-meshes, not logarithmic signatures. As with MST1, we need to make a cryptographic assumption. Let $\alpha = (a_{i,j})$ be an $[s, r]$-mesh for a permutation group G. Let H be a second group, and $f : G \to H$ be an epimorphism. Then $\beta = (b_{i,j})$, where $b_{i,j} = f(a_{i,j})$, is an $[s, r]$-mesh for H. Our assumption is:

- **Assumption 3:** Given an $[s, r]$-mesh $\alpha = (a_{i,j})$ for a group G, and an element $g \in G$, then finding a factorization

  $$g = a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,j_s}$$

  is in general an intractable problem.

Given an $[s, r]$-mesh α, we can define a surjection $\breve{\alpha} : \mathbb{Z}_{r^s} \to G$ in the same way as was done with logarithmic signatures. Since $|G| \neq r^s$ in general, this mapping is not necessarily a bijection.

We now describe MST2. The reader versed in cryptography will notice the similarity of MST2 to El Gamal's system.

Alice chooses two (preferably large) groups G and H, an epimorphism $f : G \to H$, and a random $[s, r]$-mesh $\alpha = (a_{i,i})$ for G. Alice computes $\beta = f(\alpha) = (b_{i,j}) = (f(a_{i,j}))$. She makes (α, β) public, but keeps f secret. To send a message $h \in H$ to Alice, Bob

i) Chooses a random integer $R \in \mathbb{Z}_{r^s}$,

ii) Computes $y_1 = \breve{\alpha}(R)$, $y_2 = \breve{\beta}(R)$, and $y_3 = hy_2$, and

iii) Sends $y = (y_1, y_3)$ to Alice.

To decrypt the message, Alice computes $y_2 = \breve{\beta}(R) = f(\breve{\alpha}(R)) = f(y_1)$, and obtains the message $h = y_3 y_2^{-1}$.

The questions one needs to ask about MST2 are

1. Can one easily generate $[s, r]$-meshes for a group? This is necessary to implement MST2.

2. Is Assumption 3 valid? If not, MST2 is not secure.

3. Is MST2 secure? What potential attacks are there against MST2, and can they be prevented?

4. Is MST2 practical? In particular, is it “fast” enough for practical use?

As can be seen, there are many questions to be answered before implementations of either MST1 or MST2 can be realized. The remainder of this thesis is devoted to summarizing what is already known, and furthering the theory in hopes that there will be more difinitive answers to these questions in the nead future.

Chapter 3

Logarithmic Signatures

3.1 Classes of Logarithmic Signatures

We can classify logarithmic signatures in a number of ways. In this section, we give several definitions of classes of logarithmic signatures. For reasons that will become evident, the terminology in this thesis does not follow the standard terminology used by Magliveras and others. Our definitions are motivated by, and very close to, those of Qu [24].

Let $\gamma : G = G_0 > G_1 > \cdots > G_s = 1$ be a chain of subgroups of G, and $\{B_i : i = 1, \ldots, s\}$ be an ordered collection of subsets of G with $B_i = \{\alpha[i; j] : j = 1, \ldots, r_i\}$ a complete set of right coset representatives of G_{s-i+1} in G_{s-i}. It is not hard to see that $\alpha_k = \{B_i : i = 1, \ldots, k\}$ is a logarithmic signature for G_{s-k}, so that $\alpha = \{B_i : i = 1, \ldots, s\}$ is a logarithmic signature for G. Such a logarithmic signature is called *exact right transversal* or *exact r-transversal* with respect to γ.

Similarly, if $\alpha = \{B_i : i = 1, \ldots, s\}$ is an ordered collection of subsets of G with $B_i = \{\alpha[i; j] : j = 1, \ldots, r_i\}$ a complete set of left coset representatives of G_{s-i+1} in G_{s-i}, then α is a logarithmic signature for G, and we say it is *exact left transversal*, or *exact ℓ-transversal*.

Let $\alpha = \{B_i : i = 1, \ldots, s\}$, where $B_i = \{\alpha[i; j] : j = 1, \ldots, r_i\}$. Then α is called *exact mixed-transversal* if there exists a permutation σ of $1, \ldots, s$ such that for each $t = 1, \ldots, s$, $B_{\sigma(t)}$ is either a complete set of left or right coset representatives of G_t in G_{t-1} for $1 \leq t \leq s$, where $\sigma(t+1)$ satisfies one of the following:

1. $\sigma(t+1) = \sigma(t) - 1$,
2. if $\sigma(t+1) < \sigma(t) - 1$, then $B_{\sigma(t+1)} B_{\sigma(t+1)+1} \cdots B_{\sigma(t)-1} = G_t$,
3. $\sigma(t+1) = \sigma(t) + 1$,
4. if $\sigma(t+1) > \sigma(t) + 1$, then $B_{\sigma(t)+1} B_{\sigma(t)+2} \cdots B_{\sigma(t+1)} = G_t$,

Later we will define a transformation which permutes the blocks of a logarithmic signature. To reduce the chance of confusion, we will use the term *rearrangement* instead of permutation when discussing mixed-transversal logarithmic signatures.

If $[G_{i-1} : G_i] = r_i$, then an exact transversal logarithmic signature with rearrangement σ has type $r = \big(r_{\sigma(1)}, \ldots, r_{\sigma(s)}\big)$.

The definition is simpler than it looks. An example will help illuminate. Let

$$G = G_0 > G_1 > G_2 > G_3 > G_4 > G_5 = 1$$

be a chain of subgroups, and let

$$G = G_1B_1 = (B_2G_2)B_1 = B_2(B_3G_3)B_1 = B_2B_3(G_4B_4)B_1 = B_2B_3B_5B_4B_1,$$

where each B_i is a complete set of left or right coset representatives for G_i in G_{i-1}. Then $\{B_2, B_3, B_5, B_4, B_1\}$ is an exact mixed-transversal logarithmic signature for G with rearrangement $(2, 3, 5, 4, 1)$.

It may be helpful to notice that if β is exact-mixed transversal with $B_j = G_{s-1}$, then B_i is a set of left coset representatives when $i = 1, \dots, j-1$, and B_i is a set of right coset representatives when $i = j+1, \dots, s$. We can think of B_j as a set of either left or right coset representatives.

If a logarithmic signature is exact ℓ-, r-, or mixed-transversal, we say it is *exact transversal*. In fact, an exact ℓ- or r-transversal logarithmic signature is exact mixed-transversal.

In Section 3.2, we define a transformation on exact transversal logarithmic signatures called *sandwiching*, and the result of applying this transformation to a logarithmic signature α is called a *sandwich* of α. We will call a sandwich of an exact transversal logarithmic signature a *transversal logarithmic signature.* Similarly, we define *r-transversal*, *ℓ-transversal*, and *mixed-transversal.*

If a logarithmic signature is not transversal, we shall call it *non-transversal.* A logarithmic signature for which each block is not a coset of a non-trivial subgroup of G is called a *totally non-transversal logarithmic signature.* It is clear that a totally non-transversal logarithmic signature is non-transversal.

There are cases, for instance when G is abelian, when a permutation of the blocks of a logarithmic signature will also result in a logarithmic signature. A logarithmic signature for which some permutation of the blocks produces an exact transversal logarithmic signature is called a *permutably exact transversal logarithmic signature.* A logarithmic signature for which some permutation of the blocks produces a transversal logarithmic signature is called a *permutably transversal logarithmic signature.*[1] If a logarithmic signature is not permutably transversal, we call it a *non-permutably transversal logarithmic signature.*

The last three classes will be invaluable. A logarithmic signature α is called *r-canonical* if $\alpha[i;1] = 1$ for $i = 2, 3, \ldots, s$. A logarithmic signature α is called *ℓ-canonical* if $\alpha[i;1] = 1$ for $i = 1, 2, \ldots, s-1$. A logarithmic signature α is called

[1] An alternative definition for permutably transversal logarithmic signature could be a logarithmic signature that is the sandwich of a permutably exact transversal logarithmic signature. This is not equivalent to our definition, and has several disadvantages.

canonical if $\alpha[i;1] = 1$ for $i = 1, 2, \ldots, s$. In other words, if it is both ℓ- and r-canonical.

Figure 3.1 gives the notations we will use for the various classes of logarithmic signatures we have defined. In the figure, G is a group of order $\prod_{i=1}^{s} r_i$, γ is a chain of subgroups of G, $r = (r_1, \ldots, r_s)$ is a type, and σ is a rearrangement of $1, \ldots, s$. There are several notations we have not included because they don't have a well defined meaning. For instance, $\mathcal{F}(\cdot, \sigma, \cdot)$ and $\mathcal{F}(\cdot, \sigma, r)$ don't make sense because, as we have discussed, we need a chain of subgroups for the concept of rearrangement to have meaning.

Notice that a logarithmic signature is (exact) mixed-transversal if and only if it is (exact) transversal, so we usually omit the modifier *mixed*.

3.2 Logarithmic Signature Transformations

In this section, we will look at different transformations on the set of logarithmic signatures of a group. We are particularly interested in transformations that will produce inequivalent logarithmic signatures, so that we may determine a lower bound on the number of unique permutations $\widehat{\alpha}$ a group will have. We will investigate the properties of the transformations in Section 3.6, giving only definitions and trivial results

Figure 3.1: Logarithmic Signature Class Notations

Symbol	Set of logarithmic signatures of G
Λ,Λ_G	all logarithmic signatures
$\mathcal{EL}$, $\mathcal{ER}$, $\mathcal{E}$	exact ℓ-, r-, and (mixed-)transversal logarithmic signatures
$\mathcal{LT}$, $\mathcal{RT}$, $\mathcal{T}$	ℓ-, r-, and (mixed-)transversal logarithmic signatures
$\mathcal{NT}$	non-transversal logarithmic signatures
$\mathcal{TNT}$	totally non-transversal logarithmic signatures
$\mathcal{PE}$	permutably exact transversal logarithmic signatures
$\mathcal{PT}$	permutably transversal logarithmic signatures
$\mathcal{NPT}$	non-permutably transversal logarithmic signatures
$\mathcal{LC}$, $\mathcal{RC}$, $\mathcal{C}$	ℓ-canonical, r-canonical and canonical logarithmic signatures
$\mathcal{F}_L$, $\mathcal{F}_R$, $\mathcal{F}_C$	$\mathcal{F} \cap \mathcal{LC}$, $\mathcal{F} \cap \mathcal{RC}$, and $\mathcal{F} \cap \mathcal{C}$, where $\mathcal{F}$ is any class
$\mathcal{F}(\cdot, \cdot, r)$	logarithmic signatures of class $\mathcal{F}$ with type r, where $\mathcal{F}$ is any of the classes
$\mathcal{F}(\gamma, \cdot, \cdot)$	logarithmic signatures of class $\mathcal{F}$ with respect to γ, where $\mathcal{F}$ is one of $\mathcal{EL}$, $\mathcal{ER}$, $\mathcal{E}$, $\mathcal{LT}$, $\mathcal{RT}$, or $\mathcal{T}$
$\mathcal{F}(\gamma, \cdot, r)$	logarithmic signatures of class $\mathcal{F}$ of type r with respect to γ, where $\mathcal{F}$ is one of $\mathcal{EL}$, $\mathcal{ER}$, $\mathcal{E}$, $\mathcal{LT}$, $\mathcal{RT}$, or $\mathcal{T}$
$\mathcal{F}(\gamma, \sigma) = \mathcal{F}(\gamma, \sigma, r)$	logarithmic signatures of class $\mathcal{F}$, with respect to γ with rearrangement σ, where $\mathcal{F}$ is $\mathcal{T}$ or $\mathcal{E}$

in this section. The results of this section are generalized from those of Magliveras and Memon [20].

The first transformation involves acting on a logarithmic signature $\alpha \in \Lambda$ by an element $t \in \mathbf{T}$, where

$$\mathbf{T} = G \times \mathcal{S}_n \times \cdots \times \mathcal{S}_n \times G$$

is a direct product with n the degree of $G \leq \mathcal{S}_n$, and the symmetric group $\mathcal{S}_n$ occuring

$s-1$ times. Let $t = (t_0, t_1, \ldots, t_s) \in \mathbf{T}$, and let t act on α by $(t, \alpha) \rightarrow \alpha^t$, where

$$\alpha^t = (t_0^{-1}, \ldots, t_0^{-1}; \ldots; t_{s-1}^{-1}, \ldots, t_{s-1}^{-1}) \cdot \alpha \cdot (t_1, \ldots, t_1; \ldots; t_s, \ldots, t_s).$$

Thus, each elements of block i is multiplied on the left by t_{i-1}^{-1}, and on the right by t_i. It is not hard to see that $\alpha^1 = \alpha$, and $(\alpha^x)^y = \alpha^{xy}$, so $\mathbf{T}$ acts on the collection of logarithmic signatures Λ having s blocks.

We will actually restrict our attention to those transformations in $\mathbf{T}' \subset \mathbf{T}$, where

$$\mathbf{T}' = G \times G \times \cdots \times G \times G.$$

This insures that the elements of α^t will be contained in G.

There are three special cases of this transformation. If $t_0 = t_s = 1$, then α^t is called a *sandwich* of α. Recall that the sandwich of an exact transversal logarithmic signature is called a *transversal logarithmic signature.* If $t_0 = t_1 = \cdots = t_{s-1} = 1$, then α^t is called a *right translation* of α. If $t_1 = t_2 = \cdots = t_s = 1$, then α^t is called a *left translation* of α. For simplicity, when $Gg \in G$, we will talk about right or left translation by g instead of by $t = (1, 1, \ldots, 1, g)$ or $t = (g, 1, \ldots, 1)$. For convenience, we will denote right translation of α by $g \in G$ by αg, and left translation of α by $g \in G$ by $g\alpha$. Notice we abuse the definition slightly for left translation. Technically left translation by g corresponds to multiplying the last block by g^{-1}, not g.

The following theorem, due to Magliveras and Kreher, shows the relationship between the sandwich transformation and equivalent logarithmic signatures, and first appeared in [20].

Theorem 3.1 *Let G be a finite group and α and β two logarithmic signatures of the same type $r = (r_1, \ldots, r_s)$. Then α and β are equivalent if and only if they are sandwiches of each other.*

In other words, a transversal and non-transversal logarithmic signature of the same type cannot be equivalent. In fact, Magliveras and Memon [20] give an algorithm which can determine in polynomial time whether or not a logarithmic signature α is r-transversal or not, and if it is, construct an equivalent exact r-transversal logarithmic signature β. We will show that this is true of all transversal logarithmic signatures.

Let α be a logarithmic signature of G of type $(r_1, \ldots, r_i, r_{i+1}, \ldots, r_s)$. Then we can create a new logarithmic signature α' by *fusing* blocks i and $i+1$ into a single block of length $r_i \cdot r_{i+1}$. More formally, we map the blocks B_j of α to the blocks B'_j of α' as follows:

- For $1 \leq j < i$, $B'_j = B_j$,

- $B'_i = P(B_i \otimes B_{i+1})$, where P is some permutation of the $r_i \cdot r_{i+1}$ elements.

- For $i < j < s$, $B'_j = B_{j+1}$,

Notice that there are $(r_i \cdot r_{i+1})!$ possibilities for the ordering of the elements in block B'_i. We call α a *refinement* of α'.

If

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

is a logarithmic signature, then so is

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

We call α' the *inversion* of α.

It should be clear that reordering the elements within each block of any (transversal or non-transversal) logarithmic signature α will produce a new logarithmic signature. We will call this transformation *element shuffling.* We will discuss the *element shuffling* transformation for non-transversal logarithmic signatures later.

The element shuffle is actually a special case of a the *shuffle* transformation, which can be applied to only transversal logarithmic signatures. We discuss this transformation next.

Let G be a group, $\gamma : G = G_0 > G_1 > \cdots > G_s = 1$ a chain of subgroups, and $\beta = \{B_i : i = 1, \ldots, s\}$ a transversal logarithmic signature of G with respect to γ with rearrangement $\sigma = (i_1, \ldots, i_s)$. Then B_{i_k} is a set of right or left coset representatives of G_k in G_{k-1}, for $k = 1, \ldots, s$. Let B'_{i_k}=$h_{i_k,j} \cdot B(i_k, j)$ (or $B_{i_k} = B(i_k, j) \cdot h_{i_k,j}$) if B_{i_k} is a set of right (or left) coset representatives of G_k in G_{k-1}, where $h_{i_k,j} \in G_{k-1}$. Then the resulting collection $\beta' = \{B'_i : i = 1, \ldots, s\}$ is a new transversal logarithmic signature for G.

This transformation essentially changes the coset representatives of each block, so we call it a *coset shuffle*. When both a *coset shuffle* and *element shuffle* are applied, the transformation is called a *shuffle*. We can formally define the *shuffle* transformation as follows. Recall the rearrangement σ defined for a transversal logarithmic signature β.

Let **M** be the group of elements of the form

$$M = (H_1 \times H_2 \times \cdots \times H_s),$$

where $H_{\sigma(k)}$ is an $r_{\sigma(k)} \times r_{\sigma(k)}$ monomial matrix with entries in G_k. Each $H_{\sigma(k)}$ can be thought of as $r_{\sigma(k)} \times r_{\sigma(k)}$ permutation matrix whose unit entries have been replaced by elements of G_k. Think of each block $B_{\sigma(k)}$ as a row vector. Then M acts on β by

$$\beta' = \beta^M = \{B_i^{H_i} : i = 1, \ldots, s\},$$

where $B_{\sigma(k)}^{H_{\sigma(k)}} = H_{\sigma(k)} B_{\sigma(k)}^T$, if $B_{\sigma(k)}$ is a set of right coset representatives of G_k in

G_{k-1}, and $B_{\sigma(k)}^{H_{\sigma(k)}} = B_{\sigma(k)}H_{\sigma(k)}^T$, if $B_{\sigma(k)}$ is a set of left coset representatives of G_k in G_{k-1}. It is clear that $B_{\sigma(k)}^{H_{\sigma(k)}}$ is still a set of coset representatives.

An example will be useful at this point. As before, let

$$G = G_0 > G_1 > G_2 > G_3 > G_4 > G_5 = 1$$

be a chain of subgroups, and

$$G = G_1B_1 = (B_2G_2)B_1 = B_2(B_3G_3)B_1 = B_2B_3(G_4B_4)B_1 = B_2B_3B_5B_4B_1,$$

where each B_i is a complete set of left or right coset representatives for G_i in G_{i-1}, and $B_5 = G_4$. Then $\beta = \{B_2, B_3, B_5, B_4, B_1\}$ is an exact mixed-transversal logarithmic signature for G. If $M = (H_2, H_3, H_5, H_4, H_1)$, then

$$\beta^M = \{B_2H_2^T, B_3H_3^T, B_5H_5^T, H_4B_4^T, H_1B_1^T\}.$$

Lemma 3.1 *The action of* $\mathbf{M}$ *on* $\mathcal{T}(\gamma, i)$ *is regular.*

Proof. Let $\alpha = \{A_1, \ldots, A_s\}, \beta = \{B_1, \ldots, B_s\} \in \mathcal{T}(\gamma, i)$. Since the blocks A_i and B_i only differ in the choice of coset representatives and the order in which the coset representatives are listed, we can find an H_i such that $A_i^{H_i} = B_i$. Thus, $\mathbf{M}$ is transitive. This, along with the fact that $\beta^{M_1} = \beta^{M_2}$ if and only if $M_1 = M_2$ gives the result. □

Thus,

$$|\mathcal{T}(\gamma, i)| = |\mathbf{M}| = \prod_{i=1}^{s} |G_{s-i+1}|^{r_i} r_i! = \prod_{i=1}^{s} \left(\prod_{j=i+1}^{s} r_j \right)^{r_i} r_i!$$

Notice that when G is abelian, then permuting the blocks of a logarithmic signature always produces a logarithmic signature. In general, we can apply this transformation to logarithmic signatures of any group G, resulting in pseudo-logarithmic signatures. We call this transformation a *block shuffle.* We are particularly interested in the cases when the result of a block shuffle is indeed a logarithmic signature. From our definition, it is clear that a logarithmic signature is permutably transversal if and only if it is a block shuffle of a transversal logarithmic signature.

3.3 Canonical Logarithmic Signatures

It turns out we can restrict our attention to the canonical logarithmic signatures when we are concerned about the permutations they induce. We start with an important theorem.

Theorem 3.2 *Let α be a logarithmic signature of G of type r. Then there exists a unique equivalent ℓ-canonical logarithmic signature of type r, and a unique equivalent r-canonical logarithmic signature of type r. In other words, if a permutation in $\mathcal{S}_{|G|}$ has a logarithmic signature corresponding to it, then it has unique ℓ-canonical and*

r-canonical logarithmic signatures corresponding to it.

Proof. The following algorithm produces an r-canonical logarithmic signature as a sandwich of the given logarithmic signature.

```
for  $(i = s; i > 1; i = i - 1)$
     $x = A(i, 1)$
     $A_i = A_i \times x^{-1}$
     $A_{i-1} = A_{i-1} \times x$
```

At each step the selected element x is the unique element that can result in the identity being placed in the first position of block i. Since sandwiching is the only way to produce an equivalent logarithmic signature of the same type, the resulting logarithmic signature is the unique r-canonical logarithmic signature equivalent to α. The proof is similar for the ℓ-canonical case. □

Corollary 3.1 *A logarithmic signature is ℓ-transversal (r-transversal) if and only if the equivalent ℓ-canonical (r-canonical) logarithmic signature is exact ℓ-transversal (r-transversal).*

We will prove the analogous result for transversal logarithmic signatures in Section 3.5. The following is an easy corollary to Theorem 3.2.

Corollary 3.2 *Let G be a group of order $\prod_{i=1}^{s} r_i$, and let $r = (r_1, \ldots, r_s)$. Then*

1. $|\widehat{\mathcal{RC}}(\cdot, \cdot, r)| = |\mathcal{RC}(\cdot, \cdot, r)| = |\widehat{\mathcal{LC}}(\cdot, \cdot, r)| = |\mathcal{LC}(\cdot, \cdot, r)|,$

2. $|\widehat{\mathcal{C}}(\cdot,\cdot,r)| = |\mathcal{C}(\cdot,\cdot,r)|$, *and*

3. $\widehat{\mathcal{F}_R}(\cdot,\cdot,r) = \widehat{\mathcal{F}_L}(\cdot,\cdot,r) = \widehat{\mathcal{F}}(\cdot,\cdot,r)$, *where* $\mathcal{F}$ *is any class closed under the sandwich transformation.*

The last statement says that the set of permutations obtainable from logarithmic signatures is the same as the set obtainable from just ℓ-canonical or r-canonical logarithmic signatures. Notice that $\widehat{\mathcal{C}}(\cdot,\cdot,r)$ is the set of permutations in $\widehat{\Lambda}(\cdot,\cdot,r)$ which fix 1.

It was mentioned earlier that restricting to logarithmic signatures whose entries were in G was not a problem. It turns out that the concept of ℓ-canonical and r-canonical makes this easy to show.

Theorem 3.3 *Let* $G \leq \mathcal{S}_n$*, and* α *a logarithmic signature of* G *with elements from* $\mathcal{S}_n$*. Then there exists a logarithmic signature* β *of* G *with element from* G *such that* $\widehat{\alpha} = \widehat{\beta}$*.*

Proof. Let β be the r-canonical logarithmic signature equivalent to α. Then since blocks 2 through s contains the identity, the elements of the first block must be contained in G. Since blocks 3 through s contain the identity, and the elements of the first block are in G, the elements of the second block must be in G. Continuing in this fashion, it is clear that every element of β is contained in G. □

We will discuss canonical logarithmic signatures more fully in Section 3.8

3.4 Exact Transversal Logarithmic Signatures

Recall the assumptions we made in the introduction. A permutation group G is assumed to be given by a number of generators polynomial in the degree. In fact, every permutation group of degree n can be generated by at most n^2 generators [3]. We also assume that when we have a chain of subgroups, $\gamma : G = G_0 > G_1 > \ldots > G_s = 1$, that for $i = 1, \ldots, s$, $[G_{i-1} : G_i]$ is bounded by a polynomial in n.

Let G be a permutation group which acts on the set $X = \{1, 2, \ldots, n\}$, and let $\gamma : G = G_0 > G_1 \ldots > G_s = 1$ be a chain of nested stabilizers in G. That is, the subgroup G_i fixes pointwise the letters $1, 2, \ldots, i$. The following was shown in [8].

Theorem 3.4 *Let G be a permutation group which acts on the set $X = \{1, 2, \ldots, n\}$, and let $\gamma : G = G_0 > G_1 \ldots > G_s = 1$ be a chain of nested stabilizers in G. Then there is a polynomial-time algorithm for building a logarithmic signature in $\mathcal{ER}(\gamma, \cdot, \cdot)$.*

As the next theorem shows, an exact transversal logarithmic signature with respect to a stabilizer chain γ is supertame. We give the proof for exact r-transversal logarithmic signatures, but it is easy to see that it can be modified for transversal logarithmic signatures in general, assuming the rearrangement σ is known. We will show in the next section that there is a polynomial-time algorithm to compute this rearrangement.

Theorem 3.5 *Let G be a permutation group which acts on the set $X = \{1, 2, \ldots, n\}$, let $\gamma : G = G_0 > G_1 > \ldots > G_s = 1$ be a chain of nested stabilizers in G, and let α be an exact transversal logarithmic signature with respect to γ. Then α is supertame.*

Proof. By Theorem 2.1, the orbit of of i under G_{i-1} has size $|G_{i-1}|/|G_i| = r_i$. Let $\{\delta_1 = i, \delta_2, \ldots, \delta_{r_i}\}$ be the orbit of i under G_{i-1}. We can write

$$G_{i-1} = G_i\alpha[i;1] + \ldots + G_i\alpha[i;r_i].$$

Let $x \in G_{i-1}$ move i to δ_j. Then $x \in G_i\alpha[i;k]$, for some k, and $\alpha[i;k]$ also moves i to j. Since this is true for every $j = 1, \ldots, r_i$, and since each $\alpha[i;j]$ can only move i to one value, the $\alpha[i;j]$ must each take i to a different δ_j. Then, after relabeling the δ_j, we can write

$$G_{i-1} = G_i\alpha[i;1] + \ldots + G_i\alpha[i;r_i],$$

where $\alpha[i;j]$ moves i to δ_j. Thus, $x \in G_{i-1}$ belongs to the coset $G_i\alpha[i;j]$ if and only if x moves i to δ_j. The correct coset can be found in time $O(r_i) = O(n)$.

Notice that $y = \alpha[i;j]^{-1} \cdot x$ fixes $1, \ldots, i$, so y belongs to G_i, and we can find the coset of G_{i+1} to which y belongs in the same manner. The product $\alpha[i;j]^{-1}x$ can be computed in $O(n)$ steps.

Now, given $g \in G$, we can descend the stabilizer chain as above and compute $x\alpha[s;j_s]^{-1} \cdots \alpha[2;j_2]^{-1}\alpha[1;j_1]^{-1} = 1$. Solving for x yields $x = \alpha[1;j_1] \cdots \alpha[s;j_s]$. Since the stabilizer chain has depth at most n, and at most $O(n)$ work is done at each level, the factorization can be found in time $O(n^2)$. Thus α is supertame. □

Theorems 3.4 and 3.5 yield the following result.

Corollary 3.3 *Let G be a permutation group of degree n, and $x \in \mathcal{S}_n$. Then there is a polynomial time algorithm to determine whether or not $x \in G$.*

Corollary 3.4 *Let G be a permutation group of degree n, and $x, y \in \mathcal{S}_n$. Then there is a polynomial time algorithm to determine whether or not $x \in G\,y$.*

Proof. Since $x \in G\,y$ is equivalent to $x \cdot y^{-1} \in G$, this follows from Corollary 3.3. □

There is actually a polynomial-time algorithm to build an exact transversal logarithmic signature with respect to any subgroup chain γ (not just a stabilizer chain). In general, exact transversal logarithmic signatures are tame, as we show next. Again, the proof is given for r-transversal logarithmic signatures.

Theorem 3.6 *Let G be a permutation group, $\gamma : G = G_0 > G_1 > \cdots > G_s = 1$ a chain of subgroups, and α an exact transversal logarithmic signature with respect to γ. Then α is tame.*

Proof. To find the factorization of $x \in G$, we first determine which coset $G_1\,\alpha[1; j]$ x belongs to, which can be done in polynomial time by Corollary 3.4 and by the fact that $\alpha[1]$ has a polynomial number of entries. To proceed, we calculate $y = \alpha[1; j]^{-1}x$, which can be done in time $O(n)$, and recursively find the factorization of y in G_1. In the end, we will have $x \cdot \alpha[s; j_s]^{-1} \cdots \alpha[1; j_1]^{-1} = 1$, which we can solve for x to obtain $x = \alpha[1; j_1] \cdots \alpha[s; j_s]$, the desired factorization. The chain has depth at most n, each requiring a polynomial amount of work. Thus, the factorization can be done in polynomial time, so α is tame. $\square$

Given the results of this section, it should be clear that, given a polynomial number of generators for a group G, we can determine the order of G and membership in G in polynomial time. We will need these facts in the next section.

3.5 Transversal Logarithmic Signatures

In the last section, we saw that exact transversal logarithmic signatures are in general tame. This section is devoted to two more general results. First, we can "recognize" a transversal logarithmic signature in polynomial time, and second, transversal logarithmic signatures are tame.

We start with an algorithm that determines whether or not a given logarithmic signature is exact transversal. In fact, the algorithm gives the rearrangement σ of indices. There is an obvious algorithm to solve the problem in time proportional to $s!$ (try all possible orderings), but this is not efficient. We develop an efficient dynamic programming solution.

Let $\langle A_{i_1}, \ldots, A_{i_k} \rangle$ denote the subgroup generated by the collection of elements in blocks A_{i_1} through A_{i_k}. Then $\alpha = \{A_i : i = 1, \ldots, s\}$ is an exact transversal logarithmic signature for G if and only if $\langle A_{i_1}, \ldots, A_{i_k} \rangle = G_{s-k}$ for each $k = 1, \ldots, s$.

Now, for $1 \leq i \leq j \leq s$, we define

$$M[i,j] = \begin{cases} 1 & \text{if } A_i, \ldots, A_j \text{ is an exact transversal} \\ & \text{logarithmic signature for } \langle A_i, \cdots, A_j \rangle, \\ 0 & \text{otherwise.} \end{cases}$$

If $M[1,s] = 1$, then α is exact transversal. Given M, we can easily compute the subgroup chain, as we will see. To compute M, we start by noticing that $M[i,i] = 1$ if and only if A_i is a subgroup. Then in general,

$$M[i,j] = \begin{cases} 1 & \text{if either } M[i,j-1] = 1 \text{ or } M[i+1,j] = 1, \\ & \text{and } \langle A_i, \cdots, A_j \rangle \text{ is a subgroup of order } r_i \cdots r_j \\ 0 & \text{otherwise.} \end{cases}$$

We can determine the order of $\langle A_i, \cdots, A_j \rangle$ in polynomial time by the methods mentioned in the last section, so given $M[i+1,j]$ and $M[i,j-1]$, we can compute $M[i,j]$ in polynomial time. Since we need to compute about s^2 values, where s is polynomial, this gives a polynomial-time algorithm to determine whether or not a logarithmic signature is exact transversal.

The algorithm to compute the chain is not hard to see. We know $M[1,s] = 1$, and at least one of $M[2,s]$ and $M[1,s-1]$ is 1. Therefore, either $\langle A_2, \cdots, A_s \rangle$ is a subgroup and A_1 a set of coset representatives, or $\langle A_1, \cdots, A_{s-1} \rangle$ is a subgroup and A_s a set of coset representatives. From this we determine i_s, and continue with either $M[2,s]$ or $M[1,s-1]$ with the same method to find $i_{s-1}, \ldots, i_1$.

Since we can find the rearrangement σ in polynomial time, exact transversal logarithmic signatures are tame by the method given in the last section. We now turn to showing that transversal logarithmic signatures are recognizable. Notice that by definition, given a transversal logarithmic signature β, there exists an equivalent exact transversal logarithmic signature α.

Lemma 3.2 *Let G be a group, and $\gamma : G = G_0 > G_1 > \cdots > G_s = 1$ be a chain of subgroups of G. Let $\beta \in \mathcal{T}(\gamma, \cdot, \cdot)$, and $\alpha \in \mathcal{E}(\gamma, \cdot, \cdot)$ such that $\widehat{\alpha} = \widehat{\beta}$. If $\alpha[i] \cdots \alpha[i+k-1] = G_{s-k}$, then $\beta[i] \cdots \beta[i+k-1] = hG_{s-k}^g$, for some $g, h \in G$. Consequently, if $1 \in \beta[i] \cdots \beta[i+k-1]$, then $\beta[i] \cdots \beta[i+k-1] = G_{s-k}^g$, for some*

$g \in G$.

Proof. Notice that for each $j \in \{1, \ldots, s\}$, $\beta[j] = g_{j-1}^{-1}\alpha[j]g_j$, for some $g_j \in G$, where $g_0 = g_s = 1$. Thus

$$\begin{aligned}
\beta[i]\cdots\beta[i+k-1] &= g_{i-1}^{-1}\alpha[i]g_i g_i^{-1}\alpha[i+1]\cdots g_{i+k-2}^{-1}\alpha[i+k-1]g_{i+k-1} \\
&= g_{i-1}^{-1}\alpha[i]\cdots\alpha[i+k-1]g_{i+k-1} \\
&= g_{i-1}^{-1}G_{s-k}g_{i+k-1} \\
&= g_{i-1}^{-1}g_{i+k-1}g_{i+k-1}^{-1}G_{s-k}g_{i+k-1} = g_{i-1}^{-1}g_{i+k-1}G_{s-k}^{g_{i+k-1}} \\
&= hG_{s-k}^{g},
\end{aligned}$$

where $h = g_{i-1}^{-1}g_{i+k-1}$, and $g = g_{i+k-1}$. Since a coset is a subgroup if and only if it contains the identity, the second statement follows. □

Lemma 3.3 *Let G be a group, and $\gamma : G = G_0 > G_1 > \cdots > G_s = 1$ be a chain of subgroups of G. Let $\beta \in \mathcal{T}(\gamma, \cdot, \cdot)$, and $\alpha \in \mathcal{E}(\gamma, \cdot, \cdot)$ such that $\widehat{\alpha} = \widehat{\beta}$.*

If $\alpha[1]\cdots\alpha[s-1] = G_1$, and $1 \in \beta[i]$ for $i = 1, \ldots, s-1$, then $\beta \in \mathcal{E}(\gamma', \cdot, \cdot)$, where γ' is a conjugate chain of γ.

If $\alpha[2]\cdots\alpha[s] = G_1$, and $1 \in \beta[i]$ for $i = 2, \ldots, s$, then $\beta \in \mathcal{E}(\gamma', \cdot, \cdot)$, where γ' is a conjugate chain of γ.

Proof. For each $k = 1, \ldots, s-1$, $G_{s-k} = \alpha[i] \cdots \alpha[i+k-1]$ for some i. By Lemma 3.2, $B_i \cdots B_{i+k-1} = G_{s-k}^g$ for some $g \in G$. Therefore, $\beta \in \mathcal{E}(\gamma', \cdot, \cdot)$, a conjugate chain. □

Corollary 3.5 *Let G be a group, and $\gamma : G = G_0 > G_1 > \cdots > G_s = 1$ be a chain of subgroups of G. Let $\beta \in \mathcal{T}(\gamma, \cdot, \cdot)$, α_l be the equivalent ℓ-canonical logarithmic signature, and α_r be the equivalent r-canonical logarithmic signatureto β. Then at least one of α_l and α_r is exact transversal.*

Proof. Let α be the equivalent exact transversal logarithmic signature to β. Clearly it is also equivalent to α_l and α_r. Since α is exact transversal, either $\alpha[1] \cdots \alpha[s-1] = G_1$, or $\alpha[2] \cdots \alpha[s] = G_1$ If $\alpha[1] \cdots \alpha[s-1] = G_1$, then by Lemma 3.3, α_r is exact transversal. If $\alpha[2] \cdots \alpha[s] = G_1$, then by Lemma 3.3, α_l is exact transversal. □

Given a logarithmic signature, in polynomial-time we can determine whether or not it is transversal. In addition, given a transversal logarithmic signature α, we can compute the unique r-canonical or ℓ-canonical logarithmic signature equivalent to α in polynomial time. This establishes the fact that transversal logarithmic signatures are tame.

We will conclude this section with a few examples to help illustrate some of the concepts. Let $G = Z_8 = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = 1\}$.

Consider the following logarithmic signatures for G.

$$\alpha = \{(1, a), (1, a^4), (1, a^2)\}$$

$$\beta = \{(1, a^4), (1, a), (1, a^2)\}$$

$$\delta = \{(1, a, a^4, a^5), (1, a^2)\}$$

It is straightforward to check that each of α, β, and δ is indeed a logarithmic signature for G. Since $(1, a^4)$ and $(1, a^4) \otimes (1, a^2) = (1, a^2, a^4, a^6)$ are both subgroups, α is exact transversal with rearrangement $\sigma = (1, 3, 2)$,

Since neither $(1, a^4) \otimes (1, a) = (1, a, a^4, a^5)$ nor $(1, a) \otimes (1, a^2) = (1, a^2, a, a^3)$ is a subgroup of G, β is not exact transversal. Since β is canonical (and therefore ℓ-canonical and r-canonical), β is not transversal either. It is permutably exact transversal, however, since we can permute the first and second blocks to obtain α.

Neither block of δ is a subgroup, or even a coset (since each contains the identity, this is clear). Thus, δ is totally non-transversal. It may be interesting to note that Z_8 is the smallest group which has a totally non-transversal logarithmic signature.

Let $\alpha = \{(a^6, a^5), (a^5, a), (a^6, 1)\}$. Then

$$(a^6, a^5) \otimes (a^5, a) \otimes (a^6, 1) = (a^3, a^7, a^2, a^6) \otimes (a^6, 1) = (a, a^5, 1, a^4, a^3, a^7, a^2, a^6),$$

so α is a logarithmic signature for G. To see if α is transversal we compute the r-canonical and ℓ-canonical equivalents. We first compute the ℓ-canonical equivalent:

$$\begin{aligned}\{(a^6,a^5),(a^5,a),(a^6,1)\} &\rightarrow \{(a^6,a^5)a^2,a^6(a^5,a),(a^6,1)\} = \{(1,a^7),(a^3,a^7),(a^6,1)\}\\ &\rightarrow \{(1,a^7),(a^3,a^7)a^5,a^3(a^6,1)\} = \{(1,a^7),(1,a^4),(a,a^3)\}\end{aligned}$$

Thus, $\alpha_l = \{(1,a^7),(1,a^4),(a,a^3)\}$. Only $(1,a^4)$ is a subgroup, and neither $(1,a^7)\otimes(1,a^4) = (1,a^4,a^7,a^3)$ nor $(1,a^4)\otimes(1,a^3) = (1,a^3,a^4,a^7)$ is a subgroup, so α_l is not exact transversal. Now we compute the r-canonical equivalent:

$$\begin{aligned}\{(a^6,a^5),(a^5,a),(a^6,1)\} &\rightarrow \{(a^6,a^5),(a^5,a)a^6,a^2(a^6,1)\} = \{(a^6,a^5),(a^3,a^7),(1,a^2)\}\\ &\rightarrow \{(a^6,a^5)a^3,a^5(a^3,a^7),(1,a^2)\} = \{(a,1),(1,a^4),(1,a^2)\}\end{aligned}$$

So the r-canonical equivalent of α is $\alpha_r = \{(a,1),(1,a^4),(1,a^2)\}$. Notice that $(1,a^4)$ and $(1,a^4)\otimes(1,a^2) = (1,a^2,a^4,a^6)$ are both subgroups, so α_r is exact transversal with rearrangement $(1,3,2)$. Since α is a sandwich of α_r, α is transversal.

3.6 Properties of Transformations

As before, in this section, we assume a fixed η, and when $F \subseteq \Lambda$, we write $\widehat{F}= \{\widehat{\alpha} : \alpha \in F\}$. From what we have seen previously, it is easy to see that $\widehat{\mathcal{T}} = \widehat{\mathcal{E}}$. The sets $\widehat{\mathcal{T}}$ and $\widehat{\Lambda}$ are of interest, as are the groups $\mathcal{G}_{\mathcal{T}} = \langle\widehat{\mathcal{T}}\rangle \subseteq \mathcal{S}_{|G|}$ and $\mathcal{G}_{\Lambda} = \langle\widehat{\Lambda}\rangle \subseteq \mathcal{S}_{|G|}$.

It is clear that $\mathcal{G}_{\mathcal{T}} \subseteq \mathcal{G}_{\Lambda} \subseteq \mathcal{S}_{|G|}$, but whether or not equality holds is not known for every group. However, the following result, due to Magliveras and Memon [20], shows that in almost all cases, $\mathcal{G}_{\mathcal{RT}} = \mathcal{G}_{\Lambda} = \mathcal{S}_{|G|}$.

Theorem 3.7 *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, and 276, where q is a prime power and n is a positive integer, then $\widehat{\mathcal{T}}$ is 2-transitive and $\mathcal{G}_{\mathcal{RT}} = \mathcal{S}_{|G|}$.*

Although this is a very strong result, there is room for improvement. For instance, there are many groups which do not satisfy the necessary conditions, and the structures of $\widehat{\mathcal{T}}$, $\widehat{\Lambda}$, etc, are also of interest.

Experimental results suggest that, unless $G = Z_{p^2}$, then $\langle \mathcal{RT} \rangle = \mathcal{S}_{|G|}$, and that $\langle \mathcal{T} \rangle = \mathcal{S}_{|G|}$ for all groups G. In fact, experiments with small groups suggest that given a single transversal logarithmic signature α, α and it's inversion generate $\mathcal{S}_{|G|}$ quite often.

The next several sections examine in more detail the transformations discussed in Section 3.2. In particular, we are interested in whether or not the transformations leave each of the classes of logarithmic signatures we have defined invariant, and when transformations produce inequivalent logarithmic signatures.

3.6.1 Inversion

Although inversion is in some sense a mundane transformation, it allows us to treat r-transversal and ℓ-transversal logarithmic signatures in the same manner. Since inversion sends left (right) cosets to right (left) cosets, inversion of an r-transversal logarithmic signature is an ℓ-transversal logarithmic signature. Thus, inversion defines a mapping between $\mathcal{RT}$ and $\mathcal{LT}$. It not hard to see that inversion preserves the classes $\mathcal{T}$, $\mathcal{PT}$, $\mathcal{NT}$, and $\mathcal{TNT}$.

Some experimental results relating to the inversion transformation proved interesting. Given a random transversal logarithmic signature α, and it's inversion α_I, it is often the case that

$$\langle \widehat{\alpha}, \widehat{\alpha_I} \rangle = \mathcal{S}_{|G|}.$$

The relationship between $\widehat{\alpha}$ and $\widehat{\alpha_I}$ is not immediately apparent, although further analysis may shed some light on the situation.

3.6.2 Sandwich

According to Theorem 3.1, the sandwich transformation always produces an equivalent logarithmic signature, which, by definition, is r-transversal, ℓ-transversal, or transversal, if and only if the original one is. Also, it is not hard to see that the sandwich transformation preserves the totally non-transversal property, since if $L \subseteq G$ is a coset, then so is gL or Lg for any $g \in G$.

Thus, sandwiching preserves the classes $\mathcal{RT}$, $\mathcal{LT}$, $\mathcal{T}$, $\mathcal{NT}$, and $\mathcal{TNT}$. The sandwich transformation does not preserve the class $\mathcal{PT}$, as we will see in Section 3.7.

3.6.3 Element and Coset Shuffle

We will start with the *element shuffle* transformation. It should be clear that the element shuffle transformation preserves all of the classes of logarithmic signatures we defined earlier.

We will define this transformation more formally, and show that, given a logarithmic signature α, the set of permutations corresponding to *element shuffles* of α forms a coset of a certain group in $\mathcal{S}_{|G|}$.

Let G be a group of order $m = \prod_{i=1}^{s} r_i$, and α be a logarithmic signature of type $r = (r_1, r_2, \ldots, r_s)$, Let $\Psi_r = \mathcal{S}_{r_1} \times \mathcal{S}_{r_2} \times \cdots \times \mathcal{S}_{r_s}$, where each group $\mathcal{S}_{r_i}$ acts on the set $\{1, \ldots, r_i\}$. In other words, $\psi = (\psi_1, \ldots, \psi_s) \in \Psi_r$ acts as a permutation in $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$ by $\psi(p_1, \ldots, p_s)$=$(\psi_1(p_1), \ldots, \psi_s(p_s))$.

Define $\widehat{\psi} = \lambda^{-1}\psi\lambda$. Then $\widehat{\psi} \in \mathcal{S}_m$, and we can define $\widehat{\Psi}_r = \{\widehat{\psi} : \psi \in \Psi_r\} \subseteq \mathcal{S}_m$. It is clear that $\widehat{\Psi}_r$ is a subgroup of $\mathcal{S}_m$.

Theorem 3.8 *Let $m = \prod_{i=1}^{s} r_i$, and let $r = (r_1, r_2, \ldots, r_s)$. Let $\psi, \theta \in \Psi_r$. Then $\widehat{\psi\theta} = \widehat{\psi}\widehat{\theta}$. Consequently, $\widehat{\Psi}_r \leq \mathcal{S}_m$.*

Proof. The statement follows since

$$\widehat{\psi}\widehat{\theta} = (\lambda^{-1}\psi\lambda)(\lambda^{-1}\theta\lambda) = \lambda^{-1}\psi\theta\lambda = \widehat{\psi\theta}.$$

□

Let $\psi = (\psi_1, \psi_2, \ldots, \psi_s) \in \Psi_r$ act on α by $(\psi, \alpha) \to \alpha_\psi$, where

$$\alpha_\psi = (\alpha[1, \psi_1(1)], \ldots, \alpha[1, \psi_1(r_1)]; , \ldots ; \alpha[s, \psi_s(1)], \ldots, \alpha[s, \psi_s(r_s)]).$$

In other words, ψ permutes the elements within each block of the logarithmic signature. Since $\alpha_1 = \alpha$, and $(\alpha_\psi)_\phi = \alpha_{\psi\phi}$, Ψ_r acts on the collection of logarithmic signatures of G having type $(r_1, \ldots, r_s)$.

Notice that for $p \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$,

$$\begin{aligned}
\Theta_\alpha(\psi(p)) &= \Theta_\alpha(\psi_1(p_1), \ldots, \psi_s(p_s)) \\
&= \alpha[s; \psi_s(p_s)] \cdots \alpha[1; \psi_1(p_1)] \\
&= \alpha_\psi[s; p_s] \cdots \alpha_\psi[1; p_1] = \Theta_{\alpha_\psi}(p).
\end{aligned}$$

Therefore, $\psi\Theta_\alpha = \Theta_{\alpha_\psi}$. An important consequence of this is the following.

Theorem 3.9 *Let G be a group of order $m = \prod_{i=1}^{s} r_i$, α be a logarithmic signature of type $r = (r_1, r_2, \ldots, r_s)$, and $\psi \in \Psi_r$. Then $\widehat{\alpha}_\psi = \widehat{\psi}\widehat{\alpha}$.*

Proof. In light of the previous discussion, it is not hard to see that

$$\begin{aligned} \widehat{\alpha}_\psi &= \breve{\alpha}_\psi \breve{\eta}^{-1} = \lambda^{-1}\Theta_{\alpha_\psi}\breve{\eta}^{-1} \\ &= \lambda^{-1}\psi\Theta_\alpha\breve{\eta}^{-1} = \lambda^{-1}\psi\lambda\lambda^{-1}\Theta_\alpha\breve{\eta}^{-1} \\ &= \widehat{\psi}\breve{\alpha}\breve{\eta}^{-1} = \widehat{\psi}\widehat{\alpha} \end{aligned}$$

□

Corollary 3.6 *Let G be a group of order $m = \prod_{i=1}^{s} r_i$, and let $r = (r_1, r_2, \ldots, r_s)$. Then $\widehat{\mathcal{F}}(\cdot,\cdot,r) = \widehat{\Psi_r}\widehat{\mathcal{F}}(\cdot,\cdot,r)$, where $\mathcal{F}$ is any of the classes of logarithmic signatures defined earlier. In other words, $\widehat{F}(\cdot,\cdot,r)$ is the union of right cosets of $\widehat{\Psi_r}$.*

Proof. That $\widehat{\mathcal{F}}(\cdot,\cdot,r) \subseteq \widehat{\Psi_r}\widehat{\mathcal{F}}(\cdot,\cdot,r)$ is clear. If $\alpha \in \mathcal{F}$, and $\psi \in \Psi_r$, then $\widehat{\psi}\widehat{\alpha} = \widehat{\alpha}_\psi \in \widehat{F}$ by Theorem 3.9, and the fact that the shuffle preserves the class $\mathcal{F}$. □

When discussing coset shuffles, we are obviously discussing logarithmic signatures in $\mathcal{T}(\gamma,\sigma)$ for some chain of subgroups γ and rearrangement σ. It is obvious that a shuffle (coset shuffle and element shuffle) will remain transversal, and does not apply to the other classes of logarithmic signatures.

We have already seen that $|\mathcal{T}(\gamma,\sigma)|$ can easily be computed, but what about $|\widehat{\mathcal{T}}(\gamma,\sigma)|$? Given the concept of ℓ-canonical and r-canonical logarithmic signatures, this is easy to compute.

Consider the class $\mathcal{T}(\gamma,\sigma)$ of transversal logarithmic signatures. Either $\sigma(1) = 1$, and the first block corresponds to the coset representatives for G_1 in G_0, or $\sigma(1) = s$, and the last block corresponds to the coset representatives for G_1 in G_0. In the first case, the r-canonical equivalent to a transversal logarithmic signature is exact-transversal, and in the second, the ℓ-canonical equivalent to a transversal logarithmic signature is exact-transversal. Without loss of generality, we assume the first case for the remainder of this section.

Let $\alpha \in \mathcal{T}(\gamma,\sigma)$, and β be the equivalent r-canonical logarithmic signature. Then the number of inequivalent shuffles α is the number of shuffles of β which are r-canonical. Since a shuffle only permutes elements, and changes coset representatives, it is not hard to see that a shuffle of β is r-canonical if and only if it leaves the entries $\beta[i;1] = 1$ invariant for $i = 2, \ldots s$.

When H is a matrix, define

$$H' = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & H & \\ 0 & & & \end{bmatrix}.$$

Let H_1 be an $r_1 \times r_1$ monomial matrix with entries in G_1, and for $k = 2, \ldots, s$ let $H_{\sigma(k)}$ be an $(r_{\sigma(k)} - 1) \times (r_{\sigma(k)} - 1)$ monomial matrix with entries in G_k. Then the set $\mathbf{M}'$ of elements of the form

$$M' = (H_1 \times H_2' \times \cdots \times H_s')$$

is a subgroup of $\mathbf{M}$. It is now straightforward to observe that $\mathbf{M}'$ is precisely the subgroup that preserves the r-canonical property. Thus, we have the following.

Theorem 3.10 *Let G be a group of order $m = \prod_{i=1}^{s} r_i$, $\gamma : G = G_0 > G_1 > \cdots > G_s = 1$ be a chain of subgroups such that $[G_{i-1} : G_i] = r_i$, and σ be a rearrangement of $1, \ldots, s$. Then*

$$|\widehat{\mathcal{T}}(\gamma, \sigma)| = \prod_{j=1}^{s} \left[(r_{\sigma(j)})! \left(\prod_{k=j+1}^{s} r_{\sigma(k)} \right)^{r_{\sigma(j)}-1} \right].$$

Proof. From the previous discussion, it is clear that $|\widehat{\mathcal{T}}(\gamma, \sigma)| = |\mathbf{M}'|$. The size of H_1 is $r_1! \times |G_1|$, and the size of $H_{\sigma(j)} = (r_{\sigma(j)} - 1)! \times |G_j|$. Noticing that $|G_j| = \prod_{k=j+1}^{s} r_{\sigma(k)}$, and doing a little algebra yields the result. □

We have previously seen a formula for $|\mathcal{T}(\gamma, \sigma)|$, and now we have a nice formula for $|\widehat{\mathcal{T}}(\gamma, \sigma)|$. In fact, we know how to obtain every member of both $\mathcal{T}(\gamma, \sigma)$ and $\widehat{\mathcal{T}}(\gamma, \sigma)$.

Given the results about $\mathcal{T}(\gamma,\sigma)$ and $\widehat{\mathcal{T}}(\gamma,\sigma)$, we can prove a few easy results pertaining to $\mathcal{T}(\gamma,\cdot,r)$ and $\mathcal{T}(\gamma,\cdot,\cdot)$. We will start by formally defining two sets which relate types and rearrangements. Let $\gamma : G = G_0 > G_1 > \cdots > G_s = 1$ be a chain of subgroups of G, such that $[G_{i-1} : G_i] = r_i$, and $t = (t_1, \ldots, t_s) = \sigma(r)$ be some rearrangement of $r = (r_1, \ldots, r_s)$. Define

$$\sigma_t = \{\sigma : \sigma \in \mathcal{S}_s \text{ and } t = (r_{\sigma(1)}, \ldots, r_{\sigma(s)})\}, \text{ and}$$

$$r_\sigma = \{(r_{\sigma(1)}, \ldots, r_{\sigma(s)}) : \sigma \in \mathcal{S}_s\}.$$

Essentially, σ_t is the set of rearrangements of t which yield type r, and r_σ is the set of every rearrangement of $r = (r_1, \ldots, r_s)$. Then

$$\mathcal{T}(\gamma,\cdot,r) = \cup_{\sigma\in\sigma_r}\mathcal{T}(\gamma,\sigma).$$

Also, we can see that

$$\mathcal{T}(\gamma,\cdot,\cdot) = \cup_{r\in r_\sigma}\mathcal{T}(\gamma,\cdot,r) = \cup_{\sigma\in\mathcal{S}_s}\mathcal{T}(\gamma,\sigma).$$

Let σ and σ' be different rearrangements of $1, \ldots, s$, $\alpha \in \mathcal{T}(\gamma,\sigma) \cap \mathcal{T}(\gamma,\sigma')$, and $\sigma(s)$ and σ'(s) correspond to the block containing G_{s-1}. Thus either $\sigma(s) = \sigma'(s)$, or G_{s-1} is a set of coset representatives of G_{k-1} in G_k, for some $k < s-1$. Clearly, $G_{s-1} \subset G_k$, so the second case is impossible. Thus, $\sigma(s) = \sigma'(s)$. Now, either

$\sigma(s-1) = \sigma'(s-1)$, or the coset representatives of G_{s-1} in G_{s-2} are also the coset representatives for G_{k-1} in G_k for some $k < s-2$. Again, this is impossible. We have the result by induction. Thus, $\mathcal{T}(\gamma, \sigma) \cap \mathcal{T}(\gamma, \sigma') = \emptyset$. Therefore, the above unions are disjoint, and

$$|\mathcal{T}(\gamma, \cdot, r)| = |\sigma_r| \cdot |\mathcal{T}(\gamma, \sigma)|, \text{ and}$$

$$|\mathcal{T}(\gamma, \cdot, \cdot)| = s! \cdot |\mathcal{T}(\gamma, \sigma)|.$$

Lastly, we discuss $\mathcal{T}$. It is clear that

$$\mathcal{T} = \cup_\gamma \mathcal{T}(\gamma, \cdot, \cdot),$$

where γ runs over all possible subgroup chains. However, if G is a direct product, then it can happen that

$$\mathcal{T}(\gamma, \cdot, \cdot) \cap \mathcal{T}(\gamma', \cdot, \cdot) \neq \emptyset$$

For instance, if $G = KN$, then $\alpha = \{N, K\}$ is clearly a logarithmic signature for G. If $\gamma : G > K > 1$, and $\gamma' : G > N > 1$, then $\alpha \in \mathcal{T}(\gamma, \cdot, \cdot) \cap \mathcal{T}(\gamma', \cdot, \cdot)$.

Therefore, a closer study of the specific group G is needed to further investigate $\mathcal{T}$.

3.6.4 Right and Left Translation

Recall that for each $g \in G$, we have defined g_r (g_l) as the image under the right (left) regular representation of g in $\mathcal{S}_G$, and the group $R_G = \{g_r : g \in G\} \leq \mathcal{S}_G$ ($L_G = \{g_l : g \in G\} \leq \mathcal{S}_G$). Of course, we have that $R_G \cong G \cong L_G$. We now define the subgroups $\widehat{R}_G, \widehat{L}_G \leq \mathcal{S}_{|G|}$ which are also isomorphic to G. For $g \in G$, we define $\widehat{g_r} = \breve{\eta} g_r \breve{\eta}^{-1}$, and $\widehat{g_l} = \breve{\eta} g_l \breve{\eta}^{-1}$. Then $\widehat{R}_G = \{\widehat{g_r} : g \in G\}$, and $\widehat{L}_G = \{\widehat{g_l} : g \in G\}$. Define $\widehat{\mathcal{G}} = \langle \widehat{L}_G, \widehat{R}_G \rangle$. Notice that $\widehat{\mathcal{G}}$ is in general not isomorphic to G. In fact, as was the case with $\mathcal{G}$,

$$\widehat{\mathcal{G}} = \widehat{L}_G \widehat{R}_G, \text{ and}$$

$$|\widehat{\mathcal{G}}| = \frac{|G|^2}{|Z(G)|}.$$

Therefore $\widehat{\mathcal{G}}$ is isomorphic to G if and only if G is abelian.

We will consider a simple example using D_4, the dihedral group of order 8. We represent the elements as the integers $1 \ldots 8$. The multiplication table for D_4 is given in Figure 3.2. The rows of the multiplication table are the canonical representations of the elements of the left regular image of D_4, and the columns are the canonical representations of the elements of the right regular image of D_4. Given the multiplication table, the center is easy to find–it is the set of elements whose row and column are identical. For D_4, $Z(D_4) = \{1, 3\}$. Therefore when $G = D_4$, $|\widehat{\mathcal{G}}| = 8^2/2 = 32$.

Figure 3.2: Multiplication table for D_4

D_4	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	3	4	1	8	5	6	7
3	3	4	1	2	7	8	5	6
4	4	1	2	3	6	7	8	5
5	5	6	7	8	1	2	3	4
6	6	7	8	5	4	1	2	3
7	7	8	5	6	3	4	1	2
8	8	5	6	7	2	3	4	1

Let G be a group of order $\prod_{i=1}^{s} r_i$, α a logarithmic signature for G, and $h \in G$. Let $x \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$. Then

$$\begin{aligned} h_r(\Theta_\alpha(x)) &= h_r(\alpha[1, p_1] \cdots \alpha[s, p_s]) = \alpha[1, p_1] \cdots \alpha[s, p_s] \cdot h \\ &= (\alpha h)[1, p_1] \cdots (\alpha h)[s, p_s] = \Theta_{\alpha h}(x) \end{aligned}$$

Thus, for $h \in G$, $\Theta_{\alpha h} = \Theta_\alpha h_r$. Similarly,

$$\begin{aligned} h_l(\Theta_\alpha(x)) &= h_l(\alpha[1, p_1] \cdots \alpha[s, p_s]) = h \cdot \alpha[1, p_1] \cdots \alpha[s, p_s] \\ &= (h\alpha)[1, p_1] \cdots (h\alpha)[s, p_s] = \Theta_{h\alpha}(x), \end{aligned}$$

so for $h \in G$, $\Theta_{h\alpha} = \Theta_\alpha h_l$.

From this, we can show

Theorem 3.11 *Let G be a group, α a logarithmic signature of G, and $h \in G$ any element. Then $\widehat{\alpha h} = \widehat{\alpha}\widehat{h_r}$, and $\widehat{h\alpha} = \widehat{\alpha}\widehat{h_l}$.*

Proof. It is straightforward to see that

$$\widehat{\alpha h} = \lambda^{-1}\Theta_{\alpha h}\breve{\eta}^{-1} = \lambda^{-1}\Theta_{\alpha}h_r\breve{\eta}^{-1} = \lambda^{-1}\Theta_{\alpha}\breve{\eta}^{-1}\breve{\eta}h_r\breve{\eta}^{-1} = \widehat{\alpha}\widehat{h_r}$$

A similar argument shows that $\widehat{\alpha}_l = \widehat{\alpha}\widehat{h_l}$. □

At first glance, the fact that $\widehat{\alpha}_l \neq \widehat{h_l}\widehat{\alpha}$ seems odd. However, whether we multiply a logarithmic signature on the left or right by an element of G does not effect the order in which the operators h_l and h_r are performed.

Theorem 3.12 *Let G be a group, α a logarithmic signature of G, and $g \in G$ any element. Then αg and $g\alpha$ are transversal, respectively totally non-transversal, if and only if α is.*

Proof. Notice that $(\alpha g)g^{-1} = \alpha$ so we only need to prove one direction. Assume that α is transversal. Then there exists a sandwich $T = (t_1, t_2, \ldots, t_{s-1})$ which transforms α into an exact transversal logarithmic signature α'. Either $G_1 = \alpha'[1] \cdots \alpha'[s-1]$, or $G_1 = \alpha'[2] \cdots \alpha'[s]$. In the first case, αg simply multiplies $\alpha[s]$ by g, changing the coset representatives of G_1. In the second case, we can rewrite $\alpha[1]\alpha[2] \cdots \alpha[s]g = \alpha[1]g^{-1}g\alpha[2] \cdots \alpha[s]g$, so $G_1^g = \alpha[2] \cdots \alpha[s]$. In either case, αg is transversal.

For $i = 1, \ldots, s$, let $H_i = \alpha'[i] \cdots \alpha'[s] \leq G$. Then we claim that the sandwich $T' = (g^{-1}t_1, g^{-1}t_2, \ldots, g^{-1}t_{s-1})$ will transform $g\alpha$ into an exact transversal logarithmic signature β. This is true since for $i = 2, \ldots, s$,

$$\beta[i] \cdots \beta[s] = g^{-1}\alpha'[i] \cdots \alpha'[s]g = g^{-1}H_i g,$$

which is just a conjugate subgroup, and

$$\beta[1] \cdots \beta[s] = g^{-1}\alpha'[1] \cdots \alpha'[s] = g^{-1}G = G.$$

Therefore, $g\alpha$ is transversal.

Notice that $L \subseteq G$ is a coset if and only if gL and Lg are cosets for any $g \in G$. Therefore, translations of the blocks preserves cosets, so αg and $g\alpha$ are totally non-transversal if and only if α is. □

Theorems 3.11 and 3.12 lead to an interesting result about the structures of several classes of logarithmic signatures.

Theorem 3.13 *Let G be a group of order $m = \prod_{i=1}^{s} r_i$, let $r = (r_1, r_2, \ldots, r_s)$ and let $\widehat{\mathcal{F}}$ be one of $\widehat{\Lambda}(\cdot,\cdot,r)$, $\widehat{\mathcal{NT}}(\cdot,\cdot,r)$, $\widehat{\mathcal{TNT}}(\cdot,\cdot,r)$ and $\widehat{\mathcal{T}}(\cdot,\cdot,r)$. Then $\widehat{\mathcal{F}} = \widehat{\mathcal{F}}\widehat{\mathcal{G}}$.*

Proof. Let α be a logarithmic signature of G, and $C_\alpha = \{\widehat{\alpha}\widehat{g} : \widehat{g} \in \widehat{\mathcal{G}}\}$. That is, C_α is the left coset of $\widehat{\mathcal{G}}$ to which $\widehat{\alpha}$ belongs. Let $\widehat{g} \in \widehat{\mathcal{G}}$. We can write $\widehat{g} = \widehat{g}_1\widehat{g}_2 \ldots \widehat{g}_k$ where

$\widehat{g}_i \in \widehat{R}_G \cup \widehat{L}_G$ for $i = 1, \ldots k$, for some k. Repeated applications of Theorem 3.11 will produce a logarithmic signature α' such that $\widehat{\alpha}' = \widehat{\alpha}\widehat{g}$. Therefore $C_\alpha \subseteq \widehat{\Lambda}(\cdot, \cdot, r)$, and since this is true of any $\widehat{\alpha} \in \widehat{\Lambda}(\cdot, \cdot, r)$, $\widehat{\Lambda}(\cdot, \cdot, r)$ is the union of left cosets of $\widehat{\mathcal{G}}$.

The above and Theorem 3.12 give the result for the remaining cases. □

Corollary 3.7 *Let G be a group, and let $\widehat{\mathcal{F}}$ be one of $\widehat{\Lambda}$, $\widehat{\mathcal{T}}$, $\widehat{\mathcal{NT}}$, and $\widehat{\mathcal{TNT}}$. Then $\widehat{\mathcal{F}} = \widehat{\mathcal{F}}\widehat{\mathcal{G}}$. In other words, $\widehat{\mathcal{F}}$ is the union of left cosets of $\widehat{\mathcal{G}}$.*

3.6.5 Fusing and Refining

Depending on the order the elements are placed in the combined block(s), fusing can produce either an equivalent or inequivalent logarithmic signature. Most of the orderings will produce an inequivalent logarithmic signature. Similarly, depending on how a logarithmic signature is refined, a fusion may or may not be equivalent.

3.6.6 Block Shuffling

In this section, we are restricting our attention to block shuffles that produce logarithmic signatures. When we say the block shuffle preserves a class, we mean when a block shuffle is indeed a logarithmic signature, then it is in the same class.

It is not hard to see that the block shuffle transformation preserves the classes $\mathcal{PT}$ (by definition), and $\mathcal{TNT}$. Notice that a block shuffle of a transversal logarithmic signature is not necessarily transversal, so the classes $\mathcal{T}$ and $\mathcal{NT}$ are not preserved.

We introduce some terminology which allows us to be more precise about the effects of block shuffling when G is abelian. Let $\alpha = \{\alpha[1], \ldots, \alpha[s]\}$ be a logarithmic signature of G, φ be a permutation of $1, \ldots, s$, and $\alpha_\varphi = \{\alpha[\varphi(1)], \ldots, \alpha[\varphi(s)]\}$. Given a permutation φ, we define a mapping $\check{\varphi} : \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s} \mapsto \mathbb{Z}_{r_{\varphi(1)}} \times \cdots \times \mathbb{Z}_{r_{\varphi(s)}}$ by $\check{\varphi}(p_1, \ldots, p_s) = (p_{\varphi(1)}, \ldots, p_{\varphi(s)})$. Define

$$m_i' = \begin{cases} 1 & \text{if i=1, and} \\ \prod_{j=1}^{i-1} r_{\sigma(j)} & \text{otherwise,} \end{cases}$$

and $\lambda_\varphi : \mathbb{Z}_{r_{\varphi(1)}} \times \cdots \times \mathbb{Z}_{r_{\varphi(s)}} \to \mathbb{Z}_{|G|}$ by

$$\lambda_\varphi(p_{\varphi(1)}, \ldots, p_{\varphi(s)}) = \sum_{j=1}^{s} p_{\varphi(j)} m_i'.$$

Lastly, define $\widehat{\rho}_\varphi = \lambda_\varphi^{-1} \check{\varphi}^{-1} \lambda$. Notice that $\widehat{\rho}_\varphi \in \mathcal{S}_M$.

If G is abelian, it is easy to see that for any $(p_{\varphi(1)}, \ldots, p_{\varphi(s)}) \in \mathbb{Z}_{r_{\varphi(1)}} \times \cdots \times \mathbb{Z}_{r_{\varphi(s)}}$,

$$\begin{aligned} \Theta_{\alpha_\varphi}(p_{\sigma(1)}, \ldots, p_{\varphi(s)}) &= \alpha[i_1, p_{\varphi(1)}] \cdots \alpha[\varphi(s), p_{\varphi(s)}] \\ &= \alpha[1, p_1] \cdots \alpha[s, p_s] \\ &= \Theta_\alpha(p_1, \ldots, p_s), \end{aligned}$$

where $(p_1, \ldots, p_s) \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$. Thus, $\check{\varphi}\Theta_{\alpha_\varphi} = \Theta_\alpha$, and we can see that

$$\breve{\alpha}_\varphi = \lambda_\varphi^{-1} \Theta_{\alpha_\varphi} = \lambda_\varphi^{-1} \check{\varphi}^{-1} \lambda \lambda^{-1} \check{\varphi} \Theta_{\alpha_\varphi} = \widehat{\rho}_\varphi \lambda^{-1} \Theta_\alpha = \widehat{\rho}_\varphi \breve{\alpha},$$

so that

$$\widehat{\alpha}_\varphi = \breve{\alpha}_\varphi \breve{\eta}^{-1} = \widehat{\rho}_\varphi \breve{\alpha} \breve{\eta}^{-1} = \widehat{\rho}_\varphi \widehat{\alpha}.$$

Thus, when G is abelian, and α is a logarithmic signature of G, every block shuffle of α is a logarithmic signature of G, and we know exactly the effect of applying the block shuffle. Notice that if α' is a sandwich of α, then the previous discussion makes it clear that $\widehat{\alpha}'_\varphi = \widehat{\alpha_\varphi}$

When G is non-abelian, things are not so clear. For instance, if α is a transversal logarithmic signature for G, and φ a permutation of $1, \ldots, s$, then α_φ is often not a logarithmic signature for G. Even when φ is such that α_φ is a logarithmic signature for G the relationship between $\widehat{\alpha}$ and $\widehat{\alpha}_\varphi$ is not immediately clear. In addition, if α' is a sandwich of α, then it is not necessarily the case that α'_φ is a logarithmic signature for G, and even if it is, the relationship between $\widehat{\alpha}'_\varphi$ and $\widehat{\alpha}_\varphi$ is not evident. We take a closer look at block shuffles as they relate to transversal logarithmic signatures in the next section.

3.7 Permutably Transversal Logarithmic Signatures

Permutably transversal logarithmic signatures are an interesting class. For instance, if we can "recognize" a permutably transversal logarithmic signature in polynomial time, and we know the relationship between $\widehat{\alpha}$ and $\widehat{\alpha}_{\varphi}$, then we have a new class of logarithmic signatures which are tame. On the other hand, if relationship between $\widehat{\alpha}$ and $\widehat{\alpha}_{\varphi}$ is understood, but we cannot "recognize" permutably transversal logarithmic signatures in polynomial time, this may be the trap-door we need for MST1.

As we saw in the last section, if G is abelian, the relationship between $\widehat{\alpha}$ and $\widehat{\alpha}_{\varphi}$ is perfectly understood.

The case when G is non-abelian is more difficult. Given a logarithmic signature α, and an ordering φ such that α_{φ} is also a logarithmic signature, we can certainly find some permutation $\widehat{p}_{\varphi}$ such that $\widehat{p}_{\varphi}\widehat{\alpha} = \widehat{\alpha}_{\varphi}$. However, it is not the case that $\widehat{p}_{\varphi}\widehat{\beta} = \widehat{\beta}_{\varphi}$, for every logarithmic signature of β of the same type. We illustrate this fact with D_4, the dihedral group of order 8. We will represent the elements of D_4 by the numbers $1, \ldots, 8$. A multiplication table for D_4 given in Figure 3.3

Figure 3.3: Multiplication table for D_4

D_4	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	3	4	1	8	5	6	7
3	3	4	1	2	7	8	5	6
4	4	1	2	3	6	7	8	5
5	5	6	7	8	1	2	3	4
6	6	7	8	5	4	1	2	3
7	7	8	5	6	3	4	1	2
8	8	5	6	7	2	3	4	1

Figure 3.4 shows some logarithmic signatures and their block shuffles according to $\varphi = (1,3,2)$. The permutations are expressed in canonical form. Given this information, it is easy to compute $\widehat{\alpha}_\varphi \widehat{\alpha}^{-1} = [1,7,2,4,5,3,6,8]$, and $\widehat{\beta}_\varphi \widehat{\beta}^{-1} = [1,3,2,4,5,7,6,8]$. Clearly, $\widehat{\alpha}_\varphi \widehat{\alpha}^{-1} \neq \widehat{\beta}_\varphi \widehat{\beta}^{-1}$.

Figure 3.4: Block Shuffles in D_4, with $\varphi = (1,3,2)$.

Name	Logarithmic Signature	Permutation	Inverse
α	$\{(1,3),(1,2),(7,1)\}$	$[7,1,6,2,5,3,8,4]$	$[2,4,6,8,5,3,1,7]$
α_φ	$\{(1,3),(7,1),(1,2)\}$	$[7,8,1,2,5,6,3,4]$	
β	$\{(1,5),(1,3),(2,5)\}$	$[2,5,4,7,6,1,8,3]$	$[6,1,8,3,2,5,4,7]$
β_φ	$\{(1,5),(2,5),(1,3)\}$	$[2,4,5,7,6,8,1,3]$	

In general, there is no clear relationship between the reordering φ and the resulting permutation α_φ. Thus, permutably transversal logarithmic signatures for non-abelian groups cannot be used as trap-doors, since $\widehat{\alpha}_\varphi^{-1}$, or equivalently $\widehat{p}_\varphi^{-1}$, are not computable.

The second concern relating to permutably transversal logarithmic signatures is whether or not they can be "recognized" in polynomial time. An obvious algorithm to determine whether or not a logarithmic signature α is permutably transversal or not is to check whether or not α_φ is transversal for all $\varphi \in \mathcal{S}_s$. Unfortunately, this requires $s!$ tests, which may be exponential in n.

It is not immediately obvious how to improve upon the above approach, and at this stage there is no known efficient algorithm to recognize a permutably transversal logarithmic signature. On the other hand, we do not view this as enough evidence that permutably transversal logarithmic signatures are not recognizable to suggest they are wild at this time. We survey several facts about permutably transversal logarithmic signature, mostly by example, to show why some of the "obvious" methods will not work.

Our method of recoginizing transversal logarithmic signatures depended on the fact that every transversal logarithmic signature is equivalent to an exact transversal logarithmic signature. In other words, we first computed a (r- or ℓ-) canonical equivalent to a logarithmic signature, and then tested to see if it was exact transversal. The same approach does not work for permutably transversal logarithmic signatures.

We will start with a few examples that will demostrate how sandwiching and permuting are, in some sense, not compatible.

Example 1: Consider Figure 3.5. Notice that α and β are both logarithmic signatures since the tensor computed is a permutation. In fact, they are transversal, as can be easily checked. Since the permutation is the same for both α and β, it is clear that α and β are sandwiches of each other. When we reorder the blocks of α and β according to $\varphi = (2, 1, 3)$, we see that α_φ is a logarithmic signature, but that

β_φ is not.

Figure 3.5: Sandwich and Block Shuffle in D_4, with $\varphi = (2, 1, 3)$.

Name	Logarithmic Signature	Tensor
α	$\{(1,8),(1,6),(5,1)\}$	$[5,1,4,6,2,8,7,3]$
β	$\{(8,1),(2,7),(1,5)\}$	$[5,1,4,6,2,8,7,3]$
α_φ	$\{(1,6),(1,8),(5,1)\}$	$[5,1,2,8,4,6,7,3]$
β_φ	$\{(2,7),(8,1),(1,5)\}$	$[7,3,2,8,2,8,7,3]$

Example 2: In Figure 3.6 we see that α and β are equivalent, so they are sandwiches of each other. When we apply φ to each, α_φ is a transversal logarithmic signature, but β_φ is not a logarithmic signature at all. In other words, α is permutably transversal with reordering φ, but β is not.

Figure 3.6: Sandwich and Block Shuffle in D_4, with $\varphi = (3, 2, 1)$.

Name	Logarithmic Signature	Tensor
α	$\{(4,5),(1,7),(1,5)\}$	$[4,6,8,2,5,1,3,7]$
β	$\{(1,6),(1,5),(4,6)\}$	$[4,6,8,2,5,1,3,7]$
α_φ	$\{(1,5),(1,7),(4,5)\}$	$[4,5,6,3,8,1,2,7]$
β_φ	$\{(4,6),(1,5),(1,6)\}$	$[4,7,6,1,6,1,4,7]$

These examples demostrate a couple of facts. First, the sandwich of a permutably transversal logarithmic signature is not necessarily permutably transversal. Second, if some reordering of a transversal logarithmic signature is a logarithmic signature, it is not necessarily the case that the same reordering of a sandwich is also a logarithmic signature.

Notice that in the last example, β is not permutably transversal, but the r-canonical equivalent, α is. One might think we could simply modify the definition of permutably transversal so that they are invariant under sandwiching. And perhaps we can recognize whether or not a logarithmic signature is permutably transversal based on the r- or ℓ-canonical equivalent, as was the case with mixed-transversals. Unfortunately, the next example demostrates that this is not the case.

Example 3: In Figure 3.8 is given a multiplication table for $\mathcal{S}_4$, where the elements are represented by the integers $1, \ldots, 24$. In figure 3.7, α is a transversal logarithmic signature for $\mathcal{S}_4$, and α_φ is a permutably transversal logarithmic signature for $\mathcal{S}_4$, where $\varphi = (2, 1, 3)$. Notice that the r- or ℓ-canonical equivalents, $(\alpha_\varphi)_r$ and $(\alpha_\varphi)_l$, of α_φ, are non-transversal but not permutably-transversal.

Figure 3.7: Block Shuffles and Canonical Logarithmic Signatures for $\mathcal{S}_4$, with $\varphi = (2, 1, 3)$

Name	Logarithmic Signature	Type
α	$\{(1,16,18),(9,5,1,3),(19,18)\}$	$\mathcal{T}$
α_φ	$\{(9,5,1,3),(1,16,18),(19,18)\}$	$\mathcal{PT}$
$(\alpha_\varphi)_r$	$\{(1,9,5,20),(1,14,7),(23,22)\}$	$\mathcal{NT}$
$(\alpha_\varphi)_l$	$\{(23,15,19,8),(1,7,14),(1,4)\}$	$\mathcal{NT}$
$((\alpha_\varphi)_r)_{\varphi^{-1}}$	$\{(1,14,7),(1,9,5,20),(23,22)\}$	Not LS
$((\alpha_\varphi)_l)_{\varphi^{-1}}$	$\{(1,7,14),(23,15,19,8),(1,4)\}$	Not LS

This last example makes it clear that we cannot depend on the r- or ℓ-canonical equivalents to determine whether or not a logarithmic signature is permutably transver-

Figure 3.8: Multiplication table for $\mathcal{S}_4$

$\mathcal{S}_4$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	2	3	4	1	15	16	13	14	8	5	6	7	18	19	20	17	11	12	9	10	24	21	22	23
3	3	4	1	2	20	17	18	19	14	15	16	13	12	9	10	11	6	7	8	5	23	24	21	22
4	4	1	2	3	10	11	12	9	19	20	17	18	7	8	5	6	16	13	14	15	22	23	24	21
5	5	6	7	8	9	10	11	12	1	2	3	4	21	22	23	24	13	14	15	16	17	18	19	20
6	6	7	8	5	23	24	21	22	12	9	10	11	14	15	16	13	3	4	1	2	20	17	18	19
7	7	8	5	6	16	13	14	15	22	23	24	21	4	1	2	3	10	11	12	9	19	20	17	18
8	8	5	6	7	2	3	4	1	15	16	13	14	11	12	9	10	24	21	22	23	18	19	20	17
9	9	10	11	12	1	2	3	4	5	6	7	8	17	18	19	20	21	22	23	24	13	14	15	16
10	10	11	12	9	19	20	17	18	4	1	2	3	22	23	24	21	7	8	5	6	16	13	14	15
11	11	12	9	10	24	21	22	23	18	19	20	17	8	5	6	7	2	3	4	1	15	16	13	14
12	12	9	10	11	6	7	8	5	23	24	21	22	3	4	1	2	20	17	18	19	14	15	16	13
13	13	14	15	16	17	18	19	20	21	22	23	24	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	16	13	3	4	1	2	20	17	18	19	6	7	8	5	23	24	21	22	12	9	10	11
15	15	16	13	14	8	5	6	7	2	3	4	1	24	21	22	23	18	19	20	17	11	12	9	10
16	16	13	14	15	22	23	24	21	7	8	5	6	19	20	17	18	4	1	2	3	10	11	12	9
17	17	18	19	20	21	22	23	24	13	14	15	16	9	10	11	12	1	2	3	4	5	6	7	8
18	18	19	20	17	11	12	9	10	24	21	22	23	2	3	4	1	15	16	13	14	8	5	6	7
19	19	20	17	18	4	1	2	3	10	11	12	9	16	13	14	15	22	23	24	21	7	8	5	6
20	20	17	18	19	14	15	16	13	3	4	1	2	23	24	21	22	12	9	10	11	6	7	8	5
21	21	22	23	24	13	14	15	16	17	18	19	20	5	6	7	8	9	10	11	12	1	2	3	4
22	22	23	24	21	7	8	5	6	16	13	14	15	10	11	12	9	19	20	17	18	4	1	2	3
23	23	24	21	22	12	9	10	11	6	7	8	5	20	17	18	19	14	15	16	13	3	4	1	2
24	24	21	22	23	18	19	20	17	11	12	9	10	15	16	13	14	8	5	6	7	2	3	4	1

sal.

Alternative definitions for permutably transversal have been proposed. For instance, if a logarithmic signature is obtained by a block shuffle of a transversal one, it could be called *permutably exactly transversal*, and a sandwich of an permutably exactly transversal logarithmic signature could be called *permutably transversal*. Unfortunately, the problems we encounter here remain.

One possible definition which would allow us to use the r- and ℓ-canonical equivalents to detect whether or not a logarithmic signature is permutably transversal would be to define permutably transversal as the sandwich of an r-canonical or ℓ-canonical logarithmic signature whose blocks can be permuted into a transversal logarithmic signature. There are two disadvantages to this definition. First, it is too restrictive. Second, we don't even know how to determine whether or not a r- or ℓ-canonical logarithmic signature is permutably transversal, so we still have the recognition problem.

In summary, there is currenlty no known efficient method of determining whether or not a logarithmic signature is permutbly transversal, no matter how we "tweak" the definition.

Since the sandwich transformation seems to mask the permutably-transversal property, it is possible this will lead to the needed trap-door. Even if we find an efficient algorithm to recognize permutably transversal logarithmic signatures, the previous discussion suggests it is unlikely that we can detect the sandwich of a permutably transversal logarithmic signature. Since the number of sandwich transformations is large, trying them all is not feasible.

3.8 More on Canonical Logarithmic Signatures

The following simple lemmas are used in the next few theorems.

Lemma 3.4 *Let G be a group of order $\prod_{i=1}^{s} r_i$, and $r = (r_1, \ldots, r_s)$. Let $\alpha \in \mathcal{C}(\cdot, \cdot, r)$ and $g \in G$. Then $\alpha g \in \mathcal{LC}(\cdot, \cdot, r)$, and $g\alpha \in \mathcal{RC}(\cdot, \cdot, r)$.*

Proof. Let $\alpha' = \alpha g$. Since $\alpha \in \mathcal{C}(\cdot, \cdot, r)$, $\alpha[i; 1] = 1$ for $i = 1, \ldots, s$. α' is the same as α, except in the first block, so regardless of what g is, $\alpha'[i; 1] = 1$ for $i = 2, \ldots, s$, and $\alpha' \in \mathcal{LC}(\cdot, \cdot, r)$ as needed. The proof is similar for $\mathcal{RC}$. □

Lemma 3.5 *Let G be a group of order $\prod_{i=1}^{s} r_i$, and $r = (r_1, \ldots, r_s)$. If $\alpha \in \mathcal{RC}(\cdot, \cdot, r)$, then $g = \alpha[1; 1]^{-1}$ is the unique element such that $\alpha' = g\alpha \in \mathcal{C}(\cdot, \cdot, r)$. Similarly, if $\alpha \in \mathcal{LC}(\cdot, \cdot, r)$, then $g = \alpha[s; 1]^{-1}$ is the unique element such that $\alpha' = \alpha g \in \mathcal{C}(\cdot, \cdot, r)$.*

Proof. If α is r-canonical, $\alpha[i; 1] = 1$ for $i = 2, \ldots, s$. The only difference between α and α' occurs in the first block, where $\alpha'[1; 1] = \alpha[1; 1]g = \alpha[1; 1]\alpha[1; 1]^{-1} = 1$. Thus, $\alpha'[i; 1] = 1$ for $i = 1, \ldots, s$, and $\alpha' \in \mathcal{C}(\cdot, \cdot, r)$. Clearly $g = \alpha[1; 1]^{-1}$ is the only element by which we can multiple α on the right to assure that $\alpha[1; 1] = 1$. The proof is similar if α is ℓ-canonical. □

Theorem 3.14 *Let G be a group of order $\prod_{i=1}^{s} r_i$, and $r = (r_1, \ldots, r_s)$. Let $\alpha \in$*

$\Lambda(\cdot,\cdot,r)$. Then there is a unique $\beta \in \mathcal{C}(\cdot,\cdot,r)$, and $t \in G$ such that $\widehat{\alpha} = \widehat{\beta}\widehat{t_r}$. Also, there is a unique $\beta \in \mathcal{C}(\cdot,\cdot,r)$, and $t \in G$ such that $\widehat{\alpha} = \widehat{t_l}\widehat{\beta}$.

Proof. By Theorem 3.2, there exists a unique r-canonical logarithmic signature β' such that $\widehat{\alpha} = \widehat{\beta'}$. Let $t = \beta'[1;1]$, and $\beta = \beta' t^{-1}$. By Lemma 3.5, t is the unique element for which $\beta = \beta' t^{-1} \in \mathcal{C}(\cdot,\cdot,r)$. By Theorem 3.11, $\widehat{\alpha} = \widehat{\beta'} = \widehat{\beta}\widehat{t_r}$. The proof is similar for the other case. □

Theorem 3.15 *Let G be a group of order $\prod_{i=1}^{s} r_i$, and let $r = (r_1,\ldots,r_s)$. Then $\mathcal{LC}(\cdot,\cdot,r) = \mathcal{C}(\cdot,\cdot,r)G$, and $\mathcal{RC}(\cdot,\cdot,r) = G\mathcal{C}(\cdot,\cdot,r)$. Further, for each element $\alpha \in \mathcal{RC}(\cdot,\cdot,r)$, there are unique elements $\alpha_L \in \mathcal{C}(\cdot,\cdot,r)$ and $g \in G$ such that $\alpha = \alpha_L g$. Similarly, there are unique elements $\alpha_R \in \mathcal{C}(\cdot,\cdot,r)$ and $h \in G$ such that $\alpha = \alpha_R h$.*

Proof. $\mathcal{C}(\cdot,\cdot,r)G \subseteq \mathcal{RC}(\cdot,\cdot,r)$ by Lemma 3.4. Since α is canonical, the proof of Theorem 3.14 shows that we can find a $\beta \in \mathcal{C}(\cdot,\cdot,r)$ and $t \in G$ such that $\alpha = \beta t$. Thus $\mathcal{RC}(\cdot,\cdot,r) \subseteq \mathcal{C}(\cdot,\cdot,r)G$. Uniquiness follows as well. The proof is similar for the other case. □

Corollary 3.8 *Let G be a group of order $\prod_{i=1}^{s} r_i$, $r = (r_1,\ldots,r_s)$, and $\mathcal{F}$ any class closed under right and left translation. Then $\widehat{\mathcal{F}}(\cdot,\cdot,r) = \widehat{\mathcal{F}_C}(\cdot,\cdot,r)\widehat{R}_G = \widehat{\mathcal{F}_C}(\cdot,\cdot,r)\widehat{L}_G$. Further, for each element $\widehat{\alpha} \in \widehat{\mathcal{F}}(\cdot,\cdot,r)$, there are unique elements $\widehat{\alpha}_L \in \widehat{\mathcal{F}}_C(\cdot,\cdot,r)$*

and $\widehat{g} \in \widehat{L}_G$ such that $\widehat{\alpha} = \widehat{\alpha}_L \widehat{g}$. Similarly, there are unique elements $\widehat{\alpha}_R \in \widehat{\mathcal{F}_C}(\cdot, \cdot, r)$ and $\widehat{h} \in \widehat{R}_G$ such that $\widehat{\alpha} = \widehat{\alpha}_R \widehat{h}$.

Proof. This is any easy corollary of Theorem 3.15. It can also be deduced from Theorems 3.11 and 3.14. □

Theorem 3.16 *Let G be a group of order $\prod_{i=1}^{s} r_i$, $r = (r_1, \ldots, r_s)$, and $\mathcal{F}$ be any class closed under right and left translation. Then each of the following is true*

1. $|\widehat{\mathcal{F}}(\cdot, \cdot, r)| = |\widehat{\mathcal{F}_C}(\cdot, \cdot, r)| \cdot |G|$
2. $|\widehat{\mathcal{F}}(\cdot, \cdot, r)| = |\mathcal{F}(\cdot, \cdot, r)| / |G|^{s-1}$
3. $|\mathcal{F}(\cdot, \cdot, r)| = |\widehat{\mathcal{F}_C}(\cdot, \cdot, r)| \cdot |G|^s$

Proof. Statement 1 is an obvious corollary of Theorem 3.15. Since there are precisely $|G|^{s-1}$ orbit elements under sandwiching for each logarithmic signature, statement 2 follows. Apply statements 1 and 2 and trivial algebra to get statement 3. □

3.9 Counting Logarithmic Signatures

In this section, we give some results relating to logarithmic signatures with two blocks. Logarithmic signatures with two blocks may not meet the polynomial-size requirement, so are not really logarithmic signatures under the strict definition. However, the resutls are still of interest.

Lemma 3.6 *Let α be a logarithmic signature of type $r = (r_1, r_2, \ldots, r_s)$. Then there exist equivalent logarithmic signatures of types $(\prod_{i=1}^{k} r_i, \prod_{j=k+1}^{s} r_j)$, for $k = 1, \ldots, s-1$. If α is r-transversal or ℓ-transversal, the logarithmic signatures constructed will be. If α is transversal, then either the logarithmic signature of type $(r_1, \prod_{j=2}^{s} r_j)$ or type $(\prod_{i=1}^{s-1} r_i, r_s)$ is transversal.*

Proof. Fusing the blocks in an appropriate way gives an equivalent logarithmic signature of the required type. Fusing either constructs a larger subgroup or a larger set of coset representatives, maintaining the ℓ-transversal or r-transversal property. The result for transversal is obvious. □

An easy corallary is the following.

Corollary 3.9 *The set $\widehat{\Lambda}$ is the union of $\widehat{\Lambda}(\cdot, \cdot, r)$, where r ranges over all types of logarithmic signatures with two blocks. Also, $\widehat{\mathcal{RT}}$ ($\widehat{\mathcal{LT}}$) is the union of $\widehat{\mathcal{RT}}(\cdot, \cdot, r)$ ($\widehat{\mathcal{LT}}(\cdot, \cdot, r)$) where r ranges over all types of logarithmic signatures with two blocks.*

In other words, if we are interested in the set of permutations which correspond to logarithmic signatures, we need only study logarithmic signatures with two blocks, especially if we are intersted in transversal logarithmic signatures. This is very helpful, as many things can be shown of logarithmic signatures with two blocks. It should be noted that the study of non-transversal logarithmic signatures cannot necessarily be restricted to logarithmic signatures with two blocks, as there may be non-transversal logarithmic signatures with more blocks whose fusions into two blocks are are transversal.

Theorem 3.17 *Let G be a group of order r_1r_2. Then $|\Lambda(r_1, r_2)| = |\Lambda(r_2, r_1)|$, and $|\widehat{\Lambda}(r_1, r_2)| = |\widehat{\Lambda}(r_2, r_1)|$. The same is true for $\mathcal{T}$, $\mathcal{NT}$, and $\mathcal{TNT}$.*

Proof. Apply the inversion transformation. □

Corollary 3.10 *Let G be a group of order r_1r_2 with N subgroups of order r_2. Then*

$$|\widehat{\mathcal{RT}}(r_2, r_1)| = |\widehat{\mathcal{LT}}(r_1, r_2)| = N \cdot r_1!(r_2)^{r_1} \cdot (r_2 - 1)!.$$

Proof. Apply Theorem 3.10 to each of the N subgroups. Since each of the logarithmic signatures constructed are canonical, they are inequivalent. □

Theorem 3.18 *Let G be a group of order $p_1^{a_1}p_2^{a_2}\cdots p_t^{a_t}$, where the p_i are distinct primes. Then there are $\prod_{i=1}^{t}(a_i+1)-2$ possible logarithmic signatures types containing two blocks.*

We present two easy upper bounds on $|\widehat{\Lambda}(\cdot,\cdot,r)| = |\widehat{\Lambda}_R(\cdot,\cdot,r)|$.

Theorem 3.19 *Let G be a group of order $m = \prod_{i=1}^{s} r_i$, let $r = (r_1, r_2, \ldots, r_s)$, and let $k = \sum_{i=1}^{s} r_i - s + 1$. Then*

1. $|\widehat{\Lambda}(\cdot,\cdot,r)| \leq \binom{m}{r_s} r_s! \prod_{i=1}^{s-1} \binom{m-1}{r_i - 1}(r_i - 1)! = m \prod_{i=1}^{s} \frac{(m-1)!}{(m-r_i)!}$, *and*

2. $|\widehat{\Lambda}(\cdot,\cdot,r)| \leq \frac{m!}{(m-k)!} = m(m-1)(m-2)\cdots(m-k+1)$.

Proof. Since the set of logarithmic signatures is a subset of the set of pseudo-logarithmic signatures, we can upper bound the number of logarithmic signatures by giving upper bounds on the number of pseudo-logarithmic signatures. Since each block of a logarithmic signature is composed of distinct permutations, an upper bound on $|\widehat{\Lambda}(\cdot,\cdot,r)|$ is the number of r-canonical pseudo-logarithmic signatures of type r whose blocks have distinct entries. The right hand side of 1 is this number.

Notice that k is the number of entries of an r-canonical logarithmic signature which are not equal to the identity. Given a permutation $p \in \mathcal{S}_{|G|}$, we can construct an r-canonical pseudo-logarithmic signature by filling in the k non-identity elements by examining k appropriate points of p. The number of ways of doing this is the right hand side of 2. □

Corollary 3.11 *Let G be a group of order $m = \prod_{i=1}^{s} r_i$, and let $r = (r_1, r_2, \ldots, r_s)$. Then*

$$\frac{|\widehat{\Lambda}(\cdot,\cdot,r)|}{|\mathcal{S}_{|G|}|} \leq \frac{1}{(m - \sum_{i=1}^{s} r_i + s - 1)!}.$$

That is, the probability that a random permutation from $\mathcal{S}_{|G|}$ has a corresponding logarithmic signature is at most $1/(m - \sum_{i=1}^{s} r_i + s - 1)!$.

Since $\sum_{i=1}^{s} r_i + s - 1 = O(\log m)$, the probability above is generally very small.

3.10 Logarithmic Signatures, Permutations, and Cosets

We have shown that collections of permutations corresponding to classes of logarithmic signatures of G are the union of left and right cosets of several different groups. In this section we summarize the results relating to cosets.

Let G be a group of order $m = \prod_{i=1}^{s} r_i$, and $r = (r_1, r_2, \ldots, r_s)$. Then

1. If $\mathcal{F}$ is any class of logarithmic signature we have defined, then

$$\widehat{\mathcal{F}}(\cdot,\cdot,r) = \widehat{\Psi_r}\widehat{\mathcal{F}}(\cdot,\cdot,r).$$

2. If $\mathcal{F} \in \{\Lambda, \mathcal{T}, \mathcal{NT}, \mathcal{TNT}\}$, then

$$\widehat{\mathcal{F}}(\cdot,\cdot,r) = \widehat{\mathcal{F}}(\cdot,\cdot,r)\widehat{\mathcal{G}}.$$

3. If $\mathcal{F} \in \{\Lambda, \mathcal{T}, \mathcal{NT}, \mathcal{TNT}\}$, then

$$\widehat{\mathcal{F}}(\cdot,\cdot,r) = \widehat{\mathcal{F}_C}(\cdot,\cdot,r)\widehat{R_G} = \widehat{\mathcal{F}_C}(\cdot,\cdot,r)\widehat{L_G}.$$

For 1, we can take as coset representatives the “lexicographic least” logarithmic signatures. In other words, given a logarithmic signature in $\mathcal{F}(\cdot,\cdot,r)$, permute the elements in each block so they are in increasing order to obtain the coset representative.

For 3, it is easy to see that $\widehat{\mathcal{F}_C}(\cdot,\cdot,r)$ is a set of distinct coset representatives. In other words, the coset representatives are the elements which fix ’1’.

Chapter 4

$[s, r]$-meshes, the Coset Intersection Problem, and MST2

In this chapter we explore the issues surrounding the implementation and security of MST2.

4.1 Possible Attacks on MST2

There are two security issues that must be explored. The first is whether somebody can break Alice's key and eavesdrop on *any* messages sent to her. The second is whether somebody can decrypt a *given* message.

The only way to break Alice's key is to find an homomorphism $f' : G \to H$ such that $f'(\alpha) = \beta$. Given such a homomorphism, anyone can compute $f'(y_1) = f(y_1) = y_2$, and given y_2 compute the message $y_3 y_2^{-1}$, thus breaking the system. Notice that one need not find Alice's exact mapping f.

There are three ways to decrypt a given message. The first way is to break the key as above. The second is to find an $R' \in \mathbb{Z}_{r^s}$ such that $y_1 = \breve{\alpha}(R')$. Given this, anyone can compute $\breve{\beta}(R') = \breve{\beta}(R) = y_2$, and obtain the message as $y_3 y_2^{-1}$. As with the mapping f, one need not find Bob's exact number R. The final method of decrypting a message is to determine y_2 directly. Perhaps it should be noted that guessing the message $h \in H$ is also a method of decrypting the message, but it should be obvious that this is a hopeless attack.

Finding an R' such that $y_1 = \breve{\alpha}(R')$ is equivalent to finding a factorization with respect to the $[s, r]$-mesh, which, according to Assumption 3, is intractable. In fact, we give strong evidence for Assumption 3 in the next section. Thus, this attack is hopeless for large G.

The only possible attack, then, seems to be finding an "equivalent" mapping f'. In Section 4.3 we examine this attack in the case when $H = G$ and the homomorphism f is conjugation by an element $g \in G$.

4.2 Factoring with respect to an $[s, r]$-mesh is hard

There is strong evidence that indicates that Assumption 3 from Section 2.5.3 is indeed true. In this section we show that factoring with respect to an $[s, r]$-mesh is at least as hard as another problem that is generally regarded as being intractable.

We define more formally the $[s, r]$-mesh factoring problem.

Problem: $[s, r]$**-mesh factoring (MF)**

Instance: Let G be a group, $\alpha = (a_{i,j})$ be an $[s, r]$-mesh for G, and $g \in G$ a random element.

Solution: Find a factorization of G with respect to the $[s, r]$-mesh. That is, write

$$g = a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,j_s}.$$

The Discrete Logarithm Problem is a well known problem:

Problem: Discrete Logarithm Problem (DLP)

Instance: Let $q = p^n$ be a prime power, $\mathbb{F}_q$ be a finite field, $a \in \mathbb{F}_q^*$ be a primitive element, and $b \in \mathbb{F}_q^*$.

Solution: Find a positive integer c such that $a^c = b$.

DLP is generally believed to be intractable. In fact, the well known cryptosystem of El Gamal is based on that assumption. It is not hard to show that MF is at least as hard as DLP. In fact, DLP is a special case of MF.

Theorem 4.1 *MF is at least as hard as DLP.*

Proof. Let $q = p^n$ be a prime power, $\mathbb{F}_q$ be a finite field, $a \in \mathbb{F}_q^*$ be a primitive element, and $b \in \mathbb{F}_q^*$. Let $r = \lceil \log n \rceil$, $s = 2$, and $\alpha = (a_{i,j})$ be given by

$$a_{i,j} = \begin{cases} 1 & \text{if i=1, and} \\ a^{2^{j-1}} & \text{if i=2.} \end{cases}$$

That is,

$$\alpha = [1, a; 1, a^2; 1, a^4; \ldots; 1, a^{\left(2^{\lceil \log n \rceil}\right)}].$$

Let $b = a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,j_s}$ be the factorization of b with respect to α. Then

$$c = \sum_{i=1}^{r} (j_i - 1)\left(2^{i-1}\right).$$

Thus, a solution to MF gives a solution to DLP, so MF is at least as hard as DLP. □

4.3 The Coset Intersection Problem

In this section, we concern ourselves with a special case of MST2. Let G be a group, $\alpha = (a_{i,j})$ an $[s, r]$-mesh for G, and let $g \in G$. We set $H = G$, and let $f : x \mapsto x^g$ be conjugation by an element $g \in G$. That is, we define $\beta = (b_{i,j}) = (a_{i,j}^g)$.

To break Alice's key, one needs to find *any* $g' \in G$ such that $b_{i,j} = a_{i,j}^{g'}$ for $1 \leq i \leq s$ and $1 \leq j \leq r$. A secure implementation of MST2 in this case would require that computing such an element be difficult. In order to ascertain the difficulty of this task, we need to discuss how one would go about computing such an element.

We assume that finding an element $u_{i,j} \in G$ such that $b_{i,j} = a_{i,j}^{u_{i,j}}$ is easy. Given $x, y, z \in G$ such that $x^y = z$, it is not hard to see that $\{w \in G : x^w = z\} = C_G(x)y$.

Thus, to break MST2, one needs to find an element in

$$\Theta = \bigcap_{i,j} C_G(a_{i,j})u_{i,j}.$$

For which groups G is computing an element in Θ difficult? There is, so far, no easy answer to this question. There is, however, at least a partial answer to the opposite question– For which groups G is computing an element in Θ easy? Although this does not tell us what groups we should use, it gives us a list of groups that should *not* be used.

In this section, X is a set of cardinality n, and whenever $G \leq S_X$, G is represented by $< n^2$ generators. Sim's Method [28], which runs in polynomial time [7], can produce such a generating set. When a group is output from an algorithm, we again assume it is output via a set of $< n^2$ generators.

The GRAPH-ISOMORPHISM problem (GRAPH-ISO) is well known:

Problem: GRAPH ISOMORPHISM (GRAPH-ISO)

Input: Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$

Question: Are G_1 and G_2 Isomorphic? That is, is there a bijection $f : V_1 \rightarrow V_2$ such that $\{u, v\} \in E_1$ if and only if $\{f(u), f(v)\} \in E_2$

Many people do not consider GRAPH-ISO to be hard in practice [13]. In fact, when applied to random graphs, even naive graph isomorphism algorithms are provably fast on average. Yet, although GRAPH-ISO has been studied extensively, there is no known polynomial-time algorithm to solve it in general. That is, every known approach to solving the problem has exponential worst-case running time. It is widely believed that GRAPH-ISO is neither polynomial nor NP-Complete [9].

We define three other problems:

Problem: SUBGROUP INTERSECTION (INT)

Input: $G, H \leq S_X$.

Find: $G \cap H$.

Problem: COSET INTERSECTION(COS-INT)

Input: $G, H \leq S_X$, and two permutations $g, h \in S_X$.

Find: $Gg \cap Hh$.

Problem: CENTRALIZER (CENT)

Input: $G \leq S_X$, and $g \in S_X$.

Find: $C_G(x)$, the centralizer of x in G.

The following theorems give some evidence that these three problems are hard to solve in general.

Theorem 4.2 *The problems INT, COS-INT, and CENT are polynomial-time equivalent. [13]*

Theorem 4.3 *GRAPH-ISO is polynomial-time reducible to INT, COS-INT, and CENT. [13]*

Thus, INT, COS-INT, and CENT are all "at least as hard as" GRAPH-ISO. More precisely, a polynomial-time algorithm to solve any of INT, COS-INT or CENT would lead to a polynomial-time algorithm to solve GRAPH-ISO. The fact that it is widely believed that GRAPH-ISO cannot be solved in polynomial time, along with the fact that no polynomial-time algorithm to solve INT, COS-INT or CENT has been found yet, leads most people to believe that these problems are not solvable in polynomial time in general.

However, as with GRAPH-ISO, these problems are generally not considered to be hard in practice. In other words, researchers have so far been able to compute INT, COS-INT, and CENT for groups of interest. This certainly leaves open the possibility that there are groups for which the currently available tools would not suffice. Nothing is currently known about how fast the naive INT, etc, algorithms work on average, as the notion of an "average group" is not as easily defined as with graphs.

With MST2 in mind, we are ultimately interested in groups for which COS-INT and CENT are difficult (i.e. not polynomial). Thus, our search involves those classes of groups for which the currently known algorithms aren't fast enough. If it is indeed the case that there are no polynomial-time algorithms to solve COS-INT and CENT, then there must be some groups for which the problem is not efficiently computable. We shall start by eliminating certain classes of groups for which there are known polynomial-time algorithms.

The cases for which INT (equivalently COS-INT) is known to be solvable in polynomial time are given below. [2, 12, 1, 23].

Theorem 4.4 *Let $G, H \subseteq S_X$. Then $G \cap H$ can be computed in polynomial time if*

1. $G \in \Gamma_d$, *or*
2. $H \lhd \lhd \langle G, H \rangle$

Notice that case 1 includes solvable groups, and case 2 includes the case where G normalizes H and when G and H are subgroups of a nilpotent group. Although these are the only known cases when a special technique has been applied to obtain polynomial-time algorithms for INT, this does not mean than any group other than these will suffice. These are the only groups where INT has been *proven* to be solvable in polynomial time, which is not to say that there aren't others.

Another result of Luks that is of interest is the following.

Theorem 4.5 *Let $G, H \subseteq S_X$. Then $Core_G(G \cap H)$ can be found in polynomial time.*

It may be of interest to the reader that this result is based on the classification of finite simple groups. Although it is doubtful that there are any practical implementations of the algorithm thus far, the possibility does exist. Given this algorithm one should be able to compute $\mathrm{Core}_G(\Theta)$ in polynomial time, which would mean that Alice should avoid choosing her element g from this subgroup.

Chapter 5

Summary and Further Research

We have already mentioned that since logarithmic signatures are at the center of MST1, an in depth understanding of them is required to implement MST1, and to ensure its security. In particular, knowing which logarithmic signatures are tame and which are wild is of central importance. We have been able to classify logarithmic signatures in several important ways, increasing our understanding of the permutations to which they correspond. We have shown that transversal logarithmic signatures are tame, increasing the set of known tame logarithmic signatures significantly. We also are able to give exact formulas for the number of logarithmic signatures in the sets $\mathcal{T}(\gamma, \sigma)$, $\mathcal{T}(\gamma, \cdot, r)$, and $\mathcal{T}(\gamma, \cdot, \cdot)$, and the number of permutations in $\widehat{\mathcal{T}}(\gamma, \sigma)$.

Since there are $|G|^{s-1}$ unique sandwiches of each logarithmic signature α, there are $|G|^{s-1}$ unique logarithmic signatures that are equivalent to α. Since they all correspond to the same permutation, we would like to be able to consider only one of them. We have shown that there is a unique r-canonical and a unique ℓ-canonical equivalent of α, so that we can restrict our attention to only the r-canonical or ℓ-canonical logarithmic signatures. More specifically, whenever $\mathcal{F}$ is a class of logarithmic signatures closed under the sandwich transformation, we have shown that $\widehat{\mathcal{F}}(\cdot,\cdot,r) = \widehat{\mathcal{F}_R}(\cdot,\cdot,r) = \widehat{\mathcal{F}_L}(\cdot,\cdot,r)$.

We have analyzed the right and left translation transformations, and concluded that whenever $\mathcal{F}$ is a class of logarithmic signatures closed under these operations, then $\widehat{\mathcal{F}} = \widehat{\mathcal{F}}\widehat{\mathcal{G}}$. Similarly, due to the analysis of the element shuffle, we have shown that whenever $\mathcal{F}$ is a class of logarithmic signatures closed under element shuffling, then $\widehat{\mathcal{F}}(\cdot,\cdot,r) = \widehat{\Psi}_r\widehat{\mathcal{F}}(\cdot,\cdot,r)$. In other words, in each case the sets of permutations $\widehat{\mathcal{F}}$ is the union of cosets of the groups $\widehat{\Psi}_r$ and $\widehat{\mathcal{G}}$. This gives much more insight into the structures of these sets than was known previously.

We introduced the class of permutably transversal logarithmic signatures, and gave evidence that permutably transversal logarithmic signatures may be able to provide a trap-door for use with MST1 if G is abelian, although more research is needed to determine whether or not this is really the case. We believe that it will soon be shown that either permutably transversal logarithmic signatures are tame when G is abelian, or that they can be used as trap-doors.

We gave insight into the challenges to an implementation of MST2, including a discussion of how the subgroup intersection problem relates to the security of MST2. With these results come several important questions for future study.

- Can we identify other classes of logarithmic signatures which are tame besides the transversals?
- Are permutably transversal logarithmic signatures tame or wild? If they are wild, can they be used as a trap-door for MST1?
- We conjectured that for every group G, $\langle \widehat{T} \rangle = S_{|G|}$. Can we prove this?
- Is there a way of obtaining a wild logarithmic signature as a product of tame ones? If so, we can build a trap-door for MST1.
- Conversely, given a generic logarithmic signature, can we find a set of tame logarithmic signatures such that their product is α? If so, MST1 cannot be made secure.
- How can we use the knowledge of the structure of $\mathcal{F}$ and $\widehat{\mathcal{F}}$ for the various classes of logarithmic signatures to answer any of the above questions?

Bibliography

[1] L. Babai, P.J. Cameron, and P.P. Palfy. On the orders of primitive groups with restricted nonabelian composition factors. *J. of Alg.*, 79:161–168, 1982.

[2] L. Babai, W.M. Kantor, and E.M. Luks. Computational complexity and the classification of finite simple groups. *Proc. 24th IEEE Symp. on Found. of Comp. Sci.*, pages 162–171, 1983.

[3] G. Butler. *Fundamental Algorithms for Permutation Groups.* Lecture Notes in Computer Science (559). Springer-Verlag, Germany, 1991.

[4] W. Diffie and M.E. Hellman. Multiuser cryptographic techniques. *AFIPS Conference Proceedings*, 45:109–112, 1976.

[5] W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22:644–654, 1976.

[6] T. ElGamal. A new public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31:469–472, 1985.

[7] M. Furst, J. Hopcroft, and E.M. Luks. Polynomial-time algorithms for permutation groups. *Proc. 21st IEEE Symp. on Found. Comp. Sci.*, pages 36–41, 1980.

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

[9] M.R. Garey and D.S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness.* W. H. Freeman, New York, 1979.

[10] T. Horvath, S.S. Magliveras, and T. Trung. A parallel permutation multiplier for a PGMcrypto-chip. In *Advances in Cryptology – Crypto '94*, volume 839, pages 108–113, California, 1994. Springer-Verlag.

[11] J.S. Leon. Partitions, refinements, and permutation group computation. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 28:123–158, 1997.

[12] E.M. Luks. Isomorphism of graphs of bounded valence can be tested in polynomial time. *J. Comp. Sys. Sci.*, 25:42–65, 1982.

[13] E.M. Luks. Permutation groups and polynomial-time computation. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 11:139–175, 1993.

[14] E.M. Luks. Hypergraph isomorphism and structural equivalence of boolean functions. *Proc. 31st ACM Symposium on Theory of Computing*, pages 652–658, 1999.

[15] E.M. Luks, F. Rakoczi, and C.R.B. Wright. Some algorithms for nilpotent permutation groups. *J. Symb. Comp.*, 23:335–354, 1997.

[16] S.S. Magliveras. A cryptosystem from logarithmic signatures of finite groups. *Proc. of the 29th Midwest Symposium on Circuits and Systems*, pages 972–975, 1986.

[17] S.S. Magliveras and Nasir D. Memon. Complexity tests for cryptosystem PGM. *Congressus Numerantium*, 79:61–68, 1990.

[18] S.S. Magliveras and N.D. Memon. Linear complexity profile analysis of the PGMcryptosystem. *Congressus Numerantium*, 72:51–60, 1989.

[19] S.S. Magliveras and N.D. Memon. Properties of cryptosystem PGM. In *Advances in Cryptology – Crypto '89*, volume 435, pages 447–460, Berlin, 1989. Springer-Verlag.

[20] S.S. Magliveras and N.D. Memon. Algebraic properties of cryptosystem PGM. *Journal of Cryptology*, 5:167–183, 1992.

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

[22] S.S. Magliveras, D.R. Stinson, and T. Trung. New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups. submitted, 2000.

[23] P.P. Palfy. A polynomial bound for the orders of primitive solvable groups. *J. of Alg.*, 77:127–137, 1982.

[24] M. Qu. *Subset Factorizations in Finite Groups and Their Cryptographic Significance.* Ph.D. dissertation, University of Waterloo, 1994.

[25] R.L. Rivest, A. Shamir, and L Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[26] J.J. Rotman. *An Introduction to the Theory of Groups.* Wm. C. Brown Publishers, Dubuque, Iowa, 3rd edition, 1988.

[27] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *Siam. J. Comput.*, 26(5):1484–1509, October 1997.

[28] C.C. Sims. Some group-theoretic algorithms. *Springer Lect. Notes in Math.*, 697:108–124, 1978.

[29] D.R. Stinson. *Cryptography Theory and Practice.* CRC Press, inc., 1995.