ISSN: 2395-6607, Vol. 1, No. 1 March 2015, pp. 35–40

COLLISION RESISTANT ALTERNATE FORM OF TILLICH-ZEMOR HASH FUNCTION WITH NEW GENERATORS

Joju K.T.[1] and Lilly P.L.[2]
[1]*Department of Mathematics, Prajyoti Niketan College, Pudukad*
[2]*Department of Mathematics, St. Joseph's College, Irinjalakuda*
E-mail: [1]jojukt@gmail.com, [2]sr.christy@gmail.com

Abstract—*At CRYPTO '94, Tillich and Zemor proposed a family of hash functions, based on computing a suitable matrix product in groups of the form $SL_2(F_2n)$. Markus Grassl, Ivana Illich, Spyros Magliveras and Rainer Steinwandt constructed a collision between palindrome bit strings of length 2n+2 and Christophe Petit, Jean-Jacques Quisquater found the second preimage for Tillich and Zemor's construction. In this paper we construct a hash function by using different matrices for the image of the bits 0 and 1 and found the collision and second preimage for the new construction.*

Keywords*: Collision, Euclidean Algorithm, Groups, Hash Function, Irreducible Polynomial, Palindrome, Preimage*

INTRODUCTION

A cryptographic hash function can provide assurance of data integrity. A hash function is used to construct a short "finger print" of some data; if the data is altered, then the finger print will no longer be valid. Even if the data is stored in an insecure place, its integrity can be checked from time to time by recomputing the finger print and verifying that the finger print has not changed [3]

A hash family is a four–tuple (X, Y, K, H) where the following conditions are satisfied:

X is a set of possible messages

Y is a finite set of possible message digests

K, the key space, is a finite set of possible keys

For each k ∈ K, there is a hash function H_k ∈ H. Each H_k: X → Y

An unkeyed hash function is a function H: X → Y.An unkeyed hash function is a hash family in which there is only one possible key.

Security of Hash Functions: [11]

The following three properties are essential for a secured hash function.

Preimage Resistance

It should be computationally infeasible to find an input which hashes to a specified output.

Second Preimage Resistance

It should be computationally infeasible to find a second input that hashes to the same output of a specified input

Collision Resistance

It should be computationally infeasible to find two different inputs that hash to the same output.

Early suggestions (SHA family) did not really use any mathematical ideas apart from Merkle-Damgard [9] 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.

At CRYPTO ’94, Tillich and Zemor [10] proposed a family of hash functions, based on computing a suitable matrix product in groups of the form SL_2 (F_2n).Tillich-Zemor suggested a mathematical hash function, which hash bit by bit. That is”0”bit is hashed to a particular 2x2 matrix $A_0$and the “1” bit is hashed to another 2x2 matrix A_1. For example 11000100 is hashed to the matrix $A_1^2A_0^3A_1A_0^2$.It is possible only when this pair of elements A_0, A_1 should be from an Algebraic structure. Tillich and Zemor use matrices A_0, A_1 from the group $SL_2(R)$ where $R = F_2[x]/(q(x))$ [4]. Where F_2 is the field of two elements, $F_2[x]$ is the ring of polynomials over F_2 and (q(x)) is the ideal of $F_2[x]$ generated by an irreducible polynomial q(x) of degree n where n is a prime.

For example

$q(x)=x^{167}+x^7+x^6+x^5+x^4+x+1$ [5].

Thus $R=F_2[x]/(q(x))$ isomorphic to F_2n the field with 2^n elements.The matrices A_0 and A_1 are the following:

$A_0 = \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$ $A_1 = \begin{pmatrix} \alpha & \alpha+1 \\ 1 & 1 \end{pmatrix}$, where ∝ is the root of the irreducible polynomial q(x).

For the bitstring $v = b_1.....b_m \in V = \{0,1\}^*$, where $\{0,1\}^*$is the collection of bit strings of arbitrary length. The Tillich –Zemor hash function h' is defined as follows:

$h' (b_1......b_m) = A_{b_1}......A_{b_m}$.

In [7] Markus Grassl, Ivana Illich, Spyros Magliveras and Rainer Steinwandt constructed a collision between palindrome bit strings of length 2n+2 and in[2] Christophe Petit, Jean-Jacques Quisquater found the second preimage for Tillich and Zemor hash function. In [6] we defined the following hash function:

Let B_0 and B_1 be the following matrices

$B_0=A_0^{-1}$ and $B_1=A_1^{-1}$ then $B_0 = \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix}$ and $B_1 = \begin{pmatrix} 1 & \alpha+1 \\ 1 & \alpha \end{pmatrix}$.

For the bitstring $v = b_1 \ldots\ldots b_m \in V$ we define the new hash function h as follows:

$h (b_1....b_m) = B_{b_1}...........B_{b_m}$.

PALINDROME COLLISIONS

Let $v \in V$ and |v| denote the length of the bitstring v.If $v=b_1....b_m \in V$ is of length m, we denote $v^r = b_m.....b_1$ the reversal of v. In our attack we will make use of palindromes, that is, bitstrings $v \in V$ satisfying $v=v^r$.

In order to find the palindrome collision we use the matrices $C_0 =B_0$ and

$C_1= B_OB_1B_0^{-1}$. That is

$C_0=\begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix}$ and $C_1=\begin{pmatrix} 0 & 1 \\ 1 & \alpha+1 \end{pmatrix}$

We define $H (b_1....b_m) = C_{b_1}.....C_{b_m}$

Proposition 1 [6]

Let v, v' ∈ V. Then h (v) = h(v') if and only if H(v) = H(v').

The above proposition says that collision in h and H are equivalent.

Now we work inside the group $SL_2(F_2[x])$ of unimodular matrices over the polynomial ring $F_2[x]$ rather than F_{2^n}.Let $D_0, D_1 \in SL_2(F_2[x])$ with polynomial entries as follows:

$D_0 = \begin{pmatrix} 0 & 1 \\ 1 & x \end{pmatrix}$, $D_1 = \begin{pmatrix} 0 & 1 \\ 1 & x+1 \end{pmatrix}$ and

we define $H': V \to SL_2(F_2[x])$ by

$H'(b_1......b_m) = D_{b_1}......D_{b_m} \in SL_2(F_2[x])$.

That is H' is defined as H,except that $H'(v) \in SL_2(F_2[x])$.

We apply H' to a particular subset of elements of V, namely, the set of all palindromes in V.

Lemma 1 [6]

Let v ∈ V be a palindrome and write $H'(v) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Then b=c and d has degree, deg d= |v| and we have max. (deg a, deg b)≤|v|.

Define ρ: $V \to F_2[x]^{2\times 2}$ is defined by

$\rho(v) = H'(0v0) + H'(1v1)$.

We are interested in evaluating ρ modulo a given irreducible polynomial, because ρ (v) ≡ $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ modq(x) if and only if

H (0v0) = H (1v1) is indeed a collision in $SL_2(F_2[x]/(q(x)))=G$.

Proposition 2[6]

If v ∈ V is a palindrome of length |v|, then $\rho(v) = \begin{pmatrix} 0 & d \\ d & d \end{pmatrix}$ where d ∈ $F_2[x]$ has degree |v|. Moreover, d is the lower right entry of H' (v).

Proposition 3[6]

If v ∈ V is a palindrome of even length then $H'(v) = \begin{pmatrix} a^2 & b \\ b & d^2 \end{pmatrix}$ for some a, b, d ∈ $F_2[x]$.

Corollary 1 [6]

Let v ∈ V be a palindrome of even length. Then $\rho(v) = \begin{pmatrix} 0 & d^2 \\ d^2 & d^2 \end{pmatrix}$ for some d ∈ $F_2[x]$ with deg d = |v|/2. More specifically $d^2$is the lower right entry of H'(v).

Corollary 2 [6]

Let $b_n.....b_1b_1......b_n \in V$ be a palindrome of length 2n.Then for 0≤ i≤ n, the square root p_i of the lower right entry of $H'(b_i.........b_1b_1......b_i)$ is given by

$$p_i = \begin{cases} 1 & if\ i = 0 \\ x + b_i + 1 & if\ i = 1 \\ (x+i)p_{i-1} + p_{i-2} & if\ 1 < i \le n \end{cases}$$

COLLISION AND EUCLIDEAN ALGORITHM

Construction of Palindrome

From corollaries 1 and 2 we see that the square roots of the lower right entries of $H'(b_1b_1)$, $H'(b_2b_1b_1b_2)$,$H'(b_3b_2b_1b_1b_2b_3)$,etc, satisfy Euclidean algorithm sequence(in reverse order) where each quocient is either x or x+1[2]. Those sequences are often called maximal length sequences for the Euclidean algorithm or maximal length Euclidean sequences and they have long been a topic of interest in number theory.

Mesirov and Swweet [8] showed that, when q(x)∈ F[x] is irreducible there exist exactly two polynomials p(x) such that q(x) and p(x) are the first terms of a maximal length Euclidean sequence. They also provide an algorithm to compute them, which will be given below.

Proposition 4

(Mesirov and sweet). Given any irreducible polynomial q of degree n over F_2, there is a sequence of polynomials $p_n, p_{n-1}, \ldots\ldots, p_0$ with $p_n = q$, and $p_0 = 1$ and additionally the degree of p_i is equal to i and $p_i \equiv p_{i-2} \bmod p_{i-1}$.

Note that once we know a polynomial p= p_{n-1} as mentioned in proposition 4 which matches our given polynomial p_n = q, the Euclidean algorithm will uniquely compute the sequence

$p_n, p_{n-1}, \ldots\ldots p_1, p_0 = 1$.

The quotients x + β_i (i= 1,.....,n) occurring in Euclid's algorithm allow us to derive the bits b_i of the palindrome in corollary 2.

We have $p_1 = x + b_1 + 1$ and therefore $b_1 = \beta_1 + 1$, while $b_i = \beta_i$ for i>1. That is the bit β_1 has to be inverted. Thus the desired collision will be

H $(0\beta_n \ldots\ldots \beta_1^{-1}\beta_1^{-1} \ldots\ldots \beta_n 0)$ = H $(1\beta_n \ldots\ldots \beta_1^{-1}\beta_1^{-1} \ldots\ldots \beta_n 1)$

Where, β_1^{-1} indicates the inversion of β_1

To Find the Maximal Length Euclidean Sequence

1. Construct a matrix A ∈ $F_2^{(n+1)\times n}$ from the n+1 polynomials $g_o = x^0 \bmod q(x)$,

$g_i = x^{i-1} + x^{2i-1} + x^{2i} \bmod q(x)$ for i= 1,2,......,n

Placing in the i^{th} row of A the coefficients

$a_{i,0}$, $a_{i,1}$,......$a_{i,n-1}$ of the polynomial

$g_i = a_{i,0} + a_{i,1}x + \ldots\ldots a_{i,n-1}x^{n-1}$.

2. Solve the linear system $Au^t = (10\ldots\ldots01)$ where $u = (u_1 \ldots\ldots u_n)$.
3. Compute p(x) by multiplying q(x) by $\sum_{i=1}^{n} u_i x^{-i}$ and taking only the non negative powers of x.

COLLISIONS FOR SPECIFIED POLYNOMIALS

Example 1.[6]

Let $q(x) = x^2 + x + 1$ be the irreducible polynomial. We have the following collisions

$$H(011110) = \begin{pmatrix} 0 & 1 \\ 1 & x+1 \end{pmatrix} = H(111111).$$

$$H(000000) = \begin{pmatrix} 0 & 1 \\ 1 & x \end{pmatrix} = H(100001).$$

Example 2.[6]

Let $q(x) = x^3+x+1$

The collision are

$$H(01111110) = \begin{pmatrix} 0 & 1 \\ 1 & 1+X \end{pmatrix} = H(11111111) \text{ and } H(00100100) = H(10100101).$$

By Proposition 1. Collision in h and H are equivalent. For higher degree irreducible polynomials q(x) we implement the attack in the computer algebra system Magma[1] on a standard PC.For each q(x) there will be two solutions for p(x) so we obtain two bit strings $v_1, v_2 \in \{0,1\}^n$ with

$H(0v_iv_i^r0) = h(1v_iv_i^r1)$ for i=1,2.

That is, we obtain two collisions of bit strings of length 2n+2.The value v_2 can be obtain by reversing v_1 followed by inverting the first and last bit.

In example 1, $v_1 = 11$, $v_2 = 00$

In example 2, $v_1 = 111$, $v_2 = 010$.

NEW HASH FUNCTION

As the function H is not collision resistant. We define a new hash function H_1, which is collision resistant, as follows:

$H_1(b_1 \ldots b_m) = trB_{b_1} \ldots\ldots trB_{b_m}$, where tr $B_0 = \alpha$ and tr $B_1 = \alpha + 1$. Now we prove that H_1 is collision resistant.

In example 1, we have the collisions

$$H(011110) = \begin{pmatrix} 0 & 1 \\ 1 & x+1 \end{pmatrix} = H(111111) \text{ and } H(000000) = \begin{pmatrix} 0 & 1 \\ 1 & x \end{pmatrix} = H(100001).$$

But $H(011110) = \alpha$, $H_1(111111) = 1$ and $H_1(000000) = 1$, $H_1(100001) = \alpha+1$.

In example 2, we have the collisions

$$H(01111110) = \begin{pmatrix} 0 & 1 \\ 1 & 1+X \end{pmatrix} = H(11111111) \text{ and } H(00100100) = H(10100101).$$

But $H_1(01111110) \neq H_1(11111111)$ and $H_1(00100100) \neq H_1(10100101)$.

Hence H_1 is collision resistant. Similarly we can verify collision resistance using The Magma Algebra System [1].

REFERENCES

Wieb Bosma, John Cannon, and Catherine Playoust, The Magma Algebra System I: The User Language. Journal of Sympolic Computation, 24 (1997), pp. 235-265.

Christophe Petit and Jean-Jacques Quisquater, Preimage for the Tillich-Zemor hash function. Proceedings of SAC 2010, pp. 282-301.

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

John R Durbin, Modern Algebra, John Wiley & Sons.

Joju K.T and Sr. Lilly P.L Alternate form of Hashing with Polynomials. Proceedings of the International workshop in Cyber Security, St. Joseph's College, Irinjalakuda pp.2011,(IWCS2k11) 43-45, 2011

Joju K.T and Sr. Lilly P.L Tillich-Zemor Hash function with new Generators and Analysis International Research Journal of Pure Algebra.,2(11), 338-343.

Markus Grassl, Ivana Ilic, Spyros Magliveras, and Rainer Steinwadt, Cryptanalysis of the Tillich-Zemor Hash function, Cryptology ePrint Archive, Report 2009/376, 2009, http://eprint.iacr.org/.

Jill P. Mesirov and Melvin M. Sweet. Continued Fraction Expansions of Rational Expressions with Irreducible Denominators in Characteristic 2. Journal of Number Theory, 27 (1987), pp.144-148.

Stefan Lucks, Design principles of Iterated Hash function, ePrint Archive: Report (2004), pp.1-22.

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.

Vladimir Shpilrain, Hashing with polynomials, Proceedings of ICISC 2006, Springer (2006), pp. 22-28.