Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India
सत्यमेव जयते

IEEE COMPUTER SOCIETY Bangalore Chapter
IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

5th INTERNATIONAL CONFERENCE ON

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS (PKIA 2024)

SEPTEMBER 5-6th, 2024

On the Comparative Study of Recent Information Set Decoding (ISD) attacks for QC-LDPC Code-based McEliece Cryptosystem

Sourabh Biswas, Dept. of Mathematics, IIIT Kalyani,
Indivar Gupta, SAG, DRDO,
Debasish Bera, Dept. of Comp. Science, IIIT Kalyani

Introduction

- PQC (Post Quantum Cryptography) algorithms are designed to be resistant to attacks by quantum computers. Code-based Cryptography is one of the main candidates in the field PQC. LEDAcrypt [3] has been selected NIST PQC competetions at second round.

ISD (Information Set Decoding) is a cryptanalytic method used in Code-based cryptography to attack, first introcued by Prange. After that Stern's ISD (ISD_{Stern}) [11], FS's ISD (ISD_{FS}) [4], and MMT's ISD (ISD_{MMT}) [6] draw a significant attentions.

- LEDAcrypt [3] is a public-key cryptographic scheme. It has the components, Key-Generation, Encryption, and Decryption.
- A Codeword Finding Problem (CFP) is defined as given a parity check matrix 'H', and codeword weight 'w', find 'c' such that $Hc^t = 0$ holds, where weight of 'c'=w.

Introduction (Contd..)

- **A detailed comparative study of ISD_{Stern} and the recent two ISD algorithms ISD_{FS} and ISD_{MMT} concerning LEDAcrypt PQC (Post-Quantum Cryptography) system.**
- **In this regard, a detailed cost calculation for partial RREF (Row Reduced Echelon Form), which is an important tool in ISD, is performed.**
- **The parameter table of LEDAcrypt (see table-1 of [3]) from the original document has been modified, resulting in Table- [3]. This table includes the optimal values for parameters p (partical error/codeword weight) and l (number of zeros in the codeword/number of zero rows in the permuted matrix) to obtain the minimum ISD costs of the given algorithms [11],[4],[6],[5]. These optimizations are provided for different sets of n,k, and t' values, corresponding to the original table-1 of [3]).**

Literature Review

- We have studied Key-Generation, Encryption, and Decryption algorithms of LEDAcrypt.
- We have studied key recovery attack of LEDAcrypt by solving codeword finding problem. This method [3] can be done by finding low weight codewords in the QC-LDPC code.
- We have studied Prange's [8], Lee-Brickell's [9], Leon's [10], Stern's [11], FS's [4], and MMT's [6] ISD algorithm.
- Our previous paper [1] gave an overiew of some ISD algorithms related to attack of LEDAcrypt.

Stern's ISD

- In this ISD_{Stern} algorithm [11],[5] meet-in-the-middle strategy is used to find codeword vector. Here permuted parity check matrix after rref computation has the form given as,

$$\hat{\mathbf{H}} = \left[\mathbf{I}_{(n-k-m)} \mid \mathbf{X}_{(n-k-m)\times(k+m)} \mid \mathbf{Y}_{(n-k-m)\times(k+m)}\right]. \quad (1)$$

- Here randomly 'l' positions are choosen among (n-k) rows, let the set of positions be Rw.
- Do sum of the columns of A matrix and do the same for matrix B. Store all possible A matrices then select pair (A, B) such that sum of the columns of A and B are same at those positions in Rw.
- Then check weight of the sum of the columns of A and B. If the weight of sum is (w-p) we will get solution.

FS's ISD

In this ISD_{FS} algorithm [4],[5] meet-in-the-middle strategy is used to find codeword vector. This algorithm improves ISD_{Stern} by introducing partial RREF computation instead of doing full RREF. Here permuted parity check matrix after partial RREF computation has the form given as,

$$\hat{\mathbf{H}} = \begin{bmatrix} \mathbf{I}_{(n-k-l)} & \mathbf{X}'_{(n-k-l)\times(k+l)} \\ \mathbf{0}_{l\times(n-k-l)} & \mathbf{X}''_{l\times(k+l)} \end{bmatrix}. \quad (2)$$

- Here partial RREF computation is used instead of doing full R REF computaions.
- Here, 'p/2' indices are choosen among '(k+l)/2' co-ordinates of X' submatrix in equation (2)
-

MMT’s ISD

In this ISD_{MMT} algorithm [6],[5] representation technique [12] is used and solve subset sum problem to solve CFP. Here permuted parity check matrix after RREF computation has the form given as

$$\hat{\mathbf{H}} = \begin{bmatrix} \mathbf{I}_{(n-k-l)} & \mathbf{X}'_{(n-k-l)\times(k+l)} \\ \mathbf{0}_{l_1\times(n-k-l)} & \mathbf{X}''_{l_1\times(k+l)} \\ \mathbf{0}_{l_2\times(n-k-l)} & \mathbf{X}'''_{l_2\times(k+l)} \end{bmatrix} \quad (3)$$

- **Here partial RREF computation is used instead of doing full R REFcomputaions.**
- **Improves ISD_{FS} algorithm by using representation techniques used in solving subset-sum problem.**

Optimal values of Parameters (‘p’ and ‘l’) obtained for Stern, FS, and MMT’s ISD w.r.t LEDAcrypt parameters

n	k	t’=2v	A(p, l), Stern’s ISD parameters	B(p, l), FS’s ISD parameters	C(p, l), MMT’s ISD parameters
46742	23371	142	(6,51)	(6,51)	(15,75)
48201	32134	158	(6,51)	(6,51)	(35,79)
53588	40191	166	(6,52)	(6,52)	(51,81)
81574	40787	206	(6,54)	(6,54)	(19,105)
85233	56822	234	(6,55)	(6,55)	(51,109)
91604	68703	246	(6,55)	(6,55)	(75,137)
123434	61717	274	(6,56)	(6,56)	(27,135)
128031	85354	306	(6,57)	(6,57)	(63,165)
142028	106521	326	(6,58)	(6,57)	(99,195)

References

[1] Guha, Dibyasree, Debasish Bera, and Sourabh Biswas. "Security Analysis of LDPC Code-Based Encryption." 2022 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA). IEEE, 2022.

[2] McEliece, Robert J. "A public-key cryptosystem based on algebraic." Coding Thv 4244 (1978): 114-116.

[3] Baldi, Marco, et al. "LEDAcrypt: Low-density parity-check code-based cryptographic systems." NIST round 2 (2020).

[4] Finiasz, Matthieu, and Nicolas Sendrier. ``Security bounds for the design of code-based cryptosystems.'' Advances in Cryptology- ASIACRYPT 2009: 15th International Conferencce on the theory and application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings 15. Springer Berlin Heidelberg, 2009.

References (Contd..)

[5] Baldi, Marco, et al. "A finite regime analysis of information set decoding algorithms." Algorithms 12.10 (2019): 209.

[6] May, Alexander, Alexander Meurer, and Enrico Thomae. ``Decoding random linear codes in $O(2^{0.054n})$''. Advances in Cryptology- ASIACRYPT 2011: 17th International Conference on the theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings 17. Springer Berlin Heidelberg, 2011.

[7] Wagner, David. "A generalized birthday problem." Advances in Cryptology-CRYPTO 2002: 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18-22, 2002 Proceedings 22. Springer Berlin Heidelberg, 2002.

[8] Prange, Eugene. "The use of information sets in decoding cyclic codes." IRE Transactions on Information Theory 8.5 (1962): 5-9.

References (Contd..)

[9] Lee, Pil Joong, and Ernest F. Brickell. ``An observation on the security of McEliece's public-key cryptosystem.'' Advances in Cryptology-EUROCRYPT'88: Workshop on the Theory and Application of Cryptographic Techniques Davos, Switzerland, May 25-27, Proceedings 7. Springer Berlin Heildelberg, 1988.

[10] Leon, Jeffrey S. "A probabilistic algorithm for computing minimum weights of large error-correcting codes." IEEE Transactions on Information Theory 34.5 (1988): 1354-1359.

[11] Stern, Jacques. "A method for finding codewords of small weight." Coding theory and applications 388 (1989): 106-113.

[12] Howgrave-Graham, Nick, and Antoine Joux. "New generic algorithms for hard knapsacks." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

THANK YOU