Christopher Foley

Mehrdad Nojoumain

COT6427 Secret Sharing Protocols

29 April 2018

Teaching Secret Sharing

1. Abstract

The goal of this essay is to introduce students to Secret Sharing / Threshold Computing. The topics are presented in a manner for students who have taken High School Mathematics, who may or may not have taken College Algebra. It is not the intent of this essay to go into the topics with great detail, but give students a taste for what is happening.

2. Introduction

The majority of the mathematics involved in Secret Sharing are not beyond the grasp of students who have taken High School Mathematics and may or may not have taken College Algebra. Secret Sharing or Threshold computing involves the mathematics that can be complicated, however if presented in small sets, the fundamental concepts are clear to most students. In this essay, the material presented on Modular Arithmetic and Basic Encryption (Alice/Bob exchange keys) was excerpted from the *Mathematical Ideas* text book used at Broward College at Broward College in Coconut Creek, Florida where I teach as an Adjunct Professor and the material on Secret Sharing is being developed as a unit for the Fall 2018 semester.

The students were surprisingly excited to learn about the Mathematics behind encryption and the underlying concepts can easily be related to their experiences from K-4 through High School.

3. Mathematical Background

The essential concept key to the understanding of Secret Sharing and Cryptology is the ability to trust Mathematics. One side effect of the modern era with the Internet and easy access by hand held computer systems is that each student believes they can be experts by looking up answers. Many were taught that all opinions are equally valid and regretfully they have not learned how to discern fact from fiction and most will side with the idea that if the solution feels right to them it must be correct, thus Live Water and non vaccinations still survive.

With the mathematics given here, if students trust Mathematics, then the work that derives from mathematics is more likely to be trusted. Students will attempt to create their own proof and counterpoints and care must be taken. The objective of this series of lessons is to reduce the math to basic High-School algebra level which will increase the level of trust held by the students.

3.1. Prime and composite Numbers

An introductory lesson in prime numbers is usually presented early in the lessons. In this lesson the students are introduced to the concept of prime numbers and elementary methods for finding them.

3.2. Zero-Knowledge proofs

The intent of zero-knowledge proofs is to demonstrate that one has a secret, or portion of a secret, without giving away any of the secret. Terrorists and criminals, on television, send photos of the kidnapped victim against a blank background holding a current newspaper. Indicating that they have current possession of the victim without revealing the specific location of the hideout. In secret sharing the intent is to demonstrate that a valid portion of the secret is present, without giving away the secret.

3.3. Modular Arithmetic

Modular arithmetic in the classroom is usually shrouded in mystery. However, most students have had experience with modular arithmetic when they view it through the lens of a cyclic system.

3.4. Threshold Computing

Teaching the key element of secret sharing, threshold computing, should be done in three parts: the equation of a line, the equation of a curve, interpolation.

a) Equation of a Line

The key concept here is that two points create a line and that the secret will be a point on the line, the y-intercept. Students who have completed high school are familiar with the concept of a straight line and how to find the equation given two points. They will need the equations for slope and the point slope equation:

$$m=\frac{y_2-y_1}{x_2-x_1} \quad \text{and} \quad y-y_1=m(x-x_1)$$

given these equations, the ability to form create an equation in the *Slope-Intercept* form (*y=mx+b)* is critical.

b) Equation of a curve

Students may or may not already know that the equation of a curve of degree *n* may be discovered with *n+1* points, on the curve. Examples involving quadratic equations are best, although quartic and quintic may be used, depending on student understanding.

c) Interpolation

Lagrange interpolation is introduced for curves of degree 2 or higher. Here the topic of “faith” in mathematics is critical, depending on the experience level of the students. The mathematics may be presented in a manner sufficient for a High School Algebra 2 student to be able to correctly calculate the desired values. The formula for Lagrange interpolation appears confusing, but with two or three examples most students will understand.

Given a set of *n* data points

$(x_{1,} y_1),(x_{2,} y_2),\ldots,(x_j, y_j),\ldots,(x_n, y_n)$

where no two x_j are the same, the interpolation polynomial in the Lagrange form is

$$L(x)=\sum_{i=1}^{n} y_i l_i(x)$$

and

$$l_i(x)=\prod_{\substack{1\leq k<n \\ k\neq i}} \frac{x-x_k}{x_j-x_k}$$

3.5. Basic Encryption

The basics of Key Exchange and encryption may be discussed. I have successfully used simplified examples similar to that used in Simon Singh's *The Code Book* in my Survey of Mathematics class.

3.6. Simple codes

Simple codes may be used and taught. Bud Johnson's *Break The Code Cryptography for Beginners* has many examples of substitution codes for children. If students respond well to the lessons on modular arithmetic then *Bite My Shiny Metal X* should be used, with emphasis on the section involving Alien Languages, in particular Alien Language 2.

4. Lesson

To teach Secret sharing a number of concepts should be covered. I would generally begin with Zero-knowledge proofs, prime numbers, modular arithmetic and progress to threshold computing and encryption.

Depending on the level of knowledge, it might be a good idea to teach encryption after a summary of zero knowledge proofs, then Threshold computing with a threshold of 2. Students can verify that they can recover the encrypted message/secret and compare the **encrypted** secrets to demonstrate possession of the secret without revealing the secret.

4.1. Zero-Knowledge proofs

Zero-Knowledge proofs involve demonstrating that one can possess or demonstrate evidence of a secret without revealing the secret. In his paper, Blum notes a method for proving the existence of a secret involving an example of the three color theorem. The story "*The Strange Cave of Ali Baba"* outlined in the Quisquater, Guillou and Berson paper is a perfect example. In the story, Ali Baba repeatedly demonstrates knowledge of a secret with random input and success in excess of that expected with random selection (100% accuracy). In the Ali Baba example, the authors show that through repeated experimentation the likelihood of successful trials is ½^{n}. They also demonstrate that a rigged demonstration where only successful trials are recorded will appear the same as if one actually possessed the secret.

In Verifiable secret sharing, we show possession of the secret through recreation of the encrypted secret and demonstrate that our encrypted secrets are identical. This is similar to the Naor and Reingold variations on this, using the ubiquitous "Where's Waldo?" problem. One suggestion was to have “Alice” demonstrate to “Bob” that she knows Waldo’s location by cutting Waldo out from a duplicated page or blocking a view of the book/page except where Waldo appears. This shows she has found Waldo without divulging his location.

4.2. Prime Numbers

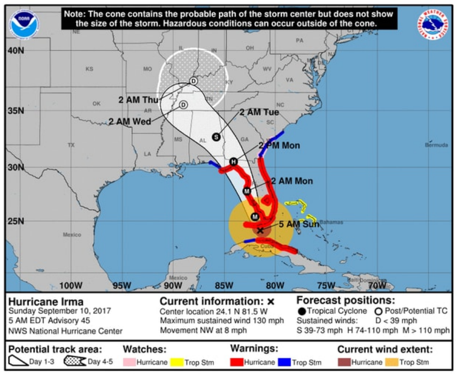
Students should be taught about prime numbers and their importance. The rules for Divisibility can be taught as a leadin to the lesson on primes. The Sieve of Eratosthenes should be taught to give the students a feel for the difficulty of factoring primes. Emphasis should be placed on the idea that when multiplying a prime number by another prime, the resulting should only have two factors. Students should be informed that prime numbers are criticial to the encryption.

4.3. Modular Arithmetic

When teaching I begin with a lesson using analog clocks and relate that to their experiences with clocks and “Army/Military” time. Students with military experience (active/reserve service, JROTC) usuallay pick up the concept quickly.   Manipulatives, similar to those used in primary grades, to teach analog time may be used.

Another example is the calendar, given month X what month is Y months from X.   In 2018 I used the following examples:

1. If I have buy a car in June and have a 36 month loan, during what month will I pay off the loan? This leads to the idea of mod 12. Of particular note is that 36 months has a remainder of zero when divided by 12,
2. My son entered the Army in October. His contract is for 41 months. When will his current contract be up? (March)
3. Using tropical weather patterns common to Florida, is to ask if a Hurricane hits in August, when will the baby boom occur? (Ans: 9 months from August is May).


Note: The cone contains the probable path of the storm center but does not show the size of the storm. Hazardous conditions can occur outside of the cone.
40N
35N
30N
25N
100W
95W
90W
85W
80W
75W
70W
2 AM Thu
2 AM Wed
2 AM Tue
2 PM Mon
2 AM Mon
5 AM Sun
Bermuda
Bahamas
Mexico
Cuba
Hurricane Irma
Sunday September 10, 2017
5 AM EDT Advisory 45
NWS National Hurricane Center
Current information: ×
Center location 24.1 N 81.5 W
Maximum sustained wind 130 mph
Movement NW at 8 mph
Forecast positions:
● Tropical Cyclone ○ Post/Potential TC
Sustained winds: D < 39 mph
S 39-73 mph H 74-110 mph M > 110 mph
Potential track area:
Day 1-3
Day 4-5
Watches:
Hurricane
Trop Stm
Warnings:
Hurricane
Trop Stm
Current wind extent:
Hurricane
Trop Stm

Examples are then extended to other example primes and usually a large number demonstrated.

Once students have mastered the concept of finding remainders, they are then exposed to the idea that when doing modulus, the modulus of a sum or product is product of the moduli, or simply

mod before you multiply

The idea is not foreign, as early on I introduce them to the idea that math with small numbers is easier and less likely to have errors. Since I use the Miller text, I use the examples of Clock arithmetic and residues of large numbers.

One area of concern will be the use of modulus during interpolation. Students will need, depending on their mathematical background, to calculate the values of fractions. They need to be taught/recall/given that in modular arithmetic a^{-1} is the multiplicative inverse NOT the reciprocal. Therefore the following would apply:

$$\frac{4}{3} mod\, 7 = 4 * 3^{-1} mod\, 7$$

The multiplicative inverse of 3 is 5 mod 7 because 1=3*5 mod 7. Therefore,

$$\frac{4}{3} mod\, 7 = 4 * 3^{-1} mod\, 7 = 4 * 5\, mod\, 7 = 6$$

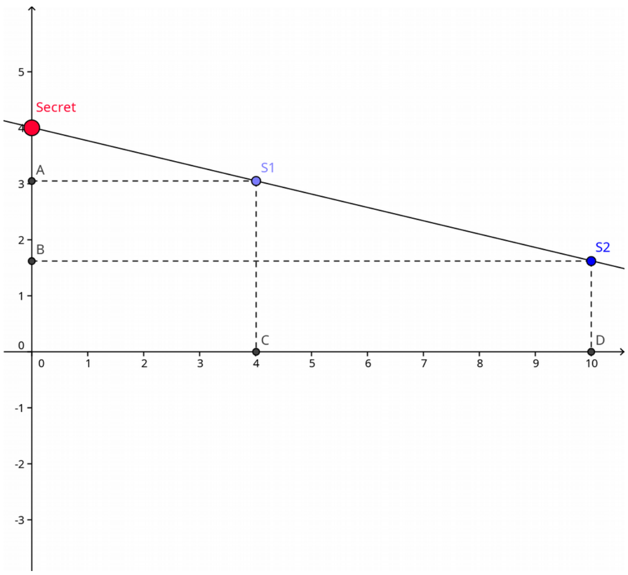
When teaching it might be necessary to give the students the values of the inverses, unless their skill level is sufficient to compute inverses. An example is given in Appendix B.

4.4. Threshold Computing

To understand the key concept of Secret Sharing, threshold computing, I introduce the students to the idea that a secret is a point on the y axis. It can be a number as big or small as needed to convey all the information. It can be 20,000,000 digits (the size of a novel) but the important part is that the secret is mapped to a point on the y axis. For demonstration purposes, I use a point near the x axis. We then remind the students that, in their 9th grade geometry class, they learned that through a point there may be an infinite number of lines/curves. We begin by exploring straight lines, since they are most familiar with those.

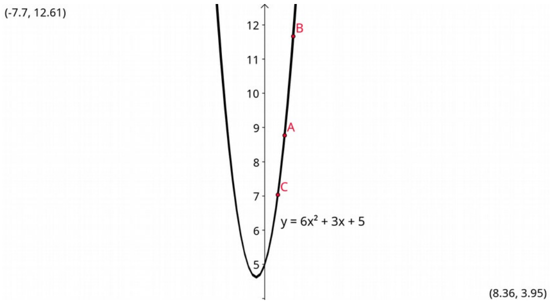
a) Equation of a Line

To split the secret into two parts, we create a random line through the point defined by the secret. The students are then told that the x coordinate represents the id of the shareholder , the secret holder has id 0, and that we use the equation of the line to determine the share value. We then select two arbitrary points on the line and then distribute the points as shares of the secret. This is usually done by providing an example with simple integer values asking the students to reliably (calculate) the secret value given only one point. They quickly realize that they need two points to define a line.



The key concept here is that two points create a line and that the secret will be a point on the line, the y-intercept. Using only one point you have infinite guesses at the secret, but with two points the secret is obvious. Students who have completed high school are familiar with the concept of a straight line and how to find the equation given two points. A standard example would be give the class a point and have them determine the secret, then give a second point and have them compute the secret.

b) Equation of a curve



Students may or may not already know that the equation of a curve of degree *n* may be discovered with *n+1* points, on the curve. Examples involving quadratic equations are best, although quartic and quintic may be used, depending on student understanding. It is similar to the process for a line, where the secret is a point on the y axis and the independent value(s) are the id's for the secret shareholders. A simple example, sharing a secret of 5 would be as follows:

Given: threshold=3, modulus = 13

We share the secret through a random polynomial where f(0)=5

$$f(x)=5+3x+6x^2 \in \mathbb{Z}_{13}[n]$$

We then distribute shares (modulo 13)

$$\begin{gathered} P_1=(1,f(1))=(1,1) \\ P_2=(2,f(2))=(2,9) \\ P_3=(3,f(3))=(3,3) \\ P_4=(4,f(4))=(4,9) \end{gathered}$$

It is clear that each of the participants does not have the full share or any idea of the secret.

c) Interpolation

Lagrange interpolation is introduced for curves of degree 2 or higher. Here the topic of "faith" in mathematics is critical, depending on the experience level of the students. The mathematics may be presented in a manner sufficient for a High School Algebra 2 student to be able to correctly calculate the desired values or the formulas may be given directly depending on the level of ability and the desired outcome.

Using points 1-3 above, we calculate the secret, by letting x=0 and we get the following:

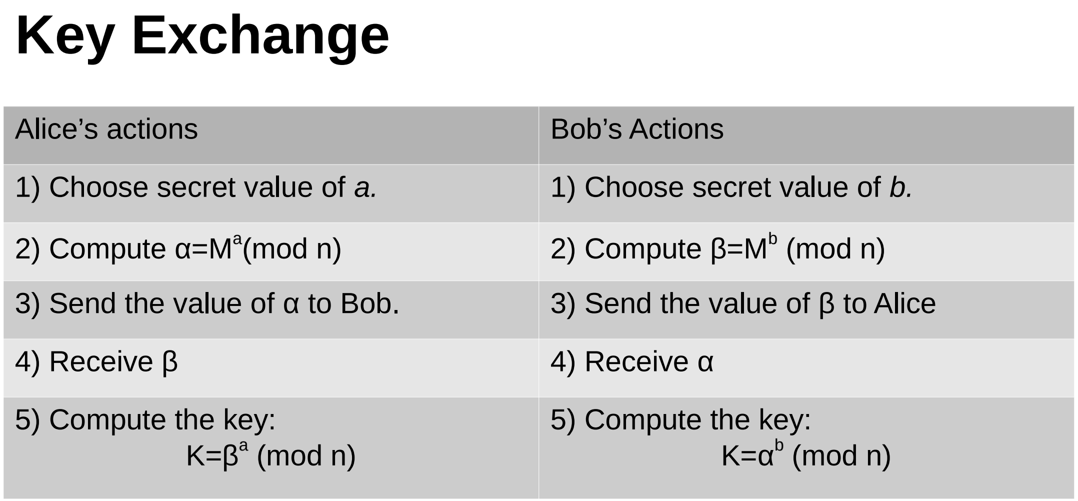
$$\begin{gathered} \alpha=f(0)=\frac{2}{2-1}*\frac{3}{3-1}*f(1)+\frac{1}{1-2}*\frac{3}{3-2}*f(2)+\frac{3}{1-3}*\frac{2}{2-3}*f(3) \\ \alpha=\frac{2}{2-1}*\frac{3}{3-1}*1+\frac{1}{1-2}*\frac{3}{3-2}*9+\frac{3}{1-3}*\frac{2}{2-3}*3 \\ \alpha=2*\frac{3}{2}*1+\frac{1}{-1}*\frac{3}{1}*9+\frac{3}{-2}*\frac{2}{-1}*3 \\ \alpha=-21 mod\, 13=5 \end{gathered}$$

Recalling that $3/2 = 3*2^{-1}$ mod 13 and 2^{-1} mod 13 = 7

Again, I must emphasise that this lesson may/should be abbreviated if the level of comprehension is not at the level desired.

4.5. Key Exchange

To give the benefits of key exchange to students, describe the key exchange between Alice and Bob as noted in *The Code Book*. A good outline is given in the Miller text as shown below:



Key Exchange

Alice’s actions	Bob’s Actions
1) Choose secret value of *a.*	1) Choose secret value of *b.*
2) Compute $\alpha=M^a$(mod n)	2) Compute $\beta=M^b$ (mod n)
3) Send the value of α to Bob.	3) Send the value of β to Alice
4) Receive β	4) Receive α
5) Compute the key: $K=\beta^a$ (mod n)	5) Compute the key: $K=\alpha^b$ (mod n)

Students should discuss the aspects of the key exchange and it is recommended that an example be done to show that both Alice and Bob arrive at the same values. To aid in understanding I compute using the following values: M=7, n=13, a=5 and b=8 (note that a and b are randomly selected, I use small numbers to make the calculations understandable to the student).

After demonstrating a key exchange we then demonstrate encryption and codes.

4.6. Encryption and codes

For a discussion of encryption and coding we discuss different historical approaches. I specicifally refer to a secret decoder rings and other substitution codes. The Alien Language Codes of Futurama are excellent examples of codes. However, it must be emphasized that these contain patterns which may then be used to decrypt the message. Using the Miller text I give a simple demonstration of the RSA algorithm for encoding/decoding, as shown in Appendix A.

4.7. Zero-Knowledge and Verifiable Secret Sharing

One aspect of secret sharing is to demonstrate that the user has a portion of the secret, without revealing the secret. If time permits an exercise (or homework) assignment could be :

1. Encrypt a message similar to the example in Appendix A[1].
2. Share the encrypted secret with three or more, using a threshold of 2.
3. Each share of the encrypted secret should be combined with another share and demonstrate that all combinations of 2 or more shares, yield the same value. (Verifiable Secret Sharing). It should be noted in the exercise that now you have verified that everyone has a share of the secret, buy no one knows the secret.
4. Take two shares from above to reconstruct the encrypted secret.
5. Decrypt the secret using the example in Appendix A.
6. Show that you have the same secret.

Students could be paired for this exercise and could write their answers on index cards as each step is performed allowing for validation by instructor.

[1] It is not necessary to have a message, although it is fun. Inverted numbers on a calculator may be used to create a “secret” message, although care should be taken to have the message reflect the maturity and sensibilities of the students and their litigious parents. See: https://en.wikipedia.org/wiki/Calculator_spelling

5. Conclusions and Observations

My underlying philosophy in Math and Computer Science education is that it is critical to relate the subject taught to the real world, in a fun way. I present this to the students with the disclaimer that the real world is more complicated than our examples, but they do relate and through the use of computers, we can understand and do more than we could a century ago. The mathematics involved in Secret Sharing are not beyond the grasp of students who have taken High School Mathematics and may or may not have taken College Algebra. Secret Sharing or Threshold computing involves the mathematics that can be complicated, however if presented in small sets, the fundamental concepts are clear to most students. When I taught the subset in the Spring of 2018, the students were excited to learn about the Mathematics behind encryption and the underlying concepts can easily be related to their experiences from K-4 through High School.

6. Appendices

6.1. RSA Basics

This appendix contains the content of the overhead slides I used to present RSA basics, the example is based upon the extensions segments in the Miller, Heeren text I use:

- Alice (the receiver) completes the following steps:
    1. Choose two prime numbers, $p=7$ and $q=13$ which are secret
    2. Compute the modulus $n = p * q = 7 * 13 = 91$
    3. Compute $\ell=(p-1)(q-1)=(7 – 1)(13 – 1) = 72$
    4. Chose $e=11$ to be relatively prime between 1 and ℓ
    5. Find the decryption exponent d such that

       $11*d=1$ mod (mod 7)

       d=59
    6. Provide Bob with a public Key ($n=91$ and $e=11$, *p & q are secret*)

- Bob (the sender) completes the following to send Alice a secure message (“HI”, H is letter 8 and I is letter 9) :
  7. Convert the message to Alice into a number M (“HI” = 89)
  8. Encrypt M using Alice’s public key

$$C=M^{e}\ (mod\ n)$$
$$C=89^{11}$$
$$C=89^{1+2+8}$$
$$C=(89^{1}\ mod\ 91)(89^{2}\ mod\ 91)(89^{4}\ mod\ 91)$$
$$C=(89\ mod\ 91)(7921\ mod\ 91)(3.936588806E15\ mod\ 91)$$
$$C=89*4*74\ mod\ 91$$
$$C=26344\ mod\ 91$$
$$C=45$$

  9. Transmit C to Alice

- When Alice receives C, she completes the final step:

  10. Decrypt C using the private key

$$M=C^{d}\ (mod\ n)$$
$$M=45^{59}\ mod\ 91$$
$$M=45^{1+2+8+16+32}\ mod\ 91$$
$$M=(45^{1}*45^{2}*45^{8}*45^{16}*45^{32}\ )mod\ 91$$
$$M=45*23*16*74*16\ mod\ 91$$
$$M=\ 19607040\ mod\ 91$$
$$M=89=\text{”HI” (our original message)}$$

See the footnote above with respect to alternate messages.

6.2. Computing inverse modulo

When we compute the inverse, we are seeking the multiplicative inverse. So if we seek the inverse of a mod n, we look for a number b such that ab = 1 mod n.

a) Computing inverse when modulus is prime

When the modulus and value are relatively prime, their inverse may be computed the inverse may be computed through a variation of Eulers Theorem.

$$a^{\phi(m)} \equiv 1 \, mod \, m$$

which can be shortened to

$$a^{\phi(m)-1} \equiv a^{-1} \, mod \, m$$

if m is prime we get

$$a^{-1} \equiv a^{m-2} \, mod \, m$$

b) Computing the inverse using the Extended Euclidean Algorithm

If two numbers are relatively prime, their Greatest Common Divisor (GCD) is 1. Using the algorithm the equations may be back substituted to solve the equation

$$ax + my = 1$$

Which is then simplified to

$$ax - 1 = (-ym)$$

or, since -ym = 0 mod m

$$ax \equiv 1 \, mod \, m$$

Works Cited / Referenced

- Blum, M. “*How To Prove A Theorem So No One Else Can Claim It”*. *Proceedings of the International Congress of Mathemeticians*. Berkeley, California, USA, (1986) Vol 1.2 American Mathemetical Society, 1444-1451
- Caballero-Gil, Pino and Bruno-Castaneda, Carlos. “A cryptological way of teaching mathematics”. *Teaching Mathematics and Its Applications*, Volume 26, No. 1 2007 (doi:10.1093/teamat/hrl008) , pp 2-16
- “Calculator Spelling.” Wikipedia: The Free Encyclopedia, Wikipedia Foundation, Inc. 13 April 2018 Web accessed 24-April-2018, https://en.wikipedia.org/wiki/Calculator_spelling
- Gaines, Helen Fouché. *Cryptanalysis – a study of ciphers and their solution.* Formerly published as Elementary Cryptanalysis. Dover Publications; New York, New York (1939, 1956)
- Johnson, Bud. *Break The Code Cryptography for Beginners.* Dover Publications; New York, New York (1997).
- Miller, Charles and Heeren,Vern and Hornsby, John and Heeren, Christopher. *Mathematical Ideas, 13th Edition.* Excerpted from *Mathematical Ideas for College and Finite Mathematics Custom Edition for Broward College*, Pearson Learning Solutions, 1026.
- “Modular Multiplicative inverse.” Wikipedia: The Free Encyclopedia, Wikipedia Foundation, Inc. 20 March 2018 Web accessed 27-April-2018, https://en.wikipedia.org/wiki/Modular_multiplicative_inverse

- Naor, M., Naor, Y. and Reingold, O. (1999) “Applied Kid Cryptography” Journal of Cryptology, 1 (1999), Accessed 23-Apr-2018, http://www.wisdom.weizmann.ac.il/~naor/PAPERS/waldo.pdf
- Nojoumian, M. Lecture Notes, COT6427 Secret Sharing Protocols, Florida Atlantic University, Spring 2018
- Quisquater JJ. et al. (1990) How to Explain Zero-Knowledge Protocols to Your Children. In: Brassard G. (eds) Advances in Cryptology — CRYPTO’ 89 Proceedings. CRYPTO 1989. Lecture Notes in Computer Science, vol 435. Springer, NeMw York, NY (doi:https://doi.org/10.1007/0-387-34805-0_60)
- Singh, Simon. “*The Code Book*”, Anchor Books (1999)
- Tsutsui, Hisa. “An Introduction to The Threshold Secret Sharing Scheme in Entry Level Mathematics Courses”. *Mathematics And Computer Education* xxxx, pp. 341-347.
- “Bite My Shiny Metal X.” *Benders Big Score*. DVD_ROM (Extra material): Fox, 2007.