Flow Secure Message in Parity Matrix

[1]P.Ramya, [2]P.Sandhya, [3]R.Varun

[1,2,3]Assistant Professor, Electronics and Communication Engineering
Aksheyaa College of Engineering, Kancheepuram,India
[1]*ramya1401@gmail.com;* [2]*sandynakshatra@gmail.com;* [3]*varuntr88@gmail.com*

***Abstract*—** The goal of security is confidential ,integrity and availability to decrypt the messages.In recent years,many researchers has said about how to secure high-value data on hard disk.proposed system explains about the high grade cryptosystem one which even an attacker possessing both a copy of your encryption engine and knowledge of your operation.

Keywords- *Encryption engine,Keying information and operational procedure for their secure use.*

*****

I. INTRODUCTION

The McEliece type cryptosystem is a public key cryptosystem proposed by Celiac in 1978 built over rational goppa codes. It is crucial in this cryptosystem to keep secret key for the security in a system. The two basic attacks known against McEliece type cryptosystems: Decoding attacks and direct attacks on private key. A dual variant of the system proposed by Niederreiter can provide slightly improved efficiency with equivalent security. This dual system can additionally be used to construct a digital signature scheme. Recovering the secret scrambler and secret permutation is different from the code equivalence problem. In McEliece finds a transformer between two equivalent codes. The Niederreiter decides whether 2 linear codes are equivalent.

A Goppa code is a new class of linear non-cyclic error correcting code. The properties of goppa codes are:

(1) There exists Q-ary goppa codes with lengths and redundancies comparable to BCH codes for the same redundancy, the goppa codes is typically one digit longer

(2) All goppa codes have an algebraic decoding algorithm which will correct upto a certain number of errors comparable to half the designed distance to BCH codes.

(3) For binary Goppa codes the algebraic decoding algorithm assumes a special form.

(4) Long goppa codes have actual minimum distances much greater than twice the number of errors.

II. LITERATURE SURVEY

[1]Daniel J. Bernstein is said that new parameters for the McEliece and Niederreiter cryptosystems achieving standard levels of security against all known attacks. The new parameters take account of our improved attack; the recent introduction of list decoding for binary Goppa codes; and the possibility of choosing code lengths that are not a power of 2. We achieve considerably smaller public key sizes than previous parameter choices for the same level of security.

[2] A. Schmid to provide detailed insight into the state of art of cryptanalysis of the McEliece cryptosystem and the effect on different cryptographic applications. We conclude, that for code based cryptography a public key of 88KB offers sufficient security for encryption, while we need a public key of at least 597KB for secure signing.

[5]Elwyn r. Berlekamp is said that Goppa codes have actual minimum distances much greater than twice the number of errors, which are guaranteed to be correctable by the algebraic decoding algorithm. In fact, long irreducible Goppa codes asymptotically meet the Gilbert bound. although at any Fixed rate the lower bound on the distance of these new codes is asymptotically weaker than that for comparable BCH codes.

III. EXISTING SYSTEM

The natural reduction of McEliece to a hidden subgroup problem yields negligible information about the secret key. Thus they rule out the direct analogue of the quantum attack that breaks, for example, RSA. Of course, our results do not rule out other quantum (or classical) attacks. Neither do they establish that a quantum algorithm for the Celiac cryptosystem would violate a natural hardness assumption, as do recent lattice cryptosystem constructions whose hardness is based on the Learning With Errors problem.

IV. PROPOSED SYSTEM OVERCOME EXISTING SYSTEM

In the existing system, the private key subjects to quantum attacks. This system uses rational goppa codes. The syndrome acts as cipher text and message acts as error pattern. The key generation centre could decrypt any messages addressed to specific users by generating their private keys. This is not suitable for data sharing scenarios where the data owner would like to make their private data only accessible to designated users. The efficiency of security on secrete key is very low rated on the system. So to overcome this disadvantage ,moving on to the high rated cryptosystem which is the dual variant of the system with improved efficiency of equivalent security which subjected to two basic attacks on private key

(i) Decoding (ii) Direct attack

This system uses classical goppa codes. It is additional to construct digital signature scheme. Key idea: Flow secure message is parity matrix in cryptosystem.

The private key of the user consists of 3 matrices: a k*n matrix M over a finite field F_q & n*n permutation matrix P. In this, M is the generator matrix of a q ary [n, k] linear code of length n and M is the parity check matrix of a q ary linear code of length n.

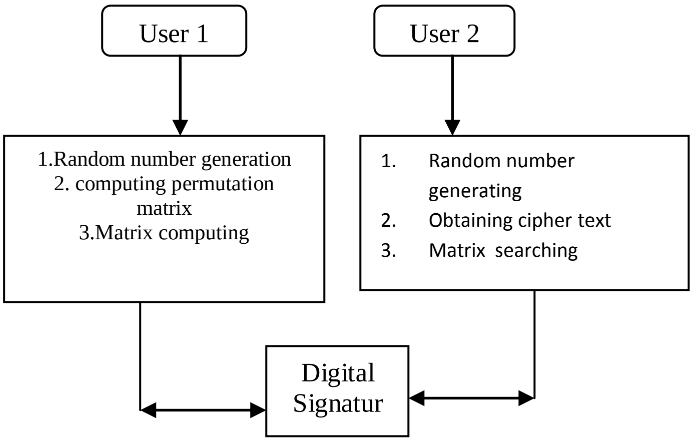

Figure 1: Block diagram for proposed system

A. Key Generation

1. Selecting binary (n,k) linear goppa code G with ‘t’ errors. Efficient decoding algorithm with nonce value,V
2. Generates (n,k)*n parity check matrix H for code,G.
3. Selects binary non-singular matrix,S=(n,k)*(n,k)
4. Permutation matrix,P=(n*n)
5. Computes (n-k)*n matrix , H^{Pub} =SHPV
6. Public Key (H^{Pub} ,t) and private key (S,H,P)

B. Encryption

1. Encodes message ‘m’ as binary string of length ‘n’ and weight atmost ‘t’ .
2. Cipher text, C=H^{PUB} m^T

C. Decryption

1. Upon receipt of, C= H^{pub} m^T
2. Computes S^{-1}C =HPm^T
3. Applies syndrome decoding algorithm for G to recover Pm^T
4. Computes message, m via mT=P^{-1}Pm^T

D. Sandwidch the message with signature

1. M – signing of length N
2. Compute z=h(m)
3. Calculating X= Z.P^{-1}
4. Split X in (X1,X2,……,Xi) ;Xi =1,2,….l
5. Decode a1=deck(Xi),i=1,2…..l

   A=(a1,a2,a3….ai)

   Y=a.S^{-1} ; Y is signature.
6. Hash the document‘d’ to be signed.
7. Decrypt this hash value.
8. Append the decrypt message to the document as a signature.

V. ATTACKS

C. Side channel attack

When two user are connected to a computer over secure shell (SSH).All the commands and response are encrypted and authenticated. This results in eavesdropper cannot figure out the process happening in the remote system.

VI. CONCLUSION

A new way to secure the message in parity matrix by use of classical goppa codes used in the dual variant of the system with improved efficiency of equivalent security and additionally to construct the digital signature scheme was implemented and message a secured in very effective way in parity matrix.

REFERENCES

[1] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Attacking and defending the McEliece cryptosystem.In PQCrypto ’08: Proceedings of the 2nd International Workshop on Post-Quantum Cryptography, pages 31–46, Berlin, Heidelberg, 2008. Springer-Verlag. ISBN 978-3-540- 88402-6.

[2] D. Engelbert, R. Overbeck, and A. Schmidt. A summary of McEliece-type cryptosystems and theirsecurity. J. Math. Crypt., 1:151199, 2007

[3] Sean Hallgren, Cristopher Moore, Martin R¨otteler, Alexander Russell, and Pranab Sen. Limitations of quantum coset states for graph isomorphism. In STOC ’06: Proceedings of the thirty-eighth annual ACM symposium on Theory of computing, pages 604–617, 2006.

[4] V. M. Sidelnikov and S. O. Shestakov. On insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Mathematics and Applications, 2(4):439–444, 1992.

[5] Elwyn r. Berlekamp goppa codes, ieee transactions on information theory, vol. It-19, no. 5, september 1973.