ISSN NO. 2320-5407

Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/18867
DOI URL: http://dx.doi.org/10.21474/IJAR01/18867

RESEARCH ARTICLE

A KEYED CAYLEY HASH FUNCTION USING DISCRETE HEISENBERG GROUP

Dr. V. Vibitha Kochamani
Assistant Professor, Department of Mathematics, Mar Dionysius College, Pazhanji, Kerala.

……………………………………………………………………………………………………....

Manuscript Info

……………………….

Manuscript History
Received: 10 April 2024
Final Accepted: 14 May 2024
Published: June 2024

Key words:-
Cayley Hash Function, Discrete Heisenberg Group, Cayleygraph, Hash Function

Abstract

……………………………………………………………………

We introduce a New Cryptographic Hash functions using Discrete Heisenberg Group by concatenating the key to it, which will give a new hashed values corresponding to the keyed generators.The new Keyed Hash functions using Discrete Heisenberg Group will enhance the security properties of the Cayley Hash Functions.

……………………………………………………………………………………………………....

Introduction:-

Hash functions [3, 11, and 12] 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 [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.The basic idea initiated in the paper [14] is of looking for potentially good Hash functions among Cayley Graphs is that girth is a relevant parameter to hashing the group G = SL2(Fp), the group of matrices of determinant 1 over the integers modulo a prime p
and $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

andthey analysed the girth of the Cayley graph of the group.

At CRYPTO 94 [12], Tillich and Zemor, proposed a family of hash functions, based on computing a suitable matrix product in groups of the form SL2(F2n).[14] and [15] In that papers 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, $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$

Corresponding Author:- Dr. V. Vibitha Kochamani
Address**:-** Assistant Professor, Department of Mathematics, Mar Dionysius College, Pazhanji, Kerala.

and $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ then the Hashed value is the computed product. A multiplication by 'A' or 'B' in Heis(Fp) requires essentially 9 additions, so hashing an n bit text requires 9n additions of logp bits, which is reasonably fast.In this paper, we propose a new version of hash function which is a modification of a Cayley Hash Function using a Discrete Heisenberg group.

Preliminaries

Definiton:A hash function h: D → R where the domain D= {0, 1}*, and the range R = {0,1}n for some n ≥ 1.

Definiton:

In [8],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).

In [8], 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 ≠ x' such that h(x) = h(x')).

Definition:In [5] , the vertices 'x' of the graph G and one draws a directed edge from x to y, labelled by the group element g for any x, g ЄG if and only if y=xg. The group consisting of all such vertices and edges will be denoted by Cay (G, G).

Definition:Let G be a group and S be the generating set of G (i.e) S = {s0, s1, s2,…. sk−1} ⊂ G .Write m=m1m2……….mN withmi = {0,1,......,k − 1}and defineH(m) = Sm1, Sm2,… SmN.Computation of the Cayley Hashesis walk in the Cayley graph.[5]

The Girth of a graph G̊ , the largest integer g such that given any two vertices u and v , any pair of distinct paths joining u to vwill 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.

Definition:[2,4 and 8]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 matrixmultiplication. 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"). 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 $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

Definition:[14] Let □= $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and□= $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ be a pair of generators of Heis(Fp) and let □ = □1□2…. □□be a binary string. Then H(m) = π (m1)π (m2) . . . . π (mn) , where π (mi) = {A fori = 0; Bfori = 1}; 0≤ i ≤ n.This hash function is strongly related to the Cayley Graph associated with Heis(□□) and generators A, B denoted by G̊. Properties Of Hash Functions [14]

Concatenation property: If x and y are two texts, then their concatenation x++y is the H(xy) = H(x)H(y)hashed value.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 g1 to g2 if and only if g−1g2 ∈ S.If we replace 'u' consecutive elements of the product ,with 'v' string of consecutive elements which have the same hashed value, then max (u,v) ≥ g.In other words, if we can obtain cayley graph with a large girth 'g', we protect against "Local Modifications of the Text".

Theorem:The Girth of the Cayley Graph of Heis(F p) with generators A and B is greater than log2(p). Keyed Form

1.DEFINITION: Let K={(k1, k2, ... , kn): ki = 0 or 1} be the key space. Then this key K holds 2n elements.Now We describe the new hash function as follows:
H1(m) = π (b1)k1π (b1)k2 . . . . π (b1)knπ (bn+1)k1 , where π (bi)ki = {1i f ki = 0; π (bi)i f ki = 1}
If we choose the ki = 1 for all i, then our newly defined Hash function and the Hash function using Discrete Heisenberg group.
SecurityProperties
Theorem:If we know a message m, such that H(m) = h, then we can efficiently find a message x′, for every message x such that
H1(x) = H(x′).
Pr o o f: Let m be a binary string such thatH(m) = h.Let$x = x_1x_2\ldots\ldots x_n$andAssume that,$x' = x_1x_2\ldots\ldots x_g m x_{g+1}\ldots\ldots x_{2g} m x_{2g+1}\ldots\ldots x_n$.Thenitgivesthat$H_1(x) = H(x)$.

Lemma: Let $K = \{\{k_1, k_2\ldots\ldots k_k\}: K_i = 0(or)1\}$bethekeyspace.Let$S_1$,$S_2$,....$S_t$∈$\{A,B\}$with

$$M = S_1^{k_1}S_1^{k_2}S_1^{k_3}\ldots\ldots\ldots S_1^{k_k}S_1^{k_1}\ldots\ldots S_1^{k_i} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$ where $k_i \in (k_1, k_2, \ldots\ldots k_k)$ then a,b,c,d,e,f,g,h,i≤t.

Proof:We Prove this lemma by induction on t.
Suppose t=1 then M = Sk1 ,if k1 = 0(or)1 . In both cases all the entries of the matrix A and B are either 1 or 0 which gives theinduction is true for t=1.
Assume that the lemma holds for l < t, then we get a, b, c, d, e, f, g, h, i ≤ l. We need to prove that the induction is true for t.
Let S1, S2, ... St ∈ {A, B}.

Define,$M = S_1^{k_1}S_1^{k_2}S_1^{k_3}\ldots\ldots\ldots S_1^{k_k}S_1^{k_1}\ldots\ldots S_1^{k_i} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$, where ki ∈ (k1, k2, ... kk) then a, b, c, d, e, f, g, h, i ≤ t − 1.

If we choose, Ski then the product of M . Ski≤ t either in both cases k1 = 0(or)1.Hence by induction hypothesis, the lemma holds for t.
Lemma: Let the bit '0' be mapped to the matrix A = and the bit '1' be mapped to the matrix .Let K = {k1, k2 k): Ki = 0(or)1}. Iftwo distinct messages k and l hashes to same value then length of either k or l is at least logt(p).
Proof:Let$M = S_1^{k_1}S_2^{k_2}S_3^{k_3}\ldots\ldots\ldots S_k^{k_k}S_{k+1}^{K_1}\ldots\ldots S_t^{K_i}$,wherek$_i$∈(k$_1$,k$_2$,...k$_k$)bethegivenmessage.Let$S_1^{k_1}S_2^{k_2}S_3^{k_3}\ldots\ldots\ldots S_k^{k_k}$and $T_1^{k_1}T_2^{k_2}T_3^{k_3}\ldots\ldots\ldots T_l^{k_k}$bethetwodifferentstringsofA'sandB'swith$l, k < log_t(p)$afterapplyingthe keys from the key space.The product ofthese strings can only have thesameformifk=l.Then$S_k^{k_k} = T_l^{k_k}$,bycancelling$S_k^{k_k}$frombothsidesanditeratingthisargument,weseethat$S_i = T_i$,forall1≤i≤k.Thustheproductof$S_1^{k_1}S_2^{k_2}S_3^{k_3}\ldots\ldots\ldots S_k^{k_k}andT_1^{k_1}T_2^{k_2}T_3^{k_3}\ldots\ldots\ldots T_l^{k_k}$mustbedifferent.
Hencetwodistinctmessageskandlhashestosamevaluethen lengthofeitherkorlisatleastlog$_t$(p).

References:-

1. Bart Van Romp,Analysis and Design of Cryptographic hash functions.MAC algorithms and Block Ciphers Doctoral Dissertation,KU Leuven 2004D/2004/7515 ISBN 90-5682-527-5.
2. 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
3. Daugles R Stinson, Cryptography theory and practice, Second Edition, Chapman & Hall/CRC.
4. Brian C. Hall (2004). Lie Groups, Lie Algebras, and Representations: An Elementary Introduction. Berlin:Springer.J th Joseph.A.Gallian, Contemporary Abstract Algebra, 8 1133599702 | ISBN-13: 9781133599708
5. Edition University of Minnesota, Duluth,ISBN-10:

6. Lilly P.L and Vibitha Kochamani.V, Hashing with Discrete Heisenberg Group using New generators, In Journal of Theoretical and Computational Mathematics, Vol-2, No-2, Nov 2016 pp 14-18
7. A.de Mesmay (2009),The Heisenberg Group and Pansu's Theorem, Available from www.gipsalab. fr/ ~arnaud.demesmay/ mesmay.pdf
8. B. Praneel: Analysis and Design of Cryptographic Hash Functions. Doctoral Dissertation K.U .Leuven Jan. 1993.
9. Jean-Pierre Tillich and Gilles Zémor, Group theoretic hash functions, Proceedings of the First French-Israeli
10. Workshop on Algebraic Coding (London, UK), Springer-Verlag, 1993,pp. 90–110.
11. V. Shpilrain. Hashing with polynomials, In ICISC 2006, pages 22–28. Springer, 2006, Lecture Notes in Computer Science No. 4296.
12. 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.
13. Gilles Zémor, Hash functions and Cayley Graph. To appear in Designs, Codes and Cryptography.
14. Gilles Zémor, Hash functions and graphs with large girths, EUROCRYPT (Donald W. Davies, ed.), Lecture Notes in Computer Science, vol. 547, Springer, 1991,pp.
15. Vibitha Kochamani.V, Lilly P.L, and Joju K.T, Hashing with Discrete Heisenberg Group and Graph with large girth, In Journal of Theoretical Physics and Cryptography, Vol-11, May 2016.
16. Vibitha Kochamani.V, Lilly P.L, Modified Form of Cayley Hash Function, Asian Journal of Engineering and Applied Technology ,Vol. 8 No. 2, 2019, ISSN 2249-068X , 34-36, The Research Publication.
17. Vibitha Kochamani.V, Lilly P.L, Security Aspects of the Cayley Hash Function using Discrete Heisenberg Group, Journal of Discrete Mathematical Sciences and Cryptography,doi:10.1080/09720529.2019.1638613, ISSN 0972-0529 (print), ISSN 2169-0065 (online).
18. Vibitha Kochamani.V, Lilly P.L, Vectorial version of the Cayley Hash Function using Discrete Heisenberg group, Malaya Journal of Matematik,Vol.S,No.1,720-724,2019, https://doi.org/10.26637/MJM01/0128.
19. Vibitha Kochamani.V, Lilly P.L, Neighbourhoods in $\mathbb{P}2$, International Journal of Research and Analytical Reviews,2019, E- ISSN 2348-1269, P- ISSN 2349-5138, vol.6(2).
20. V.Vibitha Kochamani and P.L.Lilly,Hash Function Using Free Generators Theorem Over The Projective General Linear Group, 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.