New Zémor-Tillich Type Hash Functions Over $\mathbf{GL_2}\left(\mathbb{F}_{p^n}\right)$

Hayley Tomkins, Monica Nevins*, and Hadi Salmasian†

Department of Mathematics and Statistics, University of Ottawa, Ottawa K1N 6N5, Canada

Abstract. We present a large class of new Zémor-Tillich type hash functions whose target space is the finite group $\mathrm{GL}_2\left(\mathbb{F}_{p^n}\right)$ for any prime p and power n. To do so, we use a novel group-theoretic approach that uses Tits' "Ping-Pong Lemma" to outline conditions under which a set of matrices in $\mathrm{PGL}_2\left(\mathbb{F}_p(\!(x)\!)\right)$ generates a free group. The hash functions we form are secure against known attacks, and simultaneously preserve many of the desired features of the Zémor-Tillich hash function. In particular, our hash functions retain the *small modifications property*.

Keywords: Hash functions · Cayley hash · free groups.

1 Introduction

Hash functions are an essential part of many cryptographic schemes, principally as tools of message authentication and modification detection. In [1] and [2] Gilles Zémor introduced the idea of building hash functions from Cayley graphs of large girth. The remarkable property of these Cayley graph hash functions, known as the *small modifications property*, is that any small modification of a message necessarily changes its hash value. This idea was popularized by a later construction due to Tillich and Zémor [3]. Recalling that $\{0,1\}^*$ denotes the set of all finite sequences of $0s$ and $1s$, the fundamental construction is as follows.

Associated hash: *Given a group G and $g_1,\ g_2 \in G$, the associated [Cayley] hash H is the map defined for any message $m = m_1 \cdots m_k \in \{0,1\}^*$ by $H(m) = H(m_1) \cdots H(m_k) \in G$ where $H(0) = g_1$ and $H(1) = g_2$.*

Formally one chooses $N \sim \log(|G|)$ and an injective map $\psi : G \to \{0,1\}^N$, then uses $\psi(H(m))$ as a hash value. However, we will consider the hash values as elements of G. Seeing our hash values in this way allows notions such as collision, second preimage, and preimage resistance to be easily restated as mathematical problems that for a general group are believed to be hard. As an example, the

* † Throughout this work the research of Monica Nevins was supported by an NSERC Discovery Grant (RGPIN-2015-06294) and the research of Hadi Salmasian was supported by an NSERC Discovery Grant (RGPIN-2018-04044).

notion of collision resistance is the group-theoretic *balance problem*: Given a set of elements S generating a group G, find an efficient algorithm that returns two distinct reduced words over S (with lengths bounded by some parameter L) whose products are equal in G [4].

Following Zémor's original motivation, our goal in this paper is to preserve the property of the Zémor-Tillich hash function that small modifications of text are detected. As conventional, we write $q = p^n$, and view $\mathbb{F}_q$ as the quotient $\mathbb{F}_q \cong \mathbb{F}_p[x]/\langle r_n(x)\rangle$ for some irreducible polynomial $r_n(x)$ of degree n. Further, we write $\mathbb{F}_p(\!(x)\!)$ for the field of formal Laurent series over $\mathbb{F}_p$ and write $\mathrm{M}_{2\times 2}\big(\mathbb{F}_p[x]\big)$ for the set of matrices with entries in the polynomial ring $\mathbb{F}_p[x] \subseteq \mathbb{F}_p(\!(x)\!)$.

Our hash function construction: *Let A, $B \in \mathrm{M}_{2\times 2}\big(\mathbb{F}_p[x]\big)$ and set*

$$\mathcal{D} = \big\{M \in \mathrm{M}_{2\times 2}\big(\mathbb{F}_p[x]\big) \;\mid\; r_n(x) \nmid \det(M)\big\}.$$

Define the projection map

$$\pi_{r_n} : \mathcal{D} \to \mathrm{GL}_2\big(\mathbb{F}_q\big)$$

to be the map taking entries of a matrix to their projections in $\mathbb{F}_q$ under the quotient by $\langle r_n(x)\rangle$. We then construct a hash function H by taking the associated hash for $g_1 = \pi_{r_n}(A)$, $g_2 = \pi_{r_n}(B)$, and $G = \mathrm{GL}_2\big(\mathbb{F}_{p^n}\big)$.

To make such choices of A and B, we use our novel Free Generators Theorem (Theorem 1, Section 2), which we will prove in Sections 2.2 and 2.3 using the geometry of projective space over $\mathbb{F}_p(\!(x)\!)$. We present a simplified version here.

Free Generators Theorem, Simplified *Let p be a prime and let $d \in \mathbb{N}_0$ be such that $d \neq 0$ if $p = 2$. Furthermore, fix nonzero $f, \tilde{f} \in x^{2d+1}\mathbb{F}_p[x]$, $c \in \{0,1\}$, and $a, b, \tilde{a}, \tilde{b} \in \mathbb{F}_p[x]$ such that*

$$g \not\equiv h \mod x^{d+1} \quad \textit{for each} \quad g, h \in \begin{cases} \{b, \tilde{a}, \tilde{b}\} & \textit{if } c = 0 \\ \{a, b, \tilde{a}, \tilde{b}\} & \textit{if } c = 1. \end{cases}$$

Then the matrices

$$A = \begin{pmatrix} cb - af & c(f-1) \\ ab(1-f) & cbf - a \end{pmatrix} \;\textit{ and }\; B = \begin{pmatrix} \tilde{b} - \tilde{a}\tilde{f} & \tilde{f} - 1 \\ \tilde{a}\tilde{b}(1-\tilde{f}) & \tilde{b}\tilde{f} - \tilde{a} \end{pmatrix}$$

generate a free monoid in $\mathrm{M}_{2\times 2}\big(\mathbb{F}_p[x]\big)$ and a free subgroup of $\mathrm{GL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$.

Corollary *Let A, $B \in \mathrm{M}_{2\times 2}\big(\mathbb{F}_p[x]\big)$ be matrices produced using the Free Generators Theorem such that $r_n(x) \nmid \det(A)$ and $r_n(x) \nmid \det(B)$. Let H be the associated hash for $g_1 = \pi_{r_n}(A)$, $g_2 = \pi_{r_n}(B)$, and $G = \mathrm{GL}_2\big(\mathbb{F}_{p^n}\big)$. Then H satisfies the* small modifications property *for alterations of up to n/δ bits, where δ is the maximum degree of entries of A and B (Proposition 9). In particular,*

this implies that H has no collisions *for messages of length at most n/δ.*

Note that from now on we assume $r_n(x)$ does not divide $\det(A)$ or $\det(B)$, so that $\pi_{r_n}(A)$ and $\pi_{r_n}(B)$ are defined. In Section 3, we take A and B to have entries of degree much smaller than n, so this condition will hold automatically. Moreover, when clear from context we use π instead of π_{r_n}.

The Free Generators Theorem allows us to create infinitely many hash functions over $\mathrm{GL}_2(\mathbb{F}_q)$ as we vary p and n. For example, notice that for $p > 2$, taking $c = 0$, $a = 1$, and b, $\tilde{a}$, and $\tilde{b}$ to be -1, 0, and 1 in some order satisfies the (Simplified) Free Generators Theorem for any choice of $d \geq 0$. These possible choices of b, $\tilde{a}$, and $\tilde{b}$ give us 6 different pairs (A, B), and are shown in Table 1. With each of these choices, we can take $d = 0$ and any $f, \tilde{f} \in \mathbb{F}_p[x]$ such that f and $\tilde{f}$ have a zero constant term. We let $S_1(f, \tilde{f}), \ldots, S_6(f, \tilde{f})$ be these choices of $\{A, B\}$. The (Simplified) Free Generators Theorem then gives the following.

Corollary *Each pair of matrices $S_i(f, \tilde{f})$ in Table 1 generates a free group in $\mathrm{GL}_2(\mathbb{F}_p(\!(x)\!))$. In particular, $S_i(f, \tilde{f})$ also generates a free monoid in $\mathrm{M}_{2\times 2}(\mathbb{F}_p[x])$.*

Table 1. The matrices A and B produced using the (Simplified) Free Generators Theorem for $p > 2$, $d = 0$, $a = 1$, $c = 0$, $f, \tilde{f} \in x\mathbb{F}_p[x]$, and given choices of b, $\tilde{a}$, and $\tilde{b}$.

$\{A, B\}$	A	B	b	$\tilde{a}$	$\tilde{b}$
$S_1(f, \tilde{f})$	$\begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \tilde{f}+1 & 1-\tilde{f} \\ 1-\tilde{f} & \tilde{f}+1 \end{pmatrix}$	0	1	-1
$S_2(f, \tilde{f})$	$\begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \tilde{f}+1 & \tilde{f}-1 \\ \tilde{f}-1 & \tilde{f}+1 \end{pmatrix}$	0	-1	1
$S_3(f, \tilde{f})$	$\begin{pmatrix} f & 0 \\ f-1 & 1 \end{pmatrix}$	$\begin{pmatrix} \tilde{f} & \tilde{f}-1 \\ 0 & 1 \end{pmatrix}$	1	-1	0
$S_4(f, \tilde{f})$	$\begin{pmatrix} f & 0 \\ f-1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1-\tilde{f} \\ 0 & \tilde{f} \end{pmatrix}$	1	0	-1
$S_5(f, \tilde{f})$	$\begin{pmatrix} f & 0 \\ 1-f & 1 \end{pmatrix}$	$\begin{pmatrix} \tilde{f} & 1-\tilde{f} \\ 0 & 1 \end{pmatrix}$	-1	1	0
$S_6(f, \tilde{f})$	$\begin{pmatrix} f & 0 \\ 1-f & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & \tilde{f}-1 \\ 0 & \tilde{f} \end{pmatrix}$	-1	0	1

For an example of generators with $p = 2$, take $d = 1$, $a = 1$, $c = 0$, $b = 0$, $\tilde{a} = 1$, and $\tilde{b} = x$. Then, for any $f, \tilde{f} \in x^3\mathbb{F}_2[x]$, the (Simplified) Free Generators Theorem implies that $A = \left(\begin{smallmatrix} f & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} \tilde{f}+x & \tilde{f}+1 \\ x\tilde{f}+x & x\tilde{f}+1 \end{smallmatrix}\right)$ generate a free subgroup in $\mathrm{GL}_2(\mathbb{F}_2(\!(x)\!))$.

In this work, we show that educated choices of generators produced using the Free Generators Theorem give hash functions that both are resistant to the previous attacks on the Zémor-Tillich hash function and possess numerous useful properties, including many that popularized the Zémor-Tillich hash function (see Section 1.1). For instance, using the Free Generators Theorem affords us a

stronger version of the property that small modifications are detected (Proposition 10), as well as a new method of preventing against specific small relations (Proposition 12), such as the relation used in an initial attack in [5]. More broadly, the Free Generators Theorem provides many choices of g_1 and g_2 over *any* characteristic and offers a great amount of control in the degrees and form of the entries in our generators. The Free Generators Theorem also extends to allow an arbitrary number of generators (Theorem 4). Further, as Cayley hashes, our constructions are both *scalable*, meaning we can control the size of the output, and possess the *concatenation property*; $H(m_1m_2) = H(m_1)H(m_2)$, which easily allows for hash values to be *computed in parallel*. The concatenation property also has a real-life application: in [6] Quisquater and Joye showed it made the Zémor-Tillich hash function ideal for authenticating video sequences.

To further highlight the strength of the Free Generators Theorem, we note that the inductive degree argument Tillich and Zémor use to show that their matrices A and B generate a free monoid [3, Lemma 3.5] can only be extended to matrices with a particular relation between the degrees of their entries. Our method of choosing generators using the Free Generators Theorem, Theorem 1, is preferable in many ways. For example, in Section 3 we find precise conditions on our parameters for generating a large enough set of hash values (Propostions 15 and 16), and see that the freeness allows us to prevent against attacks using short relations (Proposition 12). As well, our theorem substantially increases freedom in the choice of generators, which we believe should make the corresponding hash function less susceptible to attacks that are dependent on the structure of the generators themselves, such as Grassl et al's palindrome attack [7]. Moreover, the Free Generators Theorem provides many choices of generators that could not be produced using the extended degree argument alluded to above, such as any of the sets $S_1(f, \tilde{f}), \ldots, S_6(f, \tilde{f})$ from Table 1.

The ideas in this paper are also mathematically interesting beyond their immediate application to hash functions. For one, the use of Breuillard and Gelander's [8] version of Tits' Ping-Pong argument in our proof of the Free Generators Theorem (see Sections 2.2 and 2.3) offers a concrete mechanism by which to apply their results to generate free subgroups of $\mathrm{PGL}_n(\mathbb{K})$, for any n and any local field $\mathbb{K}$. For another, when $\mathbb{K}$ is non-Archimedean one can interpret A and B as acting by translations on the Bruhat-Tits tree of $\mathrm{PGL}_2(\mathbb{K})$; it would be an interesting question to interpret the conditions for freeness of the group they generate to the geometry of this building.

This work is organized as follows. In Section 1.1 we give a brief review of prior work related to this paper. In Section 2 we state the Free Generators Theorem and give its proof. In Section 3 we analyse our hash function constructions and their beneficial properties in great detail, including presenting the stronger version of the small modification property (Proposition 10) and our method of preventing against given sets of small relations (Proposition 12). We then consider some potential attacks in Section 4, and summarize the robustness of our proposed hash functions in Section 5. Appendix A serves as a mathematical background and is auxiliary.

1.1 Previous Work

Zémor originally suggested generators $g_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $g_2 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and the target group $G = \mathrm{SL}_2(\mathbb{F}_p)$ [1, 2], and though soon broken in [9], his construction inspired numerous subsequent hash functions, with many constructions using expander graphs [10–15]. In particular we note that Lauter, Charles, and Goren [16] proposed two constructions for a patent, one using Pizer graphs over elliptic curves, and another using LPS expander graphs.

Most recently, Bromberg et al. [17] suggested extending a pair of generators proposed in [9] to pairs of the form $g_1 = \left(\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right)$ and $g_2 = \left(\begin{smallmatrix} 1 & 0 \\ s & 1 \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{F}_p)$ for p a large prime, and showed that for $r = s = 2$ and $r = s = 3$ these choices remain impervious to known attacks, including the lifting attack presented in [9]. However, we note that our approach produces a much larger and more flexible class of generators, and further it is applicable to the $\mathrm{GL}_2(\mathbb{F}_q)$ setting.

Zémor's construction also inspired our hash function of interest, the Zémor-Tillich hash function. This hash function was introduced in 1994 by Tillich and Zémor [3] and is defined as the associated hash of $G = \mathrm{SL}_2(\mathbb{F}_{2^n})$ and

$$g_1 := \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}, \qquad g_2 := \begin{pmatrix} x & x+1 \\ 1 & 1 \end{pmatrix}$$

where x is a root of the defining polynomial of $\mathbb{F}_{2^n}$.

From its introduction the Zémor-Tillich hash function was well-received for many reasons. Remarkably, the Zémor-Tillich hash function was *comparable in computation speed* to current cryptographic standards [18]. In a world where computational speed is usually sacrificed for having security based on some mathematical problem, or vice versa, it is rare to satisfy both these properties. Further, the Zémor-Tillich hash function retained the property that made Zémor's original construction so appealing: *small modifications of messages are detected* [3]. Another noteworthy feature of the Zémor-Tillich hash function is that the distribution of all possible hash values of messages of length ℓ *approaches the uniform distribution* as ℓ approaches infinity [3].

The first attack on the Zémor-Tillich hash function was made by Charnes and Pieprzyk [5], which was later followed by [19]. However, these attacks were easily avoided as they were specific to the choice of polynomial used to define the finite field $\mathbb{F}_{2^n}$. The first attack defined independently of this choice was by Geiselmann, but was considered impractical [20]. It was not until 2011 that a feasible attack was found on Tillich and Zémor's construction by Grassl et al. [7], which was later extended into a preimage attack [21]. However, this attack was very specific to both the characteristic of the underlying finite field, and Tillich and Zémor's choice of generators.

Some general attacks on hash functions over $\mathrm{SL}_2(\mathbb{F}_q)$ have been investigated [22, 23], including an approach utilizing factoring techniques over $\mathrm{SL}_2(\mathbb{F}_{2^n})$ [24, 25], but they are infeasible for a sufficiently large p^n. Consequently Tillich and Zémor's construction is still considered of interest for $G = \mathrm{SL}_2(\mathbb{F}_{p^n})$ [4, 26]. This leaves an open question: what choices of generating matrices and underlying

finite fields produce, based on Tillich and Zémor's initial construction, a hash function which retains the strengths of the Zémor-Tillich hash function but is more robust to attacks?

While some alternative generators for the Zémor-Tillich hash function have been suggested [21, 4], few have been presented with thorough analysis, and almost all suggestions are in $\mathrm{SL}_2\big(\mathbb{F}_{2^n}\big)$. Expanding the search for alternative generators to characteristic p, an odd prime, or the larger group $\mathrm{GL}_2\big(\mathbb{F}\big)$, where $\mathbb{F}$ is a finite field, appears to be almost entirely new and is the aim of this work.

2 Statement of the Free Generators Theorem

In this section we present and prove the Free Generators Theorem (Theorem 1), which provides an abundant source of pairs of matrices that generate a free subgroup of $\mathrm{GL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$, and from which we can algorithmically construct infinitely many pairs of generators as we vary p and n.

In the following $|\cdot|$ denotes the norm in $\mathbb{F}_p(\!(x)\!)$, $[u]$ and $[u_1 : u_2]$ denote the respective images of a vector u and a vector (u_1, u_2) in $\mathbb{P}^1$, and $d(\ ,\ )$ is the distance we equip to $\mathbb{P}^1$. Precise definitions are given in Appendix A.

Theorem 1 (Free Generators Theorem) *Let p be a prime and let $d \in \mathbb{N}_0$ be such that $d > 0$ if $p = 2$. Choose any $a, b, c, \tilde{a}, \tilde{b} \in \mathbb{F}_p(\!(x)\!)$, $f, \tilde{f} \in \mathbb{F}_p(\!(x)\!)^\times$, such that*

$\boldsymbol{\Xi_1}$ **:** $d([u],[v]) > \frac{1}{p^{d+1}}$ *for each pair of* $[u],[v]$ *in* $\big\{[a:c],[1:b],[1:\tilde{a}],[1:\tilde{b}]\big\}$, *and*

$\boldsymbol{\Xi_2}$ **:** $\min\{|f|,|f^{-1}|\} \leq \frac{1}{p^{2d+1}}$, *and* $\min\{|\tilde{f}|,|\tilde{f}^{-1}|\} \leq \frac{1}{p^{2d+1}}$.

Then the matrices

$$A = \begin{bmatrix} ab - cf & a(f-1) \\ cb(1-f) & abf - c \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} \tilde{b} - \tilde{a}\tilde{f} & \tilde{f} - 1 \\ \tilde{a}\tilde{b}(1-\tilde{f}) & \tilde{b}\tilde{f} - \tilde{a} \end{bmatrix} \tag{1}$$

generate a free group in $\mathrm{PGL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$. *In particular, any inverse images of A and B in* $\mathrm{GL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$ *also generate a free group.*

Note that this last statement follows because $\mathrm{PGL}_2\big(\mathbb{F}_p(\!(x)\!)\big) = \mathrm{GL}_2\big(\mathbb{F}_p(\!(x)\!)\big)/\mathrm{Z}$ where Z is the subgroup of invertible scalar matrices.

Notation: Given a prime p, we define $\mathfrak{S}_p$ to be the set of pairs of matrices $S = (\tilde{A}, \tilde{B})$ such that $\tilde{A}$, $\tilde{B} \in \mathrm{M}_{2\times 2}\big(\mathbb{F}_p[x]\big)$ are preimages of the matrices A, B in $\mathrm{PGL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$ described by Theorem 1. Further, we write $\mathfrak{S}$ when p is clear from context. We take $\mathfrak{H}$ to be the set of all hash functions constructed from Theorem 1 using the construction presented in Section 1.

2.1 Notes on parameters and extensions of the Free Generators Theorem

We first note that to satisfy condition Ξ_2, we need only take f and $\tilde{f}$ to be elements of sufficiently small norm in $\mathbb{F}_p(\!(x)\!)$, for instance any elements of $x^{2d+1}\mathbb{F}_p[x]$. To understand the feasibility of satisfying condition Ξ_1, we present the following proposition about the extraordinary geometry of $\mathbb{P}^1$ [27, Proposition 4.3.7]. Note that $\mathcal{O}$ denotes $\mathbb{F}_p[[x]]$, the set of series in $\mathbb{F}_p(\!(x)\!)$ with no negative powers. Write $N(u,\varepsilon) = \left\{[v] \in \mathbb{P}^1 \mid d([u],[v]) \leq \varepsilon\right\}$ for the closed ball of radius epsilon centred at u.

Proposition 2 *For each $d \in \mathbb{N}_0$ there exist $p^d(p+1)$ disjoint neighbourhoods of radius $\frac{1}{p^{d+1}}$ such that for any point $[u] \in \mathbb{P}^1$, $N\left([u], \frac{1}{p^{d+1}}\right)$ is precisely one of these neighbourhoods. They are*

1. *for each $(a_0, a_1, ..., a_d) \in \mathbb{F}_p^{d+1}$, $\{[1 : a_0 + a_1 x + \ldots + a_d x^d + r] \mid r \in x^{d+1}\mathcal{O}\}$, and*
2. *for each $(0, a_1, ..., a_d) \in \mathbb{F}_p^{d+1}$, $\{[a_1 x + \ldots + a_d x^d + r : 1] \mid r \in x^{d+1}\mathcal{O}\}$.*

Interestingly, we can obtain the neighbourhoods of radius $\frac{1}{p^{d+2}}$ by partitioning each of the $p^d(p+1)$ neighbourhoods of radius $\frac{1}{p^{d+1}}$ into p new ones.

Note that $[1 : g] = [g^{-1} : 1]$. Proposition 2 not only guarantees the existence of elements satisfying condition Ξ_1, but also explicitly shows how to choose such elements. Further, we see the case $d = 0$ is excluded when $p = 2$ as it would be impossible to satisfy condition Ξ_1; when $p = 2$ and $d = 0$ there are only 3 distinct $\frac{1}{p^{d+1}}$-neighbourhoods in $\mathbb{P}^1$, and at least four are needed.

For $[1 : g] \in \mathbb{P}^1$ such that $|g| \leq 1$, the condition $d([u],[v]) > \frac{1}{p^{d+1}}$ can be seen more intuitively in terms of congruences modulo powers of x, which we state as a lemma below.

Lemma 3 *For arbitrary $g, h \in \mathbb{F}_p(\!(x)\!)$ such that $h \in \mathcal{O}$ and $d \in \mathbb{N}_0$ we have $d([1 : g], [1 : h]) \leq \frac{1}{p^{d+1}}$ if and only if $g \equiv h \mod x^{d+1}$.*

Proof. As $h \in \mathcal{O}$, we can write $h = h_0 + h_1 x + \ldots + h_d x^d + h'$ for some $h_0, \ldots, h_d \in \mathbb{F}_p$ and $h' \in x^{d+1}\mathcal{O}$. By Proposition 2, there is a unique neighbourhood of radius $\frac{1}{p^{d+1}}$ containing h, namely $\{[1 : h_0 + h_1 x + \ldots + h_d x^d + r] \mid r \in x^{d+1}\mathcal{O}\}$. We see this set is precisely the set of elements $[1 : g]$ in $\mathbb{P}^1$ such that g is congruent to h modulo x^{d+1}.

Extension to non-binary hash functions: The proof of the Free Generators Theorem extends to a larger set of generators. Namely, for any $\ell > 0$ we can replace the matrix B in the Free Generators Theorem with the set of ℓ distinct matrices

$$\left\{ B_i := \begin{bmatrix} b_i - a_i f_i & f_i - 1 \\ a_i b_i (1 - f_i) & b_i f_i - a_i \end{bmatrix} \mid 1 \leq i \leq \ell \right\}$$

where

$\boldsymbol{\Xi_1'}$ **:** $d([u],[v]) > \frac{1}{p^{d+1}}$ for each pair of $[u],[v]$ in

$$\big\{[a:c],[1:b]\big\} \cup \big\{[1:a_i],[1:b_i] \;\mid\; 1 \leq i \leq \ell\big\}, \text{ and}$$

$\boldsymbol{\Xi_2'}$ **:** $\min\{|f|,|f^{-1}|\} \leq \frac{1}{p^{2d+1}}$, and $\min\{|f_i|,|f_i^{-1}|\} \leq \frac{1}{p^{2d+1}}$ for $1 \leq i \leq \ell$

for some $d \geq 0$ such that $p^d(p+1) \geq 2\ell + 3$.

Theorem 4 *The set of matrices $\{A, B_1, \ldots, B_\ell\}$ is a set of free generators of a free group in $\mathrm{PGL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$. In particular, any inverse images of $\{A, B_1, \ldots, B_\ell\}$ in $\mathrm{GL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$ form free generators of a free group.*

This provides $\ell+1$ generators, allowing us to hash messages written in base $\ell+1$. We note the proof of this result follows the proof of Theorem 1 identically, and is sketched in [27, Proposition 5.8.1].

The asymmetry in the generator set given by Theorem 4 corresponds to the asymmetry of the description of points in $\mathbb{P}^1$; we can view $\mathbb{P}^1$ as $\{[1:g] \mid g \in \mathbb{F}_p(\!(x)\!)\} \cup \{[0:1]\}$. The matrix A allows for the choice of $[0:1]$ as an eigenvector, and thus provides a slightly more general statement than having only elements of the form B_i.

Extensions to other groups and fields: The methods here can be extended to finding generators of free groups in $\mathrm{GL}_\ell\left(\mathbb{F}_p(\!(x)\!)\right)$ or $\mathrm{PGL}_\ell\left(\mathbb{F}_p(\!(x)\!)\right)$ for $\ell > 2$. For this extension there are some subtle technical issues that need to be addressed. A more straightforward extension would be applying the ideas of the proof of the Free Generators Theorem to produce free generators of general linear groups over other local fields, such as $\mathbb{Q}_p$, by equipping them with an analogous distance. However, $\ell = 2$ and $\mathrm{GL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$ seem to be the most cryptographically applicable choices.

Keyed hash functions: As the Free Generators Theorem produces not one, but many hash functions, we could also use the Free Generators Theorem to produce a keyed hash function, by choosing hash functions from a subset of hash functions in $\mathfrak{H}$ that satisfy the desired conditions we present in Section 3.3.

2.2 The strategy for the proof of the Free Generators Theorem

The motivation behind the proof of the Free Generators Theorem is to use Tits' "Ping-Pong Lemma", recalled here as Proposition 6. To this end, we are inspired by Breuillard and Gelander's [8] consideration of the Ping-Pong Lemma for projective linear groups over local fields. Breuillard and Gelander consider such groups as acting on an associated projective space, and show free groups can be found using group elements which map points of sufficient distance from a specified *repulsing point* close to a specified *attracting point*. With this in mind, we consider the action of A and B on $\mathbb{P}^1$ by considering the action of the preimages of A and B in $\mathrm{GL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$ on $\mathbb{P}^1$. Again, we emphasize that our applications of this idea in this section are new.

To see how a general matrix $U \in \mathrm{GL}_2(\mathbb{F}_p(\!(x)\!))$ acts on $\mathbb{P}^1$, suppose that U has eigenvectors u_1 and u_2, with corresponding eigenvalues λ_1 and λ_2. Then, given a general vector $[v] = [ru_1 + su_2] \in \mathbb{P}^1$, we have that

$$U \cdot [v] = [r\lambda_1 u_1 + s\lambda_2 u_2] = [ru_1 + s\frac{\lambda_2}{\lambda_1} u_2].$$

We notice that if $|\lambda_2| > |\lambda_1|$ and $s \neq 0$, then U moves $[v]$ closer to $[u_2]$ and away from $[u_1]$. This motivates us to investigate what a general form for A and B looks like in terms of the eigenvectors and eigenvalues of their preimages.

Lemma 5 *Let $\tilde{A}$, $\tilde{B} \in \mathrm{GL}_2(\mathbb{F}_p(\!(x)\!))$. Suppose that $\tilde{A}$ has distinct eigenvectors (a, c), $(1, b) \in V$ with corresponding eigenvalues g, $h \in \mathbb{F}_p(\!(x)\!)$ and that $\tilde{B}$ has distinct eigenvectors $(1, \tilde{a})$, $(1, \tilde{b}) \in V$ with corresponding eigenvalues $\tilde{g}$, $\tilde{h} \in \mathbb{F}_p(\!(x)\!)$. Then the respective images of $\tilde{A}$ and $\tilde{B}$ in $\mathrm{PGL}_2(\mathbb{F}_p(\!(x)\!))$ are*

$$A = \begin{bmatrix} ab - cf & a(f-1) \\ cb(1-f) & abf - c \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} \tilde{b} - \tilde{a}\tilde{f} & \tilde{f} - 1 \\ \tilde{a}\tilde{b}(1-\tilde{f}) & \tilde{b}\tilde{f} - \tilde{a} \end{bmatrix} \tag{2}$$

where $f = \frac{h}{g}$, $\tilde{f} = \frac{\tilde{h}}{\tilde{g}} \in \mathbb{F}_p(\!(x)\!)$.

Proof. We show this for $\tilde{A}$, as the proof for $\tilde{B}$ is identical. By linear algebra $A = \left[\begin{smallmatrix} a & 1 \\ c & b \end{smallmatrix}\right] \left[\begin{smallmatrix} g & 0 \\ 0 & h \end{smallmatrix}\right] \left[\begin{smallmatrix} b & -1 \\ -c & a \end{smallmatrix}\right] \in \mathrm{PGL}_2(\mathbb{F}_p(\!(x)\!))$, where the last matrix has been scaled by $ab - c$, which is invertible as $[a : c]$ and $[1 : b]$ are necessarily distinct.

As we are working over $\mathrm{GL}_2(\mathbb{F}_p(\!(x)\!))$ we note the eigenvalues of $\tilde{A}$ are nonzero, and in particular $g \neq 0$. Thus, up to $\mathrm{PGL}_2(\mathbb{F}_p(\!(x)\!))$ we can scale by $\frac{1}{g}$, obtaining $A = \left[\begin{smallmatrix} a & 1 \\ c & b \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & 0 \\ 0 & f \end{smallmatrix}\right] \left[\begin{smallmatrix} b & -1 \\ -c & a \end{smallmatrix}\right] = \left[\begin{smallmatrix} ab-cf & a(f-1) \\ cb(1-f) & abf-c \end{smallmatrix}\right]$, where $f = \frac{h}{g}$.

We note that, by Remark 18, we can assume that any four distinct elements of $\mathbb{P}^1$ are represented by the points $[a : c]$, $[1 : b]$, $[1 : \tilde{a}]$, and $[1 : \tilde{b}]$ for some a, b, c, $\tilde{a}$, $\tilde{b} \in \mathbb{F}_p(\!(x)\!)$. Thus, for elements A and B in $\mathrm{PGL}_2(\mathbb{F}_p(\!(x)\!))$, Lemma 5 is as general as possible.

Lemma 5 greatly simplifies our main argument: to find conditions for which A and B generate a free subgroup of $\mathrm{PGL}_2(\mathbb{F}_p(\!(x)\!))$ it is sufficient to consider A and B of the form in equation (2) as done in Free Generators Theorem. The proof of Theorem 1 uses the following proposition due to Jacques Tits [28, Prop 1.1], known as the Ping-Pong Lemma.

Proposition 6 (Ping-Pong Lemma) *Let P be a set, I an index set, G a group acting on P, $(G_i)_{i\in I}$ a family of subgroups generating G, $(P_i)_{i\in I}$ a family of subsets of P and $[z]$ a point of $P \setminus \bigcup_{i\in I} P_i$. Assume that for all $i, j \in I$ with $i \neq j$ and all $g_G \in G_i \setminus \{1\}$, one has $g_G(P_j \cup \{[z]\}) \subset P_i$. Then G is the free product of the subgroups G_i $(i \in I)$.*

In what follows, we take $P = \mathbb{P}^1$, $I = \{A, B\}$, $G_A = \langle A \rangle = \{A^k \mid k \in \mathbb{Z}\}$, $G_B = \langle B \rangle = \{B^k \mid k \in \mathbb{Z}\}$, and G to be the subgroup of $\mathrm{PGL}_2(\mathbb{F}_p(\!(x)\!))$ generated by A and B.

Let $\tilde{A}$ and $\tilde{B}$ be respective preimages of A and B in $\mathrm{GL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$. By Lemma 5, up to scaling $\tilde{A}$ has eigenvectors $(a:c)$ and $(1:b)$ with respective eigenvalues 1 and $f \in \mathbb{F}_p(\!(x)\!)$. Correspondingly, $\tilde{B}$ has eigenvectors $(1:\tilde{a})$ and $(1:\tilde{b})$ with respective eigenvalues 1 and $\tilde{f} \in \mathbb{F}_p(\!(x)\!)$.

By condition Ξ_2 we know that either $|f|$ or $|f^{-1}| \leq \frac{1}{p^{2d+1}}$, and that $|\tilde{f}|$ or $|\tilde{f}^{-1}| \leq \frac{1}{p^{2d+1}}$. For our argument we assume that $|f|, |\tilde{f}| \leq \frac{1}{p^{2d+1}}$. To see that we are able to make this assumption, notice that if A and B generate a free group in $\mathrm{PGL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$, then so do A^{-1} and B. Further, notice that by the construction in Lemma 5, A^{-1} is obtained from A by replacing f with f^{-1}.

As we are assuming the case that $|f| \leq \frac{1}{p^{2d+1}}$, we have that the eigenvalue corresponding to $[a:c]$ is large in absolute value compared to the corresponding eigenvalue of $[1:b]$, and so A will map elements of $\mathbb{P}^1$ towards $[a:c]$. An analogous observation can be made for B, as we are assuming $|\tilde{f}| \leq \frac{1}{p^{2d+1}}$. That is, B will map elements of $\mathbb{P}^1$ towards $[1:\tilde{a}]$.

With this in mind we consider the closed neighbourhoods of radius $\frac{1}{p^{d+1}}$ centred at each of these eigenvectors:

$$N_{[a:c]} = N\left([a:c], \frac{1}{p^{d+1}}\right) \quad \text{and} \quad N_{[1:b]} = N\left([1:b], \frac{1}{p^{d+1}}\right).$$

Similarly, we consider

$$N_{[1:\tilde{a}]} = N\left([1:\tilde{a}], \frac{1}{p^{d+1}}\right) \quad \text{and} \quad N_{[1:\tilde{b}]} = N\left([1:\tilde{b}], \frac{1}{p^{d+1}}\right).$$

We note that neighbourhoods in $\mathbb{P}^1$ take one of two forms, as given in Proposition 2. With this intuition, we choose

$$P_A = N_{[a:c]} \cup N_{[1:b]} \quad \text{and} \quad P_B = N_{[1:\tilde{a}]} \cup N_{[1:\tilde{b}]}. \tag{3}$$

We also need a point $[z] \in \mathbb{P}^1$ such that $[z] \in \mathbb{P}^1 \setminus (P_A \cup P_B)$. The existence of such a point is guaranteed by Proposition 2 by noting that $p^d(p+1) > 4$, except when $p = 3$ and $d = 0$. The proof of Theorem 1 in the case $p = 3$ and $d = 0$ can be done instead by a slightly modified argument, as shown in [27, Proposition 4.7.3].

Figure 1 allows us to visualize the neighbourhoods composing P_A and P_B as subsets of $\mathbb{P}^1$; however, we caution this image is of $\mathbb{P}^1(\mathbb{R})$ (the unit circle with antipodal points identified) and not of our non-Archimedean setting. With Proposition 2, condition Ξ_1 implies that our $\frac{1}{p^{d+1}}$-neighbourhoods are necessarily disjoint. This will be important for the proof of the Free Generators Theorem.

Of final importance in the proof of Theorem 1 will be ensuring A and B indeed map the constructed neighbourhoods as intended. Namely, looking at A, we would like A to map elements outside of $N_{[1,b]}$ to inside of $N_{[a,c]}$. This property, and a useful corollary, are shown below.

Proposition 7 *Suppose $A \in \mathrm{PGL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$ is as in Theorem 1, and $[u] \in \mathbb{P}^1 \setminus N_{[1:b]}$. Then $A \cdot [u] \in N_{[a:c]}$.*

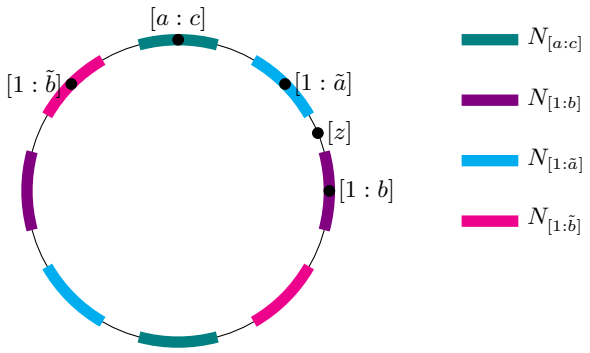


Fig. 1. A visual representation of the $\frac{1}{p^{d+1}}$-neighbourhoods of the eigenvectors of A and B and the point $[z] \in \mathbb{P}^1$. To satisfy conditions Ξ_1 and Ξ_2 of Theorem 1 these neigbourhoods must be disjoint and the point $[z]$ must lie outside each neighbourhood.

Proof. We suppose that $[u] \notin N_{[1:b]}$; we wish to show that $[Au] \in N_{[a:c]}$. By scaling appropriately, we may choose the eigenvectors representing $[1:b]$ and $[a:c]$ to be in the form $(1,x)$ or $(x,1)$ with $|x| \leq 1$; this defines four cases. We treat the first one, where $a \neq 0$ and $|b|, |ca^{-1}| \leq 1$.

Since $[u] \notin N_{[1:b]}$, we may choose its representative from $\{e_2, (1,g) \mid |g-b| \geq p^{-d}\}$, by Proposition 2. We use Cramer's rule to write u in terms of the eigenvectors as

$$u = \frac{r}{ca^{-1}-b}\begin{pmatrix}1\\ b\end{pmatrix} + \frac{s}{ca^{-1}-b}\begin{pmatrix}1\\ ca^{-1}\end{pmatrix}$$

for some $r, s \in \mathbb{F}_p(\!(x)\!)$ so that $Au = fr(1,b) + s(1,ca^{-1}) = (fr+s, frb+sca^{-1})$ up to scaling. Note that $|b-ca^{-1}| \leq 1$.

We claim $fr+s \neq 0$. If $u = e_2$, then $r = -1$ and $s = 1$, whence $|fr+s| = 1$. If $u = (1,g)$, with $|g-b| \geq p^{-d}$, then $s = g-b$ and $r = ca^{-1}-g = (ca^{-1}-b)-s$, whence $fr+s = f(ca^{-1}-b)+(1-f)(g-b)$. Since $|f(ca^{-1}-b)| \leq |f| \leq p^{-(2d+1)}$ but $|(1-f)(b-g)| = |b-g| \geq p^{-d}$, by the ultrametric inequality the sum $fr+s$ has norm at least p^{-d}, and in particular is nonzero.

Write $[Au] = [1 : \frac{frb+sca^{-1}}{fr+s}] = [1 : ca^{-1} + \frac{fr(b-ca^{-1})}{fr+s}] = [1 : ca^{-1}+\mu]$, setting $\mu = \frac{fr(b-ca^{-1})}{fr+s}$. To prove that $[Au]$ lies in $N_{[1:ca^{-1}]}$ we need to show that $|\mu| \leq p^{-(d+1)}$ (for all u as above).

If $u = e_2$ then since $|fr+s| = 1$, we have $|\mu| = |-f(b-ca^{-1})| \leq |f| \leq p^{-(2d+1)} \leq p^{-(d+1)}$. If $u = (1,g)$, with $|g-b| \geq p^{-d}$, then there are two possibilities. If $|b-g| \leq 1$, then also $|r| \leq 1$ by the ultrametric inequality. Thus $|fr(b-ca^{-1})| \leq p^{-2d-1}$ while $|fr+s| \geq p^{-d}$, whence $|\mu| \leq p^{-2d-1}p^d \leq p^{-(d+1)}$. If instead $|g-b| > 1$, then since $|b| \leq 1$ we deduce $|s| = |g| > 1$. It follows also that $|r| = |s| = |fr+s| = |g|$. Thus $|r/(fr+s)| = 1$, whence $|\mu| = |f||b-ca^{-1}| \leq p^{-2d-1} \leq p^{-(d+1)}$, as required.

An analogous careful analysis gives each of the other three cases. We refer the reader to [27, Section 4.6] for the full proof.

Corollary 8 *Suppose A is as in Theorem 1. Then $A^{-1}\left(\mathbb{P}^1 \setminus N_{[a:c]}\right) \subset N_{[1:b]}$.*

Proof. Suppose that $A^{-1}\left(\mathbb{P}^1 \setminus N_{[a:c]}\right) \not\subset N_{[1:b]}$. Then there exists an element $[u] \in \mathbb{P}^1 \setminus N_{[a:c]}$ such that $A^{-1} \cdot [u] \in \mathbb{P}^1 \setminus N_{[1:b]}$. Since $A^{-1} \cdot [u] \in \mathbb{P}^1 \setminus N_{[1:b]}$, by Proposition 7 we have $A \cdot \left(A^{-1} \cdot [u]\right) = [u] \in N_{[a:c]}$. As we know $[u] \in \mathbb{P}^1 \setminus N_{[a:c]}$, this is a contradiction.

2.3 Proof of the Free Generators Theorem

To show that the conditions of Proposition 6 are satisfied, and thus prove Theorem 1, we need to show that for all $g_A \in G_A \setminus \{1\}$, $g_A(P_B \cup \{[z]\}) \subset P_A$ and for all $g_B \in G_B \setminus \{1\}$, $g_B(P_A \cup \{[z]\}) \subset P_B$. We notice that if we replace $[a : c]$ with $[1 : \tilde{a}]$, $[1 : b]$ with $[1 : \tilde{b}]$, and f with $\tilde{f}$, we obtain B from A. As B has the same form as A, we thus need only show that for any $g_A \in G_A \setminus \{1\}$ we have $g_A(P_B \cup \{[z]\}) \subset P_A$.

We prove a stronger statement. More specifically, in Proposition 7 we showed that

$$A\left(\mathbb{P}^1 \setminus N_{[1:b]}\right) \subseteq N_{[a:c]} \tag{4}$$

and in Corollary 8 that

$$A^{-1}\left(\mathbb{P}^1 \setminus N_{[a:c]}\right) \subseteq N_{[1:b]}. \tag{5}$$

These mappings are illustrated in Figure 2.

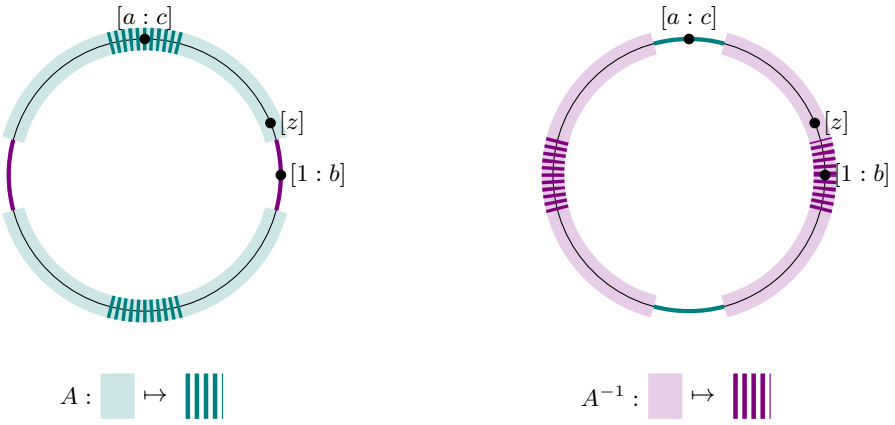


Fig. 2. A visual representation of the action of A (left figure) and the action of A^{-1} (right figure) on $\mathbb{P}^1$. We see that A maps $\mathbb{P}^1 \setminus N_{[1:b]}$ to $N_{[a:c]}$ and that A^{-1} maps $\mathbb{P}^1 \setminus N_{[a:c]}$ to $N_{[1:b]}$.

Suppose that $g_A \in G_A \setminus \{1\}$. Then either $g_A = A^\ell$ or $g_A = A^{-\ell}$ for some $\ell \in \mathbb{N}$. Since the proof is identical, we assume without loss of generality that $g_A = A^\ell$. We proceed by induction on ℓ.

Note that $[z] \in \mathbb{P}^1 \setminus N_{[1:b]}$. Condition Ξ_1 implies that $P_B = N_{[1:\tilde{a}]} \cup N_{[1:\tilde{b}]} \subseteq \mathbb{P}^1 \setminus N_{[1:b]}$. By (4) we have that A maps $\mathbb{P}^1 \setminus N_{[1:b]}$ into $N_{[a:c]}$. Thus we have $A(P_B \cup \{[z]\}) \subset N_{[a:c]}$.

Now suppose that $A^{\ell-1}(P_B \cup \{[z]\}) \subset N_{[a:c]}$. Again, condition Ξ_1 of Theorem 1 implies that $N_{[a:c]} \subset \mathbb{P}^1 \setminus N_{[1:b]}$, so $A^{\ell-1}(P_B \cup \{[z]\}) \subset \mathbb{P}^1 \setminus N_{[1:b]}$. By (4) we therefore have $A^\ell(P_B \cup \{[z]\}) = A(A^{\ell-1}(P_B \cup \{[z]\})) \subset N_{[a:c]} \subset P_A$, as required. Thus A and B generate a free group in in $\mathrm{PGL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$.

3 Properties of our hash functions

In this section we investigate three properties of the hash functions constructed from Theorem 1 (in $\mathfrak{H}$). First, we show that if the degrees of the entries of A and B are small compared to n, then the small modifications property holds (Proposition 9), as well as a slightly stronger result (Proposition 10). We note that Proposition 9 is applicable to any choice of A and B that generate a free monoid in $\mathrm{M}_{2\times 2}\big(\mathbb{F}_p[x]\big)$, and that our construction of such a hash function could also extend to any such choices, such as those alluded to in Section 1. Second, we show that given a relation in $\pi(A)$, $\pi(B)$ and their inverses (where we recall π from Section 1), we can find a new choice of defining polynomial under which such a relation does not hold (Proposition 12). This ensures that, unlike for the Zémor-Tillich generators, there are no general relations to be exploited. Third, we show that under certain easily satisfiable conditions the group generated by $\pi(A)$ and $\pi(B)$ contains $\mathrm{PGL}_2\big(\mathbb{F}_q\big)$ (Propositions 15 and 16), which is to say, the set of hash values is a sufficiently large subset of $\mathrm{GL}_2\big(\mathbb{F}_q\big)$ (and in some cases will be the entire group).

3.1 The small modifications property holds

Recall that, as in Tillich and Zémor's construction, one of the main goals of our construction is to preserve the small modifications property. With this in mind, suppose that A and B generate a free monoid in $\mathrm{M}_{2\times 2}\big(\mathbb{F}_p[x]\big)$, and let $\delta = \max\{\deg(A), \deg)B\}$. Let H be the hash function associated to $\pi_{r_n(x)}(A)$ and $\pi_{r_n(x)}(B)$ with values in $\mathrm{GL}_2\big(\mathbb{F}_q\big)$ where $\mathbb{F}_q = \mathbb{F}_p[x]/\langle r_n(x)\rangle$.

Our first result is that small modifications are detected.

Proposition 9 *For every distinct pair of bitstrings $m \in \{0,1\}^\ell$ and $m' \in \{0,1\}^{\ell'}$ where $0 \le \ell, \ell' < n/\delta$, we have $H(m) \neq H(m')$.*

Proof. Let M and M' be the respective products yielding $H(m)$ and $H(m')$ in $\mathrm{M}_{2\times 2}\big(\mathbb{F}_p[x]\big)$ before they are projected into $\mathrm{GL}_2\big(\mathbb{F}_q\big)$, so that $\pi(M) = H(m)$ and $\pi(M') = H(m')$. We see the entries of M are of degree at most $\ell\delta$ and the entries of M' are of degree at most $\ell'\delta$. Since $\ell, \ell' < n/\delta$, we know that each

of the entries of M and M' has degree less than $n = \deg(r_n(x))$, and therefore $\pi(M) = \pi(M') \in \mathrm{GL}_2(\mathbb{F}_q)$ if and only if $M = M' \in \mathrm{M}_{2\times 2}(\mathbb{F}_p[x])$.

We know that M, $M' \in \langle A, B\rangle$, and by our hypothesis that A, B generate a free monoid in $\mathrm{M}_{2\times 2}(\mathbb{F}_p[x])$. This implies that $M \neq M'$ since m and m' are distinct. Thus it is impossible that $\pi(M) = \pi(M')$ in $\mathrm{GL}_2(\mathbb{F}_q)$.

We in fact have a stronger property for the sets of generators we have produced. Recall that each k in $\mathbb{F}_q$ is the image of a unique polynomial in $\mathbb{F}_p[x]$ of degree less than n; let the degree be denoted $\deg(k)$.

Proposition 10 *Suppose $(A, B) \in \mathfrak{S}$. Then for every distinct pair of bitstrings $m \in \{0,1\}^\ell$ and $m' \in \{0,1\}^{\ell'}$ where $0 \leq \ell, \ell' < n/\delta$, we have that $H(m) \neq kH(m')$ for any $k \in \mathbb{F}_q$ such that $(\deg(k) + \ell'\delta) < n$. In particular, $H(m) \neq kI$ for any $k \in \mathbb{F}_q$, whence as elements of $\mathrm{GL}_2(\mathbb{F}_q)$, $\pi(A)$ and $\pi(B)$ have order at least n/δ.*

Proof. Notice that since (A, B) are in $\mathfrak{S}$, their images in $\mathrm{PGL}_2(\mathbb{F}_p(\!(x)\!))$ generate a free subgroup of $\mathrm{PGL}_2(\mathbb{F}_p(\!(x)\!))$. This implies that $M \neq gM'$ for any $g \in \mathbb{F}_p(\!(x)\!)$.

Suppose that $\pi(M) = k\pi(M')$ in $\mathrm{GL}_2(\mathbb{F}_q)$ for some $k \in \mathbb{F}_q$. Viewing k as its inverse image in $\mathbb{F}_p[x]$ of lowest degree, we then have that $M = kM' + r_n(x)T$ for some $T \in \mathrm{M}_{2\times 2}(\mathbb{F}_p[x])$. By our hypothesis we know that $\deg(k) + \deg(M') < n$, so $\deg(kM') < n$. Since the entries of M each also have degree less than n, this implies $T = 0$, thus $M = kM'$, which is a contradiction.

Finally, note that if one takes m' to be the identity string, we have $\ell' = 0$, so $\deg k < n$ for any $k \in \mathbb{F}_q$. The last assertion of the proposition follows.

We interpret these propositions concretely for the case of our generators in Table 1.

Corollary 11 *Suppose A and B are from Table 1. If m and m' are bitstrings in $\{0,1\}^*$ such that $H(m) = H(m')$ then at least one of m, m' has length at least $n/\max\{\deg(f), \deg(\tilde{f})\}$.*

3.2 Guarding against attacks using known identities

Here we prove a property which allows us to prevent against specific relations of the form $W(\pi(A), \pi(B)) = kI$, where $k \in \mathbb{F}_q^\times$ and $W(\pi(A), \pi(B))$ is a nontrivial word in $\{\pi(A), \pi(B), \pi(A)^{-1}, \pi(B)^{-1}\}^*$. This is important in verifying attack resistance in a broader setting. As an example, considering A and B as the Zémor-Tillich generators, Grassl et al. [7] use the relation $B^{-1}A = A^{-1}B$, which was *independent* of $r_n(x)$, to find non-palindromic collisions from their original palindromic ones. We use this as motivation for the following proposition.

Proposition 12 *Let $(A, B) \in \mathfrak{S}_p$ and let $W(A, B) \in \{A, A^{-1}, B, B^{-1}\}^*$ be a nontrivial word. Then there exists a choice of irreducible $r_n(x) \in \mathbb{F}_p[x]$ of degree n such that*

$$W(\pi_{r_n}(A), \pi_{r_n}(B)) \neq kI \in \mathrm{GL}_2(\mathbb{F}_q)$$

for any $k \in \mathbb{F}_q^\times$ when $\mathbb{F}_q = \mathbb{F}_p[x]/\langle r_n(x)\rangle$.

Proof. Define $\phi := \det(AB) \in \mathbb{F}_p[x]$. Let $\mathbb{F}_p[x]_{1/\phi}$ be the localization of $\mathbb{F}_p[x]$ at ϕ, that is $\mathbb{F}_p[x]_{1/\phi} = \left\{ g/\phi^\ell \mid g \in \mathbb{F}_p[x], \ell \geq 0 \right\}$.

Since $\frac{1}{\det A} = \frac{\det B}{\phi}$, we have $\frac{1}{\det A} \in \mathbb{F}_p[x]_{1/\phi}$. Similarly $\frac{1}{\det B} \in \mathbb{F}_p[x]_{1/\phi}$. As well, we note that $\mathbb{F}_p[x]_{1/\phi}$ is contained in the fraction field $\mathbb{F}_p(x)$ and thus in $\mathbb{F}_p(\!(x)\!)$. Consequently, we have that $A, B \in \mathrm{GL}_2\big(\mathbb{F}_p[x]_{1/\phi}\big) \subseteq \mathrm{GL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$, allowing us to work in a group setting rather than in the monoid $\mathrm{M}_{2\times 2}\big(\mathbb{F}_p[x]\big)$.

For any irreducible polynomial $r \in \mathbb{F}_p[x]$, we define the ideal

$$\mathfrak{p} := \langle r \rangle = \{ rg \mid g \in \mathbb{F}_p[x] \} \subseteq \mathbb{F}_p[x]$$

and, assuming $r \nmid \phi$, let $\mathfrak{p}_{1/\phi}$ be the localization of $\mathfrak{p}$ at ϕ, that is the ideal of $\mathbb{F}_p[x]_{1/\phi}$ defined by $\mathfrak{p}_{1/\phi} = \left\{ rg/\phi^\ell \mid g \in \mathbb{F}_p[x], \ell \geq 0 \right\} \subseteq \mathbb{F}_p[x]_{1/\phi}$.

Further, our quotient map $\mathbb{F}_p[x] \to \mathbb{F}_q$ extends naturally to another surjective map $\psi_r : \mathbb{F}_p[x]_{1/\phi} \to \mathbb{F}_q$ induced by $x \mapsto \xi$ where ξ is a root of r.

The kernel of ψ_r is $\mathfrak{p}_{1/\phi}$. Thus by the first isomorphism theorem we have

$$\mathbb{F}_p[x]_{1/\phi}/\mathfrak{p}_{1/\phi} \cong \mathbb{F}_q.$$

Further, we observe that the natural images of A and $B \in \mathrm{GL}_2\big(\mathbb{F}_p[x]_{1/\phi}\big)$ under this homomorphism are $\pi_r(A)$ and $\pi_r(B)$ respectively.

Since $A, B \in \mathfrak{S}$, the images of A, B in $\mathrm{PGL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$ generate a free group. This implies that no nontrivial word in $\{A, B, A^{-1}, B^{-1}\}$ can be I or any scalar multiple kI of I for any $k \in \mathbb{F}_p(\!(x)\!)$. We thus observe that $W(\pi_r(A), \pi_r(B)) = kI$ in $\mathrm{GL}_2\big(\mathbb{F}_q\big)$ for some $k \in \mathbb{F}_q^\times$ if and only if, viewing k as an element of $\mathbb{F}_p[x] \subset \mathbb{F}_p[x]_{1/\phi}$,

$$W(A, B) = \begin{pmatrix} k+\alpha & \beta \\ \gamma & k+\delta \end{pmatrix} \in \mathrm{GL}_2\big(\mathbb{F}_p[x]_{1/\phi}\big)$$

for some α, β, γ, $\delta \in \mathbb{F}_p[x]_{1/\phi}$ such that $\psi_r(\alpha) = \psi_r(\delta) = \psi_r(\beta) = \psi_r(\gamma) = 0$, and not all of α, β, γ, δ are the zero polynomial.

Hence it suffices to choose $r_n(x) \in \mathbb{F}_p[x]$ such that at least one of $\psi_{r_n}(\alpha)$, $\psi_{r_n}(\delta)$, $\psi_{r_n}(\beta)$, $\psi_{r_n}(\gamma)$ is nonzero. For instance, one could choose $r_n(x)$ relatively prime to one choice of nonzero α, β, γ, or δ.

We note that $r_n(x)$ could also be chosen to simultaneously satisfy the last line of the above proof for each of multiple choices of words, thus allowing us to avoid any finite collection of pre-chosen relations.

3.3 The size of the subgroup $\langle \pi(A), \pi(B) \rangle$

In [3], Tillich and Zémor showed that their choice of A and B generates all of $\mathrm{SL}_2\big(\mathbb{F}_{2^n}\big)$. It has been shown that for a randomly chosen pair of elements from $\mathrm{SL}_2\big(\mathbb{F}_{2^n}\big)$ (or $\mathrm{PSL}_2\big(\mathbb{F}_{p^n}\big)$), the probability that they generate the whole group approaches 1 as the size of $\mathrm{SL}_2\big(\mathbb{F}_{2^n}\big)$ approaches infinity [4]. However, this argument does not apply to our case as we are taking elements from $\mathfrak{H}$, and thus not choosing A and B randomly.

A well-known result of Dickson [29] determines all possible subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$. As in [3], we use its presentation by Suzuki in [30], who gives an elegant exposition of Dickson's proof. Because we do not restrict our argument to specific choices of generators, we have to do a bit more work than was needed for the argument in [3]. We now present Dickson's result [30, Theorem 6.25]. Note that $\mathrm{SL}_2(\mathbb{F}_q) \subseteq \mathrm{GL}_2(\mathbb{F}_q)$; we have $\mathrm{PSL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)/\{\pm 1\}$ and $\mathrm{PGL}_2(\mathbb{F}_q) = \mathrm{GL}_2(\mathbb{F}_q)/\mathrm{Z}$, but can naturally identify $\mathrm{PSL}_2(\mathbb{F}_q)$ as the subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$ consisting of all matrices whose determinant is a square.

Theorem 13 *Let p be a prime and $q = p^n$. Each subgroup of $\mathrm{PSL}_2(\mathbb{F}_q)$ is isomorphic to one of the following groups:*

(a) a dihedral group or one of its subgroups;
(b) a group K of order $q(q-1)/d$ where $d = \gcd(2, q-1)$ and any Sylow p-subgroup of K is normal in K, or its subgroups;
(c) the symmetric group on four elements S_4, or the alternating group on four or five elements, A_4 or A_5;
(d) $\mathrm{PSL}_2(\mathbb{F}_{p^\ell})$ or $\mathrm{PGL}_2(\mathbb{F}_{p^\ell})$ for some $\ell \mid n$, where $\mathrm{PGL}_2(\mathbb{F}_{p^\ell})$ is embedded into $\mathrm{PSL}_2(\mathbb{F}_q)$ as described in [30, Theorem 6.25 part (x)].

In [27, Lemma 5.3.6] the following lemma is proven using the theory of Sylow subgroups.

Lemma 14 *Let K be as in (b) of Theorem 13. Then up to conjugation K lies inside the Borel subgroup*

$$\mathfrak{B} = \left\{ M \in \mathrm{PSL}_2(\mathbb{F}_q) \;\middle|\; M \text{ is upper triangular} \right\}.$$

Consider now the images $[\pi(A)]$ and $[\pi(B)]$ of our hash function generators in $\mathrm{PGL}_2(\mathbb{F}_q)$. We show that the subgroup they generate contains $\mathrm{PSL}_2(\mathbb{F}_q)$, and so has index at most 2 in $\mathrm{PGL}_2(\mathbb{F}_q)$.

Proposition 15 *Let $(A, B) \in \mathfrak{S}$ and $\delta = \max\{\deg A, \deg B\}$. Assume that at least one of the following holds:*

(i) f or f' is a primitive root of $\mathbb{F}_q$, n is odd and $n/\delta > 5$ or
(ii) n is prime and $n/\delta > p(p^2-1)$.

Then $\mathrm{PSL}_2(\mathbb{F}_q) \subseteq \langle [\pi(A)], [\pi(B)] \rangle$.

Proof. To simplify notation, we write $\Pi(A)$ for $[\pi(A)] \in \mathrm{PGL}_2(\mathbb{F}_q)$ and $\Pi(B)$ for $[\pi(B)] \in \mathrm{PGL}_2(\mathbb{F}_q)$. We note that $p(p^2-1) > 5$ holds for all choices of p, so we can assume $n/\delta > 5$.

Let $G = \mathrm{PSL}_2(\mathbb{F}_q) \cap \langle \Pi(A), \Pi(B) \rangle$. We determine if $G = \mathrm{PSL}_2(\mathbb{F}_q)$, by ruling out all possible proper subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ as presented in Theorem 13.

(a) We notice that the group $\langle \Pi(A)^2, \Pi(B)^2 \rangle$ is a subgroup of G. Thus, if G is a dihedral group, or a subgroup of a dihedral group, then so is $\langle \Pi(A)^2, \Pi(B)^2 \rangle$. In particular, this means $\langle \Pi(A)^2, \Pi(B)^2 \rangle$ is either dihedral or cyclic. As $n/\delta > 4$,

Proposition 10 gives that $(\Pi(A)^2)^2 \neq I$ and $(\Pi(B)^2)^2) \neq I$, so this subgroup is not dihedral, since neither generator has order two.

To see that $\langle \Pi(A)^2, \Pi(B)^2 \rangle$ is not cyclic, suppose, that $\Pi(A)^2\Pi(B)^2 = \Pi(B)^2\Pi(A)^2$. Then, we know that $\pi(A)^2\pi(B)^2 = k\pi(B)^2\pi(A)^2$ in $\mathrm{GL}_2(\mathbb{F}_q)$. Notice the determinants of $\pi(A)^2\pi(B)^2$ and $\pi(B)^2\pi(A)^2$ are equal, so $k = \pm 1 \in \mathbb{F}_q$ must hold. Since $n/\delta > 4$ and $\deg(k) = 0$, Proposition 10 implies that $\pi(A)^2\pi(B)^2 \neq k\pi(B)^2\pi(A)^2$ for $k = \pm 1$, so this is a contradiction. Therefore, $\Pi(A)^2$ and $\Pi(B)^2$ do not commute, so this subgroup is in particular not cyclic. So G cannot fall under case (a).

(b) Suppose now that $G \subseteq K$ as in case (b). By Lemma 14, we know that K is contained in $P\mathfrak{B}P^{-1}$ for some $P \in \mathrm{PSL}_2(\mathbb{F}_q)$. Since K is conjugate to a subgroup of $\mathfrak{B}$, the upper triangular matrices, all elements share a common eigenvector. By construction, A and B have different eigenvectors, respectively $[a : c]$, $[1 : b]$ and $[1 : \tilde{a}]$, $[1 : \tilde{b}]$. Since $\delta < n$, we know that a, b, c, $\tilde{a}$, $\tilde{b}$ all must have entries of degree less than n. Thus, when we quotient by $r_n(x)$, the eigenvectors remain distinct. As a consequence G cannot be isomorphic to a subgroup of K.

(c) We note that any element in A_4 or S_4 has order at most 4, while any element in A_5 has order at most 5. In particular if $\langle \Pi(A), \Pi(B) \rangle$ were a subgroup of one of these, either $\Pi(A)^4 = I$ or $\Pi(A)^5 = I$ must hold. Thus, using Proposition 10, G cannot be in case (c) since $n/\delta > 5$.

(d) To show that G is not a subgroup of the form $\mathrm{PSL}_2(\mathbb{F}_{p^\ell})$ or $\mathrm{PGL}_2(\mathbb{F}_{p^\ell})$, for some $\ell \mid n$, we suggest two methods that are each sufficient on their own.

First, suppose that either f or f' is a primitive root of $\mathbb{F}_q$ and that n odd. We suppose without loss of generality that f is a primitive root. We recall that by construction (see Lemma 5) there is a $P \in \mathrm{PGL}_2(\mathbb{F}_q)$ such that

$$\Pi(A) = P \begin{bmatrix} 1 & 0 \\ 0 & f \end{bmatrix} P^{-1} \in \mathrm{PGL}_2(\mathbb{F}_q).$$

Thus, since f is a primitive root, $\Pi(A)$ has order $p^n - 1$.

Suppose that $G \leqslant \mathrm{PGL}_2(\mathbb{F}_{p^\ell})$ for some $\ell \mid n$. Noting that $|\mathrm{PGL}_2(\mathbb{F}_{p^\ell})| = p^\ell(p^{2\ell} - 1)$, we have $\Pi(A)^{p^\ell(p^{2\ell}-1)} = 1$, so $p^n - 1 \mid p^\ell(p^{2\ell} - 1)$. We note that $\gcd(p^n - 1, p^n) = 1$, so $\gcd(p^n - 1, p^\ell) = 1$ must hold, thus $p^n - 1 \mid (p^{2\ell} - 1)$.

In particular, this implies that $p^n - 1 \mid \gcd(p^n - 1, p^{2\ell} - 1)$. We note that $\gcd(p^n - 1, p^{2\ell} - 1) = p^{\gcd(n,2\ell)} - 1 = p^{\gcd(n,\ell)} - 1$ since n is odd. Combining these, we have $p^n - 1 \mid p^{\gcd(n,\ell)} - 1$, so in particular $\gcd(\ell, n) \geq n$. Since $\ell \mid n$, this implies $\gcd(\ell, n) = n$, so $n = \ell$ must hold. So G does not fall under case (d).

Suppose now instead that n is prime, and $n/\delta > p(p^2 - 1)$, noting neither f nor $\tilde{f}$ is now required to be a primitive root. Since n is prime, the only possible subgroups in (d) are those for $\ell = 1$, that is $\mathrm{PGL}_2(\mathbb{F}_p)$ and $\mathrm{PSL}_2(\mathbb{F}_p)$. Note that $|\mathrm{PGL}_2(\mathbb{F}_p)| = p(p^2-1)$, and $|\mathrm{PSL}_2(\mathbb{F}_p)| = p(p^2-1)$ if $p = 2$ and $p(p^2-1)/2$ if p is odd. Thus in particular $\Pi(A)^{p(p^2-1)} = I$, so by Proposition 10, if $n/\delta > p(p^2-1)$ case (d) cannot hold.

To further ensure that $[\pi(A)]$ and $[\pi(B)]$ generate all of $\mathrm{PGL}_2(\mathbb{F}_q)$, we state the following as a corollary of [27, Lemma 2.2.3].

Proposition 16 *Let A and B be matrices in $\mathrm{PGL}_2(\mathbb{F}_q)$ such that, as in Proposition 15, $\mathrm{PSL}_2(\mathbb{F}_q) \subseteq \langle [\pi(A)], [\pi(B)] \rangle$. If either $\det(\pi(A))$ or $\det(\pi(B))$ is not a square in $\mathbb{F}_q$, then $\langle [\pi(A)], [\pi(B)] \rangle = \mathrm{PGL}_2(\mathbb{F}_q)$.*

Under the hypotheses of Propositions 15 and 16, the subgroup $\mathrm{GL}_2(\mathbb{F}_q)$ generated by $\pi(A)$ and $\pi(B)$ has order at least $|\mathrm{PGL}_2(\mathbb{F}_q)| = q(q^2-1)$, since it is the preimage under a quotient map; for individual choices of generators, one could use ad-hoc techniques to verify if the group generated was all of $\mathrm{GL}_2(\mathbb{F}_q)$.

We note that of the two alternative hypothesis Proposition 15 are in practice very reasonable. For instance, we already would like to choose n, δ, such that n/δ is much larger than 5 so that our small modifications property given by Proposition 9 is practical. As well, choosing n to be prime has already been suggested to prevent against the small order attack proposed in [19].

Further, the hypothesis in Proposition 16 that one of $\alpha = \det(\pi(A))$ or $\beta = \det(\pi(B))$ is not a square in $\mathbb{F}_q$ is satisfied when p is odd if $\alpha = \det(\pi(A))$ and $\beta = \det(\pi(B))$ are primitive roots. Namely, suppose that p is odd and $\alpha \equiv \gamma^2$ for some $\gamma \in \mathbb{F}_q$. Since $\gamma \in \mathbb{F}_q^\times$, we know $\gamma^{q-1} = 1$. It follows then that $\alpha^{\frac{q-1}{2}} = (\gamma^2)^{\frac{q-1}{2}} = 1$, so $\mathrm{ord}(\alpha) \mid \frac{q-1}{2}$, so α cannot be a primitive root.

Choosing $\pi(A)$ and $\pi(B)$ such that $\det(\pi(A))$ and $\det(\pi(B))$ are primitive roots is useful for another reason. Namely, we want to ensure $\pi(A)$ and $\pi(B)$ have large enough order to prevent small collisions of the form $\pi(A)^{\mathrm{ord}(\pi(A))} = I$ and $\pi(B)^{\mathrm{ord}(\pi(B))} = I$, as well as Charnes and Pieprzyk's short relations attack [5]. In [31], the authors suggest A and B should be of order of at least $q-1$ to prevent against these collisions. For our hash functions, we observe that if $\det(\pi(A))$ is a primitive root then we necessarily have $\mathrm{ord}\,(\pi(A)) \geq q-1$, (and the analogous statement is true for $\pi(B)$).

Though finding a primitive root of small degree is not straightforward for a general case of finite field, we note that the maximum degree of such a primitive root is bounded [32]. Further, certain choices of $r_n(x)$ could make this easier. For example, many packages, such as GAP [33] and Magma [34], use Conway polynomials for $r_n(x)$, which guarantee that x itself is indeed a primitive root.

4 Possible Attacks

Unlike the Zémor-Tillich hash function, our hash functions take values in $\mathrm{GL}_2(\mathbb{F}_q)$, in which the determinant is nontrivial. In this section we briefly present four potential attacks that take advantage of information leaked by the determinant, and discuss the effect of the determinant on the distribution of hash values. Concurrently, we present methods for preventing each of these possible issues. We then consider the applicability of previous attacks on the Zémor-Tillich hash function to elements of $\mathfrak{H}$.

For this section, let $\pi(A)$, $\pi(B) \in \mathrm{GL}_2(\mathbb{F}_q)$ and let m be a message in $\{0,1\}^\ell$ with ℓ_1 zeros and ℓ_2 ones, so that $\ell_1 + \ell_2 = \ell$. Let $\alpha = \det(\pi(A))$, $\beta = \det(\pi(B))$, and $M = H(m) \in \mathrm{GL}_2(\mathbb{F}_q)$.

Under these conditions, the determinant takes on the value $\det(M) = \alpha^{\ell_1}\beta^{\ell_2}$. Utilizing this relationship yields the possible attacks given in Table 2. More details of these are given in [27, Section 5.5.1].

Table 2. Possible attacks via the determinant.

Attack	Condition	Information Leaked
1	$\alpha = \beta$	ℓ
2	$\gcd(\mathrm{ord}(\alpha), \mathrm{ord}(\beta))$ is close to $\mathrm{ord}(\alpha)$ or $\mathrm{ord}(\beta)$ in size	some divisors of ℓ_1 and ℓ_2
3	α is a primitive root, and $\beta = \alpha^\tau$ for some τ such that $\ell_1 < \tau$ and $\ell_1 + \ell_2\tau < p^n - 1$	ℓ_1 and ℓ_2
4	α is a primitive root	some divisors of ℓ_1 and ℓ

We note that Attacks 1, 3 and 4 depend on being able to calculate discrete logs in $\mathbb{F}_q$, which can be computationally difficult. As well, Attacks 1, 2, and 3 are prevented by choosing α to be a primitive root, and $\beta = \alpha^\tau$ for some τ of size $\mathcal{O}(p^n/2)$ such that $\gcd(\tau, p^n - 1) = 1$, so β is also a primitive root. Choosing α and β to be primitive roots was already suggested in Section 3.3. However, assuming dlog_α is efficiently computable, careful choices of parameters can only mitigate the amount of information leaked by Attack 4.

The determinant introduces a further problem; the hash values of messages of length ℓ cannot be distributed uniformly among all possible determinants, as their determinants must be among the $\ell + 1$ possible values of $\alpha^{\ell_1}\beta^{\ell-\ell_1}$. We would like the hash values of our hash function to be uniformly distributed as ℓ tends to infinity, as was true of the Zémor-Tillich hash function [3].

One common option in cryptography for preventing attacks based on the weaknesses mentioned above is by padding messages with some bits to obscure the original determinant of the hash value. As an example, one of the most standard forms of padding is PKCS #5, which pads messages to be a multiple of a given block length based on the amount of padding needed [35].

For elements of $\mathfrak{H}$, we propose padding our messages as follows. Namely, suppose we wish to hash messages of length at most N. We could then pad our messages to bitstrings of length $2N$ with precisely N ones and N zeros. This would ensure all outputs had determinant $\alpha^{N(1+\tau)}$, thus completely eliminating the effect of the determinant on the security and the distribution, and in particular preventing Attacks 1-4. If we choose elements of $\mathfrak{H}$ such that $\pi(A)$, $\pi(B)$ generate all of $\mathrm{GL}_2(\mathbb{F}_q)$, the number of possible hash values would be $q(q^2-1)$. This is the same size as $\mathrm{SL}_2(\mathbb{F}_q)$, and so is comparable to Zémor-Tillich for $p = 2$ and the extension of Zémor-Tillich given in [31] for p odd.

Note in the case $\alpha = \beta$, any choice of padding to a fixed length would remove the above distribution issue and prevent against the discussed attacks in Table 2.

Remark 17 *A second method considered in [27, Section 5.5.4] to obscure the determinant is to take our hash function H to be the associated hash function in*

$\mathrm{PGL}_2(\mathbb{F}_q) = \mathrm{GL}_2(\mathbb{F}_q)/\mathrm{Z}$ *of the images of* $\pi(A)$ *and* $\pi(B)$*. While this has some advantages, including that many of the desirable properties of our hash functions carry over, some padding is still necessary.*

Small Order Attacks: The first attacks on the Zémor-Tillich hash function depended on $r_n(x)$ being either such that A or B had small order [5] or such that $r_n(x)$ was decomposable (a composition of two nontrivial polynomials) [19], and thus easily extend to elements of $\mathrm{GL}_2(\mathbb{F}_q)$ [36].

For the Zémor-Tillich hash function, a randomly chosen $r_n(x)$ yields A and B with order large enough (at least $q-1$) with an extremely high probability for Tillich and Zémor's generators, so the first of these attacks was not a concern [31]. For elements in $\mathfrak{H}$, we saw in Section 3.3 that choosing $\det(A)$ and $\det(B)$ to be primitive roots will ensure A and B have order at least $q-1$. Similiarly, Regenscheid shows that in $\mathbb{F}_2$ the probability that a randomly chosen irreducible polynomial of degree n is decomposable approaches 0 as n approaches infinity [36]; these methods extend to irreducible polynomials over $\mathbb{F}_p$. The second of these attacks can also be avoided simply choosing n prime [19]. Therefore we conclude that the choices discussed at the end of Section 3.3 suffice to prevent these attacks against elements of $\mathfrak{H}$.

Embedding Attack: Geiselmann's embedding attack (see [20, 36]) could also apply for generators over $\mathrm{SL}_2(\mathbb{F}_q)$ for a general choice of $q = p^n$. The alternative proof in [36] can be easily extended to the case $p > 2$ when the generators are diagonalizable, as in the case of elements $S \in \mathfrak{S}$. The computation time of this attack depends on the computation time of computing discrete logs in $\mathrm{GL}_2(\mathbb{F}_{2^n})$; a strategy to avoid computing discrete logs is given in [13]. However, in practice Geiselmann's algorithm is considered unrealistic as a result of the extremely long strings of zeros and ones in the collisions produced [20].

Density Attack: The Zémor-Tillich hash function was proved to be resistant to density attacks [3]. Though not done here, the argument in [3] easily generalizes to elements of $\mathfrak{H}$ that satisfy the conditions in Section 3.3.

General Attacks: Assuming that Mullan's general attack in [23] is extendible to the case of $\mathrm{GL}_2(\mathbb{F}_q)$, which has not been shown, this would be the best known attack on the functions in $\mathfrak{H}$. This attack had running time $\mathcal{O}(\sqrt{q})$ and produced collisions of length $\mathcal{O}((\log q)^2/\log(\log q))$ for a general characteristic p. Other options for attacks on elements of $\mathfrak{H}$ are an optimization of the birthday attack as in [37] or an attack such as the meet-in-the-middle approach in [22]. Each of these are standard attacks that have no advantage, and may be even more difficult, for our hash functions.

5 Final Notes

We saw in Section 3 that for A and B of reasonably small degree, the hash functions in $\mathfrak{H}$ preserve the small modifications property. Further, we note that as

our construction is a Cayley hash function it is naturally parallelizable. Elements of $\mathfrak{H}$ are also scalable, meaning we are able to control the size of the output. In Section 3 and 4 we saw that under certain easily satisfiable conditions our hash functions are secure against all previous efficient attacks on the Zémor-Tillich hash function and any potential weaknesses from a badly chosen determinant. The distribution and efficiency of elements in $\mathfrak{H}$ are both properties we hope to study further in future work. We note in the literature very little is presented numerically on these points. We have done some initial implementation using GAP, and hope to extend our computational analysis of elements of $\mathfrak{H}$.

A Topology of $\mathbb{F}_p(\!(x)\!)$

Here we define the projective space $\mathbb{P}^1 = \mathbb{P}^1(\mathbb{F}_p(\!(x)\!))$ and equip it with a metric, and take note of some key facts about the neighbourhoods in this space.

Let p be a prime, $\mathbb{F}_p$ be the field with p elements, $\mathbb{F}_p(\!(x)\!)$ be the *field of formal Laurent series* over $\mathbb{F}_p$, and $\mathbb{F}_p(\!(x)\!)^\times$ the group of invertible elements of $\mathbb{F}_p(\!(x)\!)$. The elements of $\mathbb{F}_p(\!(x)\!)$ are series of the form $g(x) = \sum_{k=m}^{\infty} g_k x^k$ for $g_i \in \mathbb{F}_p$ and $m \in \mathbb{Z}$. Because we want to see elements of $\mathbb{F}_p(\!(x)\!)$ as elements of an abstract field, not as functions, we write g for an element $g(x) \in \mathbb{F}_p(\!(x)\!)$. With this notation, we use g^{-1} to mean the multiplicative inverse of $g \in \mathbb{F}_p(\!(x)\!)^\times$, not $g^{-1}(x)$.

We denote the *valuation* $v(g)$ of an element $g \in \mathbb{F}_p(\!(x)\!)$ as

$$v(g) = \begin{cases} \min\{k \mid g_k \neq 0\} & \text{if } g \neq 0; \\ \infty & \text{if } g = 0. \end{cases}$$

With this, we define the *absolute value* as $|g| = p^{-v(g)}$. For instance, the element $f = x^3 + x^6$ would have $|f| = p^{-3}$, while $g = x^{-5} + x^{-2}$ would have $|g| = p^5$. This absolute value is multiplicative, that is $|fg| = |f||g|$ for any $f, g \in \mathbb{F}_p(\!(x)\!)$. As well, this absolute value is non-Archimedean, meaning it satisfies the ultrametric (or non-Archimedean) triangle inequality $|g + h| \leq \max\{|g|, |h|\}$ for all $g, h \in \mathbb{F}_p(\!(x)\!)$. To see this, notice that for $g, h \in \mathbb{F}_p(\!(x)\!)$ the smallest index for which the Laurent series of $g + h$ could have a nonzero term cannot be strictly less than $\min\{v(g), v(h)\}$.

Consider the $2-$dimensional vector space over $\mathbb{F}_p(\!(x)\!)$

$$V = \{(u_1, u_2) \mid u_1, u_2 \in \mathbb{F}_p(\!(x)\!)\}.$$

Then, the 1-*dimensional projective space* over $\mathbb{F}_p(\!(x)\!)$ is

$$\mathbb{P}^1 = \mathbb{P}^1(\mathbb{F}_p(\!(x)\!)) := (V \backslash \{0\})/\sim$$

where $\sim$ is the equivalence relation $(u_1, u_2) \sim (v_1, v_2)$ if there exists a $k \in \mathbb{F}_p(\!(x)\!)^\times$ such that $(u_1, u_2) = (kv_1, kv_2)$. In particular, for $(u_1, u_2) \neq (0, 0)$ we define $[u] = [u_1 : u_2] \in \mathbb{P}^1$ to be the equivalence class

$$[u_1 : u_2] = \left\{ k(u_1, u_2) \in V \mid k \in \mathbb{F}_p(\!(x)\!)^\times \right\}.$$

Remark 18 *The equivalence classes* $[1:0]$ *and* $[0:1]$ *will be denoted by* $[e_1]$ *and* $[e_2]$ *respectively. Note that* $[f:g] = [1:gf^{-1}]$ *for* $f \neq 0$.

We let $\mathrm{GL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$ act on V by matrix multiplication. This action factors to a well-defined action on $\mathbb{P}^1$ by setting $g \cdot [u] = [g \cdot u]$; we note here that the subgroup $\mathrm{GL}_2\big(\mathcal{O}\big)$ acts transitively on $\mathbb{P}^1$. Since the centre of $\mathrm{GL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$ acts trivially on $\mathbb{P}^1$, the resulting action further factors to an action of $\mathrm{PGL}_2\big(\mathbb{F}_p(\!(x)\!)\big)$ (and its subgroups) on $\mathbb{P}^1$.

We take the norm in V to be the sup-norm $||(u_1, u_2)|| = \max\{|u_1|, |u_2|\}$, which is $\mathrm{GL}_2\big(\mathcal{O}\big)$-invariant. The following definition of distance is taken from Breuillard and Gelander [8].

Definition 19 *Let* $[u], [v] \in \mathbb{P}^1$ *be such that* $[u] = [u_1 : u_2]$ *and* $[v] = [v_1 : v_2]$. *Then the distance between* $[u]$ *and* $[v]$ *is defined to be*

$$d([u],[v]) = \frac{||u \wedge v||}{||u||\,||v||} = \frac{|u_1 v_2 - u_2 v_1|}{\max\{|u_1|,|u_2|\}\max\{|v_1|,|v_2|\}}. \tag{6}$$

Note that the alternating tensor product $u \wedge v$ is one-dimensional, and we take the absolute value as its norm.

This distance is independent of the choice of representatives of the classes $[u]$ and $[v]$, and can only take value zero or a nonpositive power of p. Further, $\mathrm{GL}_2\big(\mathcal{O}\big)$ acts by isometries on $\mathbb{P}^1$ relative to this distance. Another property of our distance is that it is an ultra-metric, which is expected since our absolute value is non-Archimedean.

Bibliography

[1] G. Zémor, Hash functions and graphs with large girths, Advances in Cryptology EUROCRYPT91, Springer (1991), 508–511.
[2] G. Zémor, Hash functions and Cayley graphs, Designs, Codes and Cryptography, 4 (1994), no. 3, 381–394.
[3] J.P. Tillich and G. Zémor, Hashing with SL_2, Annual International Cryptology Conference, Springer (1994), 40–49.
[4] C. Petit and J.J. Quisquater, Rubik's for cryptographers, Notices Amer. Math. Soc. 60 (2013), no. 6, 733–740.
[5] C. Charnes and J. Pieprzyk, Attacking the SL_2 hashing scheme, Advances in Cryptology ASIACRYPT'94 (1995), 322–330.
[6] J.J. Quisquater and M. Joye, Authentication of sequences with the SL_2 hash function: Application to video sequences, Journal of Computer Security 5 (1997), no. 3, 213–223.
[7] M. Grassl, I. Ilić, S. Magliveras, and R. Steinwandt, Cryptanalysis of the Tillich-Zémor hash function, Journal of Cryptology 24 (2011), no. 1, 148–156.
[8] E. Breuillard and T. Gelander, On dense free subgroups of Lie groups, Journal of Algebra 261 (2003), no. 2, 448–467.

[9] J.P. Tillich and G. Zémor, Group-theoretic hash functions, Algebraic Coding (1994), pp. 90–110.
[10] D.X. Charles, K.E. Lauter, and E.Z. Goren, Cryptographic hash functions from expander graphs, Journal of Cryptology 22 (2009), no. 1, 93–113.
[11] H. Jo, Cryptanalysis on Hash Functions Based on Ramanujan Graphs, Ph.D. thesis, Kyushu University (2017).
[12] H. Jo, Hash functions based on Ramanujan graphs, Mathematical Modelling for Next-Generation Cryptography, Springer (2018) 63–79.
[13] C. Petit, K. Lauter, and J.J. Quisquater, Cayley hashes: A class of efficient graph-based hash functions, Preprint (2007 (Accessed from https://wwwcsbhamacuk/ petitcz/, May 2017)).
[14] C. Petit, K. Lauter, and J.J. Quisquater, Full cryptanalysis of LPS and Morgenstern hash functions, International Conference on Security and Cryptography for Networks, Springer (2008), 263–277.
[15] J.P. Tillich and G. Zémor, Collisions for the LPS expander graph hash function, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer (2008), 254–269.
[16] K.E. Lauter, D.X. Charles, and E.Z. Goren, Hash function constructions from expander graphs (Jun 3 2008), US Patent 7,382,876.
[17] L. Bromberg, V. Shpilrain, and A. Vdovina, Navigating in the Cayley graph of $SL_2(\mathbb{F}_p)$ and applications to hashing, Semigroup Forum, Springer, 94 (2017) no. 2, 314–324.
[18] G. De Meulenaer, C. Petit, and J.J. Quisquater, Hardware implementations of a variant of the Zémor-Tillich hash function: Can a provably secure hash function be very efficient?, IACR Cryptology ePrint Archive 2009 (2009), no. 229.
[19] R. Steinwandt, M. Grassl, W. Geiselmann and T. Beth, Weaknesses in the $\mathrm{SL}_2(\mathbb{F}_{2^n})$ hashing scheme, Annual International Cryptology Conference, Springer (2000) 287–299.
[20] W. Geiselmann, A note on the hash function of Tillich and Zémor, IMA International Conference on Cryptography and Coding, Springer (1995), 257–263.
[21] C. Petit and J.J. Quisquater, Preimages for the Tillich-Zémor hash function, International Workshop on Selected Areas in Cryptography, Springer (2010), 282–301.
[22] C. Mullan, Some Results in Group-based crytography, Ph.D. thesis, University of London (2011).
[23] C. Mullan and B. Tsaban, SL_2 homomorphic hash functions: Worst case to average case reduction and short collision search, Designs, Codes and Cryptography 81 (2016), no. 1, 83–107.
[24] J.C. Faugere, L. Perret, C. Petit, and G. Renault, New subexponential algorithms for factoring in $\mathrm{SL}(2, \mathbb{F}_{2^n})$, Preprint (2011 (Accessed from https://wwwcsbhamacuk/ petitcz/, May 2017)).
[25] C. Petit, Towards factoring in SL_2. Designs, Codes and Cryptography, 71 (2014), no. 3, 1–23.

[26] C. Petit and J.J. Quisquater, Cryptographic hash functions and expander graphs: The end of the story?, The New Codebreakers, Lecture Notes in Computer Science, Springer, 9100 (2016), 304–311.
[27] H. Tomkins, Alternative Generators of the Zémor-Tillich Hash Function: A Quest for Freedom in Projective Linear Groups, Master's thesis, Université d'Ottawa/University of Ottawa (2018).
[28] J. Tits, Free subgroups in linear groups. Journal of Algebra, 20 (1972), no. 2, 250–270.
[29] L.E. Dickson, Linear groups with an exposition of the Galois field theory, Dover (1958).
[30] M. Suzuki, Group theory, Volume I, Springer-Verlag, New York (1982).
[31] K. Abdukhalikov and C. Kim, On the security of the hashing scheme based on SL_2, Fast Software Encryption, Springer (1998) 93–102.
[32] V. Shoup, Searching for primitive roots in finite fields, Proceedings of the twenty-second annual ACM symposium on theory of computing, ACM (1990), 546–554.
[33] The GAP Group: GAP – Groups, Algorithms, and Programming, Version 4.9.1 (2018 (Accessed from https://wwwgap-systemorg/, June 2018))
[34] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput, 24 (1997), no.3-4, 235–265.
[35] J. Katz and Y. Lindell, Introduction to modern cryptography, CRC press (2014).
[36] A.R. Regenscheid, An algebraic hash function based on SL_2, Master's thesis, Iowa State University (2007).
[37] C. Petit, J.J. Quisquater, J.P. Tillich, and G. Zémor, Hard and easy components of collision search in the Zémor-Tillich hash function: New attacks and reduced variants with equivalent security, Cryptographers Track at the RSA Conference, Springer (2009) 182–194.