On the Security of the Hashing Scheme Based on SL_2

Kanat S. Abdukhalikov[1] and Chul Kim[2] **

[1] Institute for Pure and Applied Mathematics
Pushkin Str 125, Almaty 480021, Kazakhstan
abdukh@alg.itpm.alma-ata.su, kanat@euler.kwangwoon.ac.kr
[2] Department of Mathematics, Kwangwoon University
447-1 Wolgye-Dong, Nowoon-Gu, Seoul 139-701, Korea
ckim@garam.kreonet.re.kr

Abstract. Tillich and Zémor proposed a hashing scheme based on the group of unimodular matrices $SL_2(\mathbf{F}_q)$ over a finite field $\mathbf{F}_q$ of $q = 2^n$ elements. Charnes and Pieprzyk studied the security of this scheme. They showed that for $n = 131$ and for some irreducible polynomial $P_{131}(x)$ this scheme is weak. We show that with sufficiently high probability the polynomials $P_n(x)$ can be chosen in such a way that this type of attack can be avoided. Futhermore, we generalize the Tillich-Zémor hashing scheme for any finite field $\mathbf{F}_q$ and show that the new generalized scheme has similar properties.

1 Introduction

Tillich and Zémor [7] proposed a hashing scheme based on the group of unimodular matrices $SL_2(\mathbf{F}_q)$ over a finite field $\mathbf{F}_q$ of $q = 2^n$ elements. This scheme has several attractive properties: the algorithm can be easily implemented in software by using operations in $\mathbf{F}_q$, which allows fast computations; parallelization and precomputations are possible ; small modifications to the input text can be detected; the security of the scheme is equivalent to a precise mathematical problem, for which there exist several results in favor of its difficulty.

Tillich and Zémor recommended to use the range $130 \leq n \leq 170$ and the field $\mathbf{F}_q = \mathbf{F}_2[x]/\langle P_n(x)\rangle$, where $P_n(x)$ is an irreducible polynomial of degree n. Let α be a zero of the polynomial $P_n(x)$ (for example, class of the element x in $\mathbf{F}_2[x]/\langle P_n(x)\rangle$) and

$$A(\alpha) = \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}, \qquad B(\alpha) = \begin{pmatrix} \alpha & \alpha+1 \\ 1 & 1 \end{pmatrix}$$

be matrices from $G = SL_2(\mathbf{F}_q)$. When the polynomial $P_n(x)$ is fixed we denote $A = A(\alpha)$, $B = B(\alpha)$. Define the mapping $\pi = \pi_\alpha$:

$$\pi : \{0, 1\} \to \{A, B\},$$

** This author's research was partially funded by the Korea Science and Engineering Foundation, grant 961-0106-038-2

S. Vaudenay (Ed.): Fast Software Encryption – FSE'98, LNCS 1372, pp. 93–102, 1998.

$$\pi(0) = A, \qquad \pi(1) = B.$$

The hashcode of a binary message $x_1x_2\dots x_k$ is just the matrix product

$$\pi(x_1)\pi(x_2)\dots\pi(x_k).$$

Charnes and Pieprzyk studied the security of this scheme. They showed that for $n = 131$ and for some irreducible polynomial $P_{131}(x)$ this scheme is weak. By using properties of a dihedral subgroup in G, it is proven in [1, Theorem 6] that the following relation holds in G:

$$A^{-1}B(A^{-1}B^2A^{-1})A^{-1}B = BA^{-2}B. \tag{1}$$

This identity can be produced easier. It is sufficient to note that $A^{-1}B = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$, which follows identities $(A^{-1}B)^2 = I$ and $BA^{-1}B = A$, where I is the identity matrix (the last identity is equivalent to (1)). Similarly, $B^{-1}A = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ follows $AB^{-1}A = B$.

Suppose that orders of A and B are s and t respectively. Then matrix identity $BA^{s-1}B = A$ (resp. $AB^{t-1}A = B$) means that binary strings $(1, 0^{s-1}, 1)$ and (0) (resp. $(0, 1^{t-1}, 0)$ and (1)) hash to the same value in the group G. On the other hand, the trivial factorization $A^s = I$ gives the similar result: the binary string (0^s) can be inserted into any message. But if the orders of elements A and B is approximately q then these identities are useless as actual forgeries (there is no such a case to be used as 2^{130} consecutive 0's (or 1's) in a hash input).

So, it turns out that to avoid this type of attack one has to choose an irreducible polynomial $P_n(x)$ in such a way that the orders of A and B would not be small. We will show that with sufficiently high probability the polynomials $P_n(x)$ can be chosen in such a way that the orders of elements A and B are equal to either $q-1$ or $q+1$ (maximal possible values), see Theorems 6, 13 and Table 1. We also propose an efficient algorithm for the determination of the orders of the elements $A = A(\alpha)$ and $B = B(\alpha)$ for any $P_n(x)$. We show the probability that the scheme is vulnerable against the Charnes and Pieprzyk attack is negligible (approximately 10^{-27}, see remark after theorem 7). Futhermore, we generalize the Tillich-Zémor $SL_2(\mathbf{F}_{2^n})$ hashing scheme for any finite field $\mathbf{F}_q$ and show that the new generalized scheme has similar properties.

2 Analysis of SL_2 hashing

We define recursively a sequence $f_i(x) \in \mathbf{F}_2[x]$ of functions

$$f_0(x) = 0, \quad f_1(x) = 1, \quad f_{i+2}(x) = xf_{i+1}(x) + f_i(x) \text{ for } i \geq 0. \tag{2}$$

Let

$$A(x) = \begin{pmatrix} x & 1\\ 1 & 0\end{pmatrix}, \qquad B(x) = \begin{pmatrix} x & x+1\\ 1 & 1\end{pmatrix},$$

and α is a zero of the irreducible polynomial $P_n(x) \in \mathbf{F}_2[x]$ (e.g., class of the element x in $\mathbf{F}_2[x]/\langle P_n(x)\rangle$).

Lemma 1. $A(x)^m = \begin{pmatrix} f_{m+1} & f_m \\ f_m & f_{m-1} \end{pmatrix}$ *for* $m > 0$.

Proof. We have

$$A(x) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_2 & f_1 \\ f_1 & f_0 \end{pmatrix}.$$

Suppose

$$A(x)^m = \begin{pmatrix} f_{m+1} & f_m \\ f_m & f_{m-1} \end{pmatrix}.$$

Then

$$A(x)^{m+1} = A(x)^m \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} xf_{m+1} + f_m & f_{m+1} \\ xf_m + f_{m-1} & f_m \end{pmatrix} = \begin{pmatrix} f_{m+2} & f_{m+1} \\ f_{m+1} & f_m \end{pmatrix}.$$

Thus by induction we have the result.

Lemma 2. *The order of the element A in the group G is equal to the minimum positive number k, such that $f_k(\alpha) = 0$. Equivalently, the order of element A is equal to the minimum positive number k, such that $P_n(x)$ divides $f_k(x)$.*

Proof. If $A^m = I$ then by lemma 1 we have $f_m(\alpha) = 0$. Conversely, if $f_m(\alpha) = 0$ then by (2) one has $f_{m+1}(\alpha) = \alpha f_m(\alpha) + f_{m-1}(\alpha) = f_{m-1}(\alpha)$. Futhermore, $\det A^m = 1$, thus $f_{m+1}(\alpha) \cdot f_{m-1}(\alpha) - f_m(\alpha)^2 = f_{m+1}(\alpha) \cdot f_{m-1}(\alpha) = 1$. Consequently, $f_{m+1}(\alpha) = f_{m-1}(\alpha) = 1$ and $A^m = I$.

Corollary 3. *The order of the element B in the group G is equal to the minimum positive number k, such that $f_k(\alpha + 1) = 0$. Equivalently, the order of element B is equal to the minimum positive number k, such that $P_n(x + 1)$ divides $f_k(x)$.*

Proof. The order of $B = B(\alpha)$ is equal to the order of the element

$$A^{-1}BA = \begin{pmatrix} \alpha + 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Now we can apply lemma 2 to the element $\alpha + 1$.

So, if one chooses an irreducible polynomial $P_n(x)$, for the determination of the order of the element $A = A(\alpha)$ one has to sequentially calculate

$$f_n(x) \equiv xf_{n-1}(x) + f_{n-2}(x) \pmod{P_n(x)}$$

until it gets $f_k(x) \equiv 0 \pmod{P_n(x)}$. This value of k gives the order of A. Similarly, for the determination of the order of the element $B = B(\alpha)$ one has to sequentially calculate

$$f_n(x) \equiv xf_{n-1}(x) + f_{n-2}(x) \pmod{P_n(x+1)}$$

until it gets $f_k(x) \equiv 0 \pmod{P_n(x+1)}$. Note that the polynomial $P_n(x + 1)$ is irreducible.

Lemma 4. i) $\deg f_n(x) = n-1$ *for* $n > 0$.
ii) *If* $n > 0$ *is even then* $f_n(x) = xg_n(x)^2$ *for some polynomial* $g_n(x) \in \mathbf{F}_2[x]$.
iii) *If* $n > 0$ *is odd then* $f_n(x) = h_n(x)^2$ *for some polynomial* $h_n(x) \in \mathbf{F}_2[x]$.

Proof. The case i) immediately follows from (2). Further, from (2) it is easy to see that $f_n(x)$ is a sum of monomials of odd degree for even n and a sum of monomials of even degree for odd n. Then

$$f_{2k+1}(x) = x^{2m_1} + x^{2m_2} + \cdots + x^{2m_s} = (x^{m_1} + x^{m_2} + \cdots + x^{m_s})^2,$$

$$f_{2k}(x) = x^{2m_1+1} + x^{2m_2+1} + \cdots + x^{2m_t+1} = x(x^{m_1} + x^{m_2} + \cdots + x^{m_t})^2.$$

Lemma 5. i) *Suppose* $\lambda_1 + \lambda_2 = x$, $\lambda_1\lambda_2 = 1$. *Then* $f_m(x) = \frac{1}{x}(\lambda_1^m + \lambda_2^m)$ *for* $m \geq 0$.
ii) $f_{2^m}(x) = x^{2^m-1}$.

Proof. i) For $m = 0, 1$ we have $f_0(x) = \frac{1}{x}(\lambda_1^0 + \lambda_2^0) = 0$, $f_1(x) = \frac{1}{x}(\lambda_1 + \lambda_2) = 1$. Suppose our formulae is true for all $m \leq k$. Then

$$\begin{aligned} f_{k+1}(x) &= x \cdot f_k(x) + f_{k-1}(x) \\ &= x \cdot \frac{1}{x}(\lambda_1^k + \lambda_2^k) + \frac{1}{x}(\lambda_1^{k-1} + \lambda_2^{k-1}) \\ &= \frac{1}{x}(\lambda_1 + \lambda_2)(\lambda_1^k + \lambda_2^k) + \frac{1}{x}(\lambda_1^{k-1} + \lambda_2^{k-1}) \\ &= \frac{1}{x}(\lambda_1^{k+1} + \lambda_2^{k+1} + \lambda_1\lambda_2(\lambda_1^{k-1} + \lambda_2^{k-1}) + \lambda_1^{k-1} + \lambda_2^{k-1}) \\ &= \frac{1}{x}(\lambda_1^{k+1} + \lambda_2^{k+1}). \end{aligned}$$

ii) $f_{2^m}(x) = \frac{1}{x}(\lambda_1^{2^m} + \lambda_2^{2^m}) = \frac{1}{x}(\lambda_1 + \lambda_2)^{2^m} = \frac{1}{x}x^{2^m} = x^{2^m-1}$. ∎

Remark. In fact, the elements λ_1 and λ_2 are eigenvalues of the matrix $A(x)$. They belong to an extension of the field of rational functions $\mathbf{F}_2(x)$. Thus eigenvalues of $A(x)^m$ are λ_1^m and λ_2^m. If $\mathrm{Tr}\ C$ denotes the trace of matrix C then

$$f_m(x) = \frac{1}{x}(f_{m+1}(x) + f_{m-1}(x)) = \frac{1}{x}\mathrm{Tr}\ A(x)^m = \frac{1}{x}(\lambda_1^m + \lambda_2^m).$$

The order of any nonidentity element from $SL_2(\mathbf{F}_q)$ either is equal to 2, or divides $q-1$, or divides $q+1$ (see [3]). So maximal possible values of the orders of A (and B) are $q-1$ or $q+1$. From lemmas 2 and 5 it is easy to see that for $n > 1$ the orders of A and B are not equal to 2.

Now let $P_n(x)$ be a random irreducible polynomial of degree $n > 1$ over $\mathbf{F}_2$. We are going to estimate the probability that the order of $A(\alpha)$ is equal to $q-1$ or $q+1$. Let $(2^n-1)(2^n+1) = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ be the decomposition into a product of prime numbers, where $p_1, \ldots, p_r$ are different prime numbers. Set

$$d_2(n) = 1 - \frac{1}{2}(1 + 2^{-n/2+2})\sum_{i=1}^{r}\frac{1}{p_i},$$

$$c_2(n) = 1 - (1 + 2^{-n/2+2}) \sum_{i=1}^{r} \frac{1}{p_i} = 2d_2(n) - 1.$$

Theorem 6. *Let $P_n(x)$ be a random irreducible polynomial of degree $n > 1$ with coefficients in $\mathbf{F}_2$. Then the probability, that the order of A is greater than or equal to $q-1$, is greater than $d_2(n)$. Futhermore, the probability, that both the orders of A and B are greater than or equal to $q-1$, is greater than $c_2(n)$.*

Proof. Since $2^n - 1$ and $2^n + 1$ are relatively prime numbers, they have different prime divisors. Suppose $2^n - 1 = p_1^{k_1} \cdots p_j^{k_j}$, $2^n + 1 = p_{j+1}^{k_{j+1}} \cdots p_r^{k_r}$. Then

$$\begin{aligned}
P &= \Pr\left(\mathrm{ord}(A) \geq q-1\right) \\
&= 1 - \Pr\left(\mathrm{ord}(A) < q-1\right) \\
&\geq 1 - \sum_{i=1}^{j} \Pr\left(A^{(q-1)/p_i} = I\right) - \sum_{i=j+1}^{r} \Pr\left(A^{(q+1)/p_i} = I\right) \\
&= 1 - \sum_{i=1}^{j} \Pr\left(P_n(x) \text{ divides } f_{(q-1)/p_i}(x)\right) \\
&\quad - \sum_{i=j+1}^{r} \Pr\left(P_n(x) \text{ divides } f_{(q+1)/p_i}(x)\right)
\end{aligned}$$

Since $\deg f_{(q-1)/p_i}(x) = (q-1)/p_i - 1$ and $f_{(q-1)/p_i}(x)$ is a square by lemma 4, we have

$$\Pr\left(P_n(x) \text{ divides } f_{(q-1)/p_i}(x)\right) \leq \frac{\frac{(q-1)/p_i - 1}{2n}}{S_2(n)} < \frac{\frac{q}{2np_i}}{S_2(n)},$$

where $S_2(n)$ is the number of irreducible polynomials of degree n with coefficients in $\mathbf{F}_2$. But $S_2(n) > \frac{q}{n}(1 - \frac{1}{2^{n/2-1}})$ (see [6]), thus we have

$$\Pr\left(P_n(x) \text{ divides } f_{(q-1)/p_i}(x)\right) < \frac{\frac{q}{2np_i}}{\frac{q}{n}\left(1 - \frac{1}{2^{n/2-1}}\right)} \leq \frac{1}{2p_i}\left(1 + 2^{-n/2+2}\right).$$

We have the same estimation for $\Pr\left(P_n(x) \text{ divides } f_{(q+1)/p_i}(x)\right)$. So

$$P > 1 - \frac{1}{2}\left(1 + 2^{-n/2+2}\right) \sum_{i=1}^{r} \frac{1}{p_i}.$$

Finally,

$$\begin{aligned}
&\Pr\left(\mathrm{ord}(A) \geq q-1 \text{ and } \mathrm{ord}(B) \geq q-1\right) \\
&\geq 1 - \Pr\left(\mathrm{ord}(A) < q-1\right) - \Pr\left(\mathrm{ord}(B) < q-1\right) \\
&= \left(1 - \Pr\left(\mathrm{ord}(A) < q-1\right)\right) + \left(1 - \Pr\left(\mathrm{ord}(B) < q-1\right)\right) - 1 \\
&\geq 2d_2(n) - 1 = c_2(n). \blacksquare
\end{aligned}$$

Let M be a positive integer number such that there does not exist practically a binary message containing (0^M) (that is, M consecutive 0's) or (1^M). In order to avoid low order attack it would be sufficient to have A and B with orders that are greater than M.

Table 1 shows that it is not hard to find a polynomial which results in a large order. The user can check it by lemma 2.

Theorem 7. *Let $P_n(x)$ be a random irreducible polynomial of degree $n > 3$ with coefficients in $\mathbf{F}_2$. Then the probability, that both the orders of A and B are greater than M, is greater than $1 - \frac{M^2}{2^{n-1}}$.*

Proof.

$$\Pr(\mathrm{ord}(A) \le M) \le \sum_{i=1}^{M} \Pr(P_n(x) \text{ divides } f_i(x)) \le \sum_{i=1}^{M} \frac{\frac{i-1}{n}}{S_2(n)} < \frac{M^2}{2nS_2(n)},$$

$$\Pr(\mathrm{ord}(A) > M \text{ and } \mathrm{ord}(B) > M) > 1 - \Pr(\mathrm{ord}(A) \le M) - \Pr(\mathrm{ord}(B) \le M) > 1 - \frac{M^2}{nS_2(n)} > 1 - \frac{M^2}{2^{n-1}}. \blacksquare$$

For example, let $M = 10^6$, $n = 131$. Then the probability, that both the orders of A and B are greater then M, is greater then $1 - 10^{-27}$. So the probability, that for a random irreducible polynomial $P_n(x)$ the scheme is vulnerable against the Charnes and Pieprzyk attack, is less then 10^{-27}.

We do not discuss important properties of this scheme (concatenation property, connections with associated Cayley graph, protections against local modifications, expanding properties), stability under subgroup and density attacks, easy computability, because it was done in [7,8] in detail.

Remark. One of referees drew our attention to the article [4].

3 Generalization of the hashing scheme for $p > 2$

In this section we introduce the analog of the Tillich-Zémor hashing scheme for $p > 2$. The new hash algorithm can be described as follows.

Defining Parameter. An irreducible polynomial $P_n(x)$ of degree n over a field $\mathbf{F}_p$ of p elements ($p > 2$ is prime, $q = p^n$, n is sufficiently large).

Algorithm. Let α be a zero of the polynomial $P_n(x)$ (e.g., the class of the element x in the field $\mathbf{F}_q = \mathbf{F}_p[x]/\langle P_n(x)\rangle$) and

$$A = A(\alpha) = \begin{pmatrix} \alpha & -1 \\ 1 & 0 \end{pmatrix}, \qquad B = B(\alpha) = \begin{pmatrix} \alpha & \alpha - 1 \\ 1 & 1 \end{pmatrix}$$

be matrices from $G = SL_2(\mathbf{F}_q)$. Define the mapping

$$\pi : \{0,1\} \to \{A, B\},$$

$$\pi(0) = A, \qquad \pi(1) = B.$$

The hashcode of a binary message $x_1 x_2 \dots x_k$ is the matrix

$$\pi(x_1)\pi(x_2)\dots\pi(x_k)$$

from G.

This hashing scheme has all the cryptographic properties, analogous to the Tillich-Zémor hashing scheme [7].

The following theorem shows that the set of hashcodes is the whole group $SL_2(\mathbf{F}_q)$.

Theorem 8. *For $n > 2$ the elements A, B generate the group $SL_2(\mathbf{F}_q)$.*

Proof. It can be easily checked that

$$A^{-1}B^{-1}A^2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad BA^{-2}BA = \begin{pmatrix} 1 & \alpha - 1 \\ 0 & 1 \end{pmatrix}.$$

According to Dickson's theorem (see [5,2]) the matrices $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & \alpha-1 \\ 0 & 1 \end{smallmatrix}\right)$ generate the group $SL_2(\mathbf{F}_q)$. ∎

Note that $SL_2(\mathbf{F}_q)$ has nontrivial center $Z = \{\pm I\}$, where I is the identity matrix. That is, for any $g \in SL_2(\mathbf{F}_q)$ and $z \in Z$ we have $gz = zg$. If $A^s \in Z$ then binary strings $(0^s, w, v)$, $(w, 0^s, v)$, $(w, v, 0^s)$ hash to the same value. Consequently, we have to choose irreducible polynomial $P_n(x)$ in such a way that the condition $A^s \in Z$ follows s would not be small.

Define a sequence $f_i(x) \in \mathbf{F}_p[x]$ of functions

$$f_0(x) = 0, \quad f_1(x) = 1, \quad f_{i+2}(x) = x f_{i+1}(x) - f_i(x) \text{ for } i \geq 0, \tag{3}$$

and define matrices

$$A(x) = \begin{pmatrix} x & -1 \\ 1 & 0 \end{pmatrix}, \qquad B(x) = \begin{pmatrix} x & x-1 \\ 1 & 1 \end{pmatrix}.$$

Lemma 9. $A(x)^m = \begin{pmatrix} f_{m+1} & -f_m \\ f_m & -f_{m-1} \end{pmatrix}$ *for $m > 0$.*

Proof. By induction.

Lemma 10. *$A^m \in Z$ if and only if $f_m(\alpha) = 0$. Equivalently, $A^m \in Z$ if and only if $P_n(x)$ divides $f_m(x)$.*

Proof. If $A^m \in Z$ then by lemma 9 we have $f_m(\alpha) = 0$. Conversely, if $f_m(\alpha) = 0$ then by (3) one has $f_{m+1}(\alpha) = \alpha f_m(\alpha) - f_{m-1}(\alpha) = -f_{m-1}(\alpha)$. Futhermore, $\det A^m = 1$, thus $f_{m+1}(\alpha) \cdot f_{m-1}(\alpha) = -1$. Consequently, we have either $f_{m+1}(\alpha) = -f_{m-1}(\alpha) = 1$ or $f_{m+1}(\alpha) = -f_{m-1}(\alpha) = -1$, thus either $A^m = I$ or $A^m = -I$.

Corollary 11. *$B^m \in Z$ if and only if $f_m(\alpha+1)=0$. Equivalently, $B^m \in Z$ if and only if $P_n(x-1)$ divides $f_m(x)$.*

Proof. It follows from equality

$$A^{-1}BA = \begin{pmatrix} \alpha+1 & -1 \\ 1 & 0 \end{pmatrix}$$

and lemma 9.

Lemma 12. i) *Suppose $\lambda_1+\lambda_2=x$, $\lambda_1\lambda_2=1$. Then $f_m(x)=\frac{\lambda_1^m-\lambda_2^m}{\lambda_1-\lambda_2}$ for $m\geq 0$.*

ii) $f_{2p}(x)=x^p(x^2-4)^{(p-1)/2}$.

Proof. i) If $f_k(x)=\frac{\lambda_1^k-\lambda_2^k}{\lambda_1-\lambda_2}$ and $f_{k-1}(x)=\frac{\lambda_1^{k-1}-\lambda_2^{k-1}}{\lambda_1-\lambda_2}$ then

$$\begin{aligned} f_{k+1}(x) &= xf_k(x)-f_{k-1}(x) \\ &= \frac{1}{\lambda_1-\lambda_2}((\lambda_1+\lambda_2)(\lambda_1^k-\lambda_2^k)-(\lambda_1^{k-1}-\lambda_2^{k-1})) \\ &= \frac{1}{\lambda_1-\lambda_2}(\lambda_1^{k+1}-\lambda_2^{k+1}+\lambda_1\lambda_2(\lambda_1^{k-1}-\lambda_2^{k-1})-(\lambda_1^{k-1}-\lambda_2^{k-1})) \\ &= \frac{\lambda_1^{k+1}-\lambda_2^{k+1}}{\lambda_1-\lambda_2}. \end{aligned}$$

ii) We have

$$\begin{aligned} f_{2p}(x) &= \frac{\lambda_1^{2p}-\lambda_2^{2p}}{\lambda_1-\lambda_2} = \left(\frac{\lambda_1^2-\lambda_2^2}{\lambda_1-\lambda_2}\right)^p(\lambda_1-\lambda_2)^{p-1} \\ &= (f_2)^p(\lambda_1-\lambda_2)^{p-1} = x^p(\lambda_1^2-2\lambda_1\lambda_2+\lambda_2^2)^{(p-1)/2} \\ &= x^p((\lambda_1+\lambda_2)^2-4\lambda_1\lambda_2)^{(p-1)/2} = x^p(x^2-4)^{(p-1)/2}. \blacksquare \end{aligned}$$

The group G has the unique element $-I$ of order 2 (see [3]). The order of any noncentral element from G is equal to p, $2p$ or is a divisor of $q-1$ or $q+1$. Lemmas 9 and 12 follow that for $n>1$ the order of element A (resp. B) is equal to neither p nor $2p$. Consequently, the orders of the elements A and B are divisors of $q-1$ or $q+1$.

Let $P_n(x)$ be a random irreducible polynomial of degree $n>1$ with coefficients in $\mathbf{F}_p$. We estimate the probability that the order of A is equal to $q-1$ or $q+1$. Let $(p^n-1)/2=p_1^{k_1}p_2^{k_2}\cdots p_j^{k_j}$, $(p^n+1)/2=p_{j+1}^{k_{j+1}}\cdots p_r^{k_r}$ be the decomposition into a product of primes, where $p_1,\ldots,p_r$ are different prime numbers. Set

$$d_p(n)=1-\frac{1}{2}\left(1+p^{-n/2+2}\right)\sum_{i=1}^{r}\frac{1}{p_i},$$

$$c_p(n)=1-\left(1+p^{-n/2+2}\right)\sum_{i=1}^{r}\frac{1}{p_i}=2d_2(n)-1.$$

Theorem 13. *Let $P_n(x)$ be a random irreducible monic polynomial of degree $n > 2$ with coefficients in $\mathbf{F}_p$. Then the probability, that the order of A is greater than or equal to $q-1$, is greater than $d_p(n)$. Futhermore, the probability, that both the orders of A and B are greater than or equal to $q-1$, is greater than $c_p(n)$.*

Proof. Since $(q-1)/2$ and $(q+1)/2$ are relatively prime numbers, they have different prime divisors. We have

$$\begin{aligned}
P &= \Pr\left(\mathrm{ord}(A) \geq q-1\right) \\
&= 1 - \Pr\left(\mathrm{ord}(A) < q-1\right) \\
&\geq 1 - \sum_{i=1}^{j} \Pr\left(A^{(q-1)/2p_i} \in Z\right) - \sum_{i=j+1}^{r} \Pr\left(A^{(q+1)/2p_i} \in Z\right) \\
&= 1 - \sum_{i=1}^{j} \Pr\left(P_n(x) \text{ divides } f_{(q-1)/2p_i}(x)\right) \\
&\quad - \sum_{i=j+1}^{r} \Pr\left(P_n(x) \text{ divides } f_{(q+1)/2p_i}(x)\right).
\end{aligned}$$

On the other hand,

$$\Pr\left(P_n(x) \text{ divides } f_{(q-1)/2p_i}(x)\right) \leq \frac{\frac{(q-1)/2p_i - 1}{n}}{S_p(n)} < \frac{\frac{q}{2np_i}}{S_p(n)},$$

where $S_p(n)$ is the number of monic irreducible polynomials of degree n with coefficients in $\mathbf{F}_p$. But $S_p(n) > \frac{q}{n}\left(1 - \frac{1}{p^{n/2-1}}\right)$ (see [6]), thus we have

$$\Pr\left(P_n(x) \text{ divides } f_{(q-1)/2p_i}(x)\right) < \frac{\frac{q}{2np_i}}{\frac{q}{n}\left(1 - \frac{1}{p^{n/2-1}}\right)} < \frac{1}{2p_i}\left(1 + p^{-n/2+2}\right).$$

So

$$P > 1 - \frac{1}{2}\left(1 + p^{-n/2+2}\right)\sum_{i=1}^{r}\frac{1}{p_i}.$$

Finally,

$$\begin{aligned}
&\Pr\left(\mathrm{ord}(A) \geq q-1 \text{ and } \mathrm{ord}(B) \geq q-1\right) \\
&\geq 1 - \Pr\left(\mathrm{ord}(A) < q-1\right) - \Pr\left(\mathrm{ord}(B) < q-1\right) \\
&= \left(1 - \Pr\left(\mathrm{ord}(A) < q-1\right)\right) + \left(1 - \Pr\left(\mathrm{ord}(B) < q-1\right)\right) - 1 \\
&\geq 2d_p(n) - 1 = c_p(n). \blacksquare
\end{aligned}$$

Similarly to theorem 7 one can easily prove

Theorem 14. *Let $P_n(x)$ be a random irreducible monic polynomial of degree $n > 3$ with coefficients in $\mathbf{F}_p$. Then the probability, that both the orders of A and B are greater than M, is greater than $1 - \frac{M^2}{(p-1)p^{n-1}}$.*

$p=2$			$p=3$		
n	$d_p(n)$	$c_p(n)$	n	$d_p(n)$	$c_p(n)$
130	0.64...	0.28...	80	0.55...	0.10...
131	0.83...	0.66...	81	0.59...	0.18...
132	0.55...	0.10...	82	0.64...	0.28...
133	0.81...	0.63...	83	0.74...	0.49...
134	0.73...	0.46...	84	0.48...	-0.02...
135	0.65...	0.31...	85	0.68...	0.37...
136	0.69...	0.39...	86	0.64...	0.29...
137	0.83...	0.66...	87	0.62...	0.25...
138	0.60...	0.21...	88	0.57...	0.14...
139	0.83...	0.66...	89	0.74...	0.49...

Table 1. Bounds for probability.

For example, let $p = 3$, $n = 81$, $M = 10^6$. Then the probability, that both the orders of A and B are greater then M, is greater then $1 - 10^{-26}$.

Table 1 shows some examples for $p = 2, 3$.

4 Conclusion

We have proposed fixing of the SL_2 hashing scheme against an attack by Charnes and Pieprzyk. In fact, we have proposed an algorithm to decide whether the given irreducible polynomial leads to vulnerable (against the Charnes and Pieprzyk attack) hashing. We have also shown that the negligible part of the set of all polynomials is vulnerable to this attack. Finally, we give a generalization of the Tillich-Zémor hashing scheme.

References

1. C.Charnes and J.Pieprzyk. Attacking the SL_2 hashing scheme. In Advanced in Cryptology – Proceedings of ASIACRYPT'94 (1994). LNCS 917. Springer-Verlag pp. 322–330.
2. L.E.Dickson. Linear groups with an exposition of the Galois field theory. Leibzig: Teubner 1901 (New York: Dover Publ. 1958).
3. L. Dornhoff. Group representation theory, volume I. Marcel Dekker, Inc., New York 1971.
4. W. Geiselman. A note on the hash function of Tillich and Zémor. In Fast Software Encryption Workshop. LNCS 1039. Springer-Verlag pp. 51–52.
5. M.Suzuki. Group theory, volume I. Springer-Verlag 1982.
6. H.C.A. van Tilborg. An introduction to cryrtology. Klumer, 1989.
7. J-P. Tillich and G.Zémor. Hashing with SL_2. In Advanced in Cryptology – Proceedings of CRYPTO'94 (1994). LNCS 917. Springer-Verlag pp. 40–49.
8. J-P. Tillich and G.Zémor. Group-theoretic hash functions. In First French-Israeli workshop on algebraic coding (1994) LNCS 781. Springer-Verlag pp. 90–110.