EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 17, No. 3, 2024, 1751-1761
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

Threshold Changeable Secret Sharing (TCSS) via Skew Polynomials

Angga Wijaya[1,3,*], Intan Muchtadi Alamsyah[2], Aleams Barra[2]

[1] *Doctoral Program of Mathematics, Faculty Mathematics and Natural Sciences, Institut Teknologi Bandung, Jl. Ganesha No. 10, 40132 Bandung, Indonesia*
[2] *Algebra Research Group, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Jl. Ganesha No. 10, 40132 Bandung, Indonesia*
[3] *Department of Informatics Engineering, Faculty of Industrial Technology, Institut Teknologi Sumatera, Jl. Terusan Ryacudu, 36365 South of Lampung, Indonesia*

Abstract. Secret sharing is a tool to divide a secret into multiple shares, so that to reconstruct the secret, it is necessary to collect several shares under certain conditions. Secret sharing was first introduced by Adi Shamir, the scheme is based on polynomials. The secret is represented as a constant value polynomial, and the points on the polynomial graph serve as shares. Secret reconstruction is performed through Lagrange interpolation at a minimum of k out of n points, known as a threshold scheme (k, n). In 2010, Zhang Y. designed a secret sharing scheme through skew polynomials. Involving the role of the automorphism σ in the skew polynomial ring increase the complexity in share distribution and secret reconstruction. In 2012, Zhang Z. designed a secret sharing scheme with a threshold that can change according to the participants present during the reconstruction process, known as Threshold Changeable Secret Sharing (TCSS). This aims to prevent external parties from pretending to be valid participants in order to learn the secret. In this research, a TCSS scheme will be designed using skew polynomials. The aim is to make the TCSS scheme's calculations more complex, making it harder for adversaries to access the secret.

2020 Mathematics Subject Classifications: 94A62, 12E10

Key Words and Phrases: Secret sharing, threshold changeable secret sharing, skew polynomials

1. Introduction

Initially proposed by Shamir [13] as a threshold scheme utilizing polynomials and later by Blakley [1] as a scheme involving geometric hyperplanes, the concept of secret sharing plays a pivotal role in safeguarding information among individuals or participants in a group who may not fully trust each other. The fundamental notion is to partition a secret into multiple shares in a manner that ensures no single share holds any information about

*Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v17i3.5262

Email addresses: angga.wijaya@if.itera.ac.id (A. Wijaya), ntan@itb.ac.id (I. Muchtadi Alamsyah), barra@itb.ac.id (A. Barra)

the original secret. This arrangement enables a collective group of participants who meet specific conditions to access and disclose the original secret. The applications of secret sharing span various domains, encompassing key management [6], multiparty computation [12][4], digital signature protocols [2], and more.

The (k, n) threshold scheme indicates that to reconstruct the secret, a minimum of k participants out of a total of n participants must collaborate by combining their shares. Consequently, secret sharing schemes involve two primary stages: share generation and secret reconstruction. Share generation is conducted by a trusted dealer. During the secret reconstruction phase, only a subset of participants with valid shares, comprising at least k individuals from the total n participants, is capable of executing the reconstruction process.

The issue arises when there are more than k participants gathered, but among them, there is a minimum of k valid participants, and at least one of the remaining ones acts as an adversary, pretending to be a valid participant. Of course, the adversary doesn't possess valid shares. However, with a threshold scheme (k, n), under such conditions, it is still possible to reconstruct the secret. This poses a risk as it allows adversaries who should not have access to the secret to gain knowledge they are not entitled to. Hence, the idea of a changeable threshold secret sharing (TCSS) emerged, as introduced by Martin [8] and further discussed by Meng [9]. Initially, the threshold is set as k by the dealer, but during secret reconstruction, it can be changed to k' with $k' > k$. In this scenario, each participant should have a share corresponding to the number of participants involved in the reconstruction at that time.

Moreover, advancements in secret sharing research were made by Zhang [15] and Johnson [7], who introduced the threshold secret sharing scheme (k, n) based on skew polynomials. The concept of skew polynomials was previously introduced by Noether [10] and Ore [11]. The skew polynomial ring, denoted as $R[x, \sigma]$, is defined, with R taking the form of a field, and σ representing an automorphism on R. The utilization of skew polynomials in polynomial evaluation and Lagrange interpolation introduces complexity due to the involvement of the automorphism function σ, as outlined by Eric [3] in the methodology for performing interpolation using skew polynomials. Consequently, the secret sharing scheme becomes more intricate.

In this research, the original Threshold Changeable Secret Sharing (TCSS) scheme is implemented using skew polynomials. Consequently, this process experiences an increase in computational time, making it more time-consuming for adversaries to reconstruct the secret.

2. Preliminaries

The following are definitions, basic theories and theorems from previous research.

Definition 1. *[14](Secret-Sharing Scheme) Let S be a set of secrets, where $|S| \geq 2$. A secret sharing scheme Π on $U = \{u_1, ..., u_n\}$ with domain of secrets S is a mapping from S to a set of n-tuples $\Pi_{i=1}^{n} S_i$, where S_i is called the share domain of u_i.*

Definition 2. *[5](Skew Polynomials Ring) Let R be a field, σ is a ring automorphism on R. $R[x,\sigma]$ is skew polynomial ring with usual polynomial addition and left scalar multiplication. For right scalar multiplication :*

$$x \cdot a = \sigma(a) \cdot x \text{ for all } a \in R$$

Definition 3. *[15](Skew Polynomial Ring - Evaluation) Let $R[x,\sigma]$ skew polynomial ring, $f(x) \in R[x,\sigma]$, and any $a \in R$. Define the set $\{N_n : R \to R \mid n \geq 0\}$ recursively for all $a \in \mathbb{R}$,*

$$N_0(a) = 1 \text{ and } N_{n+1}(a) = \sigma(N_n(a))a.$$

Based on remainder theorem : $f(x) = q(x)(x-a) + r$ with $r \in R$, the right remainder of $f(x)$ by $(x-a)$ is $r = \Sigma a_i N_i(a)$. So the evaluation of $f(x)$ on a :

$$f(a) = r = \Sigma a_i N_i(a)$$

Theorem 1. *[3] Let $\Delta = \{x_1, x_2, ..., x_n\}$ and $x_i \in R$, where R is division ring. Then*

(i) There exist nonzero polynomial $f \in R[x,\sigma]$ such that $f(x_i) = 0$.

(ii) The set I of polynomials vanishing on Δ form a left ideal in $R[x,\sigma]$.

(iii) If f_Δ is monic polynomial of the smallest degree in I, then $I = R[x,\sigma]f_\Delta$ where f_Δ is called minimal polynomial of Δ.

Procedure to find minimal polynomial of $\{x_1, x_2, ..., x_n\}$:

(i) Let $\Delta = \{x_1, x_2\}$

(ii) The polynomial vanishing on Δ is :

$$f_{\{x_1,x_2\}}(x) = (x - \sigma(x_2 - x_1)x_2(x_2 - x_1)^{-1})(x - x_1)$$

(iii) By recursively for $\Delta = \{x_1, x_2, ..., x_n\}$, the polynomial vanishing on Δ is :

$$f_{\{x_1,x_2,...,x_n\}}(x) = (x - \sigma(f_{\{x_1,x_2,...,x_{n-1}\}}(x_n))x_n(f_{\{x_1,x_2,...,x_{n-1}\}}(x_n))^{-1})(f_{\{x_1,x_2,...,x_{n-1}\}}(x))$$

Theorem 2. *[3] Let $\Delta = \{x_1, x_2, ..., x_n\}$ and $x_i \in R$ where R is a division ring. For any $y_1, y_2, ..., y_n \in K$ there exist a unique polynomial $f \in R$ such that $f(x_i) = y_i$ and deg $f \leq n-1$ if and only if deg $f_\Delta = n$ where f_Δ is the minimal polynomial of the set Δ.*

The Interpolation Polynomial of set Δ :

$$f(x) = \sum_{i=0}^{n} y_i \cdot L_i(x_i)^{-1} \cdot L_i(x)$$

where $L_i(x)$ is minimal monic polynomial such that $L_i(x_j) = 0$ for $i \neq j$.

3. Main Result

The outcome of this study is a secret sharing scheme outlined in three stages: setup, share generation, and secret reconstruction. Subsequently, there is a subsequent examination of the algorithmic complexity within the devised scheme.

3.1. Setup

In this stage, the dealer determines the total number of participants, denoted as n, and the initial threshold value required for secret reconstruction, denoted as k. The skew polynomial structure $R[x, \sigma]$ is also defined, with the restriction that R is a field, and σ is an automorphism on R. The dealer then selects the secret s, represented by an element in R, in other words, s is an element of R.

3.2. Share Generation Phase

(i) Dealer set polynomials :

$$f_t(x) = s + a_{t,1}x + a_{t,2}x^2 + ... + a_{t,k-1}x^{k-1} \text{ with } s = \text{secret},$$
$$t \in \{k, k+1, \ldots, n\}, a_{t,j} \in R \text{ for } j \in \{1, \ldots, t-1\} \text{ and } a_{t,t-1} \neq 0.$$

(ii) Dealer choose $X = \{x_i\}$ with $x_i \in R$ for $i \in \{1, \ldots, n\}$ and satisfy X is σ-pairwise distinct which mean for $i \neq j$, x_i and x_j is not σ-conjugate, that is for all $c \in R$, $x_i \neq \sigma(c)x_jc^{-1}$

(iii) Evaluate value x_i on polynomials $f_t(x)$ for all $i \in \{1, \ldots, n\}$ and $t \in \{k, k+1, \ldots, n\}$ using skew polynomials evaluation method.

$$f_t(x_i) = s + \sum_{u=1}^{t-1} a_{t,u}N_u(x_i)$$

with $N_0(x_i) = 0$ and $N_{v+1}(x_i) = \sigma(N_v(x_i))x_i$ for $v \geq 0$.

(iv) Set the share for participant i is $(x_i, f_t(x_i))$ for all $t \in \{k, k+1, \ldots, n\}$. So each participants has $n - k + 1$ shares which will be used to reconstruct the secret based on corresponding the value of threshold t (number of collected participants).

(v) Dealer send the corresponding share $(x_i, y_{(t,i)}) = (x_i, f_t(x_i))$ to each participants privately.

3.3. Secret Reconstruction Phase

(i) The collected participants have information about R, σ, n, k and t.

(ii) Initial threshold is k, since the number of collected participant $t \leq k$. If the number of collected participant $t > k$, the threshold change from k to t.

(iii) Participants collect their share $(x_i, y_{(t,i)})$ corresponding the value of current threshold, assume t is current threshold.

(iv) Participants interpolate the collected shares $(x_i, y_{(t,i)})$ by skew polynomials Lagrange interpolation method.

$$f_t(x) = \sum_{i=1}^{t} y_{(t,i)}(L_i(x_i)^{-1}L_i(x))$$

with $L_i(x)$ is monic minimal polynomial such that $L_i(x_j) = 0$ for $i \neq j$.

(v) Evaluate $f_t(0) = s$ as the secret.

3.4. Example

Let a dealer and set of participant $= \{p_1, p_2, p_3\}$. Number of participants $= n = 3$. Dealer determine initial threshold $k = 2$ and secret $= s = 5 + 5i \in \mathbb{C}$.
Dealer construct initial polynomial for $k = 2$:

$$f_2(x) = (5 + 5i) + (1 - i)x$$

Dealer determine x_i value for participant share :

$$x_1 = 1 + i, \quad x_2 = 1 + 2i, \quad x_3 = 1 + 3i$$

Evaluate x_i value on $f_2(x)$ using skew polynomials evaluation method:

$$\begin{aligned}
f_2(1+i) &= (5+5i)N_0(1+i) + (1-i)N_1(1+i) \\
&= (5+5i)\cdot 1 + (1-i)\sigma(N_0(1+i))\cdot(1+i) \\
&= (5+5i) + (1-i)(1+i) \\
&= 7 + 5i, \\
f_2(1+2i) &= (5+5i)N_0(1+2i) + (1-i)N_1(1+2i) \\
&= (5+5i)\cdot 1 + (1-i)\sigma(N_0(1+2i))\cdot(1+2i) \\
&= (5+5i) + (1-i)(1+2i) \\
&= 8 + 6i, \\
f_2(1+3i) &= (5+5i)N_0(1+3i) + (1-i)N_1(1+3i) \\
&= (5+5i)\cdot 1 + (1-i)\sigma(N_0(1+3i))\cdot(1+3i) \\
&= (5+5i) + (1-i)(1+3i) \\
&= 9 + 7i.
\end{aligned}$$

Dealer construct polynomial for $k = 3$:

$$f_3(x) = (5 + 5i) + (1 - 2i)x + (2 - i)x^2$$

Evaluate x_i value on $f_3(x)$ using skew polynomials evaluation method:

$$\begin{aligned} f_3(1+i) &= (5+5i)N_0(1+i) + (1-2i)N_1(1+i) + (2-i)N_2(1+i) \\ &= 10+4i, \\ f_3(1+2i) &= (5+5i)N_0(1+2i) + (1-2i)N_1(1+2i) + (2-i)N_2(1+2i) \\ &= 20, \\ f_3(1+3i) &= (5+5i)N_0(1+3i) + (1-2i)N_1(1+3i) + (2-i)N_2(1+3i) \\ &= 32-4i. \end{aligned}$$

Initial share for participant:

$$(1+i, 7+5i), (1+2i, 8+6i), (1+3i, 9+7i)$$

Participant share when there are 3 collected participants:

$$(1+i, 10+4i), (1+2i, 20), (1+3i, 32-4i)$$

That is the end of share generation phase. Next step is secret reconstruction phase. For example, there are 3 participants with their own collected share:

$$\begin{aligned} p_1 &: (1+i, 7+5i), (1+i, 10+4i) \\ p_2 &: (1+2i, 8+6i), (1+2i, 20) \\ p_3 &: (1+3i, 9+7i), (1+3i, 32-4i) \end{aligned}$$

The initial threshold is $k = 2$. Because three participant are collected, the threshold changes to $k = 3$.

Reconstruct secret using skew polynomials Lagrange interpolation:

$$f_3(x) = \sum_{j=1}^{3} y_j L_j(x_j)^{-1} L_j(x)$$

Assume:

$$\begin{aligned} x_1 &= 1+i, \\ x_2 &= 1+2i, \\ x_3 &= 1+3i \end{aligned}$$

Then,

$$\begin{aligned} L_1(x) &= (x - \sigma(x_3 - x_2)x_3(x_3 - x_2)^{-1})(x - x_2) \\ &= (x + (1+3i))(x - (1+2i)), \\ L_2(x) &= (x - \sigma(x_3 - x_1)x_3(x_3 - x_1)^{-1})(x - x_1) \\ &= (x + (1+3i))(x - (1+i)), \end{aligned}$$

$$\begin{aligned} L_3(x) &= (x - \sigma(x_2 - x_1)x_2(x_2 - x_1)^{-1})(x - x_1) \\ &= (x + (1 + 2i))(x - (1 + i)) \end{aligned}$$

Reconstruct $f_3(x)$ using skew polynomials Lagrange interpolation:

$$\begin{aligned} f_3(x) = &(10 + 4i)(L_1(1 + i))^{-1}L_1(x) + (20)(L_2(1 + 2i))^{-1}L_2(x) \\ &+ (32 - 4i)(L_3(1 + 3i))^{-1}L_3(x) \end{aligned}$$

Evaluate 0 on $f_3(x)$ to get the secret,

$$s = f_3(0) = (5 + 5i).$$

3.5. Algorithm Complexity

In this stage, a complexity comparison will be carried out between the TCSS scheme algorithm using regular polynomials and using skew polynomials. The following are the steps which are considered to determine complexity.
Share Generation Phase :

(i) Determining set of $X = \{x_i\}$ for all $i \in \{1, \ldots, n\}$.

(ii) Evaluation $f_t(x_i)$ for each participant i for all $t \in \{k, k + 1, \ldots, n\}$.

Secret reconstruction phase : interpolation polynomial $f_t(x)$.

3.5.1. TCSS via regular polynomials

In share generation phase, the requirement to determine set of $X = \{x_i\}$ is only pairwise distinct, with $i \in \{1, ..., n\}$. Which mean after select a value of x_i, next value is not allowed equal to all previous value. So the number of comparison steps:

$$T(n) = 1 + 2 + \cdots + (n - 1) = \frac{1}{2}(n - 1)n = \frac{1}{2}n^2 - \frac{1}{2}n$$

The complexity is $O(n^2)$.

For evaluation $f_t(x_i)$, the number of arithmetic operations:

$$\begin{aligned} T(n) &= n \cdot \sum_{t=k}^{n} \left((t - 1) + \sum_{j=1}^{t} (1 + (j - 1)) \right) \\ &= n \cdot \sum_{t=k}^{n} \left((t - 1) + \frac{1}{2}t(t + 1) \right) \\ &= n \cdot \sum_{t=k}^{n} \left(\frac{1}{2}t^2 + \frac{3}{2}t - 1 \right) \end{aligned}$$

For the worst case, assume the minimum $k = 1$.

$$\begin{aligned} T(n) &= n \cdot \sum_{t=1}^{n} \left(\frac{1}{2}t^2 + \frac{3}{2}t - 1 \right) \\ &= n \cdot \left(\frac{1}{2} \sum_{t=1}^{n} t^2 + \frac{3}{2} \sum_{t=1}^{n} t - \sum_{t=1}^{n} 1 \right) \\ &= n \cdot \left(\frac{1}{2} \left(\frac{1}{6}n(n+1)(2n+1) \right) + \frac{3}{2} \left(\frac{1}{2}n(n+1) \right) - n \right) \end{aligned}$$

The complexity is $O(n^4)$.

The total complexity of share generation for the case of a regular polynomial is $O(n^2) + O(n^4) = O(n^4)$.

In the secret reconstruction phase, for interpolation polynomial $f_t(x)$. The Lagrange formula:

$$f_t(x) = \sum_{i=1}^{t} \left(y_{(t,i)} \prod_{j=1, j \neq i}^{t} \frac{(x - x_j)}{(x_i - x_j)} \right)$$

For the worst case, the maximum $t = n$. Number of arithmetic operations:

$$T(n) = (n-1) \cdot (1 + (n-1) \cdot 2)$$

The complexity is $O(n^2)$.

3.5.2. TCSS via skew polynomials

In share generation phase, the requirement to determine set of $X = \{x_i\}$ is σ-pairwise distinct, with $i \in \{1, ..., n\}$. Which mean after select a value of x_i, next value is not allowed equal to all previous value or the σ-conjugate of all previous value. So the number of comparison steps:

$$T(n) = 2 + 4 + \ldots + 2(n-1) = (n-1)n = n^2 - n$$

The complexity is $O(n^2)$.

For evaluation $f_t(x_i)$, the formula:

$$f_t(x_i) = s + \sum_{u=1}^{t-1} a_{t,u} N_u(x_i)$$

with $N_0(x_i) = 0$ and $N_{v+1}(x_i) = \sigma(N_v(x_i))x_i$ for $v \geq 0$.

Number of arithmetic operations:

$$T(n) = n \cdot \sum_{t=k}^{n} \left((t-1) + \sum_{j=1}^{t} (1 + 2j) \right)$$

$$
\begin{aligned}
&= n \cdot \sum_{t=k}^{n} \left((t-1) + t + \frac{1}{2}t(t+1) \right) \\
&= n \cdot \sum_{t=k}^{n} \left(\frac{1}{2}t^2 + \frac{5}{2}t - 1 \right) \\
T(n) &= n \cdot \sum_{t=1}^{n} \left(\frac{1}{2}t^2 + \frac{5}{2}t - 1 \right) \\
&= n \cdot \left(\frac{1}{2}\sum_{t=1}^{n} t^2 + \frac{5}{2}\sum_{t=1}^{n} t - \sum_{t=1}^{n} 1 \right) \\
&= n \cdot \left(\frac{1}{2}\left(\frac{1}{6}n(n+1)(2n+1) \right) + \frac{5}{2}\left(\frac{1}{2}n(n+1) \right) - n \right)
\end{aligned}
$$

The complexity is $O(n^4)$.

The total complexity of share generation for case regular polynomial is $O(n^2)+O(n^4) = O(n^4)$.

In the secret reconstruction phase, for interpolation polynomial $f_t(x)$. The Skew Lagrange formula:

$$f_t(x) = \sum_{i=1}^{t} y_{(t,i)} \left(L_i(x_i)\right)^{-1} L_i(x)$$

with $L_i(x)$ is the monic minimal polynomial such that $L_i(x_j) = 0$ for $i \neq j$.

First, determine the number of operation for finding $L_i(x)$.

For the worst case the maximum $t = n$. Assume the number of operation for finding $L_i(x)$ that vanish 2 elements in Δ is a constant value z. By adding 1 element in Δ, the total operation for finding $L_i(x)$ is added by evaluation of new element on previous generated function. Based on evaluation of skew polynomials, the number operation of finding $L_i(x)$:

$$T(n) = z + \sum_{i=3}^{n} z + \alpha i^2 + \beta i + \gamma$$

For some constants α, β, and γ.

Then,

$$T(n) = c_3 n^3 + c_2 n^2 + c_1 n + c_0$$

For some constants c_0, c_1, c_2, and c_3.

Assume the number of operation for evaluation x_i on $L_i(x)$ is $d_2 n^2 + d_1 n + d_0$.

Number of arithmetic operations in skew Lagrange interpolation:

$$T(n) = (n-1)(c_3 n^3 + c_2 n^2 + c_1 n + c_0 + d_2 n^2 + d_1 n + d_0 + 3)$$

The complexity is $O(n^4)$.

Based on the complexity analysis of the algorithm, it is found that the algorithmic complexity during the share generation phase is the same for both secret sharing schemes, whether using regular polynomials or skew polynomials the algorithm complexity = $O(n^4)$. However, in the secret reconstruction phase, there is an increase in algorithmic complexity in the scheme using skew polynomials compared to using regular polynomials, rising from $O(n^2)$ to $O(n^4)$.

4. Conclusion

Threshold Changeable Secret Sharing (TCSS) can be performed via skew polynomials. Comparison with the regular polynomial, the algorithm complexity remains stable during share generating phase but it has increasing significant during secret reconstruction phase. This provides an advantage in preventing adversaries from easily reconstructing the secret but it doesn't quite affect to dealer for generating shares.

Acknowledgements

This work was funded by the Research and Community Service Program of the Indonesian Ministry of Education, Culture, Research and Technology 2023. The author also expresses gratitude to Institut Teknologi Sumatera for funding the author's doctoral studies during the completion of this research.

References

[1] G.R. Blakley. Safeguarding cryptographic keys. In *Proc. AFIPS NCC*, volume 48, pages 313–317, 1979.

[2] F. Ding, Y. Long, and P. Wu. Study on secret sharing for sm2 digital signature and its application. In *2018 14th International Conference on Computational Intelligence and Security (CIS)*, pages 205–209, 2018.

[3] A.L. Erić. Polynomial interpolation problem for skew polynomials. *Applicable Analysis and Discrete Mathematics*, pages 403–414, 2007.

[4] D. Escudero. An introduction to secret-sharing-based secure multiparty computation. *Cryptology ePrint Archive*, 2022.

[5] H. Gluesing-Luerssen. Skew-polynomial rings and skew-cyclic codes. *arXiv preprint arXiv:1902.03516*, 2019.

[6] G. Hanaoka. A hierarchical non-interactive key-sharing scheme with low memory size and high resistance against collusion attacks. *The Computer Journal*, 45:293–303, 2002.

[7] D. Johnson. Secret sharing schemes and noncommutative polynomial interpolation. University of Manitoba, Canada, 2018.

[8] K. M. Martin, J. Pieprzyk, R. Safavi-naini, and H. Wang. Changing thresholds in the absence of secure channels. In *Australas. Conf. Inf. Secur. Privacy, Springer*, volume 095, pages 177–178, 1999.

[9] K. Meng, F. Miao, W. Huang, and Y. Xiong. Threshold changeable secret sharing with secure secret reconstruction. *Information Processing Letters*, 157:105928, 2020.

[10] E. Noether and W. Schmeidler. Moduln in nichtkommutativen bereichen, insbesondere aus differential-und differenzenausdrücken. *Mathematische Zeitschrift*, 8:1–35, 1920.

[11] O. Ore. Theory of non-commutative polynomials. *Annals of mathematics*, pages 480–508, 1933.

[12] K. Patel. Secure multiparty computation using secret sharing. In *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, pages 863–866, 2016.

[13] A. Shamir. How to share a secret. *Comm. ACM*, 22:612–613, 1979.

[14] T. Tassa and N. Dyn. Multipartite secret sharing by bivariate interpolation. *Journal of Cryptology*, 22:227–258, 2009.

[15] Y. Zhang. A secret sharing scheme via skew polynomials. In *2010 International Conference on Computational Science and Its Applications*, pages 33–38, 2010.