Format Preserving Encryption: A Survey

Zalak Bhatt, Vinit Gupta
Department of Computer Engineering,
Hasmukh Goswami College of Engineering, Vahelal.
Gujarat Technological University

***Abstract*– Cryptography is a technique used to transmit data in a secured way using encryption and decryption. Encryption is the process of converting information from its original form (plain text) into an unintelligible form (cipher text).In Cryptography many traditional algorithms introduced to provide security to sensitive data but encrypted data changes its length and format. There is a requirement to change existing database schema. Format Preserving Encryption mechanism there is no need to change database schema. It is a way to encrypt data such that the cipher text has the same length and format as the plaintext. This paper describes various techniques of FPE, Its pros and cons and survey done on these techniques. Finally it concludes by comparison of all techniques.**

***Index Terms*– Format Preserving Encryption (FPE), Credit Card Numbers (CCN), Social Security Numbers (SSN).**

I. INTRODUCTION

Now a days, as more and more applications take shape to facilitate online shopping, money transfer and small scale enterprises are moving to third party services to store their data and associated applications, there arises a need to secure online transactions, and a need for protect data from anomaly administrators and malicious attackers.

Encrypting Credit card numbers (CCN), Social Security Numbers (SSN) in huge legacy databases has become a very complex task if it has the same problem to change existing database schema. There are many challenges First, the cost of modifying existing databases. Second, sensitive information like SSN and CCN are used as a primary key in database changes in this field may require significant schema changes. Third, applications are also related to specific data format, will require a format change. Format preserving encryption (FPE) is a solution to the above problems.

To meet these demands, Traditional as well as new and improved cryptographic methods have been constructed to achieve greater security. But, a major problem in adopting these methods is the requirement to change the existing databases to incorporate the encrypted data. This problem can be handled with a Format Preserving Encryption. With FPE, encrypted data will gain its original format.

By maintaining the format of the data being encrypted, database schema changes are zero and application changes minimized in many cases 1-2 lines of code in total. This enables us to secure our data with minimum effort and cost.FPE can be used to encrypt such sensitive information like credit card numbers and social security number.

There are different techniques applied for the Format Preserving Encryption like Prefix cipher, Cycle walking, Feistel mechanism, Feistel modes, Rank then encipher, different modes of various block cipher (AES, Blowfish, DES, 3DES) like Electronic codebook mode, Cipher block chaining mode, Cipher feedback mode, Output feedback mode and Counter mode.

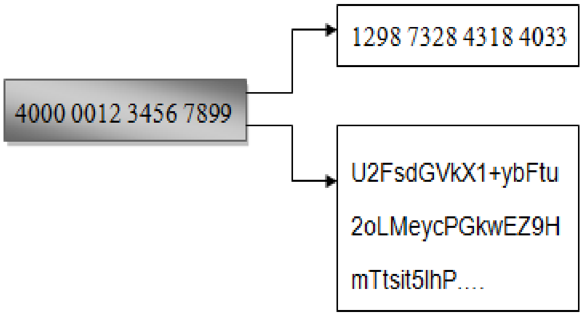

Figure: 1 Credit card number with and without FPE

II. THEORETICAL BACKGROUND

There are different techniques previously used for the Format Preserving Encryption like Prefix cipher, Cycle walking, Feistel mechanism, Feistel modes, Rank then encipher, different modes of various block cipher.

2.1 Prefix cipher

To create an FPE algorithm using prefix cipher on {0,...,*N*-1} is to assign a pseudorandom weight to each integer, then sort by weight. The weights are defined by applying an existing block cipher to each integer. Thus, to create a FPE on the domain {0,1,2,3}, given a key *K* apply AES(*K*) to each integer, giving, for example,

weight(0) = 0x56c644080098fc5570f2b329323dbf62

weight(1) = 0x08ee98c0d05e3dad3eb3d6236f23e7b7

weight(2) = 0x47d2e1bf72264fa01fb274465e56ba20

weight(0) = 0x077de40941c93774857961a8a772650d
Sorting [0,1,2,3] by weight [3,1,2,0], so your cipher is
F(0) = 3
F(1) = 1
F(2) = 2
F(0) = 0

This method is only useful for small values of *N*. For larger values, the size of the lookup table and the required number of encryptions to initialize the table gets too big to be practical.

2.2 Cycle Walking

If we have a set *M* of allowed values within the domain of a pseudorandom permutation *P* (for example *P* can be a block cipher like AES), we can create an FPE algorithm from the block cipher by repeatedly applying the block cipher until the result is one of the allowed values (within *M*).

The recursion is guaranteed to terminate. (Because *P* is one-to-one and the domain is finite, repeated application of *P* forms a cycle, so starting with a point in *M* the cycle will eventually terminate in *M*.)

This has the advantage that you don't have to map the elements of *M* to a consecutive sequence {0,...,*N*-1} of integers. It has the disadvantage, when *M* is much smaller than*P*'s domain, that too much iteration might be required for each operation. If *P* is a block cipher of a fixed size, such as AES, this is a severe restriction on the sizes of *M* for which this method is efficient.

For example, suppose that we want to encrypt 100-bit values with AES in a way that creates another 100-bit value. With this technique, apply AES-128-ECB encryption until it reaches a value which has all of its 28 highest bits set to 0, which will take an average of 2^{28} iterations to happen.

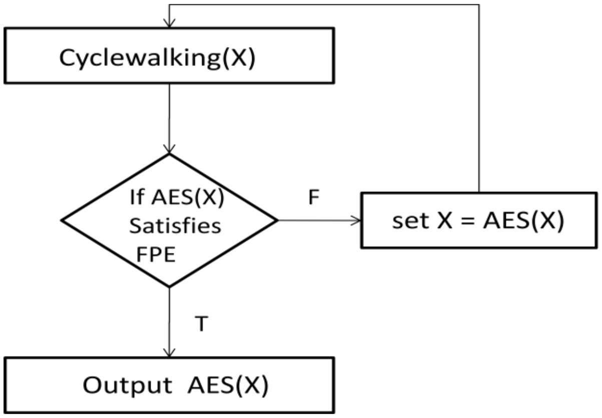

Figure 2: Cycle Walking

2.3 Feistel Mechanism

A Feistel network needs a source of pseudo-random values for the sub-keys for each round, and the output of the AES algorithm can be used as these pseudo-random values. When this is done, the resulting Feistel construction is good if enough rounds are used.

One way to implement an FPE algorithm using AES and a Feistel network is to use as many bits of AES output as are needed to equal the length of the left or right halves of the Feistel network. If a 24-bit value is needed as a sub-key, for example, it is possible to use the lowest 24 bits of the output of AES for this value.

This may not result in the output of the Feistel network preserving the format of the input, but it is possible to iterate the Feistel network in the same way that the cycle-walking technique does to ensure that format can be preserved. Because it is possible to adjust the size of the inputs to a Feistel network, it is possible to make it very likely that this iteration ends very quickly on average. In the case of credit card numbers, for example, there are 10^{16} possible 16-digit credit card numbers, and because the $10^{16} = 2^{53.1}$, using a 54-bit wide Feistel network along with cycle walking will create an FPE algorithm that encrypts fairly quickly on average.

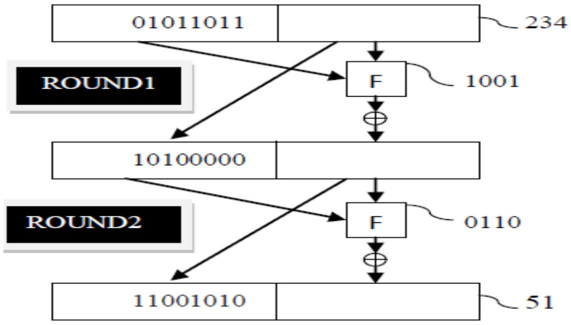

Figure 3: Feistel Mechanism

2.4 Rank then Encipher

Suppose we want to build an FPE scheme Z the slices of which may be quite complex. As an example, we might want to do length-preserving encryption of credit cards of various lengths, the CCNs of each length having a particular checksum and satisfying specified constraints on allowable substrings. It would be undesirable to design an encryption schemes whose internal workings were tailored to the specialized task in hand. Instead, what one can do is this. First, arbitrarily order and then number the points in each slice, ZN = {Z0, Z1, . . . , Zn−1} where n = |ZN|. Then, to encipher Z ∈ ZN , find its index i in the enumeration, encipher i to j in Zn using an integer FPE scheme, and then return Zj as the encryption of Z. We call this strategy the rank-then-encipher approach. It has two functions rank( ) and unrank ( ).

2.5 Block Cipher and Modes

Block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks. It is having symmetric key.

It is may be IDEA, RC5, DES, 3DES, AES, Blowfish.
DEA operates on 64-bit blocks using a 128-bit key, and consists of a series of eight identical transformations (a round) and an output transformation (the half-round). The processes for encryption and decryption are similar. IDEA derives much of its security by interleaving operations from different groups — modular addition and multiplication, and bitwise exclusive or (XOR).

RC5 is a block cipher designed by Ronald Rivest in 1994 which, unlike many other ciphers, has a variable block size (32, 64 or 128 bits), key size (0 to 2040 bits) and number of rounds (0 to 255). The original suggested choices of parameters were a block size of 64 bits, a 128-bit key and 12 rounds.

DES has a block size of 64 bits and a key size of 56 bits. 64-bit blocks became common in block cipher designs after DES. Key length depended on several factors, including government regulation.

An extension to DES, Triple DES, triple-encrypts each block with either two independent keys (112-bit key and 80-bit security) or three independent keys (168-bit key and 112-bit security). It was widely adopted as a replacement.

AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits. The block size has a maximum of 256 bits, but the key size has no theoretical maximum. AES operates on a 4×4 column-major order matrix of bytes, termed the state. It performs four operations which are substitute bytes, mix columns, shift rows and add round key.

Blowfish has a 64-bit block size and a variable key length from 1 bit up to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. Notable features of the design include the key-dependent S-boxes and a highly complex key schedule.

Modes of operation:

Electronic Codebook mode (ECB)

Cipher Block Chaining mode (CBC)

Cipher Feedback mode (CFB)

Output Feedback mode (OFB)

Counter mode

III. LITERATURE REVIEW

3.1 Using datatype-preserving encryption to enhance data warehouse security (1997, NIST) [1]

Brightwell and Smith (1997) appear to have been the first to clearly describe FPE a more general scenario, identifying they termed datatype-preserving encryption. They wanted to encrypt database entries of some particular datatype without disrupting that datatype. They have proposed a method of information protection, based on an encryption scheme which preserves the datatype of the plaintext source. They believed that this method is particularly well-suited for complex data warehouse environments. The authors proposed techniques like Indexing and Shuffling or DES. That had both negative and positive implications.

Advantages: Encrypted data allows for relational joins and blind keys.

Disadvantages: Not gave any argument about the security. Consistent Encryption exposes the data to the statistical attack.

3.2 Ciphers with Arbitrary Finite Domains (2002, Springer) [2]

Black and Rogaway (2002) proposed three methods to solve FPE problem on a special domain.

- Prefix cipher
- Cycle-Walking
- Feistel network

The prefix method constructs a random permutation in memory and uses it to encrypt data, but is only suitable for small domain. The main drawback in prefix ciphering is the time required to build the table which contains the pseudo random weight of each digit and the memory required to store the table.

The cycle-walking method encrypts plaintext with an existing block cipher repeatedly until cipher output falls in acceptable range, so it can take effect on a limited class of sets, however, its performance will be much low when the size of set is much smaller than some power of 2

The generalized-feistel cipher uses Feistel network to construct a block cipher of approximately the right size and combines with Cycle-Walking method to get output into legal range.

They have not provided any construction which works well in for intermediate-sized values of domain rather than power of 2.prefix works well nearly to strong but consumes time and space.

3.3 Feistel Finite Set Encryption Mode (2008, NIST) [3]

Spies (2008) have proposed classical Feistel and cycle walking to remove drawbacks of both feistel and cycle walking.

Feistel Finite Set Encryption Mode (FFSEM) allows encryption of a value ranging from 0..n with resultant cipher text in that same range. This mode can be used to encrypt fields where the expansion associated with a block cipher is undesirable or the format of the data must be preserved.

FFSEM have two sub functions, FFSEM-PRF, which is a Pseudo-Random Function based on some block cipher, and FFSEM-ROUND, which is an individual Feistel round. FFSEM is a somewhat unusual mode in that it does not encrypt multiple blocks of data. It inherits classical Feistel results.

Advantages: No Cipher text Expansion, Randomization

Disadvantages: Non-deterministic Performance, No authentication

3.4 Format-Preserving Encryption (2009, Springer) [4]

Bellare (2009) first introduced Rank then encipher approach for format preserving encryption. We have discussed this approach earlier in this paper in section 2.

Authors have proposed feistel mechanism FE-1 balanced opposed to that FE-2 unbalanced with rank then encipher approach.

Strongest adapts the traditional PRP notion to capture the idea that FPE is a good approximation for a family of uniform permutations on the slices. Their weaker notions are denoted MP (Message Privacy), and MR (Message Recovery), SPI (single-point indistinguishability) is a variant of the PRP notion in which there is a only a single challenge point.

Advantages: Flexible, MR, MP, SPI security

Disadvantages: Build up table for rank and unrank

3.5 The FFX Mode of Operation for Format-Preserving Encryption (2010, NIST) [5]

Bellare (2009) proposed FFX mode extension of FFSEM. This NIST submission uses alternating or unbalanced Feistel.FFX is highly parameterized. Parameter sets A2 and A10 concretize enciphering binary and decimal strings. There are two method using FFX mode. Encryption and decryption must use the same parameters. All parameter choices fixed for the lifetime of a given key.

FFX is more general, adding in support for tweaks, non-binary alphabets, and non-balanced splits. Cycle-walking can now be avoided in the setting of primary practical importance, encrypting decimal strings. FFX achieves cryptographic goals including non adaptive message-recovery security, chosen-plaintext, and even PRP-security against an adaptive chosen-cipher text attack.

Advantages: Flexible, Customizable, MR security

Disadvantages: Encryption and decryption depends upon number of parameter

3.6 Format-Preserving Encryption for Date Time (2010, IEEE) [6]

Zheli (2010) have proposed encryption of DateTime field in database, it is desirable to encrypt items from an arbitrarily sized set with the specified format described as "YYYY-MM-DD HH:MM:SS" onto that same set. Unfortunately, conventional block ciphers such as DES, 3DES or AES are unsuitable for this purpose. The solution to it belongs to the format-preserving encryption (FPE) category.

Authors have been present an FPE scheme for Date Time based on "rank-then-cipher" mode, and then analyze its security and efficiency. They have proposed a new more efficient approach named "reference-based offset encryption" to resolve the FPE problem on Date Time domain.

This method overcomes performance of “Rank then encipher”. It has a significant improvement on performance in solving FPE problems on clear order domain: upgrade the execution time of rank and unrank procedure from mini second level to micro second level.

Advantages: overcome low performance of Rte approach

Disadvantages: Not work efficiently in some cases

3.7 A Synopsis of Format-Preserving Encryption (March, 2010) [7]

Rogaway (2010) surveyed over different size of domains. The distinction among tiny space, small space, and large space assumed that the construction is block cipher based.

For tiny-space FPE the size of the message space $N = |X|$ is so small that it is feasible to spend $O(N)$ time or $O(N)$ space in order to encrypt or decrypt a point.
For small-space FPE the size of the message space $N = |X|$ is *at most* $2w$ where w is the block size of the block cipher underlying our FPE scheme.
For large-space FPE the size of the message space $N = |X|$ is *at least* $2w$ where w is again the block size of the block cipher we want to use to make our scheme.

There are different FPE schemes for the above three spaces. Those are compared by author and given detail about method, encryption applied on, description and security.

3.8 VAES3 scheme for FFX An addendum to "The FFX Mode of Operation for Format-Preserving Encryption" (2011, NIST) [8]

Vance (2011) proposed an addendum to "The FFX Mode of Operation for Format-Preserving Encryption" A parameter collection for encipher strings of arbitrary radix with sub key operation to lengthen life of the enciphering key.

VAES3 is Format Preserving Encryption (FPE) scheme. VAES conforms to the proposed FFX standard. This document outlines VAES as a set of parameters for FFX.

VAES3 was designed to meet security goals and requirements beyond the original example instantiations, and its design goals are slightly different than those of FFX. One of the unique features of VAES3 is sub key steps that enhance security and lengthen the lifetime of the key. Older version of VAES used 16 or more than round. But the performance and complexity cost was too high there seems to be no significant justification for using more rounds once the "meet-in-the-middle" attack has been overcome at 6 rounds. Therefore a round count of 10 seems to provide both performance benefits and a margin of safety.

Advantages: User's convenient FFX mode, sub key generation

Disadvantages: Possibility of dictionary attack

3.9 BPS: a Format-Preserving Encryption Proposal (NIST) [9]

Brier presented a generic format-preserving symmetric encryption algorithm BPS, which can cipher short or long string of characters from any given set.

In particular, this construction offers a tweak capability, very useful in practice when the user would like to cipher very small strings of data. The operating mode of BPS is simple and efficient. It is very similar to the well known Cipher-Block Chaining mode for block cipher encryption. It also incorporate a counter on the tweak input.

They denote by BC block cipher the internal cipher of BPS, distinguishing the encryption and the decryption processes by BC and BC^{-1} respectively. It overcomes FFX in terms of performance. FFX Can resist attacks but requires much more internal function calls than BPS.

Advantages: simple, efficient, adaptable, avoid dictionary attack

Disadvantages: Error propagation

3.10 An Efficient Format-Preserving Encryption Mode for Practical Domains (2012, Springer) [10]

Li (2012) presented RREM (random reference-based encryption mode). This mode constructs bijection between the original domain and integer set through distance computation. If an appropriate distance function is predefined, this mode can solve the FPE problem on linear equidistance domain in a more efficient way than previous methods.

According to distance function authors classified domains into three parts the linear equidistance domain class denoted by DOMI, the linear un-equidistance domain class denoted by DOMII, the class consisting of other domains denoted by DOMIII.

RtE and FFX both used some transformation to reduce FPE complexity on original complex domain to that in integer set. With the idea of transformation, the authors attempted to present the random reference-based encryption mode (RREM)

Advantages: DOMI and II are secure, reduce complexity

Disadvantages: No solution for DOMIII, More suitable for frequently used database field only, security depends upon FPE schemes.

3.11 Survey of format preserving encryption (2012, IJCER) [11]

Vidya (2012) surveyed over different format preserving methods like prefix cipher, cycle walking, feistel+cycle walking. Authors had done performance analysis of above methods. They gave advantages and disadvantages of earlier methods.

They concluded that, the prefix method works on only small data set. The Cycle walking construction, like the Prefix method, is quite simple, but works on a limited class of sets. The performance of the Feistel + Cyclic method is based on number of rounds constructed and round function PRF used in the network.

An individual technique alone is not secured for better security combination of more than one techniques used and also increase the number of permutations at the time of encryption.

3.12 Enhancement of Prefix Cipher in Format Preserving Encryption (2013, IJEI) [12]

Vidya (2013) proposed enhancement in prefix cipher. She examined prefix cipher model and add some enhancement to this proposed model. The main drawback in prefix ciphering is the time required to build the table which contains the pseudo random weight of each digit and the memory required to store the table. The pseudo random weight contains 32 digit hexadecimal numbers. Each table contains 16 entries. The authors had proposed some modifications to the Prefix method to develop new algorithm PREFIX – II. In PREFIX – II method instead of storing the 32 digit hexadecimal number in a table, select one numeric digit from it and discard the remaining digits. For all the 16 digits repeat the same process. At the end of the encryption process the cipher text contains exactly 16 digit decimal number which is same as plain text. The PREFIX – II method mainly contains three steps.

1. Generate pseudo random weighted for each digit.
2. Select one digit from the weight.
3. Adding the digit to cipher text.

Repeat the above three steps for all the digits. Finally we get 16 digit numeric cipher text.

Advantages: simple to implement, less space and time complexity, avoid drawback of prefix cipher

Disadvantages: Require small changes to get more secure result

3.13 Efficient Fpe Algorithm for Encrypting Credit Card Numbers (2013, IOSR) [13]

Chitra (2013) had proposed algorithm for FPE which is based on AES-128 encryption algorithm. The 16 digits credit card number is encrypted using AES-128At the end of the last round two more additional steps are added to retain the format and data type of the plaintext , XOR and hexadecimal to 2421 conversion to retain 16 digit cipher text. There is no need to change the database structure, queries and application programs to handle this cipher text. They concluded that proposed FPE algorithm is very useful for real time applications such as encrypting credit card number. Future work is to apply this algorithm for all the data types not only for numeric data type. For further improvement make modification in AES.

Advantages: No range limitation, single iteration, no need for any additional storage, simple to implement

Disadvantages:

3.14 Format Preserving Encryption using Feistel Cipher (2013, IJCA) [14]

Vidya (2013) had proposed a new technique using Feistel network for FPE. The existing technique uses the combination of Feistel and cycle walking .The proposed technique simplifies the encryption process and also reduces the number of iterations by using only Feistel. The main advantage in Feistel network is the size of the input can be changed. The sub keys are generated at each round.

Feistel cipher uses product cipher that is combination of substitution and transposition. That is cryptographically more secured. The security in Feistel network depends on the key length and number of rounds. The round function should also complex. Due to key length and sub key generated in each round the basic cryptanalysis method brute force attack cannot be applied.

The decryption of cipher is same as encryption but requirement is reverse of key schedule. The size of the code and the hardware implementation are very less compared to other structures.

Advantages: No range limitation, single iteration

Disadvantages: Depends upon number of rounds. More rounds slow encryption and decryption process

3.15 Performance analysis of format preserving encryption (FIPS PUBS 74-8) over block ciphers for numeric data (2013, IEEE) [15]

Mallaiah (2013) had discussed overhead of FPE (FIPS-74-8).It was a NIST standard based on DES. Instead of using DES, use of AES or Blowfish will give better performance and security for Format preserving of numeric data. FPE is useful in storing the encrypted data in database schemas without changing schema and associated applications. The authors analyzed performance of FPE over block ciphers such as AES, Blowfish, 3DES, DES with different key sizes. They had applied FIPS PUBS (74-8) standard technique over block ciphers to map digits onto digits using CFB Mode of operation which improves the security.

The proposed Format Preserving encryption mechanism can be applied to encryption of PAN numbers, PIN numbers, SSL, keys and any numeric data to preserve the format after encryption. Algorithms, which are considered in this implementation, are well known secured block ciphers.

Advantages: No need for any additional storage, secured

Disadvantages: No authentication, No randomization

3.16 Evaluation of format preserving encryption algorithms for critical infrastructure protection (2014, Springer) [16]

Agbeyibor (2014) had compared NIST standards FPE mechanisms FF1 (FFX), FF2 (VAES3), FF3 (BPS) according to plaintext dataset design, experimental design, implementation and entropy measurement, hardware implementation, security and performance. They concluded that the FF3 algorithm requires the least hardware resources, has the lowest operational latency and has similar security performance as the other two algorithms.

	FPE Literature	Technique Used	Pros	Cons
3.1	Brightwell et al. [1] Datatype Preserving (1997,NIST)	Indexing and Shuffling, DES	Encrypted data allows for relational joins and blind keys.	Not gave any argument about the security. Statistical attack.
3.2	Black et al [2] ciphers with arbitrary finite domain (2002,Springer)	Prefix, Cycle-Walking, Generalized Feistel	Prefix is nearly too strong	Each method has their drawbacks described earlier
3.3	Spies et al[3]FESEM (2008, NIST)	FFSEM (Feistel+Cycle Walking)	Cipher text Expansion, Randomization	Non-deterministic Performance, No authentication
3.4	Bellare et al. [4] FPE (2009,Springer)	Rank then encipher FE-1 ,FE-2	Flexible, MR, MP, SPI security	Build up table for rank unrank, low performance
3.5	Bellare et al. [7] the FFX mode for FPE (2010,NIST)	FFX mode	Flexible, Customizable, MR security	Encryption and decryption depends upon number of parameter
3.6	Zheli et al[6]FPE for DateTime (2010,IEEE)	Rank then encipher Reference based offset encryption	Overcome low performance of Rte approach	Not work efficiently in some cases
3.8	VANCE et al [8] VAES3 (2011,NIST)	VASE3	User's convenient FFX mode, sub key generation	Dictionary attack
3.9	Brier et al [9] BPS (NIST)	BPS	simple, efficient, adaptable, avoid dictionary attack	Error propagation

3.10	Li et al [10]An Efficient FPE for practical domain (2012, Springer)	RREM	DOMI and II are secure, reduce complexity	No solution for DOMIII, More suitable for frequently used database field only
3.12	S.Vidya, et al [12] Enhancement prefix cipher (2013,IJEI)	Enhancement Prefix cipher	simple to implement, less space and time complexity, avoid drawback of prefix cipher	Require small changes to get more secure result
3.13	K.Chitra, et al [13] Efficient FPE for CCN (2013,IOSR)	AES with two more operations	No range limitation, single iteration, no need for any additional storage, simple to implement	Depends upon number of rounds. More rounds slow encryption and decryption process
3.14	S.Vidya, et al [14] FPE using Feistel cipher (2013,IJCA)	Feistel cipher	No range limitation, single iteration	Depends upon number of rounds. More rounds slow encryption and decryption process
3.15	K.Mallaiah, et al [15] FPE using block cipher (2013, IEEE)	Block Cipher with CFB mode	No need for any additional storage, secured	No authentication, No randomization

Table 1: Comparisons of FPE techniques

	FPE Survey	**Comparison**
3.7	Rogaway et al [7] A synopsis for FPE (2010)	Methods for tiny space, small space, and large space domain
3.11	S.Vidya et al[11] Survey of FPE (2012, IJCER)	prefix cipher, cycle walking, feistel+cycle
3.16	Abgeyibor et al[16] Evolution of FPE (2014,Springer)	FF1, FF2, FF3

Table 2: Survey of FPE techniques

IV. CONCLUSION

This paper has surveyed the literatures on different Format Preserving Encryption approaches. All the advantages and disadvantages of each of these techniques have been pointed out. We have attempted to integrate our understanding across the surveyed literatures and tried to find out the comparative best technique for encrypting CCN and SSN.

REFERENCES

[1] H. E. Smith and M. Brightwell. Using Datatype-Preserving Encryption to Enhance Data Warehouse Security. NIST 20th National Information Systems Security Conference, pp.141, 1997.

[2] J. Black and P. Rogaway. Ciphers with Arbitrary Finite J. Black and P. Rogaway. Ciphers with Arbitrary Finite Domains. RSA Data Security Conference, Cryptographer's Track (RSA CT '02), Lecture Notes in Computer Science, vol. 2271, pp. 114-130, Springer, 2002.

[3] Spies, Terence. "Feistel finite set encryption mode." NIST Proposed Encryption Mode, 2008.

[4] M. Bellare, T. Ristenpart, P. Rogaway, and T. Stegers. “Format preserving encryption” Springer, 2009.

[5] Mihir Bellare, Phillip Rogaway, Terence Spies. 2010. “The FFX Mode of Operation for Format-Preserving Encryption” NIST, February 20, 2010.

[6] Zheli Liu, ChunfuJia, Jingwei Li, Xiaochun Cheng "Format-Preserving Encryption for Date Time" IEEE, 2010.

[7] Phillip Rogaway, "A Synopsis of Format-Preserving Encryption" March 27, 2010.

[8] J. Vance, "VAES3 Scheme for FFX: An Addendum to the FFX Mode of Operation for Format Preserving Encryption" NIST, 2011.

[9] Eric Brier, Thomas Peyrin and Jacques Stern" BPS: a Format-Preserving Encryption Proposal" NIST.

[10] LI Jingwei, LIU Zheli, XU Li, JIA Chunfu "An Efficient Format-Preserving Encryption Mode for Practical Domains" Springer, 2012.

[11] S.Vidhya,K.Chitra "Survey of format preserving encryption " International Journal Of Computational Engineering Research,2012.

[12] S.Vidhya, K.Chitra "Enhancement of Prefix Cipher in Format Preserving Encryption" International Journal of Engineering Inventions, 2013.

[13]Dr. K. Chitra, S.Vidhya "Efficient Fpe Algorithm For Encrypting Credit Card Numbers" IOSR Journal of Computer Engineering, 2013.

[14] S.Vidhya ,K.Chitra "Format Preserving Encryption using Feistel Cipher " International Journal of Computer Applications,2013.

[15] K.Mallaiah, S.Ramachandram, S.Gorantala "Performance Analysis of Format Preserving Encryption (FIPS PUBS 74-8) over block ciphers for Numeric data" IEEE, 2013.

[16] Richard Agbeyibor, Jonathan Butts, Michael Grimaila, and Robert Mills "Evaluation of format preserving encryption algorithms for critical infrastructure protection" Springer, 2014.