ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.4, 2007–2017
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.4.59 Spec. Issue on NCFCTA-2020

HASH FUNCTION USING FREE GENERATORS THEOREM OVER THE PROJECTIVE GENERAL LINEAR GROUP

V. VIBITHA KOCHAMANI [1] AND P. L. LILLY

ABSTRACT. We define the projection mapping from an algebraic structure to quotient structure which gives the images in $GL_3(F_q)$.By using Free Generators Theorem,we obtain the set of pair of matrices with entries in $F_p[x]$ which is defined in set $\mathbb{D}$.We work with the elements in $\mathbb{D}$ to construct a Cayley Hash function to protect the local modifications property and the security properties of the corresponding hash functions.We can create an infinite number of Hash functions using the Free Generators Theorem by different values of p and n.

1. INTRODUCTION

Hash functions are simple and easy-to compute,that takes a variable length input and converts it to a fixed-length output [10]. If such a function satisfies additional requirements it can be used for cryptographic applications such as, to protect the authenticity of messages sent over an insecure channel. The basic idea is that the hash result provides a unique imprint of a message, and that the protection of a short imprint is easier than the protection of message itself. A cryptographic hash function can provide assurance of data integrity. Hash functions are widely used in numerous cryptographic protocols and a lot of work has already been put into devising adequate hashing schemes.Hash functions are used as compact representations or digital finger prints of data and to provide

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 94A60, 20F65, 15A30, 11B13.

Key words and phrases. Cryptographic Hash Function, General Linear Group, Projective General Linear Group, Projection mapping, Local Modifications Property.

message integrity. Some hash functions in current use have been shown to be vulnerable. Early suggestions (particularly SHA family) did not really use any mathematical ideas apart from Merkle-Damgard [3] construction for producing collision resistant hash functions from collision resistant compression functions, the main idea was just to create a mess by using complex iterations. We have to admit that a mess might be good for hiding purposes, but only to some extent. In the period of time 1990s, Zemor [4] introduced the idea of constructing hash functions from Cayley graphs. Zemor's technique came from a desire to satisfy the following small modification property that introduced in [5].

Proposition 1.1 (Small Modifications Property)**.** *There exists a* $d \in \mathbb{N}_0$ *such that if* $m^{'}$ *is any modification of* m *affecting fewer than* d *consecutive bits then* $h(m) \neq h(m^{'})$.

The relation between the small modifications property and hash functions from Cayley graphs is now apparent.Namely, let G be a group with generating set $S = \{A, B\}$ and H be the associated hash function.If the directed girth of $C(G, S)$ is δ, then two messages of length less than δ cannot form a collision in H.From this motivation, Zemor present the idea of using hash functions over the group $SL_2(F_p)$ with two generators $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ for a large prime p which was broken by many attacks by their weakness in the factorization. [2] In 1994, Tillich and Zemor's [7] paper proposed a family of hash functions that uses the group of SL_2 over a finite field of 2^n elements as platform for their design.
Let n be a positive integer and let $p(x)$ be an irreducible polynomial of degree n over F_2. Let A_0 and A_1 be defined as follows: $A_0 = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}$ and $A_1 = \begin{pmatrix} x & x+1 \\ 1 & 1 \end{pmatrix}$.

Both A_0 and A_1 have determinant 1 over F_2. These matrices are the generators of the Tillich-Zemor hash function. Let $m = m_1 m_2 .....m_k \in \{0, 1\}^*$ be a binary string representation of a message and $K = F_2[x]/ < p_n(x) > \simeq F_{2^n}$.
The construction of the Tillich-Zemor hash functions also preserves the small modifications property using degree argument in ([7], lemma 3.5).

Lemma 1.1. *Suppose that $m, m^{'}$ are bit strings in $\{0,1\}^*$ such that $H(m) = H(m^{'})$. Then at least one of m,$m^{'}$ must have length greater than n.*

In the paper [13, 14] we have taken up the following study relevant to the above context.We devised the Hash function as follows: to an arbitrary text of $\{0,1\}^*$, associate the string of $\{A, B\}$ obtained by substituting 0 for A and 1 for B, then assign to A and B values of adequately chosen matrices of $Heis(Z)$, those could be

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

then evaluate the product associated with the string of A and B in the group $Heis(F_p)$, where F_p is the field on p elements, p being chosen large prime number and we executed a running time of the hash function using matrix multiplication and also check that the output distributed by hash functions,(that is) hashed values are uniform using the goodness-of-fit test.

2. PRELIMINARIES

Definition 2.1. *[10] A **One-Way Hash Function** is a function h that satisfies the following conditions:*

1. *The input x can be of arbitrary length and the result h(x) has a fixed length of n bits.*
2. *Given h and an input x, the computation of h(x) must be easy.*
3. *The function must be one-way in the sense that given a y in the image of h, it is hard to find a message x such that h(x)= y (pre image-resistance), and given x and h(x) it is hard to find a message $x' \neq x$ such that $h(x') = h(x)$ (second pre-image resistance).*

Definition 2.2. *[10] A **Collision-Resistant Hash Function** is a function h that satisfies the following conditions:*

1. *The input x can be of arbitrary length and the result h(x) has a fixed length of n bits.*
2. *Given h and an input x, the computation of h(x) must be easy.*
3. *The function must be collision-resistant: this means that it is hard to find two distinct messages that hash to the same result (i.e., find x and x' with*

$x \neq x'$ such that $h(x) = h(x')$). such that $h(x') = h(x)$ (second pre-image resistance).

Now, we defined the Projective General linear group over R

Definition 2.3. *[6] Let R be a commutative ring.We define the **Projective General Linear group** of degree k over R is $PGL_k(R) = GL_k(R)/Z$, where Z is the centre of $GL_k(R)$ and consists of all scalar matrices. Elements of $PGL_k(R)$ are thus cosets gZ with $g \in GL_k(R)$.*

Definition 2.4. *[6] Let p be a prime and F_p be the field with p-elements and $F_p((x))$ be the field of **formal Laurent series** over F_p.The elements of $F_p((x))$ are series of the form $f(x) = \Sigma_{k=m}^{\infty} f_k x^k$, for $f_i \in F_p$ and $m \in \mathbb{Z}$.*

In [15], we find out the general form of $A, B \in PGL_3(F_p((x)))$ in terms of eigenvalues and eigenvectors of $\tilde{A}, \tilde{B} \in GL_3(F_p((x)))$.

Lemma 2.1. *Let $\tilde{A}, \tilde{B}$ are the elements in $GL_3(F_p((x)))$.Suppose that $\tilde{A}$ has distinct eigenvectors $[a : b : c], [1 : g : h], [d : 1 : e]$ with corresponding eigenvalues $x, y, z \in F_p((x))$ and that $\tilde{B}$ has distinct eigenvectors $[1 : \tilde{b} : \tilde{c}], [1 : \tilde{g} : \tilde{h}], [\tilde{d} : 1 : \tilde{e}]$ with corresponding eigenvalues $x^{'}, y^{'}, z^{'} \in F_p((x))$ then the respective images in $PGL_3(F_p((x)))$ are*

$$A= \begin{bmatrix} a(eg-h)+b(dhf^{'}-ef)+c(f-dgf^{'}) & ae(f-1)+adh(1-f^{'})+cd(f^{'}-f) & adg(f^{'}-1)+a(1-f)+bd(f-f^{'}) \\ beg(1-f)+bh(f^{'}-1)+cg(f-f^{'}) & a(egf-hf^{'})+b(dh-e)+c(f^{'}-dgf) & ag(f^{'}-f)+bdg(f-1)+b(1-f^{'}) \\ beh(f^{'}-f)+ceg(1-f^{'})+ch(f-1) & aeh(f-f^{'})+cdh(1-f)+ce(f^{'}-1) & a(egf^{'}-hf)+b(dhf-ef^{'})+c(1-dg) \end{bmatrix}$$

and

$$B= \begin{bmatrix} (\tilde{e}\tilde{g}-\tilde{h})+\tilde{b}(\tilde{d}\tilde{h}\tilde{f}^{'}-\tilde{e}\tilde{f})+\tilde{c}(\tilde{f}-\tilde{d}\tilde{g}\tilde{f}^{'}) & \tilde{e}(\tilde{f}-1)+\tilde{d}\tilde{h}(1-\tilde{f}^{'})+\tilde{c}\tilde{d}(\tilde{f}^{'}-\tilde{f}) & \tilde{d}\tilde{g}(\tilde{f}^{'}-1)+(1-\tilde{f})+\tilde{b}\tilde{d}(\tilde{f}-\tilde{f}^{'}) \\ \tilde{b}\tilde{e}\tilde{g}(1-\tilde{f})+\tilde{b}\tilde{h}(\tilde{f}^{'}-1)+\tilde{c}\tilde{g}(\tilde{f}-\tilde{f}^{'}) & (\tilde{e}\tilde{g}\tilde{f}-\tilde{h}\tilde{f}^{'})+\tilde{b}(\tilde{d}\tilde{h}-\tilde{e})+\tilde{c}(\tilde{f}^{'}-\tilde{d}\tilde{g}\tilde{f}) & \tilde{g}(\tilde{f}^{'}-\tilde{f})+\tilde{b}\tilde{d}\tilde{g}(\tilde{f}-1)+\tilde{b}(1-\tilde{f}^{'}) \\ \tilde{b}\tilde{e}\tilde{h}(\tilde{f}^{'}-\tilde{f})+\tilde{c}\tilde{e}\tilde{g}(1-\tilde{f}^{'})+\tilde{c}\tilde{h}(\tilde{f}-1) & \tilde{e}\tilde{h}(\tilde{f}-\tilde{f}^{'})+\tilde{c}\tilde{d}\tilde{h}(1-\tilde{f})+\tilde{c}\tilde{e}(\tilde{f}^{'}-1) & (\tilde{e}\tilde{g}\tilde{f}^{'}-\tilde{h}\tilde{f})+\tilde{b}(\tilde{d}\tilde{h}\tilde{f}-\tilde{e}\tilde{f}^{'})+\tilde{c}(1-\tilde{d}\tilde{g}) \end{bmatrix}$$

where $f = \dfrac{y}{x}, f' = \dfrac{z}{x}, \tilde{f} = \dfrac{y^{'}}{x^{'}}$ and $\tilde{f}' = \dfrac{z^{'}}{x^{'}}$.

In [15] the statement of the Free Generators Theorem are stated as follows:

Theorem 2.1. *If there exist $a, b, c, g, h, d, e, \tilde{b}, \tilde{c}, \tilde{d}, \tilde{e}, \tilde{g}, \tilde{h} \in F_p((x))$, and $f, f', \tilde{f}, \tilde{f}' \in F_p((x))^*$ such that,*

(i) *$d([u], [v]) > \dfrac{1}{p^{d+1}}$, for each pair of $[u], [v]$ in $\{[a : b : c], [1 : g : h], [d : 1 : e]$, $[1 : \tilde{b} : \tilde{c}], [1 : \tilde{g} : \tilde{h}], [\tilde{d} : 1 : \tilde{e}]\}$;*

(ii) $\min\{|f|,|f^{-1}|\} \leqslant \frac{1}{p^{2d+1}}, \min\{|f'|,|(f')^{-1}|\} \leqslant \frac{1}{p^{2d+1}}$ *and* $\min\{|\tilde{f}|,|\tilde{f}^{-1}|\} \leqslant \frac{1}{p^{2d+1}}, \min\{|\tilde{f}'|,|(\tilde{f}')^{-1}|\} \leqslant \frac{1}{p^{2d+1}}$;

(iii) *there exist* $[k] \in \mathbb{P}^2$ *such that* $d([k],[u]) > \frac{1}{p^{d+1}}$ *for each* $[u]$ *in* $\{[a:b:c],[1:g:h],[d:1:e],[1:\tilde{b}:\tilde{c}],\ [1:\tilde{g}:\tilde{h}],[\tilde{d}:1:\tilde{e}]\}$, *then the matrices,*

$$A=\begin{pmatrix} a(eg-h)+b(dhf^{'}-ef)+c(f-dgf^{'}) & ae(f-1)+adh(1-f^{'})+cd(f^{'}-f) & adg(f^{'}-1)+a(1-f)+bd(f-f^{'}) \\ beg(1-f)+bh(f^{'}-1)+cg(f-f^{'}) & a(egf-hf^{'})+b(dh-e)+c(f^{'}-dgf) & ag(f^{'}-f)+bdg(f-1)+b(1-f^{'}) \\ beh(f^{'}-f)+ceg(1-f^{'})+ch(f-1) & aeh(f-f^{'})+cdh(1-f)+ce(f^{'}-1) & a(egf^{'}-hf)+b(dhf-ef^{'})+c(1-dg) \end{pmatrix}$$

and

$$B=\begin{pmatrix} (\tilde{e}\tilde{g}-\tilde{h})+\tilde{b}(\tilde{d}\tilde{h}\tilde{f}'-\tilde{e}\tilde{f})+\tilde{c}(\tilde{f}-\tilde{d}\tilde{g}\tilde{f}') & \tilde{e}(\tilde{f}-1)+\tilde{d}\tilde{h}(1-\tilde{f}')+\tilde{c}\tilde{d}(\tilde{f}'-\tilde{f}) & \tilde{d}\tilde{g}(\tilde{f}'-1)+(1-\tilde{f})+\tilde{b}\tilde{d}(\tilde{f}-\tilde{f}') \\ \tilde{b}\tilde{e}\tilde{g}(1-\tilde{f})+\tilde{b}\tilde{h}(\tilde{f}'-1)+\tilde{c}\tilde{g}(\tilde{f}-\tilde{f}') & (\tilde{e}\tilde{g}\tilde{f}-\tilde{h}\tilde{f}')+\tilde{b}(\tilde{d}\tilde{h}-\tilde{e})+\tilde{c}(\tilde{f}'-\tilde{d}\tilde{g}\tilde{f}) & \tilde{g}(\tilde{f}'-\tilde{f})+\tilde{b}\tilde{d}\tilde{g}(\tilde{f}-1)+\tilde{b}(1-\tilde{f}') \\ \tilde{b}\tilde{e}\tilde{h}(\tilde{f}'-\tilde{f})+\tilde{c}\tilde{e}\tilde{g}(1-\tilde{f}')+\tilde{c}\tilde{h}(\tilde{f}-1) & \tilde{e}\tilde{h}(\tilde{f}-\tilde{f}')+\tilde{c}\tilde{d}\tilde{h}(1-\tilde{f})+\tilde{c}\tilde{e}(\tilde{f}'-1) & (\tilde{e}\tilde{g}\tilde{f}'-\tilde{h}\tilde{f})+\tilde{b}(\tilde{d}\tilde{h}\tilde{f}-\tilde{e}\tilde{f}')+\tilde{c}(1-\tilde{d}\tilde{g}) \end{pmatrix}$$

generate a free subgroup in $PGL_3(F_p((x)))$, *where* p *is a prime and* $d \in \mathbb{N}_0$.

Definition 2.5. *[1] For a fixed point* $a \in X$. *Let* $S = \{f \in F(X) \ni f(a) \neq 0\}$ *be the set of all polynomial functions that do not vanish at a.Then the fraction* $\frac{f}{g}$ *for* $f \in F(X)$ *and* $g \in S$ *can be thought of as rational functions that are well defined at a is called the* ***Localization*** *where,* $F(X)$ *is the ring of polynomial functions on X.*

Definition 2.6. *[12] A* ***primitive root*** *of a field* F_{p^k} *is an element whose powers constitute all of* $F_{p^k}^*$. *That is, the roots is a generator of the cyclic group* $F_{p^k}^*$.

Remark 2.1. *In [12]*

(i) *An element* $g \in F_{p^k}$ *is a primitive root if and only if* $g^{(p^k-1)/q} \neq 1$, *for every prime* q *dividing* $p^k - 1$.

(ii) *If* g *is a primitive root modulo* p *then* g^r *is a primitive root if and only if* $gcd(r, p-1) = 1$.

3. HASH FUNCTIONS USING FREE GENERATORS THEOREM

We recollecting the facts that the pre-images of any pair of matrices generating a free subgroup of $PGL_3(F_p((x)))$ also generated a free subgroup of $GL_3(F_p((x)))$.We desire to obtain such a pair of matrices over $M_{3\times3}(F_p[x])$ that

were free generators of the subgroups of $GL_3(F_p((x)))$ and define the projection mapping from an algebraic structure to quotient structure which gives the images in $GL_3(F_q)$.

By using Free Generators Theorem,we obtain the set of pair of matrices with entries in $F_p[x]$ which is defined in set $\mathbb{D}$.We work with the elements in $\mathbb{D}$ to construct a Cayley Hash function to protect the local modifications property and the security properties of the corresponding hash functions are analysed.We can create an infinite number of Hash functions using the Free Generators Theorem by different values of p and n and here we clearly says that for which choices of parameters these hash functions are the best.

3.1. **Construction of the Hash Function.** We require the following definitions to construct the Hash Function.

Definition 3.1. *Let p be a prime and we define the set as* $\mathbb{D} = \{(\tilde{A}, \tilde{B}) : \tilde{A}, \tilde{B} \in M_{3\times3}(F_p((x)))$ *are pre-images of A and B in* $PGL_3(F_p((x)))\}$. *That is, we define the set of all pair of matrices* $(\tilde{A}, \tilde{B})$ *such that* $\tilde{A}, \tilde{B} \in GL_3(F_p[x])$ *are pre-images of A and B in* $PGL_3(F_p((x)))\}$ *given by the Theorem 5.2.1*

Definition 3.2. *Given a prime p and an irreducible polynomial* $r_n(x)$ *in* $F_p[x]$ *of degree n and* $F_q \cong F_p[x]/ < r_n(x) >$.*Let us define the projection function* $\pi_{r_n} : S \longrightarrow GL_3(F_q)$ *be the mapping from the set* $S = \{M \in M_{3\times3}(F_p[x]) : r_n(x) \nmid det(M)\}$ *to the group* $GL_3(F_q)$. *That is,the map yields the matrix entries to their projection in* F_q.*For ease of notation, we will write* π_{r_n} *as* π *, when* $r_n(x)$ *is not mentioned.*

Remark 3.1. *If* $det(\tilde{A})$ *and* $det(\tilde{B})$ *are not divisible by* $r_n(x)$ *then the construction of the hash function using the projection map from a choice of generators* $(\tilde{A}, \tilde{B})$ *in* $\mathbb{D}$ *to elements of* $GL_3(F_q)$.

Formal definition of the hash function is defined as follows,

Definition 3.3. *Let* p *be a prime and an irreducible polynomial* $r_n(x)$ *in* $F_p[x]$ *of degree n.Let us choose the matrices* $(\tilde{A}, \tilde{B}) \in G$ *such that* $det(\tilde{A}) \nmid r_n(x)$ *and* $det(\tilde{B}) \nmid r_n(x)$*, then the associated hash function* $H_4 : \{0,1\}^* \longrightarrow GL_3(F_q)$ *, are as follows,if* $m = m_1m_2.....m_n$ *be a binary strings. Then* $H_4(m) = h(m_1)h(m_2)$ $\ldots, h(m_n)$*, where,* $h(m_i) = \begin{cases} h(\pi_{r_n}(\tilde{A})) & if m_i = 0 \\ h(\pi_{r_n}(\tilde{B})) & if m_i = 1. \end{cases}$

We denote the set of all associated hash function of $(\tilde{A}, \tilde{B}) \in \mathbb{D}$ *and* $r_n(x)$ *as* $\mathbb{H}$. *The hash function* H_4*, which defined here is resistant to the previous attacks on the Tillch-Zemor hash function and possesses some strong properties.*

3.2. **Properties of the Hash Function.** Now first we scrutinize the properties of the elements in $\mathbb{H}$.To obtain the local modifications property,we need the degrees of the entries of $\tilde{A}$ and $\tilde{B}$ are small compared to n.

3.2.1. *Small Modification Property:* The main goal of our hash function H_4 is to protect the small modifications property by using degree argument. Suppose that $\tilde{A}$ and $\tilde{B}$ generates a free monoid in $M_{3\times3}(F_p[x])$, for any polynomial generators in $\mathbb{D}$.We need to prove the following results,

(i) part(a), which is related to the degree argument in the Tillich-Zemor's X construction.
(ii) part(b) and part(c) gives that our matrices in $\mathbb{D}$ satisfy a strong property.

Proposition 3.1. *Let* $(\tilde{A}, \tilde{B}) \in M_{3\times3}(F_p[x])$ *such that* $\tilde{A}, \tilde{B}$ *generates the free monoid* $M_{3\times3}(F_p[x])$ *and let* $r_n(x)$ *be an irreducible polynomial in* $F_p[x]$.*Suppose* H_4 *be the associated hash function defined in 6.1.3 for* $(\tilde{A}, \tilde{B})$ *and* $r_n(x)$.*Assume that* $\tau = max\{deg(\tilde{A}), deg(\tilde{B})\}$ *and that* $m \in \{0,1\}^l$ *and* $m^{'} \in \{0,1\}^k$ *are different bit strings for some* $0 \leqslant l, k \leqslant n \mid \tau$. *Then,*

- $H_4(m) \neq H_4(m^{'})$
- *If* $(\tilde{A}, \tilde{B}) \in \mathbb{D}$ *then* $H_4(m) \neq a.H_4(m^{'})$ *for any* $a \in F_q$ *such that inspecting 'a' as an element of* $F_p[x]$, $(deg(a) + k\tau) < n$
- $H_4(m) \neq a.I$ *for any* $a \in F_q$.

Proof. Let M and $M^{'}$ be the product of $\tilde{A}$'s and $\tilde{B}$'s respectively produce $H_4(m)$ and $H_4(m^{'})$ in $M_{3\times3}(F_p[x])$,before projecting M and $M^{'}$ into $GL_3(F_q)$,so that $\pi(M) = H_4(m)$ and $\pi(M^{'}) = H_4(m^{'})$. Since $l, k < n \mid \tau$ then M has degree atmost $l\tau$ and $M^{'}$ has degree at most $k\tau$. We know that, each of the entries of M and $M^{'}$ has a degree less than n then $\pi(M) = \pi(M^{'}) \in Gl_3(F_q)$ if and only if $M = M^{'} \in M_{3\times3}(F_p[x])$.

(i) Now, since m and $m^{'}$ are distinct messages then the products of $\tilde{A}$'s and $\tilde{B}$'s are also distinct. Clearly , $M, M^{'} \in (\tilde{A}, \tilde{B})$ and by our hypothesis $\tilde{A}$ and $\tilde{B}$ generates a free monoid. So, follows $M = x_1x_2.....x_l \neq y_1y_2.....y_k = M^{'}$, where $x_i, y_j \in \{\tilde{A}, \tilde{B}\}$, for all $i = 1$ to $l, j = 1$ to k. Since,m and $m^{'}$ are distinct,

we have

$$M \neq M^{'} \text{ in } M_{3\times 3}(F_p[x]) \;\Rightarrow\; \pi(M) \neq \pi(M^{'}) \text{ in } GL_3(F_q) \;\Rightarrow\; H_4(m) \neq H_4(m^{'}).$$

(ii) Since, $\tilde{A}, \tilde{B}$ in $\mathbb{D}$ then their pre-images are in $PGL_3(F_p((x)))$ generates a free subgroup of $PGL_3(F_p((x)))$ which implies that $[M] \neq [M^{'}]$, and further, that $M \neq aM^{'}$ for any $a \in F_p[x]$.

Suppose,$\pi(M) = a\pi(M^{'})$ for some $a \in F_q$ in $GL_3(F_q)$, inspecting 'a' as an element in $F_p[x]$, then $M = aM^{'} + r_n(x)M^{''}$ for some $M^{''} \in M_{3\times 3}(F_p[x])$. By hypothesis, $deg(a) + deg(M^{'}) < n \Longrightarrow deg(aM^{'}) < n$ and M has all the entries, each of degree less than n, which says that $M^{"} = 0$. Therefore, $M = aM^{'}$, which is a contradiction. Hence, $\pi(M) \neq a\pi(M^{'})$. Thus, $H_4(m) \neq aH_4(m^{'})$ for any $a \in F_q$.

(iii) It is not possible for the products in $\pi(M)$ and $\pi(M^{'})$ of length less than $n \mid \tau$ to get the identity. Therefore, $H_4(m) \neq aI$ for any $a \in F_q$ Hence, $\pi(M)$ and $\pi(M^{'})$ must have order atleast $n \mid \tau$ □

4. Resistance against different attacks

(i) To avert the collisions of the form $\pi(\tilde{A})^{ord(\pi(\tilde{A}))} = I$ and $\pi(\tilde{B})^{ord(\pi(\tilde{B}))} = I$,we consider that $\pi(\tilde{A})$ and $\pi(\tilde{B})$ must be of large order.

(ii) If $det(\pi(\tilde{A}))$ is primitive root then $order(\pi(\tilde{A})) \geqslant q - 1$.

(iii) However, avoiding short relations attack is of the form $W(\pi(\tilde{A}), \pi(\tilde{B})) = kI$, where $k \in F_q^*$ and $W(\pi(\tilde{A}), \pi(\tilde{B})) \in \{\pi(\tilde{A}), \pi(\tilde{A}^{-1}), \pi(\tilde{B}), \pi(\tilde{B}^{-1})\}$ be a non-trivial word.To avoid such relations we proved the proposition.

Proposition 4.1. *Let $(\tilde{A}, \tilde{B}) \in \mathbb{D}$ and let $W(\tilde{A}, \tilde{B}) \in \{\tilde{A}, \tilde{A}^{-1}, \tilde{B}\tilde{B}^{-1}\}$ be a non-trivial word then there exist a choice of $r_n(x)$ such that if $F_q = F_p[x] \mid< r_n(x) >$,then $W(\pi_{r_n}(\tilde{A}), \pi_{r_n}(\tilde{B})) \neq kI \in GL_3(F_q)$ for any $k \in F_q^*$.*

Proof. Let $\phi = det(\tilde{A}\tilde{B}) = det(\tilde{A})det(\tilde{B}) \in F_p[x]$. We define, the localization of $F_p[x]$ at ϕ as $F_p[x]_{1/\phi} = \{t/\phi^m : t \in F_p[x], m \geqslant 0\}$. Since, $\dfrac{1}{\phi} = \dfrac{1}{det(\tilde{A}\tilde{B})}$ we have,

$\frac{1}{det(\tilde{A})} \in F_p[x]_{1/\phi}$ and $\frac{1}{det(\tilde{B})} \in F_p[x]_{1/\phi}$. We know that,$F_p[x]_{1/\phi}$ is contained in the fraction field of $F_p(x)$ and also in $F_p((x))$.

Therefore, $\tilde{A}, \tilde{B} \in GL_3(F_p[x])_{1/\phi} \subset GL_3(F_p((x)))$. We define the ideal $< r >= \{rt : t \in F_p[x]\}$ for any irreducible polynomial $r \in F_p[x]$. Assume,$r \nmid \phi$ and let $r_{1/\phi}$ be the localization of r at ϕ, i.e, $r_{1/\phi} = \{\frac{rt}{\phi^m} : t \in F_p[x], m \geqslant 0\}$.

Now, let us consider a surjective homomorphism from $F_p[x]_{1/\phi}$ to F_q under the irreducible polynomial, i.e., $\eta_r : F_p[x]_{1/\phi} \longrightarrow F_q$ induced by $x \longrightarrow a$, where a is a root of r and has a kernel $r_{1/\phi}$. Thus,by the first isomorphism theorem gives as,$\frac{F_p[x]_{1/\phi}}{r_{1/\phi}} \cong F_q$.

Under this homomorphism, the natural images of $\tilde{A}$ and $\tilde{B}$ in $GL_3(F_q)$ is $\pi_r(\tilde{A})$ and $\pi_r(\tilde{B})$ respectively. Since $\tilde{A}, \tilde{B} \in \mathbb{D}$, then their images $\tilde{A}, \tilde{B} \in PGL_3(F_p((x)))$ also generate a free group,this says that no freely reduced (non-trivial) word in $\{\tilde{A}, \tilde{A}^{-1}, \tilde{B}, \tilde{B}^{-1}\}$ can be I or any scalar multiple kI of I for any $k \in F_q^*$.

But we observe that images of $\tilde{A}, \tilde{B}$ in $GL_3(F_q)$ under homomorphism may have $W(\pi_r(\tilde{A}), \pi_r(\tilde{B})) = kI$ for some $k \in F_q^*$ if and only if inspecting $k \in F_p[x] \subset F_p[x]_{1/\phi}$, i.e., if

$$W = \begin{pmatrix} k+\alpha & \beta & \gamma \\ \delta & k+\mu & \lambda \\ \theta & \omega & k+\nu \end{pmatrix},$$

where $\alpha, \beta, \delta, \gamma, \mu, \lambda, \theta, \omega, \nu \in F_p[x]_{1/\phi}$ and $\eta_r(\alpha) = \eta_r(\beta) = \eta_r(\delta) = \eta_r(\gamma) = \eta_r(\mu) = \eta_r(\lambda) = \eta_r(\theta) = \eta_r(\omega) = \eta_r(\nu) = 0$. Hence,we choose $r_n(x) \in F_p[x]$ such that any one of the $\eta_{r_n}(i), i \in \{\alpha, \beta, \delta, \gamma, \mu, \lambda, \theta, \omega, \nu\}$ must be non-zero. We need to choose $r_n(x)$ very carefully to avert from a small set of relations. □

5. CONCLUSION

Applying the Free Generators theorem, the hash functions are constructed and it retains its Modifications property using degree argument.Also verify the security properties of the hash functions using different attacks. Finally, Cryptographic hash functions like SHA-256 and SHA-512 have a maximum input message size of $2^{64} - 1$ bits and $2^{128} - 1$ bits ,respectively [11]. All the attacks we discussed are runs in expotential time, choosing parameters comparable to

those in cryptographic standards is expected to be sufficient to provide a secure hash function [6].

Now the NIST approved hash algorithms are SHA3-224, SHA3-256, SHA3-384, SHA3-512 [8] and these algorithms have their security strength in bits related to the numbers. For example, SHA3-512 gives 512 bits of security against a preimage or second preimage finding algorithm and 256 security bits against a collision finding algorithm. But, Mullans attack in [9] had a running time $\mathbb{O}(\sqrt{q})$ and produce collisions of length $\mathbb{O}((logq)^2/log(logq))$, which is the fastest known attack. If we choose $p^n \sim 2^{512}$ will provide equivalent security as a SHA3 family.

Thus, by choosing some suitable and satisfiable conditions to our proposed hash functions. They are secure against all the previous attacks on the Zemor-Tillich hash function.

REFERENCES

[1] A. GATHMANN: *Class Notes on Commutative Algebra*, Technische Universitat, Kaiserslautern, 2013.

[2] B. SOSNOVSKI: *Cayley graphs of semi-groups and Applications to Hashing*, Ph.D thesis, City University of New York, 2016.

[3] R. D. STINSON: *Cryptography Theory and Practice*, Second Edition, Chapman and Hall/CRC, 1995.

[4] G. ZEMOR: *Hash functions and graphs with large girths*, EUROCRYPT (Donald W. Davies, ed.), Lecture Notes in Computer Science, Springer, LNCS **547** (1991), 508–511.

[5] P. GODLEWSKI, P. CAMION: *Manipulations and errors, detection and localization*, In Advances in cryptology-EUROCRYPT'88 (Davos Ed.), Lecture Notes in Comput.Sci., **330** (1988), 97–106.

[6] H. TOMKINS: *Alternative Generators of the Zemor-Tillich Hash Function:A Quest for Freedom in Projective Linear Groups*, University of Ottawa, 2018.

[7] JP. TILLICH, G. ZEMOR: *Hashing with SL_2*, Advances in Cryptology Lecture Notes in Computer Science, Springer-Verlag, **839** (1994), 40–49.

[8] M. J. DWORKIN: *Permutation-based hash and extendable-output functions,* Technical report, 2018.

[9] C. MULLAN, B. TSABAN: *SL_2 homomorphic hash functions:Worst case to average case reduction and short collision search*, Designs, Codes and Cryptography, **81**(1) (2016), 83–107.

[10] B. PRENEEL: *Analysis and Design of Cryptographic Hash Functions*, Ph.D thesis, K. U. Leuven, 2003.

[11] Q. H. DANG: *Federal Information Processing Standards Publication*, Secure Hash Standards, Federal Inf. Process. Stds., **180**(4) (2015), 33–44.

[12] R. CRANDALL, C. POMERANCE: *Prime Numbers: A Computational Perspective*, Second Edition, Springer, 2005.

[13] V. VIBITHA KOCHAMANI, P. L. LILLY, K. T. JOJU: *Hashing with discrete Heisenberg group and graph with large girth*, International Journal of Theoretical Physics and Cryptography, **5** (2016), 1–12.

[14] V. VIBITHA KOCHAMANI, P. L. LILLY: *Security aspects of the Cayley hash function using discrete Heisenberg group*, Journal of Discrete Mathematical Sciences and Cryptography, **5** (2019), 1–10.

[15] V. VIBITHA KOCHAMANI, P. L. LILLY: *Free generators theorem in projective general linear group*, Communicated, 2020.

DEPARTMENT OF MATHEMATICS
ST.JOSEPH'S COLLEGE (AUTONOMOUS)
IRINJALAKUDA-680121, INDIA
E-mail address: myvkumari@gmail.com

DEPARTMENT OF MATHEMATICS
ST.JOSEPH'S COLLEGE (AUTONOMOUS)
IRINJALAKUDA-680121, INDIA
E-mail address: sr.christy@gmail.com