J. Cryptology (1995) 8: 157–166

Journal of
CRYPTOLOGY

The Cryptanalysis of a Public-Key Implementation of Finite Group Mappings

Simon Blackburn* and Sean Murphy
Information Security Group, Royal Holloway and Bedford New College,
University of London, Egham, Surrey TW20 0EX, England

Jacques Stern
Laboratoire d'Informatique, Ecole Normale Supérieure,
45 Rue d'Ulm, 75230 Paris 05, France

Communicated by Don Coppersmith

Received 4 March 1993 and revised 20 January 1994

Abstract. Minghua Qu and Vanstone [2] have proposed a public-key cryptosystem (FGM) which is based on factorizations of a binary vector space (i.e., transversal logarithmic signatures of an elementary abelian 2-group). In this paper a generalized (basis-independent) decryption algorithm is given, which shows that there are many equivalent private keys, and a method of efficiently obtaining such an equivalent private key is given. The FGM cryptosystem is thus rendered insecure. Although the FGM cryptosystem is defined in terms of linear algebra, the attack given here is essentially group-theoretic in nature. Thus this attack throws doubt on any cryptosystem which relies on the security of transversal logarithmic signatures.

Key words. Public-key cryptosystems, Finite group mappings, Permutation group mappings, Logarithmic signatures.

1. Introduction

The paper is organized as follows. Section 2 gives a description of the *Finite Group Mappings* (FGM) public-key cryptosystem proposed by Minghua Qu and Vanstone [2] and a generalized decryption algorithm for FGM which shows that there are many equivalent private keys. Section 3 constructs part of such an equivalent private key from the public key. The next two sections show how to decrypt with this information and construct the rest of an equivalent private key. The final section gives some conclusions.

*This author was supported by S.E.R.C. Research Grant GR/H23719.

2. The FGM Public-Key Cryptosystem

Let n be an integer such that $n > 4$ and $n \equiv 0 \bmod 4$. We describe the public-key system given in [2], which encrypts $(n-4)$-bit messages into n-bit ciphertexts.

Let $G := \mathbf{Z}_2^n$ be a vector space over $\mathbf{Z}_2$ of dimension n and let

$$\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$$

be an arbitrary basis for G. Define a chain of subspaces

$$G = G_0 > G_1 > \cdots > G_{n/2} = \{0\}, \tag{1}$$

where

$$G_i := \langle \alpha_{2i+1}, \alpha_{2i+2}, \ldots, \alpha_n \rangle$$

when i is such that $1 \leq i \leq n/2 - 1$ and where $G_{n/2} = \{0\}$.

For all integers i such that $1 \leq i \leq n/4 - 1$, define A_i by

$$\bar{A}_i := \{\bar{\alpha}[i,0], \bar{\alpha}[i,1], \bar{\alpha}[i,2], \bar{\alpha}[i,3]\},$$

where the elements $\bar{\alpha}[i,j]$ are arbitrary elements of G subject to the condition that, for any $t_1, t_2 \in \{0,1\}$,

$$\bar{\alpha}[i, t_1 + 2t_2] \equiv t_1\alpha_{2(i-1)+1} + t_2\alpha_{2(i-1)+2} \mod G_i. \tag{2}$$

Then $\bar{A}_i$ is a complete set of coset representatives of G_i in G_{i-1}.

For all integers i and h such that $n/4 \leq i \leq n/2 - 2$ and $0 \leq h \leq 3$, define

$$\bar{A}_{i,h} := \{\bar{\alpha}[i,0]_h, \bar{\alpha}[i,1]_h, \bar{\alpha}[i,2]_h, \bar{\alpha}[i,3]_h\},$$

where the elements $\bar{\alpha}[i,j]_h$ are arbitrary elements of G subject to the condition that, for any $t_1, t_2 \in \{0,1\}$,

$$\bar{\alpha}[i, t_1 + 2t_2]_h \equiv t_1\alpha_{2(i-1)+1} + t_2\alpha_{2(i-1)+2} \mod G_i. \tag{3}$$

Clearly, for any $h \in \{0, 1, 2, 3\}$, $\bar{A}_{i,h}$ is a complete set of coset representatives of G_i in G_{i-1}.

Define f to be any one-to-one function such that

$$f\colon \left\{1, 2, \ldots, \frac{n}{4} - 1\right\} \to \left\{\frac{n}{4}, \ldots, \frac{n}{2} - 2\right\}.$$

Finally, when i is an integer such that $1 \leq i \leq n/4 - 1$, we define

$$A_i := \bigcup_{h=0}^{3} \left\{\bar{\alpha}[i,h] + \bar{A}_{f(i),h}\right\} = \{\alpha[i,j] \mid 0 \leq j \leq 15\},$$

where

$$\alpha[i, s + 4h] := \bar{\alpha}[i,h] + \bar{\alpha}[f(i), s]_h \tag{4}$$

for any $h, s \in \{0, 1, 2, 3\}$.

The *public key* is the collection of blocks

$$A_i \quad \text{where} \quad 1 \le i \le \frac{n}{4} - 1.$$

In [2] the *private key* is given as the collection of blocks

$$\bar{A}_i \quad \text{where} \quad 1 \le i \le \frac{n}{4} - 1,$$

the collection of blocks

$$\bar{A}_{i,h} \quad \text{where} \quad \frac{n}{4} \le i \le \frac{n}{2} - 2 \quad \text{and} \quad 0 \le h \le 3,$$

the function f, and the basis $\{\alpha_1, \ldots, \alpha_n\}$. In fact, we may reduce the amount of information contained in the private key and still decrypt efficiently. We take the private key to be the blocks $\bar{A}_i$ and $\bar{A}_{i,h}$, the function f, and, instead of the basis $\{\alpha_1, \ldots, \alpha_n\}$, the chain of subspaces (1).

We now give a description of the encryption process. An $(n - 4)$-bit message may be regarded as an integer m such that $0 \le m \le 2^{n-4} - 1$. To encrypt, we first express m in hexadecimal as $(p_1, \ldots, p_{n/4-1})$, so $0 \le p_i \le 15$, where

$$m = p_1 + 16p_2 + \cdots + 16^{n/4-1}p_{n/4-1}.$$

We define an element $g \in G$ by

$$g := \alpha[1, p_1] + \alpha[2, p_2] + \cdots + \alpha\left[\left(\frac{n}{4} - 1\right), p_{n/4-1}\right]. \tag{5}$$

Now, we can write g as a binary n-tuple $(q_1, \ldots, q_n)$ which we may regard as a number between 0 and $2^n - 1$. We take the ciphertext c to be

$$c := q_1 + 2q_2 + \cdots + 2^{n-1}q_n. \tag{6}$$

Following [2], we decrypt as follows. Let c be the ciphertext, so we can express c in the form (6) to obtain

$$g = (q_1, \ldots, q_n).$$

We find $p_1, \ldots, p_{n/4-1}$ satisfying (5) by applying the following algorithm:

```
for $i = 1$ to $\frac{n}{4} - 1$ do:
Set $h_i = \mathit{findcoset}(g, i)$
Set $g = g - \bar{\alpha}[i, h_i]$
Return "$h_i$"

For $i = \frac{n}{4}$ to $\frac{n}{2} - 2$ do:
Set $h_i = \mathit{findcoset}(g, i)$
Set $g = g - \bar{\alpha}[i, h_i]_{h_{f^{-1}(i)}}$
Set $p_{f^{-1}(i)} = h_i + 4h_{f^{-1}(i)}$
Return "$p_{f^{-1}(i)}$"
```

Here the function *findcoset*(g, i) returns the value $t_1 + 2t_2$ where

$$g \equiv t_1 \alpha_{2(i-1)+1} + t_2 \alpha_{2(i-1)+2} \mod G_i.$$

The decryption algorithm presented here differs from that given in [2] by our drawing together that part of the algorithm concerning itself with finding the h_i into a separate subroutine *findcoset*. That part of the algorithm in [2] which corresponds to *findcoset* uses knowledge of the elements $\alpha_1, \ldots, \alpha_n$ to calculate h_i. We give a generalized algorithm which implements *findcoset* which only uses knowledge of the chain of subgroups (1). This decryption algorithm is of comparable speed to the decryption algorithm presented in [2].

```
findcoset$(g, i)$ $\left[i \le \frac{n}{4} - 1\right]$
For $j = 0$ to 3 do:
If $g - \bar{\alpha}[i, j] \in G_i$
    Set $h_i = j$.
```

```
findcoset$(g, i)$ $\left[i \ge \frac{n}{4}\right]$
For $j = 0$ to 3 do:
If $g - \bar{\alpha}[i, j]_0 \in G_i$
    Set $h_i = j$.
```

The justification for this algorithm is (2) when $i \le n/4 - 1$ and (3) otherwise. Examining the first half of the decryption algorithm, we find that the only properties of the subspaces G_k, $1 \le k \le n/4 - 1$, that the algorithm uses are:

$$\left.\begin{array}{ll} \text{(P1)} & \bar{\alpha}[i, s] \in G_k, \text{where } k + 1 \le i \le n/4 - 1. \\ \text{(P2)} & \bar{\alpha}[i, s]_h \in G_k, \text{where } n/4 \le i \le n/2 - 2, 0 \le h,\ s \le 3. \\ \text{(P3)} & \text{The cosets } \bar{\alpha}[k, s] + G_k\ (s = 0, 1, 2, 3) \text{ are distinct.} \end{array}\right\} \tag{7}$$

Hence any subspaces satisfying (P1)–(P3) may replace subspaces $G_1, \ldots, G_{n/4-1}$ in the decryption algorithm. Note that an analogous list of properties exists for subspaces $G_{n/4}, \ldots, G_{n/2-2}$, but we defer considering this list until later.

We are now ready to begin cryptanalysis of the system.

3. An Equivalent Set of Private-Key Blocks

Let K be a private key. We may, of course, assume that we know the public key associated with K. Suppose that we also know the function f. This section describes the construction of the blocks of a private key K^* which decrypts messages encrypted using the public key associated with K. Thus the private key K^* is equivalent to the private key K.

For integers i and h such that $1 \le i \le n/4 - 1$ and $0 \le h \le 3$, define the vector $\bar{\alpha}^*[i, h]$ by

$$\bar{\alpha}^*[i, h] := \alpha[i, 4h]. \tag{8}$$

We also define, for integers i, s, and h such that $1 \le i \le n/4 - 1$, $0 \le h \le 3$, and $0 \le s \le 3$, the vector $\bar{\alpha}^*[f(i), s]_h$ by

$$\bar{\alpha}^*[f(i), s]_h := \alpha[i, s + 4h] + \alpha[i, 4h]. \tag{9}$$

Finally, we define blocks $\bar{A}_i^*$ by

$$\bar{A}_i^* := \{\bar{\alpha}^*[i,0], \bar{\alpha}^*[i,1], \bar{\alpha}^*[i,2], \bar{\alpha}^*[i,3]\},$$

where i is such that $1 \le i \le n/4 - 1$, and blocks $\bar{A}_{i,h}^*$ by

$$\bar{A}_{i,h}^* := \{\bar{\alpha}^*[i,0]_h, \bar{\alpha}^*[i,1]_h, \bar{\alpha}^*[i,2]_h, \bar{\alpha}^*[i,3]_h\},$$

where i and h are such that $n/4 \le i \le n/2 - 2$ and $0 \le h \le 3$. We can now construct a key K^* defined by $\{\bar{A}_i^* \mid i \le k \le n/4 - 1\}$, $\{\bar{A}_{i,h}^* \mid (n/4) \le i \le n/2 - 2, 0 \le h \le 3\}$, f, and the chain (1). We show that K^* is a valid private key and furthermore that the public key associated with K^* is the same as the public key associated with K.

Theorem. *The key K^* defined by $\{\bar{A}_i^* \mid 1 \le i \le n/4 - 1\}$, $\{\bar{A}_{i,h}^* \mid (n/4) \le i \le n/2 - 2, 0 \le h \le 3\}$, f, and the chain* (1) *is a valid private key.*

Proof. Let i be an integer such that $1 \le i \le n/4 - 1$. Then, for any $t_1, t_2 \in \{0, 1\}$,

$$\begin{aligned}\bar{\alpha}^*[i, t_1 + 2t_2] &= \alpha[i, 4t_1 + 8t_2] \\ &= \bar{\alpha}[i, t_1 + 2t_2] + \bar{\alpha}[f(i), 0]_h.\end{aligned}$$

Hence $\bar{\alpha}^*[i, t_1 + 2t_2] \equiv \bar{\alpha}[i, t_1 + 2t_2] \equiv t_1\alpha_{2(i-1)+1} + t_2\alpha_{2(i-1)+2} \bmod G_i$ since $\bar{\alpha}[f(i), 0]_h \in G_{f(i)} < G_i$.

If i, s, and h are integers such that $n/4 \le i \le n/2 - 2$, $0 \le s$, $h \le 3$, then

$$\begin{aligned}\bar{\alpha}^*[i, s]_h &= \alpha[f^{-1}(i), s + 4h] + \alpha[f^{-1}(i), 4h] \\ &= \bar{\alpha}[f^{-1}(i), h] + \bar{\alpha}[i, s]_h + \bar{\alpha}[f^{-1}(i), h] + \bar{\alpha}[i, 0]_h \\ &= \bar{\alpha}[i, s]_h + \bar{\alpha}[i, 0]_h.\end{aligned}$$

So since $\bar{\alpha}[i, 0]_h \in G_i$, for $t_1, t_2 \in \{0, 1\}$ such that $s = t_1 + 2t_2$,

$$\bar{\alpha}^*[i, s]_h \equiv \bar{\alpha}[i, s]_h \equiv t_1\alpha_{2(i-1)+1} + t_2\alpha_{2(i-1)+2} \mod G_i.$$

Hence the elements $\bar{\alpha}^*[i, s]$ satisfy (2) and the elements $\bar{\alpha}^*[i, s]_h$ satisfy (3). So K^* is a valid private key. □

Corollary. *The private keys K and K^* are equivalent.*

Proof. Consider the public key $\{A_i^*\}$ associated with K^*. For all i, s, and h such that $1 \le i \le n/4 - 1$, $0 \le s \le 3$, and $0 \le h \le 3$,

$$\begin{aligned}\alpha^*[i, s + 4h] &= \bar{\alpha}^*[i, h] + \bar{\alpha}^*[f(i), s]_h \\ &= \alpha[i, 4h] + \alpha[i, s + 4h] + \alpha[i, 4h] \\ &= \alpha[i, s + 4h].\end{aligned}$$

Hence the public keys associated with K and K^* are identical. Therefore the private keys K and K^* are equivalent. □

We now discuss how much information we have about the blocks of K^* if we have no knowledge of f. Since (8) does not depend on f, we may still construct the blocks $\overline{A}_i^*$ where i is such that $1 \leq i \leq n/4 - 1$. If we set

$$\beta[i, s]_h := \alpha[i, s + 4h] + \alpha[i, 4h] \tag{10}$$

and define $B_{i,h}$ by

$$B_{i,h} := \{\beta[i, 0]_h, \beta[i, 1]_h, \beta[i, 2]_h \beta[i, 3]_h\},$$

then we know that, for a fixed h, the blocks $B_{i,h}$ where $1 \leq i \leq n/4 - 1$ are some rearrangement of the blocks $\overline{A}_{i,h}^*$ where $n/4 \leq i \leq n/2 - 2$. Indeed, for fixed h and s such that $0 \leq h \leq 3$ and $0 \leq s \leq 3$ we may assert that the vectors

$$\beta[i, s]_h \qquad \text{where} \quad 1 \leq i \leq \frac{n}{4} - 1$$

are some rearrangement of the vectors

$$\overline{\alpha}^*[i, s]_h \qquad \text{where} \quad \frac{n}{4} \leq i \leq \frac{n}{2} - 2.$$

In particular, the subspace H defined by

$$\begin{aligned} H &:= \left\langle \overline{\alpha}^*[i, s]_h | \frac{n}{4} \leq i \leq \frac{n}{2} - 2, 0 \leq s, h \leq 3 \right\rangle \\ &= \left\langle \beta[i, s]_h | 1 \leq i \leq \frac{n}{4} - 1, 0 \leq s, h \leq 3 \right\rangle \end{aligned} \tag{11}$$

can be constructed using only our knowledge of the public key.

4. The Beginning of the Decryption Process

In this section we analyse the top half of the chain of subgroups (1) and show how to construct the top half of an equivalent chain of subgroups, which can be used to decrypt half of any ciphertext.

Any ciphertext block c can be expressed as

$$c = q_1 + 2q_2 + \cdots + 2^{n-1}q_n,$$

where $q_1, \ldots, q_n \in \mathbf{Z}_2$. We set $g := (q_1, \ldots, q_n) \in G$. Our goal is to find

$$p_1, \ldots, p_{n/4-1} \in \{0, 1, \ldots, 15\}$$

such that

$$g = \alpha[1, p_1] + \cdots + \alpha\left[\left(\frac{n}{4} - 1\right), p_{n/4-1}\right].$$

If we write $p_i := s_i + 4h_i$, then an equivalent problem is to find

$$s_1, \ldots, s_{n/4-1}, h_1, \ldots, h_{n/4-1}$$

such that

$$g = \bar{\alpha}[1, h_1] + \cdots + \bar{\alpha}\left[\left(\frac{n}{4} - 1\right), h_{n/4-1}\right]$$
$$+ \bar{\alpha}[f(1), s_1]_{h_1} + \cdots + \bar{\alpha}\left[f\left(\frac{n}{4} - 1\right), s_{n/4-1}\right]_{h_{n/4-1}}.$$

By the previous section, we may write

$$\begin{aligned} g &= \sum_{i=1}^{n/4-1} \bar{\alpha}[i, h_i] + \sum_{i=1}^{n/4-1} \bar{\alpha}[f(i), s_i]_{h_i} \\ &= \sum_{i=1}^{n/4-1} \bar{\alpha}^*[i, h_i] + \sum_{i=1}^{n/4-1} \beta[i, s_i]_{h_i}. \end{aligned} \tag{12}$$

The construction of the top half of an equivalent chain of subgroups enables us to find the integers $h_1, \ldots, h_{n/4-1}$ in expression (12).

From Section 2 we know that the only properties of the subgroups G_k, where $1 \leq k \leq n/4 - 1$, that the algorithm uses when decrypting using key K are (P1)–(P3) given in (7). Analogously, the algorithm decrypting using key K^* uses only the properties:

(Q1) $\bar{\alpha}[i, s] \in G_k$, where $k + 1 \leq i \leq n/4 - 1$.
(Q2) $\bar{\alpha}^*[i, s]_h \in G_k$, where $n/4 \leq i \leq n/2 - 2$, $0 \leq s$, and $h \leq 3$.
(Q3) The cosets $\bar{\alpha}^*[k, s] + G_k$ $(s = 0, 1, 2, 3)$ are distinct.

Using definition (11) of H in Section 2, we may write (Q2) more succinctly as property (Q2′):

(Q2′) $H \leq G_k$.

We define subspaces G_k^* where $1 \leq k \leq n/4 - 1$ by

$$G_k^* := \left\langle \left\{ \bar{\alpha}^*[i, s] \mid k + 1 \leq i \leq \frac{n}{4} - 1, 0 \leq s \leq 3 \right\} \right\rangle + H.$$

Note that the definition of G_k^* depends only on knowledge of the public key. Clearly, G_k^* satisfies properties (Q1) and (Q2′). To see that G_k^* also satisfies property (Q3), observe that $G_k^* \leq G_k$ (since G_k satisfies (Q1) and (Q2′)). Then, for any $s, s' \in \{0, 1, 2, 3\}$ such that

$$\bar{\alpha}^*[k, s] \equiv \bar{\alpha}^*[k, s'] \mod G_k^*,$$

we have

$$\bar{\alpha}^*[k, s] \equiv \bar{\alpha}^*[k, s'] \mod G_k,$$

hence that $s = s'$. So G_k^* satisfies (Q3).

In consequence of subspaces G_k^* satisfying properties (Q1), (Q2′), and (Q3), we may use them in place of subspaces G_k in the first half of the decryption algorithm. Since the definitions of G_k^* and $\bar{\alpha}^*[i, s]$ depend only on the public key, we may use the first half of the decryption algorithm as presented in Section 1 to find the correct values of $h_1, \ldots, h_{n/4-1}$.

Hence we have already recovered half the bits of the message. We recover the remainder in the next section.

5. The End of the Decryption Process

Using the methods of the previous section, we have reduced the problem of decryption to determining the decomposition

$$g = \beta[1, s_1]_{h_1} + \cdots + \beta\left[\frac{n}{4} - 1, s_{n/4-1}\right]_{h_{n/4-1}}, \tag{13}$$

where the vector g and the integers $h_1, \ldots, h_{n/4-1}$ are known.

We first give, and justify, an algorithm for finding a one-to-one function

$$f^*\colon \left\{1, 2. \ldots, \frac{n}{4} - 1\right\} \to \left\{1, 2, \ldots, \frac{n}{4} - 1\right\},$$

and subspaces $H_1, \ldots, H_{n/4-1}$ with the following properties

(R1) $\beta[f^*(i), s]_h \in H_k$ where $k + 1 \leq i \leq n/4 - 1$, $0 \leq s, h \leq 3$.
(R2) $\beta[f^*(k), s]_0 + \beta[f^*(k), s]_h \in H_k$ where $0 \leq s, h \leq 3$.
(R3) The cosets of H_k containing the elements $\beta[f^*(k), j]_0$, where $0 \leq j \leq 3$, are distinct.

We then show that once f^* and $H_1, \ldots, H_{n/4-1}$ have been constructed, we may decompose g into the sum (13). The algorithm for finding f^* and $H_1, \ldots, H_{n/4-1}$ *findsubspaces* say, can be written in the following manner:

```
findsubspaces
Set $S = \{1, 2, \ldots, \frac{n}{4} - 1\}$
For $k = 1$ to $\frac{n}{4} - 1$ do:
Find $i_0 \in S$ such that the cosets $\beta[i_0, s]_0 + W_{i_0}$ $(s = 0, 1, 2, 3)$ are
  distinct, where
$W_{i_0} := \langle \beta[i, s]_h, \beta[i_0, s]_0 + \beta[i_0, s]_h \mid i \in S \setminus \{i_0\}, 0 \leq s, h \leq 3 \rangle$.
Set $f^*(k) = i_0$, $H_k = W_{i_0}$, $S = S \setminus \{i_0\}$.
```

This algorithm clearly produces f^*, $H_1, \ldots, H_{n/4-1}$ satisfying properties (R1)–(R3), provided that at every stage an integer i_0 can always be found which satisfies the conditions of the algorithm *findsubspaces*. We now show in the following lemma that this is indeed the case.

Lemma. *At every iteration of k between* 1 *and* $n/4 - 1$, *the algorithm* findsubspaces *produces a value* i_0.

Proof. Suppose that $\emptyset \neq S \subseteq \{1,\ldots,n/4-1\}$. Set $i_0 \in S$ to be the unique element such that

$$f(i_0) = \min_{i \in S}\{f(i)\}.$$

Now, $W_{i_0} \leq G_{f(i_0)}$, since firstly

$$\beta[i, s]_h = \bar{\alpha}^*[f(i), s]_h \in G_{f(i)-1} \leq G_{f(i_0)}$$

for all $i \in S \setminus \{i_0\}$ and $0 \leq s,\ h \leq 3$, and secondly

$$\beta[i_0, s]_0 + \beta[i_0, s]_h \in G_{f(i_0)} \qquad \text{for all} \quad 0 \leq s \leq 3, \quad 0 \leq h \leq 3.$$

However, now we may deduce that, for all $s, s' \in \{0, 1, 2, 3\}$,

$$\beta[i_0, s]_0 \equiv \beta[i_0, s']_0 \mod W_{i_0}$$

implies that

$$\beta[i_0, s]_0 \equiv \beta[i_0, s']_0 \mod G_{f(i_0)},$$

and hence that $s = s'$. Therefore W_{i_0} satisfies property (R3). Since clearly W_{i_0} satisfies properties (R1) and (R2), we deduce that i_0 is a valid choice for $f^*(k)$, as required. □

Once we have obtained f^*, $H_1,\ldots,H_{n/4-1}$, our decryption algorithm is as follows:

```
For $k = 1$ to $\frac{n}{4} - 1$ do:
Find $s_{f^*(k)}$ such that $\beta[f^*(k), s_{f^*(k)}]_0 \equiv g \mod H_k$
Set $g = g - \beta[f^*(k), s_{f^*(k)}]_{h_{f^*(k)}}$
Set $p_{f^*(k)} = s_{f^*(k)} + 4h_{f^*(k)}$
Return "$p_{f^*(k)}$"
```

At each stage of the algorithm, g is of the form

$$g = \beta\left[f^*(k), s_{f^*(k)}\right]_{h_{f^*(k)}} + \sum_{i=k+1}^{n/4-1} \beta\left[f^*(i), s_{f^*(i)}\right]_{h_{f^*(i)}}.$$

Hence

$$g \equiv \beta\left[f^*(k), s_{f^*(k)}\right]_0 \mod H_k$$

by properties (R1) and (R2). Since property (R3) is satisfied, we can determine $s_{f^*(k)}$ uniquely by finding the coset of H_k containing g.

We have found blocks $\bar{A}_i^*$ and $\bar{A}_{i,h}^*$ subspaces $G_1^*,\ldots,G_{n/4-1}^*$, $H_1,\ldots,H_{n/4-1}$, and a function f^* entirely from the public key. Since these objects form a private key equivalent to the original private key, we are now able to decrypt an arbitrary cryptogram.

6. Conclusions

In this paper we have shown Minghua Qu and Vanstone's FGM public-key cryptosystem [2] to be insecure. We were able to do this by noting that a generalized decryption algorithm exists that does not depend directly on the basis chosen. Thus there is redundant information in the private key given in [2] and there are many equivalent private keys. We have given a method to construct one of these equivalent private keys from the public key that is computationally similar to the original decryption algorithm, that is essentially calculating linear dependences of sets of vectors. We also note that even as a private-key cryptosystem, FGM is insecure against a chosen plaintext attack since the vector sums of cryptograms of a few suitably chosen plaintexts will give us much of the information we used to attack the public-key cryptosystem.

The construction at the heart of FGM can be generalized to an arbitrary group. This generalization is known as a logarithmic signature and has been proposed as the basis of cryptosystems in arbitrary groups, for example the Permutation Group Mappings (PGM) cryptosystem [1]. However, all general families of logarithmic signatures so far proposed for use in these systems are in fact transversal logarithmic signatures or simple modifications of them. A transversal logarithmic signature is based on the unique decomposition of an element of a group into a product of coset representatives associated with a tower of subgroups. In a cryptosystem based on a transversal logarithmic signature, the security of the system is based on the secrecy of this tower of subgroups. In the FGM cryptosystem the chain of vector subspaces (1) is nothing more than this tower. Our method for finding an equivalent private key does not use any of the linearity inherent in $\mathbf{Z}_2^n$, but instead treats $\mathbf{Z}_2^n$ as an abstract group and so is really a method of finding a suitable tower of subgroups. Thus our analysis is applicable to a transversal logarithmic signature in an arbitrary group and so throws doubt on the security of any cryptosystem which relies on transversal logarithmic signatures.

References

[1] S. S. Magliveras and N. D. Memon. Algebraic properties of cryptosystem PGM. *J. Cryptology*, 5 (1992), 167–183.

[2] Minghua Qu and S. A. Vanstone. New public-key cryptosystems based on factorizations of finite groups. *Advances in Cryptology—AUSCRYPT 92*, to appear.