JOURNAL OF THEORETICAL PHYSICS & CRYPTOGRAPHY
www.IJTPC.org/Publications

HASHING WITH DISCRETE HEISENBERG GROUP AND GRAPH WITH LARGE GIRTH

[1]Vibitha Kochamani .V , [2]Lilly P.L , [3]Joju K.T

[1,2]Department of Mathematics, St. Joseph's College, Irinjalakuda, Kerala, India.
[3]Department of Mathematics Prajyoti Niketan College, Pudukad, Kerala, India.

ABSTRACT

We introduce a Cryptographic Hash Functions that are in correspondence with directed Cayley Graph. We show why having a large girth and a small diameter, will satisfy the property that local modifications of a text will necessarily modify the hashed value.

Keywords

Cryptographic Hash function, Discrete Heisenberg group, Girth

1. INTRODUCTION

Hash functions [4, 14, and 15] are simple and easy-to-compute, that takes a variable length input and converts it to a fixed-length output. If such a function satisfies additional requirements it can be used for cryptographic applications, for example 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 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 [4] 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. The basic idea initiated in the paper [17] is of looking for potentially good Hash functions among Cayley Graphs is that girth is a relevant parameter to hashing the group $G = SL_2(\mathbb{F}_p)$, the group of 2x2 matrices of determinant 1 over the integers modulo a prime p and $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and they analyzed the girth of the cayley graph of the group.

At CRYPTO 94 [15], Tillich and Zemor proposed a family of hash functions, based on computing a suitable matrix product in groups of the form SL2 ($\mathbb{F}_{2n}$). In [7,8], generate a family of hash functions by replacing the generators with new generators.

2. PRELIMINARIES:

2.1 Definition: In [9] , the vertices 'x' of the graph G and one draws a directed edge from x to y, labeled by the group element g for any x, g ∈ G if and only if y=xg. The group consisting of all such vertices and edges will be denoted by Cay(G,G).

2.1.1. The Girth of a graph G, denoted g(G) is the length of the shortest cycle(if any) in G.

2.1.2. The Diameter of a graph G, denoted d(G) is the length of any longest geodesic.

Depending on these requirements Praneel [1, 12] provides the following informal definitions for two different types of hash functions.

2.2. 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 (preimage-resistance), and given x and h(x) it is hard to find a message x' ≠ x such that h(x') = h(x) (second preimage-resistance).

2.3. 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 $h(x) = h(x')$).

2.4. DEFINITION: A Hash Function h: D → R where the domain D = {0, 1}*, and the range R = $\{0,1\}^n$ for some n≥1.

The following definition is defined by [3,6, and 11]

2.5. DEFINITION: The Heisenberg group is the group of 3×3 upper triangular matrices of the form $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ under the operation of matrix multiplication. Elements *a*, *b* and *c* can be taken from any commutative ring with identity, often taken to be the ring of real numbers (resulting in the "continuous Heisenberg group") or the ring of integers (resulting in the "discrete Heisenberg group").it is denoted by Heis group.

From this definition, it is easily seen that the discrete Heisenberg group is generated by $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$

3. HASH FUNCTION

Now, we devising 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, $\boldsymbol{A} = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}$, $\boldsymbol{B} = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}$, then evaluate the product associated with the string of A's and B's in the group Heis ($\mathbb{F}_p$), where $\mathbb{F}_p$ is the field on p elements, p being chosen large prime number. The Hashed value is the computed product. A multiplication by 'A' or 'B' in Heis (F_p) requires essentially 9 additions, so hashing an n bit text requires 9n additions of logp bits, which is reasonably fast.

3.1 Let $\boldsymbol{A} = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}$ and $\boldsymbol{B} = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}$ be a pair of generators of Heis ($\mathbb{F}_p$) and let $\boldsymbol{m} = \boldsymbol{b_0 b_1} \ldots\ldots\ldots \boldsymbol{b_n}$ be a binary string. Then $H(\boldsymbol{m}) = \boldsymbol{\pi}(\boldsymbol{b_0})\boldsymbol{\pi}(\boldsymbol{b_1}) \ldots\ldots\ldots\ldots \boldsymbol{\pi}(\boldsymbol{b_n})$, where $\boldsymbol{\pi}(\boldsymbol{b_i}) = \begin{cases} \boldsymbol{A\ for\ b_i = 0} \\ \boldsymbol{B\ for\ b_i = 1} \end{cases}$; 0≤ i ≤ n. This hash function is strongly related to the Cayley Graph associated with Heis (Z_p) and generators A, B denoted by $\mathcal{G}$.

3.2 PROPERTIES OF HASH FUNCTION

Recall that the hash function construction presented above is directly associated with the cayley graph $\mathcal{G}$(G, S), where G is a group generated by the elements of the set S.

Concatenation property: If x and y are two texts, then their concatenation xy has hashed value H(xy) = H(x)H(y). This clearly allows an easy parallelization of the scheme, and pre computations when parts of the message are known in advance.

Parameters of the associated Cayley Graph: We can associate to this scheme the Cayley graph (G, S): its vertex set is G and there is a directed edge from g_1 to g_2 if and only if $g_1^{-1}g_2 \in S$. The following parameters are of fundamental importance when studying the security of the hash function.

Definition: The Girth of a graph $\mathcal{G}$, the largest integer g such that given any two vertices u and v , any pair of distinct paths joining u to v will be such that one of those paths has length g or more.The definition of the girth, immediately leads to the following property of the Hash function, for the associated cayley graph.

Proposition 1 :

If we replace 'u' consecutive elements of the product , $x = x_1x_2 \ldots\ldots\ldots x_ix_{i+1} \ldots\ldots\ldots x_{i+u}x_{i+u+1} \ldots\ldots\ldots x_t$ where $x_j \in S, j = 1\ to\ t$ with 'v' string of consecutive elements $y_{i+1}, \ldots\ldots\ldots y_{i+v} \in S$ such that $x = x_1x_2 \ldots\ldots\ldots x_iy_{i+1} \ldots\ldots\ldots y_{i+v}x_{i+u+1} \ldots\ldots\ldots x_t$ have the same hashed value, then max (u,v) ≥ g. In other words, if we can obtain cayley graph with a large 'g', we protect against local modifications of the text.

We can determine the Girth of the Cayley Graph associated with generators A and B.

To solve the Girth of the Cayley Graph, note the following lemmas

Lemma 2 : Let $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.Let $S_1, S_2, \ldots\ldots S_t \in \{A, B\}$with $M = S_1S_2 \ldots\ldots S_t = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$

with multiplication over Heis (Z_p). Then $a, b, c, d, e, f, g, h, i < 2^t$.That is, every element of M is less than 2^t.

Proof: We prove the lemma by induction on t. Suppose the lemma holds for strings of length $l < t$. Let

$S_1, S_2, \ldots\ldots, S_l \in \{A, B\}$ with $M = S_1S_2 \ldots\ldots S_l = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ then $a, b, c, d, e, f, g, h, i < 2^l$

Suppose that the induction for t, Let $S_1, S_2, \ldots\ldots S_t \in \{A, B\}$.

Define $M = S_1S_2 \ldots\ldots S_{t-1} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$.

If $S_t = A$, then $M.S_t = \begin{pmatrix} a & a+b & c \\ d & d+e & f \\ g & g+h & i \end{pmatrix}$.

Similarly if $S_t = B$,then $M.S_t = \begin{pmatrix} a & b & b+c \\ d & e & e+f \\ g & h & h+i \end{pmatrix}$. Hence in

both cases, by induction hypothesis the lemma holds for t.

Lemma 3: Let $A=\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}$ and $B=\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}$.Let

$S_1, S_2, \ldots\ldots S_t \in \{A, B\}$ with $t < \log_2(p)$.

Define $M = S_1 S_2 \ldots\ldots S_t = \begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}$ with multiplication

over Heis (Z_p). If $S_t = A$ then $a > b$ otherwise if $S_t = B$ then

$a \leq b$.

Proof: by above lemma, no reduction modulo p occurs in the

product $S_1 S_2 \ldots\ldots S_t$, as each element of the matrix will be

less than $2^t < 2^{\log_2(p)} = p$

If$S_t = A$,

Then $M.S_t = \begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix} = \begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}$ where

$a = 1 + a, b = b, c = c$.

Then we have $a > b$.

Similarly If $S_t = B$,

then $M.S_t = \begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix} = \begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}$

where $a = a, a + b = b, c = c$. Then we have $a \leq b$.

The above lemma allows us to determine a lower bound for

the girth of the cayley graph associated with A and B

THEOREM 4: The Girth of the Cayley Graph of Heis($\mathbb{F}_p$) with generators A and B is greater than $\log_2(p)$.

Proof: Let $S_1, S_2, \ldots\ldots S_K$ and $T_1, T_2, \ldots\ldots\ldots T_l$ be two different strings of A's and B's with $k, l < \log_2(p)$. The product of these strings can only have the same form if $k = l$ Then $S_K = T_l$, by cancelling S_K from both sides and iterating this argument, we see that S_i must be equal to $T_i, \forall\ 1 \leq i \leq k$.Thus the products of $S_1, S_2, \ldots\ldots S_K$ and $T_1, T_2, \ldots\ldots\ldots T_l$ must be different. Therefore the girth of the graph is at least $\log_2(p)$

THEOREM 5: The Diameter of the Cayley Graph of Heis ($\mathbb{F}_p$) with generators A and B is p+1

Proof: The proof involves powerful and arithmetic, it can be shown that (see [5] and references therein). It is true for all m, positive integer then it is true for any large prime numbers. Hence the theorem holds.

3.3 EXPANDING PROPERTIES:

While not technically, a requirement for a secure hash function, a desirable feature of any hash function is the equidistribution of the hashed values. This property can be guaranteed if the associated Cayley graph of (G, S) [15], claim the property.

Proposition 6: If (G,S) is a cayley graph such that the greatest common divisor of its length equals 1, then for the corresponding hash function, the distribution of the hashed values of texts of length n tends to equidistribution when n tends to infinity.

Proof: In practically, we need to evaluate the speed with which equidistribution is achieved. Sufficiently random graphs appear to provide the best results (for more details refer [16]).

4. ACKNOWLEDGMENTS

I would like to take this opportunity to express my gratitude to those who helped me.

5. REFERENCES

[1] Bart Van Rompay, *Analysis and Design of Cryptographic hash Functions, MAC algorithms and Block Ciphers*, Doctoral Dissertation, KU Leuven2004D/2004/7515 ISBN 90-5682-527-5

[2] László Babai, William M. Kantor, and Alexander Lubotzky, *Small-diameter Cayley graphs for finite simple groups*, *European J. Combin.* 10 (1989),507–552.

[3] Luca Capogna, Donatella Danielli, Scott D. Pauls, Jeremy Tyson, *An Introduction to the Heisenberg Group and the Sub-Riemannian Isoperimetric*, Springer Science & Business Media, 08-Aug-2007 - Mathematics - 224 pages

[4] Daugles R Stinson, *Cryptography theory and practice*, Second Edition, Chapman & Hall/CRC.

[5] P.Diaconis and L.Saloff-Coste, *Modern Growth and Random Walk on Finite Groups,Geometric and Functional Analysis*, Vol 4.No.1(1994).

[6] Brian C. Hall (2004). *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction*. Berlin: Springer.

[7] Joju K.T & Lilly P.L, *Improved form of Tillich-Zemor Hash Function* International Journal of Theoretical Physics and Cryptography, Vol. 6, August 2014.

[8] Joju K.T & Lilly P.L / *Hashing with SL2 using new generators* /International Research Journal of Pure Algebra -3(10) / Oct.-2013, 321-324.

[9] Joseph.A.Gallian,*Contemporary Abstract Algebra*, 8th Edition University of Minnesota, Duluth,ISBN-10: 1133599702 | ISBN-13: 9781133599708

[10] Mark R. Jerrum, The *complexity of finding minimum length generator sequences*, *Theor. Comput. Sci.* 36(1985), no. 2-3, 265–289

[11] A.de Mesmay (2009),*The Heisenberg Group and Pansu's Theorem*, Available from www.gipsa-lab.fr/~arnaud.demesmay/mesmay.pdf

[12] B. Praneel: *Analysis and Design of Cryptographic Hash Functions*. Doctoral Dissertation K.U .Leuven Jan. 1993.

[13] Jean-Pierre Tillich and Gilles Zémor, *Group theoretic hash functions,* Proceedings of the FirstFrench-Israeli Workshop on Algebraic Coding (London,UK), Springer-Verlag, 1993, pp. 90–110.

[14] V. Shpilrain. *Hashing with polynomials*, In ICISC 2006, pages 22–28. Springer, 2006,Lecture Notes in Computer Science No. 4296.

[15] J. P. Tillich and G. Zemor, *Hashing with SL2,* Advances in Cryptology Lecture Notes in Computer Science, vol. 839(1994), Springer-Verlag, pp. 40-49.

[16] Gilles Zémor, *Hash functions and Cayley Graph. To appear in Designs*,Codes and Cryptography.

[17] Gilles Zémor, *Hash functions and graphs with large girths*, *EUROCRYPT* (Donald W. Davies, ed.), Lecture Notes in Computer Science, vol. 547, Springer, 1991,pp. 508–511.