Trap doors from subgroup chains and recombinant bilateral transversals

Jean-Camille Birget, Spyros S. Magliveras and Wandi Wei

Abstract

Many known cryptosystems, symmetric or asymmetric, have been based on large finite abelian groups. A number of recent papers have been concerned with cryptography founded on factorizations of finite groups. In this paper we propose yet another possible scenario for constructing trap-doors, and potentially a new kind of public key cryptosystem (BMW) based on logarithmic signatures of finite permutation groups. Prompted by a recent paper of J.M. Bohli, M.I. González Vasco, C. Martínez and R. Steinwandt [1] we also pose a question which relates to finding logarithmic signatures which are hard to invert.

Keywords: PGM, logarithmic signatures, Trap-door one-way functions, group factorizations, public key cryptosystems, logarithmic signatures, finite groups.

1 Introduction

At the dawn of the 21st century only a few known public key cryptosystems remain unbroken. Most of these systems rely on the perceived difficulty of certain problems in large finite abelian groups in particular representations. It is rather unsettling that
the principles on which most of the above systems are founded would be compromised if a practical quantum computer becomes a reality.

A number of recent papers have dealt with extensions, questions and generalizations related to cryptography based on group factorizations [7, 8, 9, 10, 2, 11, 13, 1, 14]. In this paper we present a novel public-key scenario, which we call BMW, using logarithmic signatures in finite permutation groups.

The reader should be warned that BMW is currently hypothetical, in the sense that we have not studied how groups and parameter sets should be selected to ensure security or indeed whether this is possible. Some impediments for constructing secure instances of other logarithmic signature-based public-key systems have been discussed by colleagues [13] and these concerns need to be addressed again in the context of BMW. In passing we propose the notion of an anticlosed subset of a group $G$, in particular an anticlosed transversal of a subgroup. It may be the case that such transversals are the “key” to the design of wild-like logarithmic signatures.

2 Preliminaries

By the degree of an abstract finite group $G$ we mean the least integer $n$ such that $\log|G| \leq \lfloor n \log n \rfloor$. On the other hand, for permutation groups the degree $n$ has the usual meaning, that is, the number $n$ of points permuted by the elements of $G$.

If $G$ is a finite group we denote by $G[\mathbb{Z}]$ the collection of all finite sequences in $G$, and view the elements of $G[\mathbb{Z}]$ as single-row matrices with entries in $G$. Under ordinary tensor product of matrices, $G[\mathbb{Z}]$ is a monoid. The following example illustrates the operation,

$$[x_1, x_2, x_3] \otimes [y_1, y_2] = [x_1y_1, x_1y_2, x_2y_1, x_2y_2, x_3y_1, x_3y_2].$$

We simplify notation and write $XY$ for $X \otimes Y$. If $X = [x_1, x_2, \ldots, x_r] \in G[\mathbb{Z}]$, the length $r$ of $X$ is denoted by $|X|$, and $X$ denotes the element $\sum_{i=1}^r x_i$ in the group ring $\mathbb{Z}G$. It is clear that $X Y = Y X$ and $|X Y| = |X| |Y|$, for any $X, Y \in G[\mathbb{Z}]$.

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

32
Moreover, let
\[ \prod_{I=1}^{s} A_i \cdot \ldots \cdot A_s = \sum_{g \in G} a_g g, \quad a_g \in \mathbb{Z} \tag{1} \]

Then, we say that \( \alpha \) is

i) a cover for \( G \) if for all \( g \in G, \quad a_g > 0 \).

ii) a logarithmic signature for \( G \), if for all \( g \in G, \quad a_g = 1 \).

It is clear from the definition that if \( \alpha = [A_1, \ldots, A_s] \) is a logarithmic signature for \( G \), then, each element \( y \in G \) can be expressed uniquely as a product of the form
\[ y = q_1 \cdot q_2 \cdot \ldots \cdot q_{s-1} \cdot q_s \tag{2} \]

for \( q_i \in A_i \). For general covers, however, the factorization in (2) is not unique, and the problem of finding a factorization for a given \( y \in G \) is in general intractable.

Let \( \alpha = [A_1, \ldots, A_s] \) be a logarithmic signature for \( G \) with \( r_i = |A_i| \), then, the \( A_i \) are called the blocks of \( \alpha \) and the vector of block lengths \( (r_1, \ldots, r_s) \) the type of \( \alpha \). We define the length of \( \alpha \) to be the integer \( \ell = \sum_{i=1}^{s} r_i \). We say that \( \alpha \) is nontrivial if \( s \geq 2 \) and \( r_i \geq 2 \) for \( 1 \leq i \leq s \); otherwise \( \alpha \) is said to be trivial.

A logarithmic signature is called tame if the factorization in equation (2) can be achieved in time polynomial in the degree \( n \) of \( G \) and supertame if the factorization can be achieved in time \( O(n^2) \). The existence of supertame logarithmic signatures is discussed in [8]. A logarithmic signature is called wild if it is not tame. We denote by \( C(G) \), and \( \Lambda(G) \) the respective collections of covers and logarithmic signatures of group \( G \).

If \( \alpha = [A_1, \ldots, A_s] \) is a logarithmic signature for a group \( G \), then the sequence \( A_1 \otimes \ldots \otimes A_s \) contains each element of \( G \) exactly once. Thus, \( \alpha \) induces a bijection \( \hat{\alpha} : \mathbb{Z}_{|G|} \rightarrow G \).

Proofs for the following propositions are given in [8]

**Proposition 1** In the class \( \mathcal{G} \) of finite groups there are instances \( (G, \alpha) \), \( \alpha \in G \), where the factorization in (2) is equivalent to solving the discrete logarithm problem in \( G \).
**Proposition 2** Suppose that $\alpha$ is a logarithmic signature of a finite group $G$, then, $\hat{\alpha}$ is always efficiently computable. However, $\hat{\alpha}^{-1}$ is efficiently computable if and only if $\alpha$ is tame.

The following statement follows naturally:

**Proposition 3** Let $G$ be a finite group, $\alpha$ a wild logarithmic signature and $\beta$ a tame logarithmic signature for $G$, then the mapping $\hat{\alpha}\hat{\beta}^{-1} : \mathbb{Z}_{|G|} \to \mathbb{Z}_{|G|}$ is a one-way permutation.

Abusing language somewhat we use the phrase “$\alpha$ can be inverted” to mean that $\hat{\alpha}$ can be inverted efficiently, i.e. that the factorization in (2) is achievable in polynomial time.

**Definition 1** Two logarithmic signatures $\alpha, \beta$ of $G$ are said to be equivalent if $\hat{\alpha} = \hat{\beta}$.

Necessary and sufficient conditions for equivalence of two logarithmic signatures were established in [8].

**Remark 1** If $a$ and $b$ are positive integers and $a \leq b$, by $[a,b]$ we mean the set $\{a, a+1, \ldots, b\} \subset \mathbb{Z}$ (or $\{a\}$ if $a = b$).

## 3 The foundations of BMW

We assume throughout that $G$ is a fixed finite group, and begin with a rather obvious lemma.

**Lemma 1** Suppose that $G$ is a group and $1 \in H \subseteq G$. Then, $H$ is a coset of some subgroup $K \leq G$ if and only if $H \leq G$.

Consider now the following basic lemma:
Lemma 2 Let $G > H > 1$ be a proper, short chain of subgroups of a group $G$. Suppose moreover that when $[G : H] = 2$, there is an element $r \in G - H$ which is not an involution. Then, there exists a complete set $R$ of right coset representatives (right transversal) of $H$ in $G$ such that $1 \in R$, and $R$ is not a coset of any subgroup of $G$, and there exists a complete set $L$ of left coset representatives (left transversal) of $H$ in $G$ such that $1 \in L$, and $L$ is not a coset of any subgroup of $G$.

Proof. We prove the first part of the lemma. By Lemma 1, it suffices to prove the existence of a right transversal $R$ of $H$ in $G$ such that $1 \in R$, where $R$ is not a subgroup of $G$. Suppose that $R$ is any right transversal of $H$ in $G$ with $1 \in R$,

$$R = \{1, r_2, r_3, \ldots, r_m\}.$$ 

If $R$ is not a subgroup of $G$ we are done. Suppose to the contrary that $R \leq G$. Then $R \cap H = 1$ otherwise two cosets $Hr_i, Hr_j$ would be identical for $r_i \neq r_j$. Assume first that $m > 3$. Without loss of generality we can list the elements of $R$ so that $r_3 \neq r_2^{-1}$ and $r_2r_3 = r_4$. Let $h \in H - R = H - \{1\}$ and form

$$R' = \{1, hr_2, r_3, \ldots, r_m\}$$

i.e., obtain $R'$ from $R$ by replacing $r_2$ by $hr_2$. Then $R'$ is a right transversal of $H$ in $G$. $R'$ is no longer a subgroup, since $(hr_2)r_3 = h(r_2r_3) = hr_4 \in Hr_4$, and if $R'$ were a subgroup $hr_4$ would have to be equal to $r_4$, contrary to the fact that $h \neq 1$. Assume next that $m = 3$. Then $R = \{1, r_2, r_3\} \leq G$. Choose $h \in H - R = H - \{1\}$ and form

$$R' = \{1, hr_2, r_3\}.$$ 

If $R'$ were also a subgroup, we would have that $r_3^2 = hr_2 = r_2$, contrary to the fact that $h \neq 1$. Finally, when $m = 2$, let $R = \{1, r\}$, where $r$ is not an involution. Then $R$ is not a subgroup. The second part of our lemma can be handled similarly. □

Our initial goal in framing the above lemma was to develop techniques for constructing $\mathcal{TN}\mathcal{T}$ logarithmic signatures for a given group $G$. In turn, such logarithmic signatures were to be used in the construction of one-way functions in MST$_1$ [9]. However, a recent paper of J.M. Bohli, M.I. González Vasco, C. Martínez and R. Steinwandt [1] shows that a logarithmic signature can be tame as well as $\mathcal{TN}\mathcal{T}$. The
procedure in Lemma 2 can be extended to ensure that the right (left) transversal produced is far from being a subgroup. We suggest that transversals which satisfy some kind of anticlosure property might be the correct objects here.

**Definition 2** A subset S of a group G is said to be anticlosed in G if and only if \( u, v \in S - \{1\} \) implies that \( uv \notin S - \{1\} \).

It is a rather interesting question to ask under what conditions will a subgroup \( H \) of a given group \( G \) have an anticlosed right transversal \( R \). If \( R \) is a right anticlosed transversal of \( G \) then \( R^{-1} \) is clearly a left anticlosed transversal. An anticlosed transversal containing the identity will of course not be a coset of any subgroup in \( G \).

We now establish a generalization of Lemma 2

**Lemma 3** Let \( G > H > K \geq 1 \) be a chain of subgroups of a group \( G \), and if \( [G : H] = 2 \), assume further that there is an element \( f \in G - H \) such that \( f^2 \neq 1 \). Then there exists a left transversal \( L \) of \( H \) in \( G \) such that \( 1 \in L \), and \( LK \) is not a coset of any subgroup of \( G \). Moreover, there is a right transversal \( R \) of \( H \) in \( G \) such that \( 1 \in R \), and \( KR \) is not a coset of any subgroup of \( G \).

**Proof.** We consider here the case where \( [G : H] > 3 \). Let \( R = \{1, r_2, r_3, r_4, \ldots, r_m\} \) be a right transversal of \( H \) in \( G \), and assume that \( KR \) is a subgroup of \( G \). Of course \( r_2 \notin K \) (since \( r_2 \notin H \)). Without loss of generality we may also assume that \( r_3 \notin Hr_2^{-1} \), hence \( r_3r_2 \notin K \). We may thus assume that \( r_3r_2 = k_1r_4 \) for some \( k_1 \in K \).

Now, select an element \( h \in H - K \) and form the new right transversal

\[
R' = \{1, r_2, r_3, hr_4, \ldots, r_m\}
\]

obtained by replacing \( r_4 \) in \( R \) by \( hr_4 \). Now, note that \( KR' \) is not a subgroup of \( G \), for if it were, \( r_3r_2 \in Hr_4 \cap KR' \) implies that \( r_3r_2 = k_2hr_4 \) for some \( k_2 \in K \), thus

\[
r_3r_2 = k_1r_4 = k_2hr_4
\]

which implies that \( k_1r_4 = k_2hr_4 \), or that \( h \in K \) contrary to the choice of \( h \).

The case for the existence of an appropriate left transversal is handled similarly, and so are the cases where \( m = 2 \) or \( 3 \). \( \square \)
The lemma can also be proved by using an argument in [11]. We also note that Lemma 2 follows directly from Lemma 3 by letting $K = 1$.

In the sequel the assumptions required for invoking Lemmas 2 and 3 are made implicitly. We are now in a position to prove a theorem, which is fundamental for our cryptosystem.

**Theorem 1** Let $G = G_0 > G_1 > \cdots > G_{s+1} > G_{s+2} = 1$ be a chain of subgroups of $G$ with $s > 2$. Let $I = \{i_1, i_2, \cdots, i_x\}$ with $x \geq 2$, and $J = \{j_1, j_2, \cdots, j_{s+1-x}\}$ with $s \geq x$ be two subsets of the index set $[1, s + 1]$ such that

\begin{align*}
I \cup J &= [1, s + 1] \\
i_1 < i_2 < \cdots < i_x, \ j_1 < j_2 < \cdots < j_{s+1-x} \\
\{i_x, j_{s+1-x}\} &= \{s + 1, s\} \\
\text{if } i_1 = 1, \text{ then } i_2 &= 3 \\
\text{if } j_1 = 1, \text{ then } j_2 &= 3
\end{align*}

Then for an index $i \in I$, there exists a right transversal $R_i$ of $G_i$ in $G_{i-1}$, and for an index $j \in J$, there exists a left transversal $L_j$ of $G_j$ in $G_{j-1}$, such that $1 \in R_i$, $1 \in L_j$, $i \in I$, $j \in J$, and the following conditions are satisfied:

1. When $1, 3, s + 1 \in I$, none of

\begin{align*}
L_{j_{s+1-x}}G_{s+1} \\
R_y \cdots R_i R_{i_1}, \ y \in [1, x] \\
L_{j_1} L_{j_2} \cdots L_{j_{s+1-x}} R_{i_1} R_{i_{s-1}} \cdots R_{i_1} \\
L_j \ L_{j_1} L_{j_2} \cdots L_{j_{s+1-x}} G_{s+1} R_{i_1} R_{i_{s-1}} \cdots R_{i_1} \\
L_j \ L_{j_1} L_{j_2} \cdots L_{j_{s+1-x}} G_{s+1} R_{i_2} R_{i_{s-1}} \cdots R_{i_1} \end{align*}

are a coset of any subgroup of $G$. 

37
2. When $1, 3, s + 1 \in J$, none of
\[
G_{s+1} R_{y_2} \\
R_y \cdots R_{y_2} R_{i_1}, \quad y \in [1, x-1] \\
L_{j_1} L_{j_2} \cdots L_{j_1}, \quad z \in [1, s + 1 - x] \\
L_{j_1} L_{j_2} \cdots L_{j_1} G_{s+1} R_{i_2} R_{i_2-1} \cdots R_{i_2} \\
L_{j_3} L_{j_4} \cdots L_{j_3} G_{s+1} R_{y_2} R_{i_2-1} \cdots R_{i_2} R_{i_1}
\]
are a coset of any subgroup of $G$.

3. When $1, 3 \in I$ and $s + 1 \in J$, none of
\[
G_{s+1} R_{y_2} \\
R_y \cdots R_{i_2} R_{i_1}, \quad y \in [1, x-1] \\
L_{j_1} L_{j_2} \cdots L_{j_1}, \quad z \in [1, s + 1 - x] \\
L_{j_3} L_{j_4} \cdots L_{j_3} G_{s+1} R_{i_2} R_{i_2-1} \cdots R_{i_2} R_{i_3} \\
L_{j_1} L_{j_2} \cdots L_{j_3} G_{s+1} R_{y_2} R_{y_2-1} \cdots R_{y_2} R_{i_3}
\]
are a coset of any subgroup of $G$.

4. When $1, 3 \in J$ and $s + 1 \in I$, none of
\[
L_{j_3} G_{s+1} \\
R_y \cdots R_{y_2} R_{i_1}, \quad y \in [1, x] \\
L_{j_1} L_{j_2} \cdots L_{j_2}, \quad z \in [1, s - x] \\
L_{j_1} L_{j_2} \cdots L_{j_3} G_{s+1} R_{i_2} R_{i_2-1} \cdots R_{i_2} R_{i_3} \\
L_{j_3} L_{j_4} \cdots L_{j_3} G_{s+1} R_{y_2} R_{i_2-1} \cdots R_{y_2} R_{i_3}
\]
are a coset of any subgroup of $G$.

**Proof.** We now prove the first part of the theorem. In this case, $i_1 = 1$, $i_2 = 3$, $i_x = s + 1$, $j_1 = 2$, $j_{s+1-x} = s$. By Lemma 1, it suffices to prove that each of the subsets listed in the conclusion of this part contains 1 and is not a subgroup of $G$.

Applying Lemma 3 to the subchain of subgroups
\[
G_{s+1} > G_s > G_{s+1} > G_{s+2} = 1
\]
38
we know that there exists a left transversal $L_s$ of $G_s$ in $G_{s-1}$, such that $1 \in L_s$, which is $L_{j_s+1-x}$, and $L_s G_{s+1}$ is not a subgroup of $G$.

We now prove that for an index $x \in [1, s-x]$, there exists a left transversal $L_{j_x}$ of $G_{j_x}$ in $G_{j_x-1}$, such that $1 \in L_{j_x}$ and none of

$$L_{j_1} L_{j_2} \cdots L_{j_p}, \ p \in [1, z]$$

is a subgroup of $G$ by induction on the value of $z$. According to Lemma 2, the conclusion is true for $z = 1$. Suppose the conclusion is also true for $z = k \in [1, s+1-x]$. We are going to prove that the conclusion is true for $z = k+1$. Let

$$L_{j_t} = \{ c_{j_{t1}} = 1, c_{j_{t2}}, \cdots, c_{j_{tp_t}} \}, \ t \in [1, k]$$

be a left transversal of $G_{j_t}$ in $G_{j_t-1}$ such that $1 \in L_{j_t}$ and $L_{j_1} L_{j_2} \cdots L_{j_k}$ is not a subgroup of $G$. And let

$$L_{j_{k+1}} = \{ c_1 = 1, c_2, \cdots, c_q \}$$

be a left transversal of $G_{j_{k+1}}$ in $G_{j_{k+1}-1}$. Suppose that $L_{j_1} L_{j_2} \cdots L_{j_k} L_{j_{k+1}}$ is a subgroup of $G$. We have two cases to consider.

Case 1. $q > 2$.

Since $G_{j_{k+1}} > 1$, choose $g \in G_{j_{k+1}} - \{1\}$, and let $L'_{j_{k+1}} = \{ c_1 = 1, c_2 g, c_3, \cdots, c_q \}$. Then $L'_{j_{k+1}}$ is a left transversal of $G_{k+1}$ in $G_k$. We now show that $L_{j_1} L_{j_2} \cdots L_{j_k} L'_{j_{k+1}}$ is not a subgroup of $G$. Suppose to the contrary that $L_{j_1} L_{j_2} \cdots L_{j_k} L'_{j_{k+1}} \leq G$. Since $L_{j_1} L_{j_2} \cdots L_{j_k} L_{j_{k+1}} \leq G$, we have

$$c_{j_{t1}} \cdots c_{j_{t1} c_3} \cdots c_{j_{t1} c_2} = c_{j_{t1} u_t} \cdots c_{j_{u_t} a_v} c_v, \text{ for some } u_t \in [1, q], \ v \in [1, q]$$

If $v = 2$, then $c_3 = c_{j_{t1} u_t} \cdots c_{j_{u_t} a_v}$. Since $c_3 \neq 1$, some of $c_{j_{t1} u_t}, \cdots, c_{j_{u_t} a_v}$ must not be the identity. Therefore, $c_{j_{t1} u_t} \cdots c_{j_{u_t} a_v} \not\in G_{j_{k+1}-1}$. But $c_3 \in G_{j_{k+1}-1}$. Thus, $v \neq 1, 2$, and then

$$c_{j_{t1} u_t} \cdots c_{j_{u_t} a_v} c_v \in L_{j_{t1} L_{j_{t2}} \cdots L_{j_{u_t}} L'_{j_{k+1}}}$$

On the other hand,

$$c_{j_{t1} u_t} \cdots c_{j_{u_t} a_v} c_v = (c_{j_{t1} c_3}) \cdots (c_{j_{u_t} c_2 g}) \in L_{j_{t1} L_{j_{t2}} \cdots L_{j_{u_t}} L'_{j_{k+1}}}$$

39
Thus, 
\[ g = (c_{j_1} v_1 \cdots c_{j_h} v_h c_h)^{-1} (c_{j_1} u_1 \cdots c_{j_k} u_k c_k g) \in L_{j_1} L_{j_2} \cdots L_{j_k} L'_{j_{k+1}} \]
and then 
\[ g = c_{j_1} v_1 \cdots c_{j_k} v_h c_h, \text{ for some } v_t \in [1, q_t], \ h \in [1, q] \]
Since 
\[ G = L_{j_1} L_{j_2} \cdots L_{j_k} L'_{j_{k+1}} G_{j_{k+1}} \]
we know that each element of \( L_{j_1} L_{j_2} \cdots L_{j_k} L'_{j_{k+1}} G_{j_{k+1}} \) has a unique decomposition into the product of \( k + 2 \) elements each from \( L_{j_1}, L_{j_2}, \cdots, L_{j_k}, L'_{j_{k+1}}, G_{j_{k+1}} \) in this order. But \( g \) has two distinct such decompositions:
\[ g = c_{j_1} v_1 \cdots c_{j_k} v_h c_h = 1 \cdot 1 \cdot g \]
which is impossible. This proves that \( L_{j_1} L_{j_2} \cdots L_{j_k} L'_{j_{k+1}} \) is not a subgroup of \( G \).

Case 2. \( q = 2 \). By the assumption of the theorem, we have \( f \in G_{j_{k+1}} \) with \( f^2 \not\in G_{j_{k+1}+1} \). Let \( L_{j_t}, t \in [1, k] \), be the same as above and
\[ L_{j_{k+1}} = \{c_1 = 1, c_2 = f\} \]
Then \( f \not\in L_{j_1} L_{j_2} \cdots L_{j_k} \). Let \( m \) be the order of \( f \). Then \( m \geq 3 \). Since \( L_{j_1} L_{j_2} \cdots L_{j_k} L_{j_{k+1}} \) is a subgroup, we have
\[ f^2, f^3, \cdots, f^{m-1} \in L_{j_1} L_{j_2} \cdots L_{j_k} L_{j_{k+1}} \]
Therefore, \( c_{j_1} v_1 \cdots c_{j_k} v_h c_h = f^2 \) for some \( v_t \in [1, q_t], \ h \in [1, q] \). If \( h = 1 \), then \( f^2 = c_{j_1} v_1 \cdots c_{j_k} v_h \), which is impossible, because \( f^2 \in G_{j_{k+1}+1} \) but \( c_{j_1} v_1 \cdots c_{j_k} v_h \not\in G_{j_{k+1}+1} \). If \( h = 2 \), then \( e^2 = c_{j_1} v_1 \cdots c_{j_k} v_2 e, \) i.e., \( e = c_{j_1} v_1 \cdots c_{j_k} v_h \), also impossible.
We have thus proved that in this case \( L_{j_1} L_{j_2} \cdots L_{j_k} L'_{j_{k+1}} \) is not a subgroup.
Since each of \( L_{j_1}, L_{j_2}, L_{j_k} \) has not been changed in the above process, for any \( t \in [1, k] \), each \( L_{j_1} L_{j_2} \cdots L_{j_t} \) contains \( 1 \), and is not a subgroup of \( G \) by the induction hypothesis. This completes the induction.

The assertion about \( R_{i_y} \cdots R_{i_2} R_{i_1} \) can be dealt with similarly or can be obtained directly by converting the result about \( R_{i_y} \cdots R_{i_2} R_{i_1} \) in the following way.

40
For any subset $D \subseteq G$, let $D^{-1} = \{d^{-1} \mid d \in D\}$. If $L_j$ is a left transversal of $G_j$ in $G_{j-1}$ containing 1, then $(L_j)^{-1}$ also contains 1 and is a right transversal of $G_j$ in $G_{j-1}$.

Let $L_2$ be determined as above. Applying Lemma 3 to the subchain of subgroups

$$G_0 > G_1 > G_2 > G_{s+1} = 1$$

we obtain a right transversal $R$ of $G_1$ in $G_0$, such that $1 \in R$ and $G_2R$ is not a subgroup of $G$. Since $(L_2,G_2,R)$ and $(L_2,L_{j_2},\ldots,L_{j_{s+1-z}},G_{s+1},R_{i_2},\ldots,R_{i_3},R_3,R_1)$ are both logarithmic signatures for $G$, where $L_{j_2},\ldots,L_{j_{s+1-z}},G_{s+1},R_{i_2},\ldots,R_{i_3},R_3,R_1$ are determined also as above, we have

$$G_2R = L_{j_2} \cdots L_{j_{s+1-z}} G_{s+1} R_{i_2} \cdots R_{i_3} R_1$$

Therefore, $L_{j_2} L_{j_3} \cdots L_{j_{s+1-z}} G_{s+1} R_{i_2} \cdots R_{i_3}$ is not a subgroup and contains 1.

Let $R_3$ be determined as above. Applying Lemma 3 to the subchain of subgroups

$$G_1 > G_2 > G_3 > G_{s+1} = 1$$

we know that there exists a left transversal $L$ of $G_2$ in $G_1$, such that $1 \in L$ and $LG_3$ is not a subgroup of $G$.

Since $(L,G_3,R_3)$ and $(L_2,L_{j_2},\ldots,L_{j_{s+1-z}},G_{s+1},R_{i_2},\ldots,R_{i_3},R_3)$ are both logarithmic signatures for $G_1$, where $L_{j_2},\ldots,L_{j_{s+1-z}},G_{s+1},R_{i_2},\ldots,R_{i_3}$ are determined also as above, we have

$$LG_2 = L_2 L_{j_2} \cdots L_{j_{s+1-z}} G_{s+1} R_{i_2} \cdots R_{i_3}$$

Therefore, $S = L_{j_1} L_{j_2} \cdots L_{j_{s+1-z}} G_{s+1} R_{i_2} \cdots R_{i_3}$ is not a subgroup. Clearly, $1 \in S$.

\[ \square \]

The following theorem is immediate from Theorem 1
**Theorem 2** Let $G = G_0 > G_1 > \cdots > G_{s+1} > G_{s+2} = 1$ be a chain of subgroups of $G$ with $s > 3$. Then for any given $x \in [2, s]$, a logarithmic signature $(A_1, A_2, \cdots, A_s)$ for $G$ can be constructed with the property that none of
\[
A_y, \quad y \in [1, s],
\]
\[
A_1A_2\cdots A_y, \quad y \in [1, s-x],
\]
\[
A_{s+1}A_{s+2}\cdots A_s, \quad z \in [s+2-x, s]
\]
are a coset of any subgroup of $G$.

**Proof.** In the conclusion of case 1 in Theorem 1, let
\[
A_1 = L_{j_1}, \quad A_2 = L_{j_2}, \quad \cdots, \quad A_{s-x} = L_{j_{s-x}}, \quad A_{s+1-x} = L_{j_{s+1-x}}G_{s+1}
\]
\[
A_{s+2-x} = R_{l_x}, \quad A_{s+3-x} = R_{l_{x-1}}, \quad \cdots, \quad A_s = R_{l_z}R_{t_1}
\]
Then we get Theorem 2. \hfill \Box

We illustrate Theorems 1 and 2 by means of the following example.

**Example 1** Consider the parameters $s = 6$, $x = 3$, the index sets $I = \{1, 3, 7\}$, $J = \{2, 4, 5, 6\}$ and the subgroup chain
\[
G = G_0 > G_1 > G_2 > \cdots > G_6 > G_7 > G_8 = 1.
\]
$I$ induces right transversals $R_1$, $R_3$, and $R_7$, while $J$ induces left transversals $L_2$, $L_4$, $L_5$, and $L_6$, as follows:
\[
G_0 = G_1R_1
\]
\[
G_1 = L_2G_2
\]
\[
G_2 = G_3R_3
\]
\[
G_3 = L_4G_4
\]
\[
G_4 = L_5G_5
\]
\[
G_5 = L_6G_6
\]
\[
G_6 = G_7R_7
\]
i.e. the factorization:

\[ G = (L_2((L_4(L_5(L_6(G_7R_7))))R_3))R_1. \]

Rearranging parentheses we get

\[ G = (L_2)(L_4)(L_5)(L_6G_7)(R_7)(R_3R_1) = A_1A_2A_3A_4A_5A_6 \]

satisfying the properties stated in the conclusions of Theorems 1 and 2.

Now, for the purposes of the cryptosystem we describe below, we modify the above 
\((A_1, \ldots, A_6)\) by setting \(B_i = A_i\) for \(i \neq 4\) and setting \(B_4 = L_6\). That is, by removing
the subgroup \(G_7\) from \(A_4 = L_6G_7\). The product \(\overline{B_5} \cdots \overline{B_6}\) is now a proper subset of
\(G\). The new sequence \(B_i\) may further need to be modified to ensure that \(\overline{B_1} \cdots \overline{B_5}\) and \(\overline{B_2} \cdots \overline{B_6}\) are not subgroups of \(G\).

## 4 Cryptosystem BMW and Its Security

Suppose we are given a subgroup chain \(G = G_0 > G_1 > \cdots > G_{s+1} > G_{s+2} = 1\) with \(s > 3\). Then, corresponding to any case in Theorem 1, we can construct
\(A_i\)'s as in Theorem 2. Next, we construct a sequence of \(B_i \in G^{[\mathbb{Z}]}\), by setting
\(B_i = A_i\) except for the index \(i = v\) for which the subgroup \(G_{s+1}\) is hidden in \(A_v\),
(i.e. where \(A_v = L_jG_{s+1}\), or \(A_v = G_{s+1}R_k\).) For this index we set \(B_v = L_j\) or
\(R_k\) accordingly. The elements of sequences \(B_i\) are ordered in an arbitrary way,
say \(B_i = (B_{i,1}, B_{i,2}, \ldots, B_{i,\phi})\). If necessary, we further modify \((B_1, \ldots, B_s)\), so
that the products \(\overline{B_1} \cdots \overline{B_{s-1}}\) and \(\overline{B_2} \cdots \overline{B_s}\) are not subgroups of \(G\). We note that
\(\Gamma = B_1 \cdots B_s\) is now a proper subset of \(G\). Moreover, if the initial chain of subgroups
is known, for any element \(g \in \Gamma\) the factorization \(g = b_1 \cdots b_s\), \(b_i \in B_i\) can be
recovered efficiently.

The description of our cryptosystem.
• The plaintext space: \( M = \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_s} \)
• The public key: \( (B_1, B_2, \cdots, B_s) \)
• The secret key: \( (G_1, G_2, \cdots, G_{s+1}, I, J) \)
• The ciphertext space: \( \Gamma \)
• The encryption function: For \( (n_1, n_2, \cdots, n_s) \in M \),
  \[ e(n_1, n_2, \cdots, n_s) = B_{1,n_1}B_{2,n_2} \cdots B_{s,n_s} = g \in \Gamma \]
• The decryption function: For \( g \in \Gamma \),
  \[ d(g) = (n_1, n_2, \cdots, n_s) \]
where \( n_i \) are the indices satisfying \( g = B_{1,n_1} \cdots B_{s,n_s} \). These indices can be easily determined from \( g \) based on the knowledge of both the public key \( (B_1, \cdots, B_s) \) and the secret key \( (G_1, G_2, \cdots, G_{s+1}, I, J) \).

In order to decrease the computational complexity of the encryption and decryption processes and to acquire higher security for the system, we make some reasonable assumptions on the chain of subgroups \( G = G_0 > G_1 > \cdots > G_{s+1} > G_{s+2} = 1 \).

In the sequel we suppose that:

i) \( G \) is a permutation group of degree \( \Theta(n) \)
ii) \( |G| = \Theta(n^c) \), where \( c \) is a positive constant
iii) \( |G_i : G_{i-1}| = \Theta(n^{c_i}) \), where \( c_i \) is a positive constant, \( i \in [1, s] \), and \( s = \Theta(n) \)
iv) \( x/n = d_i \) a constant, so that \( 0 < d < 1 \)
v) The number of generators of \( G_i = O(d_i n) \),
vi) \( d_i \) is a positive constant
Here, we use the term ‘constant’ to mean a value independent of $n$. From its definition we know that the encryption function can be computed in time polynomial in $n$.

It is known that membership in a permutation group can be tested in time polynomial in the degree and the number of generators [4]. Therefore, under the above assumptions, decryption can be carried out in time polynomial in $n$ at each step as well as for the entire process.

Let $g \in \Gamma$ be an arbitrary encrypted message. A BMW attacker could attempt to solve the equation

$$g = g_1 g_2, \quad g_1 \in B_1 B_2 \cdots B_t, \quad g_2 \in B_{t+1} B_{t+2} \cdots B_s,$$

for some $t \in [1, s-1]$. In fact a solution exists uniquely for each $t \in [1, s-1]$. If the attacker succeeds in finding a solution $g = g_1 g_2$ to equation (3), she can continue in a similar and obvious manner until she obtains the complete factorization

$$g = b_1 b_2 \cdots b_s, \quad b_i \in B_i.$$

After finding $g_1$ and $g_2$ and at each subsequent step the attacker has to solve problems of diminishing complexity, similar to (3). The main problem is in fact a multiplicative version of the well known knapsack problem in a general group $G$.

The fact that neither of the component sets $\mathcal{L}_t = B_1 \cdots B_t$, or $\mathcal{R}_t = B_{t+1} \cdots B_s$ is a subgroup (for any $t$) provides no special help to the attacker, particularly if the left and right transversals constructed are as far away as possible from being subgroups. The attacker could make $t$ large, hence $\mathcal{R}_t$ small, so that she can attempt to solve the problem:

For which $h \in \mathcal{R}_t$ is $gh^{-1} \in \mathcal{L}_t$ ?

(There is a unique such $h \in \mathcal{R}_t$ !) A solution to this problem clearly solves (3). Choosing $\mathcal{R}_t$ small does not help because then $\mathcal{L}_t$ is large. In any case, to our
knowledge, there is no efficient algorithm to decide membership in \( \mathcal{L}_t \) if \( \mathcal{L}_t \) is not a subgroup. If the attacker did find an \( h \in \mathcal{R}_t \) such that \( gh^{-1} \in \mathcal{L}_t \) she will still have to factor \( gh^{-1} \) and \( h \) with respect to the components \( B_t \) of \( \mathcal{L}_t \) and \( \mathcal{R}_t \) respectively. The attacker might as well choose a value of \( t \) such that \( |\mathcal{L}_t| \) and \( |\mathcal{R}_t| \) are approximately equal. This leads to a meet in the middle attack which has complexity roughly \( O(\sqrt{|G|}) \) and can be discounted. If the transversals are selected so they are far from being subgroups, say anticlosed in particular, the authors of this paper know of no efficient way to obtain the required factorizations.

The attacker may also try to recover the chain of subgroups in the private key using what is known about the public key. If the attacker had to deal with factorization with respect to the original \((A_1, \ldots, A_s)\), rather than the modified \((B_1, \ldots, B_s)\), \( G_{s+1} \) would not have been removed from \( A_v \) and it would take \( O(n) \) operations to determine the index \( v \): simply test which one \( A_i A_{i+1} \) is a subgroup, where \( i \) runs over \([1, s - 2]\). After finding the value of \( i \) for which \( A_i A_{i+1} \) is a subgroup, the attacker would still need to determine which one of \( A_{i-1} A_i A_{i+1} \) or \( A_i A_{i+1} A_{i+2} \) is a subgroup. This requires 2 tests. Continuing in an obvious way, the attacker would have \( s \) steps to go, and at each step there would be two possibilities to test. Altogether there would be \( 2s \) tests to perform and this process would determine almost completely the subgroup chain. However, assuming that none of the \( B_i \), and much stronger conditions, namely that

\[
\text{none of } B_i B_{i+1} \cdots B_r \text{ are subgroups, for any } 1 \leq i \leq r \leq s.
\]

we see of no procedure that the attacker can use to recover efficiently the initial subgroup chain. Although not all of the conditions above are implied by our Theorems 1 and 2, we believe that most if not all should be achievable.

References


47


Jean-Camille Birget  
Department of Computer Science  
Rutgers University - Camden  
Email: birget@epion.rutgers.edu

Spyros S. Magliveras$^1$  
Department of Mathematical Sciences  
Florida Atlantic University  
Email: spyros@fau.edu

Wandi Wei  
Department of Computer Science  
Western Illinois University  
Email: wandi.wei@hotmail.com.

---

$^1$ The author was supported in part by NSF grant number CCR-9610138