International Journal of Smart Sensor and Adhoc Network

Volume 3 | Issue 2 Article 7

January 2022

AN EFFICIENT THRESHOLD SECRET SHARING SCHEME USING FAST FOURIER TRANSFORM

Vanashree Gupta
Department of Scientific Computing, Modeling and Simulation Savitribai Phule Pune University, Pune , Maharashtra India, vanashreegupta@gmail.com

Recommended Citation

Gupta, Vanashree (2022) "AN EFFICIENT THRESHOLD SECRET SHARING SCHEME USING FAST FOURIER TRANSFORM," *International Journal of Smart Sensor and Adhoc Network*: Vol. 3 : Iss. 2 , Article 7.
DOI: 10.47893/IJSSAN.2022.1210
Available at: https://www.interscience.in/ijssan/vol3/iss2/7

AN EFFICIENT THRESHOLD SECRET SHARING SCHEME USING FAST FOURIER TRANSFORM

Vanashree Gupta[#1]

Department of Scientific Computing, Modeling and Simulation

Savitribai Phule Pune University, Pune , Maharashtra India

[1]vanashreegupta@gmail.com

ABSTRACT

Secret Sharing is a robust key management method which is having applications in password management, secure multi party computation, e-voting etc. Threshold secret sharing is a method in which out of all the parties only predefined or certain number of parties can reconstruct the secret. In this paper we will describe the most popular Shamir's secret sharing scheme along with its limitations. In Shamir's scheme each shareholder receives one share per secret. We can use alternative way ramp (packed variant)scheme which overcomes this limitation and reduces load on each individual shareholder. But this impacts on efficiency as degree of polynomial is increased. Either we must adjust the privacy threshold or number of shares needed to reconstruct. There is need of advance technique. An efficient secret sharing needs faster polynomial evaluation and interpolation. Hereis an efficient secret sharing scheme using Fast Fourier Transform (FFT). In this polynomial evaluation as well as interpolation both speeds up. It has time complexity O(nlogn).

KEYWORDS

Secret sharing, Threshold secret sharing, Shamir's secret sharing, Ramp secret sharing, Fast Fourier Transform

1. INTRODUCTION

The important messages or things that we want to preserve are secrets. We have to handle those secrets carefully. If it is disclosed to public by accident then entire secrecy will be lost. To overcome with this problem and enhance the reliability without risk we can use secret sharing schemes. Secret sharing is important from performance point of view as they don't require any assumptions about certain problems like integer factorization, discrete logarithm etc. It also has computational advantage over homomorphic encryption. In this the secret is divided among different participants and out of that authorized set can reconstruct the share. The scheme is divided into secret distribution and secret reconstruction. There are lots of secret schemes are available like threshold secret sharing, generalized secret sharing, verifiable secret sharing etc. Each of them having advantages as well as limitations too. Here we are discussing the Shamir's secret sharing scheme followed by its ramp (packed variant). But both have some or other limitation so we come up with new approach using Fast Fourier Transform.[2] also proposed a method using FFT but it is not dynamic, number of participants must be determined previously because each output depends on all other inputs.

1.1 Organization

The rest of the paper is organized as follows :Section 2 covers related work based on Shamir's threshold secret sharing schemes and ramp (packed variant) scheme for the Shamir's secret sharing scheme. Section 3 discusses the definition of FFT and steps of proposed secret sharing scheme. Section 4 is about results and discussions. Section 5 we conclude with final remarks. Section 5 discusses about the future scope.

2. RELATED WORK

A] Shamir's Secret Sharing [1][3]

This method [1] was introduced in 1979. It is linear approach based on Lagrange interpolation. The correctness and privacy of scheme is due to this only. In this the polynomial is randomly generated and having a constraint, zero-degree term will be a secret. The polynomial is represented based on coefficients and polynomial evaluation is done using Horner's rule. Reconstruction of share happens using Lagrange interpolation. Polynomial is given in point value representation. Using Lagrange interpolation, we can get value of polynomial at any point by weighted sum of a set of constant and its values at other points. In [7] the detail algorithm along with properties and limitations are discussed in detail. They have proposed an alternative way to this.

Given (t,n)secret sharing with k as secret and n share holders { P_1,P_2,P_3, …..,P_n}. Using t-1 degree random polynomial with random coefficient.

Step 1: Polynomial construction

$f(x)=a_0+a_1x+a_2x^2+\ldots\ldots+a_{t-1}x^{t-1}(\text{mod } p)$

Step 2: Share distribution

$\text{Share}_i(s)=(x_i,f(x_i))$

Step 3: Secret recovery

Using Lagrange Interpolation formula, the polynomialf(x) can be written in the form

$$f(x) = \sum_{i=0}^{t-1} f(x_i) * L_i(x)$$

where $L_i(x)$is the Lagrange Polynomial.

$$L_i(x) = \prod_{j=0,\, j \neq i}^{t-1} \frac{x - x_j}{x_i - x_j}$$

$L_i(x)$has value 1 at x_i, and 0 at every other x_j[7].

The computation can be amortized away when we have to perform several interpolations as Lagrange constant depends only on points. If N is number of shares, R is minimum number of shares needed to reconstruct the secret, T is privacy threshold i.e., maximum number of shares that may be seen without learning nothing about the secret and K is the number of secrets shared together. Share distribution takes O(N*T) steps for each secret and reconstruction requires O(T) steps for each secret if pre computation is allowed. Here single polynomial defines single share. But by varying the degree of polynomial we can choose as many shares as we want. Homomorphic properties on addition and multiplication allow us to do so. One caveat with this is unlike addition every multiplication doubles the degree of random polynomial, so we require more shares to reconstruct. Due to which an additional step of reducing the degree must be taken while doing secure computation [1][3].

B] Ramp (Packed variant) Scheme [3]

Shamir's secret sharing scheme each shareholder receives one share per secret i.e., large number of secrets means large number of shares for each shareholder. We can reduce this limitation as well as overhead on each individual shareholder using ramp sharing. Here sampling a polynomial in coefficient representation is a constraint. So now we perform interpolation during share distribution instead of evaluation which has an impact on efficiency. If we don't worry about computational efficiency then in this scheme we have reduced number of shares each

shareholder gets. Another caveat with this is degree of polynomial is increased so we need to either adjust in privacy threshold or number of shares needed to reconstruct the secret[3].

3. PROPOSED SCHEME

As we know that an efficient secret sharing needs faster polynomial evaluation and interpolation, using advanced techniques it is possible to sample a polynomial in coefficient representation and regain efficient sharing. Here is an efficient way using Fast Fourier Transform (FFT).It is also known as fast Discrete Fourier Transform (DFT) or optimised DFT. FFT is widely used in digital signal and image processing, interpolation and decimation, pattern recognition etc. Here we are using in secret sharing for share distribution and evaluation.

Definition:

The DFT is defined by the formula: Let $x_0, x_1, \ldots, x_{N-1}$ be complex numbers

$x_N = \sum_{n=0}^{N-1} x_n e^{-i2\pi kn/N}$ k=0,1,N-1

where $e^{i2\pi/N}$ is a primitive N^{th} root of 1. If we directly evaluate above definition, it requires $O(N^2)$ operations: there are N outputs X_k, and each output requires a sum of N terms. If we compute same using FFT algorithms it requires O(N log N)operations[5][6].

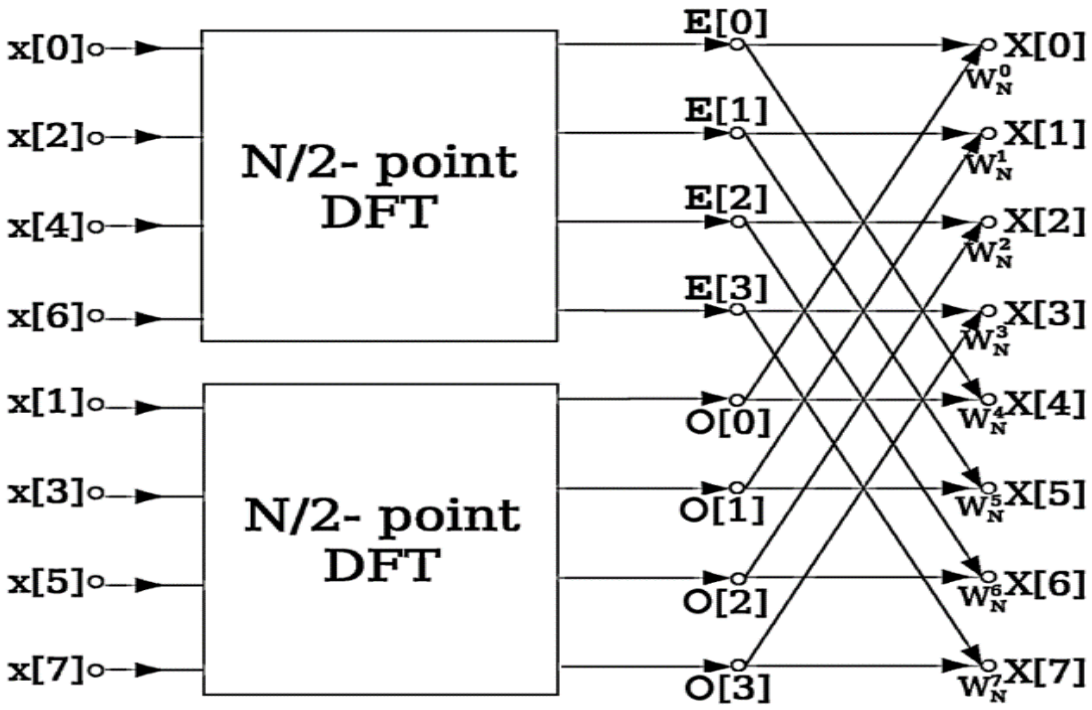


Fig.1. An example FFT algorithm structure, using a decomposition into half-size FFTs [6]

Steps of Proposed Scheme:

The standard way of evaluating polynomial is by using Horner's rule but it takes O(L*L) operations. FFT allows it to do in more efficient way as follows:

1) Assume A is a polynomial having L

coefficients and degree L-1 and Q is fixed prime number.

2) Convert list of coefficients into a list of values [A(w0), A(w1), A(w2), A(w3)] of equal length, for points w = [w0, w1, w2, w3].

There are 3 ways to do

a) i) Break A into two smaller polynomials Band C.

ii) Square the w points v = [wi * wi % Q for wi in w]

iii) compute the values of B and C at the v points.

iv) Combine results into values of A at the w points

A_values=[(B_values[i]+w[i]*C_values[i])%Q

But in this approach we are not saving much.

b) i) generator of subgroup of order 4 omega4.

ii) v points used for B and C will form a subgroup of order 2 due to the squaring; but there is no need to calculate this explicitly because implicitly it is done by generator.

#generator of subgroup of order 2

omega2=omega4*omega4%Q

A_values[i] = B_values[i % 2] + pow(omega4, i, Q) * C_values[i % 2]

c) We used divide and conquered strategy. Continue this process of diving the polynomial in half: to compute e.g. break B into two polynomials D and E and then follow the same procedure. The only requirement is that the length L is a power of 2 and that we can find a generator omegaL of a subgroup of this size.

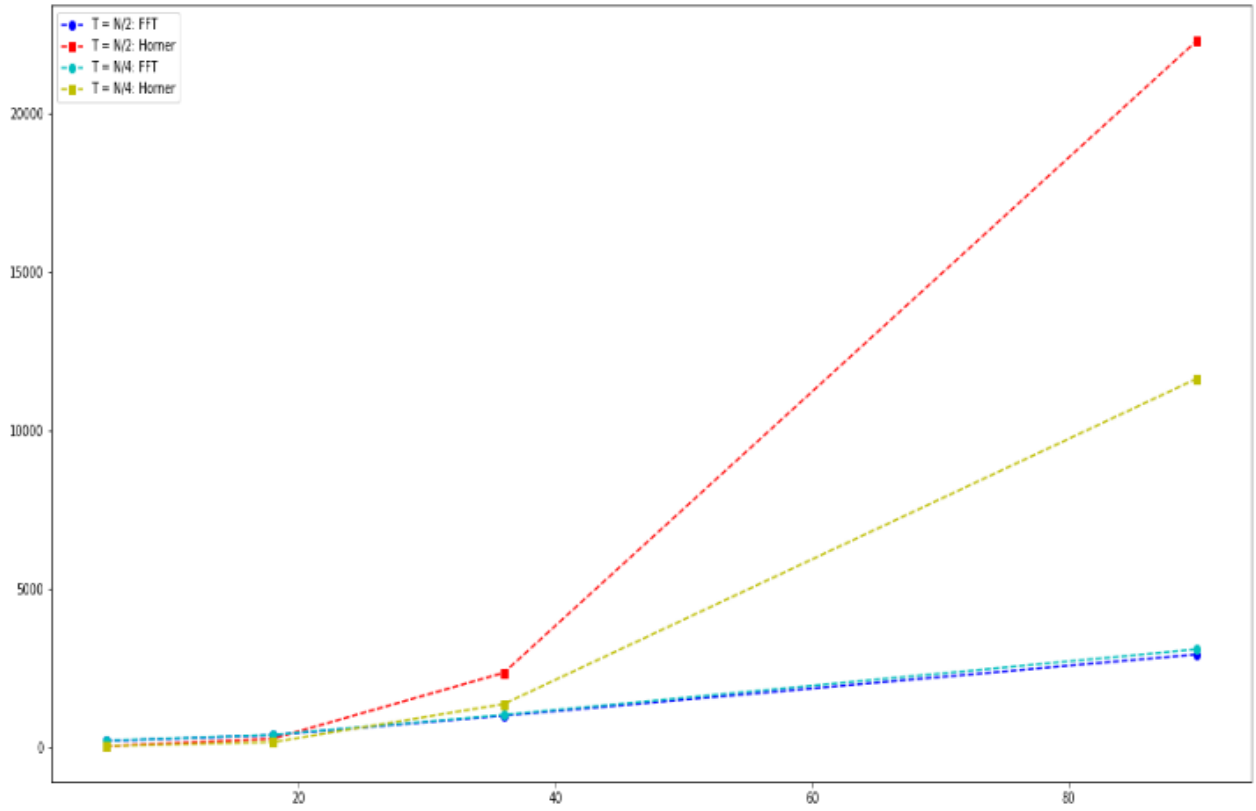
We can apply all these FFT_forward, FFT_backward, FFT for power of 2(break polynomial into 2 and use square of omega), FFT for power of 3(break polynomial into 3 and use cube of omega) to both Shamir's scheme and packed variant.

In Shamir's scheme polynomial is in coefficient representation hence it is used in share generation step. Apply forward FFT to it.

In packed variant polynomial is in point representation so using backward FFT power of 2 to convert it to coefficient form and then use forward FFT powers of 3 for share generation [4].

4. Results And Discussions

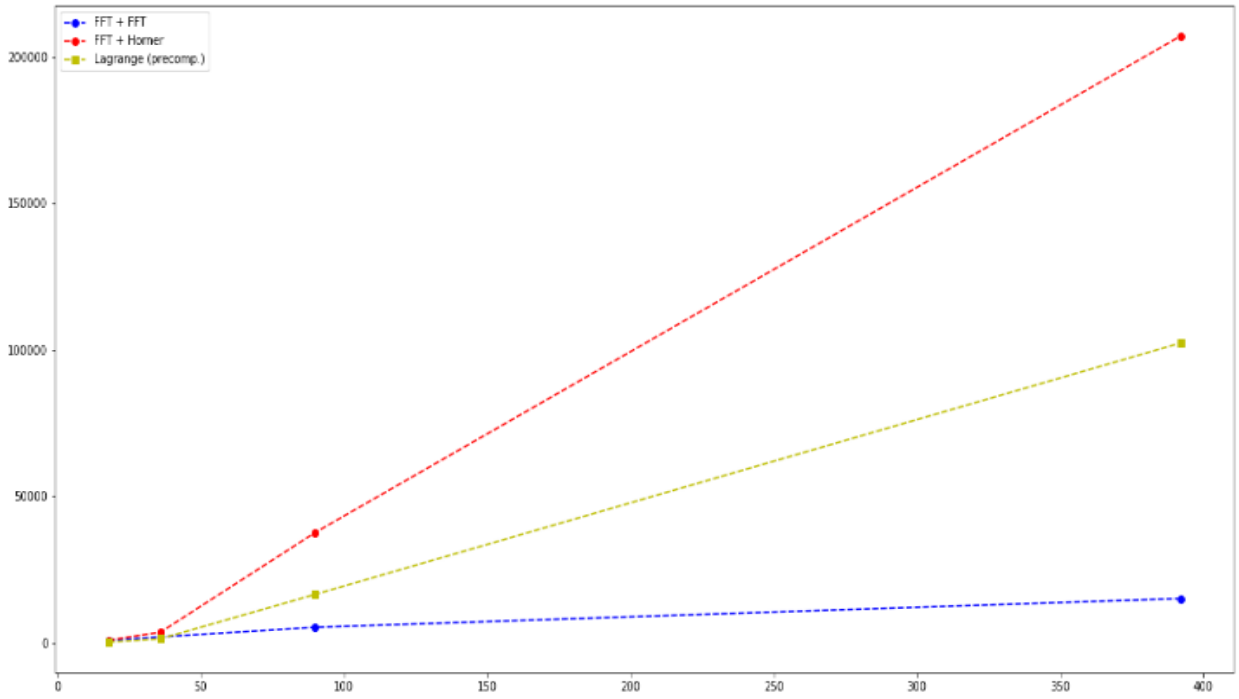
For testing we take number of shares as 5,18, 36, 90 and 392 with T = N/2 medium threshold and T = N/4 low privacy threshold for both the schemes Shamir's as well as packed.



Comparison of three different approaches staring form sampling a polynomial in point representation till share generation.

1. FFT + FFT: Convert into coefficient representation use backward FFT and then for evaluation forward FFT.
2. FFT + Horner: Convert into coefficient representation use backward FFT and then for evaluation Horner's rule.
3. Lagrange: Use already computed Lagrange constants for share generation and evaluation.

where the Lagrange requires additional storage for the pre computed constants.



Here we can see thatthe Lagrange approach will be used up to the setting with 36 shares, after which it's advisable to use the two step FFT [4].

5. CONCLUSION

In this paper we have compared two scheme Shamir's scheme and its packed variant. As per privacy threshold these methods are less efficient. So here is an efficient way using Fast Fourier Transform. It speeds up the sharing process but has a drawback in reconstruction process: it requires all shares to be present and untampered. Hence in some application traditional and slower approach of Newton or Laplace interpolation can be used.

6. FUTURE WORK

In future we will try to use it in robust reconstruction to speed up the interpolation as well as we will try to use it in some application.

REFERENCES

[1] Shamir, A., “How to Share a Secret”, Communications of the ACM, vol.22, no.11, 1979.

[2] Al-Ssulami ,A,” A Novel Threshold Secret Sharing Scheme Using FFT Algorithm”, International Journal of Information Security Science, vol2,No.1

[3] https://mortendahl.github.io/2017/06/04/secret-sharing-part1/

[4] https://mortendahl.github.io/2017/06/24/secret-sharing-part2/

[5] *Frigo, Matteo; Johnson, Steven G. (January 2007) [2006-12-19]. "A Modified Split-Radix FFT With Fewer Arithmetic Operations". IEEE Transactions on Signal Processing.* ***55*** *(1): 111–119. doi:10.1109/tsp.2006.882087. S2CID 14772428*

[6] https://en.wikipedia.org/wiki/Fast_Fourier_transform

[7]Vanashree Gupta,Smita Bedekar,“Alternative to Shamir’s Secret Sharing Scheme Lagrange Interpolation over Finite Field”,International Journal of Technical Research & Science (IJTRS),V6-I3-002, March 2021, ISSN: 2454-2024, https://doi.org/10.30780/IJTRS.V06.I03.002