Chained Hexi Codes Signature Scheme

Ilanthenral Kandasamy and K.S.Easwarakumar
ilanthenral@gmail.com easwarakumarks@gmail.com
Department of Computer Science and Engg, Anna University, Chennai, 600-036 India

Summary
In this paper, the chained hexi codes (CHC) signature scheme is proposed. This scheme is based on the BCHS1 signature scheme (signature scheme based on BCH) which was proposed by Hamdi, Harari and Bouallegue in 2006. Here a family of hexi polynomial codes is used, instead of BCH codes. The newly proposed chained hexi codes signature scheme has lesser key size and better security; when compared to the signature scheme based on McEliece cryptosystem and the BCHS1 signature scheme. A variant of this chained hexi codes signature scheme, that has lesser space and time complexity is also introduced.

Key words:
Public key cryptosystems, McEliece cryptosystem, Coding theory, Digital signature, BCHS1 signature scheme, BCH codes, hexi polynomial codes.

1. Introduction

There have been many attempts to build secure public key cryptosystems based on error-correcting codes over the last three decades, however most of them have been proved to be insecure. The disadvantage of having a large public key is the major shortcoming of many code-based cryptosystems like the McEliece public key cryptosystem [19], the Stern's Identification scheme [21] and the Courtois, Finiasz, and Sendrier signature scheme (CFS signature scheme) [7].

In 2006, Hamdi, Harari and Bouallegue, had introduced signature schemes using BCH codes known as BCHS1 and BCHS2 [10]. These schemes are secure, fast and more practical than the CFS signature scheme. The setback of large public key size can be overcome by using hexi based codes instead of the usual binary codes, without compromising the security. In this paper hexi code based digital signature scheme known as Chain Hexi Code (CHC) signature scheme is introduced. The proposed scheme is a variant of the BCHS1 signature scheme. This scheme makes use of a family of hexi polynomial codes, it has lesser public key size and better security; when compared to the signature scheme based on McEliece cryptosystem and the BCHS1 signature scheme. The rest of this paper is organised as follows: Section two discusses about code based signature schemes. Section three recalls the definition of hexi codes and other related hexi codes and their decoding algorithms. Section four introduces the signature scheme based on hexi polynomial codes known as CHC signature scheme. Section five introduces a variant of the CHC signature scheme. Security of the schemes are discussed in section six. Conclusions and further directions are provided in section seven.

2. Code-based Signature Schemes

Since the advent of code based cryptography, researchers have made several attempts to create a code based signature scheme that is secure. Most of the signature schemes have been proved to be insecure.

In 1990, Xinmei Wang introduced a digital signature scheme based on error correcting codes [24]. The scheme is similar to McEliece public key cryptosystem, but its security was based on the difficulty involved in solving the factorization of large matrices. This system was attacked and modified in 1992 by Harn and Wang [11]. Later in 1992, Alabbadi and Wicker [2] completely broke the Xinmei Wang digital signature scheme. Alabbadi and Wicker then proposed a digital signature scheme based on error correcting codes [1] in 1993.

In the same year Johan van Tilburg has carried out the cryptanalysis of the Alabbadi Wicker digital signature scheme [23]. Jacques Stern successfully broke this signature scheme in 1994 [22]. Kabatianskii, Krouk, and Smeets proposed a signature scheme based on random codes in 1997 known as the KKS signature scheme and claimed it to be secure [15]. However, in 2007, Pierr-Louis Cayrel, Otmani and Verguand [6] showed that a passive attacker intercepting just a few signatures can efficiently find the private key.

In 2011, Otmani and Tillich [20] had carried out an efficient attack on all concrete KKS proposals and broke the system. Courtois, Finiasz, and Sendrier [7] designed a code-based signature scheme in 2001, it still remains unbroken. The signature scheme is based on the Niederreiter cryptosystem and it uses Goppa code. The CFS signature scheme depends on two NP-complete problems for its security. Researchers have designed several variants of the CFS signature scheme.

Hamdi, Harari and Bouallegue, [10] in 2006 had introduced a signature scheme which is practical, secure and fast. This signature scheme made use of a family of BCH codes. It involved chaining a family of BCH codes with various dimensions. This scheme was secure, faster and more practical than the CFS signature scheme.

Manuscript received December 5, 2014
Manuscript revised December 20, 2014

In this paper, a variant of this signature scheme is presented. This scheme makes use of a family of hexi polynomial codes. The proposed new scheme has lesser key size and better security; when compared to the signature scheme based on McEliece cryptosystem and the BCHS1 signature scheme.

3. Hexi Codes and Related Hexi Codes

This section recalls some definitions regarding hexi codes and related hexi codes like hexi polynomial codes. Hexi codes and hexi polynomial codes were introduced along with other hexi codes in 2013 [12-14]. Quasi cyclic partial hexi codes, which are hexi codes have been used to introduce error correction in AES. Hexi polynomial codes have been used to reduce public key size in the hexi McEliece public key cryptosystem. Hexi rank codes have been used in variants of the GPT cryptosystem. The definition of hexi code and hexi polynomial code are recalled.

3.1 Hexi Fields

Let $S = Z_{2^4}$ be a field of 16 elements which is isomorphic to

$$\frac{Z_2[x]}{\langle x^4 + x + 1\rangle} \quad (1)$$

where $\langle x^4 + x + 1\rangle$ is the ideal generated by the irreducible polynomial $x^4 + x + 1$ in $Z_2[x]$. Now the elements are given hexadecimal notation, where 0 = 0000, 1 = 0001,

Table 1: Representations of the elements of the hexi field S

Hexi representation	*4-Tuple representation*	*Power representation*	*Polynomial representation*
0	(0 0 0 0)	0	0
1	(0 0 0 1)	α^3	α^3
2	(0 0 1 0)	α^2	α^2
3	(0 0 1 1)	α^6	$\alpha^2 + \alpha^3$
4	(0 1 0 0)	α	α
5	(0 1 0 1)	α^9	$\alpha+\alpha^3$
6	(0 1 1 0)	α^5	$\alpha + \alpha^2$
7	(0 1 1 1)	α^{11}	$\alpha + \alpha^2 + \alpha^3$
8	(1 0 0 0)	1	1
9	(1 0 0 1)	α^{14}	$1 + \alpha^3$
A	(1 0 1 0)	α^8	$1 + \alpha^2$
B	(1 0 1 1)	α^{13}	$1 + \alpha^2 + \alpha^3$
C	(1 1 0 0)	α^4	$1 + \alpha$
D	(1 1 0 1)	α^7	$1 + \alpha + \alpha^3$
E	(1 1 1 0)	α^{10}	$1 + \alpha + \alpha^2$
F	(1 1 1 1)	α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$

Table 2: Addition table $\oplus$ of the hexi field S

$\oplus$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

Table 3: Multiplication table $\otimes$ of the hexi field S

$\otimes$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	0	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	0	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	0	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	0	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	0	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	0	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	0	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	0	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	0	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	0	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	0	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	0	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	0	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A

2 = 0010, 3 = 0011, 4 = 0100, 5 = 0101, 6 = 0110, 7 = 0111, 8 = 1000, 9 = 1001, *A* = 1010, *B* = 1011, *C* = 1100, *D* = 1101, *E* = 1110 and *F* = 1111. In short S= {0, 1, …, 9, *A*, …, *F*}. Clearly $(S, \oplus, \otimes)$ is a field of order 16. The operator '$\oplus$' denotes addition XOR modulo 2, is given in Table II and each element is inverse of itself with respect to $\oplus$. The operator '$\otimes$' denotes multiplication modulo $x^4 + x + 1$ is given in Table III. This operator '$\otimes$' multiplication modulo $x^4 + x + 1$ was used in Mini AES and also described in [14]. This field is called as hexi field or $GF(2^4)$, the elements of it and their representations are given in the Table 1.

Let $V^n = \{(x_1 \ldots x_n) \mid x_i \in S;\ 1 \le i \le n\}$ be a *n*-dimensional vector space defined over the hexi field S.

3.2 Hexi Codes

Definition 1: A block code of length *n* with $(2^4)^k$ codewords is called a hexi *(n, k)* block code, denoted by $C_H(n,k)$, if and only if its $(2^4)^k$ codewords form a *k*-dimensional subspace of the vector space V^n of all *n* tuples over the hexi field S.

The method for generating the $C_H(n,k)$ code using the generator matrix *G* is as follows. *G* is given in the following matrix;

$$G = \begin{bmatrix} g_{00} & g_{01} & g_{02} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & g_{12} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,n-1} \end{bmatrix}$$

$g_{i,j} \in \mathsf{S}$; for $0 \le i \le k-1$ and $0 \le j \le n-1$. Consider $u = (u_0\ u_1\ \ldots\ u_{k-1})$, the message to be encoded, the corresponding codeword v is given by $v = u.G$. Every codeword v in $\mathsf{C}_H(n,k)$ is a linear combination of k codewords.

The decoding, error detection and error correction capacity of hexi codes and hexi polynomial codes are discussed in detail. Some definitions are recalled from [12-14] to make this paper a self contained one. The Hamming metric of the hexi code is given in the following:

Definition 2: For any 2 vectors $x = (x_1 \ldots x_n)$ and $y = (y_1 \ldots y_n)$ in V^n, the Hamming distance $d_H(x, y)$ and Hamming weight $w_H(x)$ are defined as follows:

$$d_H(x,y) = |\{x_i : x_i \neq y_i; x_i \in x; y_i \in y\}|$$
$$w_H(x) = |\{x_i : x_i \neq 0; x_i \in x\}|. \quad (2)$$

If C_H is a hexi code, the sum of two codewords is also a codeword in C_H. It follows that $d_H(x, y) = w_H(x, y)$, that is the Hamming distance between two codewords is equal to the Hamming weight of some other codeword.

Definition 3:The minimum distance $d_{H_{min}}$ of a hexi code C_H is defined as

$$d_{H_{min}} = \min_{\substack{x,y \in \mathsf{C}_H \\ x \neq y}} d_H(x,y). \quad (3)$$

The error correcting capacity of hexi code is discussed.

Theorem 1: [12] The number of errors a hexi code can correct is $t = \lfloor (d_{H_{min}} - 1)/2 \rfloor$, and this code can detect l errors where $t + l + 1 \le d_{H_{min}}$ and $l > t$.

Proof. Proof is similar to that of linear block code [17]. Since the shift to hexadecimal system from binary does not alter the calculation of Hamming weight, Hamming distance or $d_{H_{min}}$ and the error correcting capacity remains same.

Correction of errors in any code is a complicated process. There are 2^{4k} error patterns that result in same syndrome and the true error pattern e is just one of them. Determining the true error vector e is not easy. The coset leader method is used for error correction, by making use of the standard array and syndrome decoding described in [17]. The standard array is given by Table 4.

Table 4: Standard array for syndrome decoding

Coset Leaders	*Codewords*	*Syndrome*
$v_1 = 0$	$v_2 \ \cdots \ v_{2^{4k}}$	$s = 0$
e_2	$e_2 + v_2 \ \cdots \ e_2 + v_{2^{4k}}$	$e_2 H^T$
e_3	$e_3 + v_2 \ \cdots \ e_3 + v_{2^{4k}}$	$e_3 H^T$
$\vdots$	$\vdots$	$\vdots$
e_l	$e_l + v_2 \ \cdots \ e_l + v_{2^{4k}}$	$e_l H^T$
$\vdots$	$\vdots$	$\vdots$
$e_{2^{4(n-k)}}$	$e_{2^{4(n-k)}} + v_2 \ \cdots$ $e_{2^{4(n-k)}} + v_{2^{4k}}$	$e_{2^{4(n-k)}} H^T$

Here e_i's are coset leaders, $2 \le i \le 2^{4(n-k)}$; v_j's are non zero codewords, $2 \le j \le 2^{4k}$. The corrected codeword v_j is obtained by using the syndrome of the received codeword r. The coset leader e_i, related to the syndrome, is added to r to obtain the corrected codeword.

3.3 Hexi Polynomial Codes

Hexi polynomial codes are of two types, $x^n + 1$ and $x^n + z$ ($z \in \mathsf{S} \setminus \{0, 1\}$). When $x^n + 1$ is used, it forms a usual cyclic code, $g(x)$ is a polynomial which divides $(x^n + 1)$ and its coefficients are from S. To generate a $\mathsf{C}_H(n, k)$ cyclic hexi code, consider only the polynomial of the form $x^n + 1$. Instead of $x^n + 1$, consider $x^n + z$ ($z \in \mathsf{S} \setminus \{0, 1\}$), then $x^n + z = g(x) \times h(x)$, $g(x)$ and $h(x)$ are polynomials belonging to $\mathsf{S}[x]$.

Let G be the generator matrix associated with generator polynomial $g(x)$. Let H be the parity check matrix associated with the parity check polynomial $h(x)$. The $\mathsf{C}_H(n,k)$ hexi code is not cyclic. Clearly $GH^T = (0)$. If $(x_1 \ldots x_n) \in \mathsf{C}_H(n,k)$, then in general $(x_n\ x_1 \ldots x_{n-1}) \notin \mathsf{C}_H(n,k)$. $\mathsf{C}_H(n,k)$, the hexi polynomial code generated by the hexi polynomial $g(x)$ is defined as follows.

Definition 4: Let $x^n + z \in Si\ [x]$, $z \in \mathsf{S} \setminus \{0, 1\}$, be a hexi polynomial in Si $[x]$. If $x^n + z = g(x)h(x)$ where $g(x)$ is the hexi generator polynomial associated with the generator matrix G and $h(x)$ is the hexi parity check polynomial associated with the parity check matrix H. If $g(x)$ generates a code $\mathsf{C}_H(n,k)$, then $\mathsf{C}_H(n,k)$ is defined as the hexi polynomial code associated with the hexi generator polynomial $g(x)$.

Let $g(x) = g_0 + g_1 x + \ldots + g_m x^m$ be the hexi generator polynomial, then the generator matrix G of the hexi polynomial code $\mathsf{C}_H(n,k)$ is as follows:

$$G = \begin{bmatrix} g_0 & g_1 & \dots & g_m & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{m-1} & g_m & \dots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & g_0 & g_1 & \dots & g_m \end{bmatrix}$$

$g_i \in S$; for $0 \le i \le m$. The rows of the generator matrix G are linearly independent and rank of G is k, the dimension of $C_H(n,k)$, k is the number of message symbols and m is the highest degree of the generator polynomial $g(x)$ and $n = m + k$, is the length of the codeword. A message $u = u_0u_1 \dots u_{k-1}$ can be represented as $u(x) = u_0x^0 + u_1 x^1 + \dots + u_{k-1} x^{k-1}$ and can be encoded as $u(x) \times g(x)$. These hexi polynomial codes can be generated by splitting $x^n + z$ into two polynomials $g(x)$ and $h(x)$. Given n, m and k it is not possible to easily guess which polynomial has been used as the generating polynomial. These codes are not cyclic, making it hard to break. In case of hexi polynomial codes the original message u expressed in polynomial form as $u(x)$ can be encoded as $u(x) \times g(x)$ where $g(x)$ is the generator polynomial. Thus without using the generator matrix G the encoding of the message can be carried out. Like in the case of decoding usual polynomial codes [16], the error detection and error correction of hexi polynomial codes can be done without the creation of standard array for syndrome decoding.

Input: $w(x)$ - Received codeword, $g(x)$ - generator polynomial, $h(x)$ - parity check polynomial
Output: $v(x)$ - Original codeword, m - message
begin
  Compute $w(x)/g(x)$
  if $w(x)\%\ g(x) \neq 0$ **then**
    // Error is present in the $w(x)$
    $y(x) \leftarrow w(x) \times h(x) \bmod (x^n + z)$
    $e(x) \leftarrow y(x)/h(x)$
    $v(x) \leftarrow w(x) - e(x)$
    $m(x) \leftarrow v(x)/g(x)$
  else
    $m(x) \leftarrow w(x)/g(x)$
  end
  Return m
end

Algorithm 1: DECODING Algorithm for decoding and error correction of hexi polynomial codes

Let w be the received codeword, $w(x)$ is divided by the generator polynomial $g(x)$, if the division results with a reminder, it implies that an error has occurred. To perform the error correction, the received codeword $w(x)$ is multiplied with the parity check polynomial $h(x)$. The resultant is then divided by $h(x)$. Since $w = v + e$, where $v(x)$ is the original codeword and $e(x)$ is the error. This division results in error $e(x)$ as the quotient, the original codeword is obtained by $w - e$. The message is later obtained by the division of the original codeword $v(x)$ by $g(x)$. The hexi polynomial code has a error correction capacity of $n - k$ and corrects only errors that occur in parity. The algorithm for error detection and error correction of hexi polynomial codes is given in Algorithm 1.

3.4 Chained Hexi Polynomial Codes

The family of hexi polynomial codes are large enough to avoid an exhaustive attack and each hexi polynomial code $C_{H_i}(n_i, k_i)$ of the family is defined by its generator matrix (respectively a parity check matrix) M_i; $i = 1 \dots l$. The generator matrix G is given by the chaining of the respective generator matrices M_i; $i = 1 \dots l$ of the hexi polynomial codes.

$$G = \begin{bmatrix} M_1 & 0 & 0 & \dots & 0 \\ 0 & M_k & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \dots & M_l \end{bmatrix}$$

In this case the codewords and syndromes are stocked in tables. To decode a word it is compared to the table and the nearest one to the word or the equal syndrome is taken. The decoding can also be done by using Algorithm 1 and the respective generator polynomial of M_i for $i = 1, 2, \dots, l$.

4. Chained Hexi Codes Signature Scheme

The hexi code based digital signature scheme known as Chained Hexi Codes signature scheme (CHC signature scheme) is introduced in this section. The proposed scheme is a variant of the BCHS1 signature scheme. This scheme makes use of a family of hexi codes, it has lesser key size and better security; when compared to the signature scheme based on McEliece cryptosystem and the BCHS1 signature scheme. The set up of the signature scheme is as given below.

Parameters / Setup: The secret parameters are known only to the entity who is signing the document. The generator matrix G is given by the chaining of the respective generator matrices M_i; $i = 1 \dots l$ of the hexi polynomial codes. The resulting matrix G of the chaining of these hexi polynomial codes forms the trapdoor of the signature scheme.

Secret Parameters

1. A family Γ of l hexi polynomial codes. The chained hexi code is defined by its generator matrix G of size $K \times N$, where

$$K = \sum_{i=1}^{l} k_i \text{ and } N = \sum_{i=1}^{l} n_i;$$

n_i is the length and k_i is the dimension of the i^{th} code.

2. **P** is a secret $N \times N$ permutation matrix.
3. **S** is a secret $K \times K$ hexi invertible matrix.

Public Parameters

The public key

$$G' = S \times G \times P$$

G' is permuted and scrambled $K \times N$ generator matrix.

Signing Algorithm:

The document M that needs to be signed is of the length $4N$ bits is converted to hexi notation of length N nibbles. The message $h(\mathsf{M})$ is permuted using P^{-1}, the inverse of the permuted matrix P. Then the message M_p is split into word x_i's of length n_i according to the i[th] code's length. These x_i's are decoded using the table or the decoding algorithms. These a_i's are trimmed to the dimension of i^{th} code, i.e., k_i. The a_i's are concatenated into a of length K. The signature y of the document is obtained by multiplying a with S^{-1}, the inverse of the invertible matrix S. The signing algorithm of the signature scheme is given in Algorithm 2.

Input: $\mathcal{M}$ - Document, $\mathbf{P}^{-1}$ - Inverse of Permutation matrix $\mathbf{P}$, $\mathbf{S}^{-1}$ - Inverse of invertible matrix $\mathbf{S}$,
Output: y - Signature
begin
  Convert the first binary sequence of document $\mathcal{M}$ into hexi notation of length N
  $M_p \leftarrow h(\mathcal{M}) \times \mathbf{P}^{-1}$
  for $i \leftarrow 1$ *to* l **do**
    Split M_p into x_i of length n_i according to i^{th} code's length
    Decode x_i into a_i
    Trim a_i to length k_i according to code dimension
  end
  Concatenate a_i's into a, it has length K
  $y \leftarrow a \times \mathbf{S}^{-1}$
  Return y
end

Algorithm 2: SIGNING Algorithm for signing a document

Verification Algorithm:

Given the signature y, the public key G' and the document M. Here C is the sum of error correcting capacity c_j's of the codes used.

$$C = \sum_{i=1}^{l} c_i$$

The codeword b is obtained by multiplying the signature y with the public key G. The Hamming distance d_H between the codeword b and the document's message $h(\mathsf{M})$ is calculated. If it is less than the sum of error correcting capacities, then the signature is valid and it is accepted, else the signature is not valid and it is rejected. The verification algorithm of the signature scheme is given in Algorithm 3.

Input: y - Signature, $\mathcal{M}$ - Document, C - Sum of error correcting capacities, $\mathbf{G}'$ - Public key
Output: Validity of signature
begin
  $b \leftarrow y \times G'$
  Compute the hexi Hamming distance d_H between b and $h(\mathcal{M})$
  if $d_H(b, h(\mathcal{M})) < C$ **then**
    // Signature valid
  else
    // Signature not valid
  end
  Return
end

Algorithm 3: VERIFICATION Algorithm for verification of signature

Implementation:

In the implementation of the CHC signature scheme using hexi polynomial codes, these are the following ways in which a family of hexi polynomial codes can be chained together to produce the generator matrix G. A comparison of these cases is given in Table 5.

Case 1: A family based on 5 hexi polynomial codes of length 50 each, these codes can be of different dimensions like $\mathcal{C}_H$ (50, 25, 25), $\mathcal{C}_H$ (50, 20, 30), $\mathcal{C}_H$ (50, 30, 20), $\mathcal{C}_H$ (50, 40, 10) and $\mathcal{C}_H$ (50, 24, 26). The dimensions can be selected according to ones wishes. Here three such cases are handled i.e., Case 1a with $\mathcal{C}_H$ (50, 20, 30), Case 1b with $\mathcal{C}_H$ (50, 30, 20) and Case 1c with $\mathcal{C}_H$ (50, 25, 25).

Case 2: A family based on 3 hexi polynomial codes, 2 codes of length 100 each and one code of length 50, these codes can be of different dimensions like $\mathcal{C}_H$ (100, 50, 50), $\mathcal{C}_H$ (100, 60, 40), $\mathcal{C}_H$ (100, 80, 20) and so on. The code of length 50 can be of any of $\mathcal{C}_H$ (50, 25, 25), $\mathcal{C}_H$ (50, 20, 30), $\mathcal{C}_H$ (50, 30, 20), $\mathcal{C}_H$ (50, 40, 10) or $\mathcal{C}_H$ (50, 24, 26).

Case 3: A family based on 10 hexi polynomial codes of length 25 each, These codes can be different dimensions like $\mathcal{C}_H$ (25, 15, 10), $\mathcal{C}_H$ (25, 10, 15), $\mathcal{C}_H$ (25, 12, 13), $\mathcal{C}_H$ (25, 20, 5) and so on.

Case 4: A family based on 11 hexi polynomial codes, 10 codes of length 20 each and one code of length 50. These codes can be different dimensions like $\mathcal{C}_H$ (20, 10, 10), $\mathcal{C}_H$ (20, 15, 5), $\mathcal{C}_H$ (20, 16, 14) and so on. The codes of length 50 can be of any of $\mathcal{C}_H$ (50, 25, 25), $\mathcal{C}_H$ (50, 20, 30), $\mathcal{C}_H$ (50, 30, 20), $\mathcal{C}_H$ (50, 40, 10), $\mathcal{C}_H$ (50, 24, 26) and so on.

Case 5: A family based on several hexi polynomial codes of different lengths. These codes can be different dimensions and of different lengths. These codes can be of length 100, 50, 25, 20, 10 or 5. They can be of any dimensions given in the before cases. These codes can be different dimensions like $\mathcal{C}_H$ (20, 10, 10), $\mathcal{C}_H$ (20, 15, 5), $\mathcal{C}_H$ (20, 16, 14) and so on. These codes of length 10 and 5 like $\mathcal{C}_H$ (10, 5, 5), $\mathcal{C}_H$ (10, 7, 3), $\mathcal{C}_H$ (5, 3, 2) can also be used.

Table 5: Comparison of CHC signature schemes with different dimensions

Signature	*N*	*K*	*Code dimensions*	*no*
Case 1a:	250	150	50, 20,30	5
Case 1b:	250	100	50, 30,20	5
Case 1c:	250	125	50, 25, 25	5
Case 2	250	125	100, 50,50 50, 25,25	2 1
Case 3	250	130	25, 12,13	10
Case 4	250	125	50, 25,25 20, 10, 10	1 10

Case 5:	250	127	100, 50, 50 50, 25, 25 25,12, 13 20, 10, 10 5, 2,3	1 1 3 1 1

Comparison with other signature schemes

The CHC signature scheme is compared with the signature schemes like the signature scheme based on McEliece cryptosystem and the BCHS1 signature scheme. It is evident that the CHC signature scheme has smaller public key size and also a smaller signature size. A comparison of the best cases of the CHC signature schemes with the other signature schemes is given in Table 6.

Table 6: Comparison of the CHC signature scheme with other signature schemes

Signature	*McEliece*	*BCHS1*	*CHC*		
			Case 1a	Case 1b	Case 1c
Data Size	65536	1000	250	250	250
Signature length	65392	500	150	100	125
Key length	4292069312	500000	37500	25000	31250

When compared with the BCHS1 signature scheme the advantages of the CHC signature scheme are as follows:

- The signature length is 3times smaller for Case 1a, 5 times smaller for Case 1b, and 4 times smaller for Case 1c.
- The public key size is 13 times smaller for Case 1a, 20 times smaller for Case 1b, and 16 times smaller for Case 1c,
- The working of this scheme is faster because it works with a smaller key size.

The variant of the CHC signature scheme which is introduced in the next section is both space and time saving.

5. A Variant of the CHC Signature Scheme

Given the fact that the CHC signature scheme makes use of polynomial codes, the decoding of the codes can be done using Algorithm 5. In that case, the time complexity can be reduced significantly. That is the decoding of the message can be done in time complexity of $(n-k)lg(n-k)$, if $n = \Theta(n-k)$. Then there will be no necessity to have a look-up table with the codewords and the syndromes. Only some cases of CHC signature scheme can be considered. Case 1c and Case 2 will work perfectly fine with this decoding algorithm as the condition $n = \Theta(n-k)$ is satisfied. Then there will be no necessity to have a stocked up table of 2^k codewords and syndromes. To find the nearest codeword from the table, atleast 2^k comparisons of length n is necessary. The time complexity of 2^k comparisons of length n is more than $(n-k)lg(n-k)$. Thus this variant will result in lesser space and time being utilized for decoding.

6. Security of the CHC Signature Scheme

Decoding Attack: The signature scheme depends on the well known NP complete problem. The most efficient algorithms in this case are based on the information set decoding. An analysis was done by Stern [22] and several others. The analysis by Canteaut and Chabaud [5] which is the most efficient one is considered here. Given already for the BCHS1 signature scheme [10]. Consider a code of length n, of dimension k and of correction capacity t, if one uses information set decoding, one chooses a random set of k columns, an error is decodable when its support doesn't meet the k random columns. The probability for an error to be decodable is

$$P_{dec} = \frac{C_{n-k}^{t}}{C_{n}^{t}}$$

Then the estimated work factor WF to find a word of weight t can be estimated as follows

$$WF = \frac{P(k)}{P_{dec}}$$

where $P(k)$ corresponds to the cost of Gaussian elimination, $P(k)$ can be first thought as a cost in $O(k^3)$. It is given that the work factor for the BCHS1 signature scheme in 2^{88}. When the CHC signature scheme is considered, it is clear that in all cases $t = n - k$ and hence the probability for an error to be decodable is

$$P_{dec} = \frac{C_{n-k}^{t}}{C_{n}^{t}} = \frac{C_{t}^{t}}{C_{n}^{t}} = \frac{1}{C_{n}^{t}}$$

Then the estimated work factor WF to find a word of weight t can be estimated as

$$WF = \frac{P(k)}{P_{dec}}$$

$$WF = \frac{P(k)}{\frac{1}{C_{n}^{t}}} = P(k) \times C_{n}^{t}$$

where $P(k)$ corresponds to the cost of Gaussian elimination, $P(k)$ can be first thought as a cost in $O(k^3)$. The calculated work factor for the CHC signature scheme is greater than 2^{100}. The gap between this calculated work factor and the workfactor calculated from [9] is very small. It clearly shows that the signature scheme is more secure.

The codes used are neither quasi cyclic nor dyadic, hence the attacks in [8] can not be carried out on these codes.

Information Set Decoding Attack:

A generic decoding method, the information set decoding attack is a top threat against the original McEliece cryptosystem. Information set decoding depends on syndrome decoding and systematic form of the generator matrix G to break the cryptosystem. But this newly introduced hexi McEliece cryptosystem does not depend on syndrome decoding. The generator matrix G of the hexi polynomial code that is used in this cryptosystem is not given in its systematic form, hence information set decoding attack is not easily carried out on the cryptosystem.

Generalized Birthday Algorithm:
The generalised birthday algorithm is not as efficient as the information set decoding attack on code based cryptosystems. The CFS signature scheme was attacked using this method. The method makes use of very large lists. For a sufficiently large n, this cryptosystem is secure.

Structural Attack:
The complexity of structural attack on the proposed signature scheme and its public key can be measured by searching exhaustively for all possible combination of permutation ($N!$), secret codes and invertible matrix (16^K). The security of this scheme is increased due to the fact that the secret code is formed using several different hexi polynomial codes.

7. Conclusion and Further Direction

A signature scheme known as Chained Hexi Codes signature scheme (CHC signature scheme) is introduced in this paper. The proposed scheme depends on the well known Syndrome Decoding problem (SD problem), is a variant of the BCHS1 signature scheme. The scheme is based on the chaining of the generator matrix of several hexi polynomial codes of different dimensions. The major advantage of this scheme is the massive decrease in the public key size and there is also a good decrease in the signature size. Due to the small public key size, the decoding, signing and verification can be done faster. As shown in Table 7, the CHC signature scheme has smaller key and signature size, it is also faster and secure when compared to the signature scheme based on McEliece cryptosystem an BCHS1. The variant of the CHC signature scheme proposed in this paper, avoids the necessity to maintain syndrome-codeword look up tables. The decoding can be done in $(n-k)lg(n-k)$ times. This variant is faster and it is also secure.

Further Direction: A signature scheme based on the BCHS2 signature scheme using the parity check matrices of different hexi polynomial codes can be proposed and its security analysed.

References

[1] Alabbadi, M., and Wicker, S.B.: A digital signature scheme based on linear error-correcting block codes. In: Advances in cryptologyASIACRYPT '94. Proceedings of the Fourth International Conference held at the University of Wollongong, pp. 238–248 (1994)

[2] Alabbadi, M., and Wicker, S.B.: Security of xinmei digital signature scheme. Electronics Letters 28(00), 890–891 (1992)

[3] Becker, A., Joux, A., May, A., Meurer, A.: Decoding random binary linear codes in 2n/20 : How 1 + 1 = 0 improves information set decoding. In: Pointcheval, D., Johansson,T. (Eds.), EUROCRYPT 2012. In: Lect. Notes Comput. Sci., vol. 7237. Springer-Verlag,Berlin, Heidelberg, pp. 520536, 2012.

[4] Bernstein, D.J., Lange, T., Peters, C.: Smaller decoding exponents: Ball-collision decoding. In: Advances in Cryptology CRYPTO 2011. In: Lect. Notes Comput. Sci., vol.6841. Springer-Verlag, Berlin, Heidelberg, pp. 743760, 2011.

[5] Canteaut, A., Chabaud, F.: Improvements of the attacks on cryptosystems based on error-correcting codes (1995)

[6] Cayrel, P.L., Otmani, A., and Vergnaud, D.: On kabatianskii-krouk-smeets signatures. In: International Workshop on the Arithmetic of Finite Fields, WAIFI 2007, LNCS 4547, pp. 237–251(2007)

[7] Courtois, N., Finiasz, M., and Sendrier., N.: How to achieve a McEliece based digital signature scheme. Advances in Cryptology - ASIACRYPT 2001 2248(00), 157–174 (2001)

[8] Faugre, J.C., Otmani, A., Perret, L., Tillich, J.P.: Algebraic cryptanalysis of McEliece variants with compact keys. In: Gilbert, H. (Ed.), EUROCRYPT 2010. In: Lect. Notes Comput. Sci., vol. 6110. Springer-Verlag, Berlin, Heidelberg, pp. 279298, 2010.

[9] Finiasz, M. and Sendrier, N.: Security bounds for the design of code-based cryptosystems. ASIACRYPT 2009, Lect. Notes Comput. Sci., vol. 5912, pp. 88–105, 2009.

[10] Hamdi, O., Harari, S., Bouallegue, A.: Secure and fast digital signatures using bch codes.International Journal of Computer Science and Networking Security 6, 220–227 (2006)

[11] Harn, L. and Wang, D.C.: Cryptanalysis and modification of digital signature scheme based on error-correcting codes. Electronics Letters 28(00), 157–159 (1992)

[12] Ilanthenral, K., and Easwarakumar, K.S.: Design of hexi cipher. Journal of Applied Mathematics and Information Sciences 7(5), 2007–2021 (2013)

[13] Ilanthenral, K., and Easwarakumar, K.S.: Hexi McEliece Public Key Cryptosystem. Journal of Applied Mathematics and Information Sciences, 8(5), 2595-2603 (2014).

[14] Ilanthenral, K., and Easwarakumar, K.S.: Hexi code based Identification Scheme, In Proceedings of the SAPIENCE'14 International conference on Security and Authentication, pp. 38-43, (2014).

[15] Kabatianskii, G., Krouk, E., and Smeets, B.,: A digital signature scheme based on random error-correcting codes. In: Cryptography and coding. Proceedings of the 6th IMA International Conference held at the Royal Agricultural College, pp. 161–177 (1997)

[16] Lidl, R., and Pliz, G.: Applied Abstract Algebra. Springer Verlag (1984)

[17] Lin, S., and Costello, D.J.: Error Control Coding, second edn. Pearson (2005)
[18] May, A., Meurer, A., Thomae, E.: Decoding random linear codes in O(20.054n). In: Lee, D., Wang, X. (Eds.), ASIACRYPT. In: Lect. Notes Comput. Sci., vol. 7073.Springer-Verlag, Berlin, Heidelberg, pp. 107124, 2011.
[19] McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. Jet Propulsion Laboratory DSN Progress Report 42-44(00), 114–116 (1978)
[20] Otmani, A., and Tillich, J.: An efficient attack on all concrete KKS proposals. In: Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, LNCS 7071 (2011)
[21] Stern, J.: A new identification scheme based on syndrome decoding. In: Advances in CryptologyCRYPTO '93. 13th annual international cryptology conference, LNCS 773, p.1321 (1993)
[22] Stern, J.: Can one design a signature scheme based on error correcting codes. LNCS -ASIACRYPT 1994 917(00), 424–426 (1995)
[23] Van Tilburg, J.: Cryptanalysis of the alabbadi-wicker digital signature scheme. In: Proceedings of fourteenth symposium on information theory in the Benelux, pp. 114–119 (1993)
[24] Wang, X.: Digital signature scheme based on error-correcting codes. Electronics Letters 26(00), 898–899 (1990).

K. Ilanthenral is currently pursing her PhD under the guidance of Prof. K. S. Easwarakumar at Department of Computer Science and Engineering at Anna University, Chennai. She received her B.Sc. in Mathematics from Madras University, Chennai, Master of Computer Science and Application from Anna University, Chennai. Her research interests include Cryptography and Coding Theory.

K. S. Easwarakumar is a Professor at the Department of Computer Science and Engineering at Anna University, Chennai. He received his M.Tech in Computer and Information Sciences from Cochin University of Science and Technology, Cochin and Ph.D in Computer Science and Engineering from Indian Institute of Technology, Madras. His research interests include parallel and distributed computing, Data Structures and Algorithms, Graph Algorithms, Parallel Algorithms, Computational Geometry, Theoretical Computer Science and Molecular computing.