Cryptanalysis of Two Cryptosystems Based on Group Actions

Simon R. Blackburn* and Steven Galbraith**

Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, United Kingdom
{s.blackburn,s.galbraith}@rhbnc.ac.uk

Abstract. The paper cryptanalyses two public key cryptosystems based on $\mathrm{SL}_2(\mathbb{Z})$ that have been recently proposed by Yamamura.

1 Introduction

Yamamura [13,14] has recently described two public-key cryptosystems based on subsemigroups of $\mathrm{SL}_2(\mathbb{Z})$. This paper cryptanalyses both of these systems. We show that a plaintext may be efficiently obtained from the corresponding ciphertext and public key, and hence both systems are insecure.

There have been other proposals for cryptographic primitives based on group theory. A public key cryptosystem based on 'logarithmic signatures' in finite groups was proposed by Qu and Vanstone [9]. This system was cryptanalysed by Blackburn, Murphy and Stern [1,2]. Related work, for example by Magliveras and Memon [6], investigated the suitability of a cryptosystem based on permutation groups. A hybrid system, primarily based on a knapsack problem but also involving logarithmic signatures, was proposed by Qu and Vanstone [10] and was cryptanalysed by Nguyen and Stern [7]. Tillich and Zémor [12] proposed a hash function based on $\mathrm{SL}_2(\mathbb{F}_{2^n})$. Geiselmann [5] described how to find collisions for this hash function; see Charnes and Pieprzyk [3] for other comments on this scheme.

The basic cryptanalytic approach of this paper is as follows. The ciphertext in the cryptosystem described in [14] is a complex number z. It turns out that it is easy to derive the first bit of the plaintext from z. An example of the possible ciphertexts output by the cipher is given in Figure 2. These complex numbers clearly fall into two easily distinguished regions in the complex plane, depending on the first bit of the plaintext. Once the first bit has been recovered, it is easy to compute the ciphertext corresponding to the plaintext with the first bit removed. Hence we may recover all the plaintext one bit at a time.

The bulk of this paper shows that the phenomenon illustrated in Figure 2 occurs for all possible choices of private key, and so the cryptosystem proposed in [14] is insecure. We also show how to reduce the security of the cryptosystem

* This author is supported by an E.P.S.R.C. Advanced Fellowship
** This author thanks the E.P.S.R.C. for their support

K. Y. Lam, E. Okamoto and C. Xing (Eds.): ASIACRYPT'99, LNCS 1716, pp. 52–61, 1999.

proposed in [13] to the security of the cryptosystem proposed in [14]; hence both cryptosystems are insecure.

The rest of this paper is organised as follows. Section 2 contains the background on $\mathrm{SL}_2(\mathbb{Z})$ that we require. Section 3 describes the two cryptosystems that Yamamura proposes. Section 4 cryptanalyses these systems, and Section 5 discusses a slightly more general class of cryptosystems.

2 Background

Both the Yamamura cryptosystems are based on properties of the group $\mathrm{SL}_2(\mathbb{Z})$ of 2×2 integer matrices of determinant 1 under multiplication. This section summarises properties of this group that we will need.

Define matrices $A, B \in \mathrm{SL}_2(\mathbb{Z})$ by

$$A = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

It is well known that these matrices generate $\mathrm{SL}_2(\mathbb{Z})$. It is easy to check that $A^3 = B^2 = -I$, where I is the 2×2 identity matrix. In fact, it is possible to characterise $\mathrm{SL}_2(\mathbb{Z})$ in terms of abstract group theory as an 'amalgamated free product' of the cylic groups of order 6 and 4 generated by A and B respectively; see Robinson [11, Section 6.4] for any facts about amalgamated free products that we use.

The theory of amalgamated free products shows that each element $g \in \mathrm{SL}_2(\mathbb{Z})$ has a unique representation as an element in 'normal form'. More precisely, there exists a unique non-negative integer n, a unique $\epsilon \in \{I, -I\}$ and unique elements $s_1, s_2, \ldots s_n \in \{A, A^2, B\}$ such that

$$g = \epsilon s_1 s_2 \cdots s_n \tag{1}$$

and such that for all $k \in \{1, 2, \ldots, n-1\}$ either:

- $s_k \in \{A, A^2\}$ and $s_{k+1} = B$, or
- $s_k = B$ and $s_{k+1} \in \{A, A^2\}$.

We now introduce some more geometrical notions. We write $\mathrm{GL}_2(\mathbb{C})$ for the group of all 2×2 matrices with complex entries and non-zero determinant. This group acts on $\mathbb{C} \cup \{\infty\}$ by associating

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$$

with the 'Möbius transformation' defined by

$$z \mapsto (az + b)/(cz + d).$$

It is well known — see Jones and Singerman [4] — that Möbius trasformations map circles to circles (we include the limiting case of the lines in our definition of circle).

Since $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup of $\mathrm{GL}_2(\mathbb{C})$, we may associate each element of $\mathrm{SL}_2(\mathbb{Z})$ with a Möbius transformation. The Möbius transformations associated with $\mathrm{SL}_2(\mathbb{Z})$ actually preserve the upper half plane $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$.

As Yamamura observes, this action gives rise to an efficient algorithm to compute the normal form (1) of an arbitrary element $g \in \mathrm{SL}_2(\mathbb{Z})$, up to sign; we may describe this algorithm as follows. Define regions O, P, Q and R of $\mathcal{H}$ by

$$\begin{aligned} O &= \{z \in \mathcal{H} : |z| > 1, |\mathrm{Re}(z)| \leq 1/2\}, \\ P &= \{z \in \mathcal{H} : |z| \geq 1, |\mathrm{Re}(z)| \geq 1/2\}, \\ Q &= \{z \in \mathcal{H} : |z| \leq 1, |z-1| \leq 1\} \text{ and} \\ R &= \mathcal{H} - (O \cup P \cup Q). \end{aligned}$$

These regions are depicted in Figure 1.

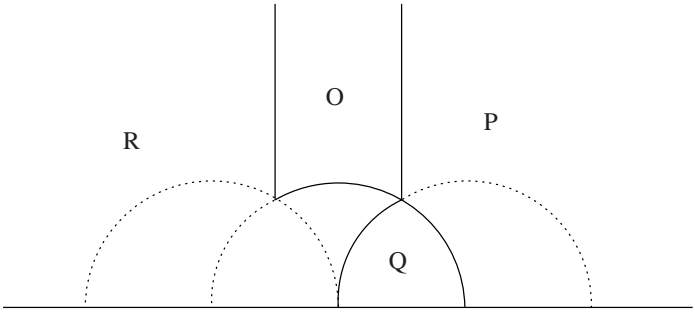

Fig. 1. The regions O, P, Q and R

(The region O is the standard fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$.) Choose a point z_0 in the interior of O; for example $z_0 = 2i$. Define $z = g(z_0)$. The following algorithm finds the normal form of g, up to sign.

Algorithm 1

1. Set $k = 0$.
2. If $z \in O$ then halt.
3. Set $k = k + 1$.
4. If $z \in P$ then set $s_k = A$, if $z \in Q$ then set $s_k = A^2$ and if $z \in R$ then set $s_k = B$.
5. Set $z = s_k^{-1}(z)$.
6. Return to step 2.

The sequence $s_1 s_2 ... s_n$ is the normal form of $\pm g$; see Yamamura [14] for details.

3 The Cryptosystems

This section describes the two public key cryptosystems proposed by Yamamura. We refer to the system proposed in [13] as the "polynomial-based scheme" and the system proposed in [14] as the "point-based scheme". We describe the two schemes in a different manner to Yamamura; we will prove below that the schemes we describe are no less general than the Yamamura schemes.

3.1 The Point-Based Scheme

A user generates its public key as follows. The user chooses words V_1 and V_2 in the generators A and B of $\mathrm{SL}_2(\mathbb{Z})$ so that V_1 and V_2 generate a free subsemigroup of $\mathrm{SL}_2(\mathbb{Z})$. This is done so that any word in V_1 and V_2 is in normal form with respect to A and B; moreover, one of V_1 and V_2 should not be an initial segment of the other. For example, for any integers i and j such that $i, j \geq 2$, a valid choice of V_1 and V_2 is $V_1 = (BA)^i$ and $V_2 = (BA^2)^j$. The user then chooses a matrix $M \in \mathrm{GL}_2(\mathbb{C})$ and a point p in the interior of the fundamental region O. The public key is defined to be an ordered triple (W_1, W_2, q) where $W_1, W_2 \in \mathrm{GL}_2(\mathbb{C})$ and $q \in \mathbb{C}$ are defined by

$$\begin{aligned} W_1 &= M^{-1} V_1 M, \\ W_2 &= M^{-1} V_2 M \\ q &= M^{-1}(p). \end{aligned}$$

The private key is the matrix M.

Encryption: Given a message of n values $i_1, i_2, \ldots, i_n \in \{1, 2\}$ the ciphertext is the point $q' = W(q) \in \mathbb{C}$ where

$$W = W_{i_1} W_{i_2} \cdots W_{i_n}.$$

Note that $M(q') = V_{i_1} V_{i_2} \cdots V_{i_n}(p)$.

Decryption: The receiver computes the point $p' = M(q') \in \mathcal{H}$. The receiver then uses Algorithm 1 to find the normal form of word $V_{i_1} V_{i_2} \cdots V_{i_n}$ in A and B. It is then easy to recover the sequence $i_1, i_2, \ldots, i_n$.

Following Yamamura, we ignore any practical issues relating to exact computation in $\mathbb{C}$. We assume that all calculations are performed to sufficient precision so that all the operations we consider may be carried out.

3.2 The Polynomial-Based Scheme

In this scheme, a user generates a public key as follows. The user chooses V_1, V_2 and M as in the point-based scheme above. The user then chooses $a \in \mathbb{C}$ and a pair $F_1(x), F_2(x)$ of 2×2 matrices over the polynomial ring $\mathbb{C}[x]$ such that $F_1(a) = V_1$ and $F_2(a) = V_2$. The public key is the pair $(W_1(x), W_2(x))$ where $W_i(x) = M^{-1} F_i(x) M$ for $i \in \{1, 2\}$. The secret key is the matrix M and the complex number a.

Encryption The sequence $i_1, i_2, \ldots, i_n \in \{1, 2\}$ is encrypted as the matrix $E(x)$ where

$$E(x) = W_2(x)W_1(x)^{i_1}W_2(x)W_1(x)^{i_2} \cdots W_2(x)W_1(x)^{i_n}W_2(x).$$

[One could have equally used the matrix $\prod_{j=1}^{n} W_{i_j}(x)$ as in the point-based scheme.]
Decryption The receiver calculates $g \in \mathrm{SL}_2(\mathbb{Z})$, where $g = ME(a)M^{-1}$. The user chooses a point p in the interior of the fundamental domain O, calculates $q = g(p)$ and recovers the message in essentially the same way as in the point-based scheme.

3.3 Some Comments

The description of the schemes above differ slightly from the presentation in Yamamura's papers [13,14]. Firstly, in the point-based scheme, Yamamura restricts M to lie in $\mathrm{GL}_2(\mathbb{R})$, and so our scheme is more general in this respect. Secondly, in both schemes Yamamura allows a user to choose any generators $A_1, B_1 \in \mathrm{SL}_2(\mathbb{Z})$ such that $A_1^3 = B_1^2 = -I$ in place of the matrices A and B. With this more general choice, our method of cryptanalysis still applies; see Section 5.

To avoid difficulties with the decryption method, Yamamura has recently [15] added the restriction that $A_1 = P^{-1}AP$ and $B_1 = P^{-1}BP$ for some matrix $P \in \mathrm{SL}_2(\mathbb{Z})$. Note that, when A_1 and B_1 are chosen in this way, then an instance of Yamamura's scheme [13,14] with a matrix M is the same as an instance of the scheme described above with M replaced by PM. Hence the schemes above are as general as the schemes described by Yamamura if A_1 and B_1 are chosen in this manner.

4 Cryptanalysis

This section contains two subsections, which cryptanalyse each of the two cryptosystems in turn.

4.1 Cryptanalysis of the Point-Based Scheme

We begin this section with an example of a cryptanalysis. Suppose $V_1 = BABA$, $V_2 = BA^2$, $p = 2i$ and

$$M = \begin{pmatrix} 0.8 - 0.3i & -0.2 + 0.4i \\ -0.8 + 0.9i & 2.7 + 0.3i \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}).$$

We will show that the points of $\mathbb{C}$ corresponding to encryptions of messages with $i_1 = 1$ are easily distinguished from those with $i_1 = 2$. This is clear for our example: Figure 2 is a plot of all points in $\mathbb{C}$ corresponding to messages of length between 1 and 9. The points fall into two regions depending on the bit i_1

of their corresponding plaintexts: those points corresponding to messages with $i_1 = 1$ correspond precisely to the lower collection of points (those with negative imaginary part). Thus, given an intercepted ciphertext q', it is easy to determine the first bit i_1 of the corresponding plaintext by finding which of the two regions q' lies in. Once i_1 has been determined, the first digit of the plaintext may be stripped off by replacing q' by $V_{i_1}^{-1}(q')$ and the process repeated to determine earlier digits until $q' = q$.

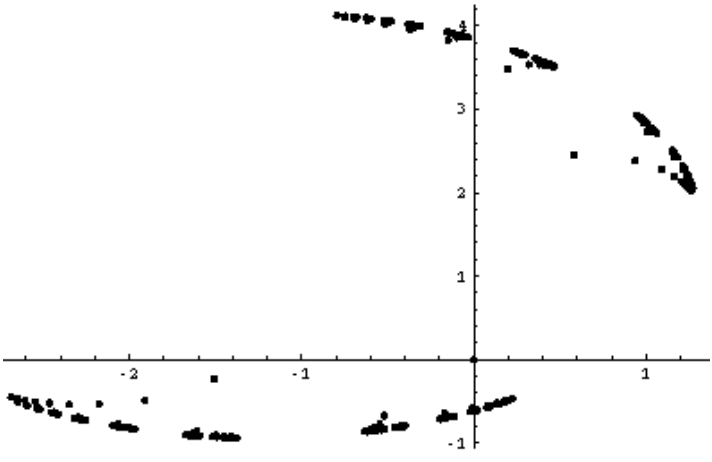

Fig. 2. Example of Ciphertexts

It remains to show that for all choices of parameters, the messages always fall into two regions in a similar way, and to show that these regions may be derived from the public key. We begin by showing that points corresponding to ciphertexts fall into two regions.

For $W_1, W_2 \in \mathrm{GL}_2(\mathbb{C})$ and $q \in \mathbb{C}$, define the set $S_q(W_1, W_2) \subseteq \mathbb{C}$ by

$$S_q(W_1, W_2) = \left\{ W(q) \in \mathbb{C} : W = \prod_{j=1}^{n} W_{i_j} \text{ where } n \geq 0 \text{ and } i_j \in \{1, 2\} \right\}.$$

Proposition 1. *Let (W_1, W_2, q) be a public key of the point-based scheme. Then the sets $W_1 S_q(W_1, W_2)$ and $W_2 S_q(W_1, W_2)$ are separated by a boundary which consists of at most 3 circle segments.*

Note: We include the limiting case of a line in our definition of 'circle'.

Proof: Consider the words V_1 and V_2, the point $p \in O$ and the matrix $M \in \mathrm{GL}_2(\mathbb{C})$ that were used to construct the public key. Without loss of generality,

the normal forms of V_1 and V_2 with respect to A and B may be written in the form

$$V_1 = \pm g A g_1 \text{ and}$$
$$V_2 = \pm g B g_2,$$

where g, g_1 and g_2 are words in A and B. The fact that the normal form algorithm of Section 2 always works implies that $g^{-1}V_1 S_p(V_1, V_2) \subseteq P \cup Q$ and $g^{-1}V_2 S_p(V_1, V_2) \subseteq R$. The boundary of $P \cup Q$ consists of 3 circle segments. We may take the image of this boundary under $M^{-1}g$ as the boundary between $W_1 S_q(W_1, W_2)$ and $W_2 S_q(W_1, W_2)$. □

In fact, the boundary that separates the two sets is usually much simpler than that constructed in the proposition. Indeed, except for the single case when $V_2 = gB$, we may take the image of the imaginary axis under $M^{-1}g$ as the boundary. Even in the exceptional case when $V_2 = gB$, the image of the imaginary axis separates the two sets once we remove single point $W_2(q)$. Hence for all practical purposes, we may assume that the two sets are separated by a circle.

It is now clear how cryptanalysis proceeds:

1. Generate some random points from $W_1 S_q(W_1, W_2)$ and $W_2 S_q(W_1, W_2)$ using the public key.
2. Find a circle that separates the two subsets that have been generated. Such a circle can be determined by a variety of methods.
3. For a ciphertext q', determine the first bit i_1 of the corresponding plaintext by determining which side of the circle q' lies.
4. Replace q' by $W_{i_1}^{-1} q'$ and, while $q \neq q'$, go to step 3.

4.2 Cryptanalysis of the Polynomial-Based Scheme

We now cryptanalyse the polynomial-based scheme, by reducing the problem to an instance of breaking the point-based scheme.

The cryptanalysis of the previous subsection makes use of the fact that $Mq \in O$. We justify why the methods will produce good results for all $q \in \mathbb{C}$ excluding a set of measure zero. We will show that all but a few points in $W_1 S_q(W_1, W_2)$ and $W_2 S_q(W_1, W_2)$ are separated by the boundary constructed in Proposition 1. This will allow us to use the same four steps above to recover almost all of the plaintext; see below.

Let $q \in \mathbb{C}$ and suppose that $p = M(q) \in \mathcal{H}$. (This is no real loss of generality, since a similar argument will work when $p \in -\mathcal{H}$.) Assume further that p is not on the boundary of any image of O under $\mathrm{SL}_2(\mathbb{Z})$. Then there is some $h \in \mathrm{SL}_2(\mathbb{Z})$ such that $h^{-1}(p)$ is in the interior of O. Let $i_1, \ldots, i_n \in \{1, 2\}$. The algorithm to find the normal form of an element of $\mathrm{SL}_2(\mathbb{Z})$ given by Yamamura works by considering the images of a point in the fundamental domain. Since our point p is in the image of the fundamental domain under the element h, the algorithm of Yamamura produces the normal form of $V_{i_1} V_{i_2} \cdots V_{i_n} h$ rather than of $V_{i_1} V_{i_2} \cdots V_{i_n}$ when given $V_{i_1} V_{i_2} \cdots V_{i_n}(p)$. Now, the normal form of $V_{i_1} V_{i_2} \cdots V_{i_n} h$ almost always begins with the word V_{i_1} — the only way this can fail to happen is if h

begins with the normal form of $(V_{i_2} \cdots V_{i_n})^{-1}$, and this bad case is extremely unlikely. Indeed, the likelihood of the bad case occurring tends to 0 exponentially as n tends to infinity. Thus, if we construct our approximations to the sets $W_1 S_q(W_1, W_2)$ and $W_2 S_q(W_1, W_2)$ by sampling words in W_1 and W_2 of small length, the methods of the previous subsection will recover all but (at worst) the last few terms of the sequence $i_1, i_2, \ldots, i_n$ with overwhelming probability. Even if problems occur with recovering the final few terms, this is easily overcome by exhaustive search.

We now cryptanalyse the polynomial-based scheme. We know that there is some $a \in \mathbb{C}$ such that the matrices $W_1(a)$ and $W_2(a)$ have determinant 1. Hence, $\gcd(\det(W_1(x)) - 1, \det(W_2(x)) - 1)$ is a polynomial which has a as a root. The roots of this polynomial may be computed to arbitrary precision by numerical methods; see Press *et al* [8] for example. One of these roots will be the value of a we are seeking. In fact, for most choices of $F_1(x)$ and $F_2(x)$, there will only be one root a. For each candidate a' for a we repeat the following process.

Let $E(x)$ be an intercepted ciphertext. Choose a point $p \in \mathbb{C}$ and compute $p' = E(a')(p)$. We now use the method described in the cryptanalysis of the point-based scheme to express $E(a')$ as a product of the matrices $W_1(a')$ and $W_2(a')$, thus giving us a candidate plaintext. If the plaintext encrypts to the intercepted ciphertext (which it is almost certain to do if $a' = a$), we have decrypted successfully.

5 More General Generators

It might be hoped that a different choice A_1, B_1 of generators of $\mathrm{SL}_2(\mathbb{Z})$ such that $A_1^3 = B_1^2 = -I$ might resist the attacks above. (If this is done, a different decryption method must be found.) However, since we only care about A_1 and B_1 up to conjugation in $\mathrm{GL}_2(\mathbb{C})$, we may assume that A_1 and B_1 are of a restricted form (as outlined in the following proposition). We may then use this restricted form to show that no choices of A_1 and B_1 resist the attacks presented above.

Proposition 2. *Let $A_1, B_1 \in SL_2(\mathbb{Z})$ be generators for $SL_2(\mathbb{Z})$ such that $A_1^3 = B_1^2 = -I$. Then there exists a matrix $N \in GL_2(\mathbb{R})$ such that*

(i) *$N^{-1} A_1 N = A$ and*
(ii) *the normal form (1) of $N^{-1} B_1 N$ with respect to A and B has the property that $s_1 = s_n = B$.*

Proof: The theory of amalgamated free products shows that any element of finite order in $\mathrm{SL}_2(\mathbb{Z})$ is conjugate (by an element of $\mathrm{SL}_2(\mathbb{Z})$) to an element in either the subgroup generated by A or the subgroup generated by B. Since A_1 has order 6, there exists $N \in \mathrm{SL}_2(\mathbb{Z})$ that conjugates A_1 to either A or A^{-1}. Conjugating by the matrix T defined by

$$T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

preserves $\mathrm{SL}_2(\mathbb{Z})$ and maps A^{-1} to A. Thus, replacing N by NT if necessary, there exists $N \in \mathrm{GL}_2(\mathbb{R})$ such that property (i) holds and that $N^{-1}B_1N \in \mathrm{SL}_2(\mathbb{Z})$.

We may assume that the normal form (1) of $N^{-1}B_1N$ with respect to A and B has the property that $s_1 = B$, for if not we replace N by Ns_1. Since $(N^{-1}B_1N)$ has finite order, the concatenation of two copies of the normal form of $N^{-1}B_1N$ cannot still be in normal form. Hence $s_n = B$ and so property (ii) holds. □

The form of A_1 and B_1 in Proposition 2 has the useful property that any word in normal form in A_1 and B_1 is also in normal form with respect to A and B once each occurence of B_1 is replaced by the normal form of B_1 with respect to A and B. Moreover, two words in A_1 and B_1 have the property that one is not an initial segment of the other if and only if the same is true for their normal forms with respect to A and B. This means that the polynomial based scheme with general A_1 and B_1 is a special case of the scheme detailed above. Moreover, the point-based scheme with general A_1 and B_1 is also a special case of the scheme described in this paper, if we allow the point p to be an arbitrary point in $\mathbb{C}$. However, the methods discussed in the cryptanalysis of the polynomial-based scheme make the cryptosystem insecure in this case.

References

1. S.R. Blackburn, S. Murphy and J. Stern, 'Weaknesses of a public-key cryptosystem based on factorizations of finite groups', in T.Helleseth (Ed) *Advances in Cryptology — EUROCRYPT '93*, Lecture Notes in Computer Science 765, Springer, Berlin, 1994, pp. 50-54. 52
2. S.R. Blackburn, S. Murphy and J. Stern, 'The cryptanalysis of a public-key implementation of Finite Group Mappings', *J. Cryptology* Vol. 8 (1995), pp. 157-166. 52
3. C. Charnes and J. Pieprzyk, 'Attacking the SL_2 hashing scheme', in J. Pieprzyk and R. Safavi-Naini (Eds) *Advances in Cryptology — ASIACRYPT '94*, Lecture Notes in Computer Science 917 , Springer, Berlin, 1995, pp. 322-330. 52
4. G. A. Jones, D. Singerman, *Complex functions*, Cambridge (1987) 53
5. W. Geiselmann, 'A note on the hash function of Tillich and Zémor' in C.Boyd (Ed) *Cryptography and Coding*, Lecture Notes in Computer Science 1025, Springer, Berlin, 1995, pp.257-263. 52
6. S.S. Magliveras and N.D. Memon, 'Algebraic properties of cryptosystem PGM', *J. Cryptology*, Vol. 5 (1992), pp. 167-183. 52
7. P. Nguyen and J. Stern, 'Merkle–Hellman revisited: A cryptanalysis of the Qu–Vanstone cryptosystem based on group factorizations' in B.S. Kaliski (Ed) *Advances in Cryptology — CRYPTO '97*, Lecture Notes in Computer Science 1294, Springer, Berlin, 1997, pp. 198-212. 52
8. W. Press, B. Flannery, S. Teukolsky and W. Vetterling, *Numerical Recipes in C*, 2nd Edition, Cambridge University Press, Cambridge, 1988. 59
9. M. Qu and S.A. Vanstone, 'New public-key cryptosystems based on factorizations of finite groups', *presented at AUSCRYPT '92.* 52

10. M. Qu and S.A. Vanstone, 'The knapsack problem in cryptography' in *Finite fields: Theory, Applications, and Algorithms*, Contemporary Mathematics Vol. 168, American Mathematical Society, 1994, pp. 291-308. 52
11. D.J.S. Robinson, *A Course in the Theory of Groups*, Springer, New York, 1982. 53
12. J-P. Tillich and G. Zémor, 'Hashing with SL_2', in Y.G. Desmedt (Ed), *Advances in Cryptology — CRYPTO '94*, Lecture Notes in Computer Science 839, Springer, Berlin, 1994, pp. 40-49. 52
13. A. Yamamura, 'Public-key cryptosystems using the modular group', in Imai, Hideki (Eds) *et al. International Workshop on the Theory and Practice of Cryptography*, Lecture Notes in Computer Science 1431, Springer, Berlin, 1998, pp. 203-216. 52, 53, 55, 56
14. A. Yamamura, *A functional cryptosystem using a group action*, ACIPS to appear. 52, 53, 54, 55, 56
15. A. Yamamura, *personal communication*, 3 March 1999. 56