Applied Mathematical Sciences, Vol. 8, 2014, no. 114, 5697 - 5703
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ams.2014.46484

A Secure Bank Locker System Using Hypergeometric Functions

M. K. Viswanath

Department of Mathematics
Rajalakshmi Engineering College, Thandalam
Chennai-602 105, TamilNadu, India

M. Ranjith Kumar

Research Scholar, Research and Development Centre
Bharathiar University, Coimbatore-641 046
TamilNadu, India

Abstract

Using the notion of the secret sharing and hypergeometric functions we develop a safe and secure Bank locker system for our Banks. The method can be applied to similar areas where secrecy and security are the primary concern.

Mathematics Subject Classification: 11T71, 14G50, 68P25, 68R01

Keywords: Secret Sharing, Hypergeometric function and Pochammer symbol

1 Introduction

In Cryptography, secret sharing refers to a method of distributing a secret amongst a group of participants each of whom is allocated a share of the secret. In real world there are many applications that require a group of participants to share a secret such as launching of a nuclear missile, opening of a bank vault, authenticating an electronic fund transaction and etc. Providing secure banking for clients and protecting the bank from fraudulent customers and officials is a primary concern of the Banking sector. Towards this end we design a security system that provides an efficient and advanced door locker system for bank lockers. This system can be used in all fields where security and secrecy are the primary concern. The proposed system will reduce theft, impersonation and unauthorized opening of the locker by the bank staff by providing full security to the locker with the help of a digital locking system.

2 Secret Sharing Schemes

The notion of secret sharing and its method of working were introduced independently by Shamir[12] and Blakley[3] in 1979. Shamir's secret sharing was based on polynomial interpolation over a finite field whereas Blakley's secret sharing was based on hyperplane geometry. A *(t, n)* secret sharing scheme is used to share a secret *S* among *n* people such that any coalition of *t* or more people from these *n* people can construct *S* but smaller coalitions of less than *t* cannot construct *S*.

3 Hypergeometric functions

Hypergeometric functions were known to Euler but it was Gauss who studied it systematically for the first time and this had a tremendous influence in many areas of mathematics.

Before we introduce hypergeometric functions we explain some notation called shifted factorial function or Pochammer symbol.

$$(a)_k = \begin{cases} a(a+1)\cdots(a+k-1) & if \;\; k = 1,2,3,\cdots \\ 1 & if \;\; k = 0 \end{cases}$$

It can be easily seen that $(a)_k = \dfrac{\Gamma(\mathrm{a+k})}{\Gamma(\mathrm{a})}$.

The hypergeometric function ${}_2F_1(a,b;c;\mathrm{x})$ is defined by the series

$${}_2F_1(a,b;c;\mathrm{x}) = 1 + \frac{ab}{c}x + \frac{a(a+1)b(\mathrm{b}+1)}{c(c+1)}\frac{x^2}{2!} + \ldots = \sum_{n=0}^{\infty}\frac{(a)_n(b)_n}{(c)_n}\frac{x^n}{\mathrm{n}!}$$

Where $|x| \le 1$and *a, b, c* are neither zero nor a negative integer so that the series is neither unity nor terminating. The series converges absolutely for $|x| < 1$and diverges for $|x| > 1$. When $|x| = 1$ the series converges absolutely if $(c-(a+b)) > 0$, $a,b,c \in$ □ . The hypergeometric function ${}_2F_1(a,b;c;\mathrm{x})$ is symmetric with respect to a, b and there is a beautiful formula of Gauss that shows ${}_2F_1\left(a,b;c;1\right)=\dfrac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)}$. Incidentally Srinivasa Ramanujan also worked extensively on hypergeometric functions throughout his life time [5].

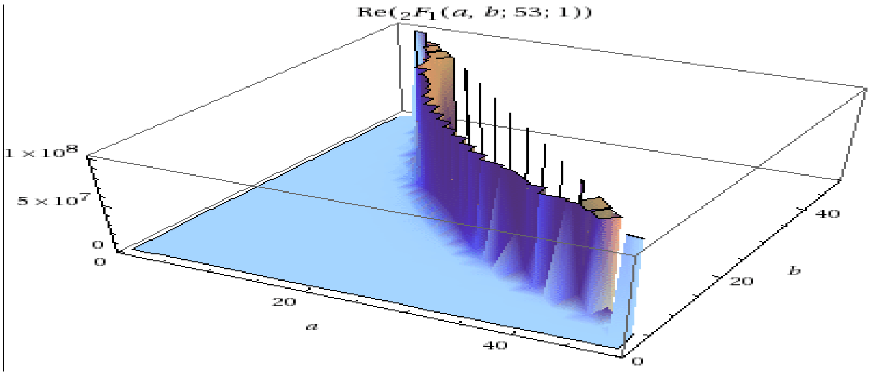

Figure 1: Hypergeometric function ${}_2F_1$(a, b; 53; 1)
(Plot as real parts of two parameter *a* and *b* vary from 1 to 49)

4 Hypergeometric functions and digital locker system

In this paper we propose a secret sharing scheme based on hypergeometric functions. A secret *c* is divided between two persons and what each one gets is called a share or shadow. The Head office of the bank assigns a secret number *c* to each one of the customers of a branch having the locker system. This secret is known only to the head office official and not known to the customer or any official of the bank branch. This secret number *c* is stored in the data base of the customer in the head office and is not known to the branch office staff.

5 Working of the system

When a customer of a bank branch wants to open his locker in the bank, the first step is that he should scan his finger print for identification. If the finger print matches with that of the stored data base then he crosses the first hurdle of getting access to the locker door which has a monitor. Once the customer scans his finger print, an alert mail is sent to the clerk, the manager and the customer for security purpose and simultaneously the control system will generate a three tuple password to open the door. This three tuple password say *(a, b, k)* is such that *c* = *a*+*b*+*k*, *k* is randomly generated such that $1\le k\le 10$ and is hidden from the customer and the bank staff. In a day only three attempts are allowed for the customer and each time the value of random k is not repeated again. Only *a* and *b* are distributed to the customer and the clerk through a secure public channel. These *a* and *b* are the shares or shadows of the customer and the clerk which they have to input respectively for the opening of the locker. The control system on receiving *a* and *b* computes $a+b+k$ and compares its value with that of *c* and proceeds further only if $c = a+b+k$. The system is pre-programmed in such a way that it calculates immediately the hypergeometric function ${}_2F_1(a,b;c;1)$ and computes $\alpha \equiv {}_2F_1(a,b;c;1) \pmod{k}$. Note that the branch staff is not aware of *c* and *k* and the head office staff is not aware of *a* and *b*. The number α is sent to the manager by the control system through a secure channel. The manager on receiving α, inputs this α into the control system and the customer can access the locker only if this α is matched. After receiving the entry mail the customer opens the locker and the manager and clerk notes down the entry time of the customer for security purpose. Further improvement to the security of the system can be made by introducing more number of participants. We mention that the above system provides a three tier security as given below.

I. First level security : Finger print of the Customer

II. Second level security : Confirmation of the shares *a* and *b* entered by the customer and the clerk in the control system.

III. Third level security : Confirmation of the manager's entry α by the system and only after this the customer can access the system.

6 The system setup

I. Customer identification

(i). Entry of the finger print by the customer to open the locker.

(ii). The control system verifies the entered finger print with the one stored in the data base and if it matches the system proceeds further and the system indicates incorrect input, otherwise.

II. Distribution of the shares

(i). The control system after identifying the finger print, selects the three tuple *(a, b, k)* from the stored data.

(ii). Distributes the shares *a* and *b* to the customer and clerk through a secure channel.

(iii). Computes $c = a+b+k$, where *c* and *k* are kept as secret and *k* is chosen at random such that $1 \le k \le 10$.

III. Verification of the shares

(i). The control system receives the shares from the customer and clerk say *a'* and *b'*.

(ii). The system computes $a'+b'+k$ and compares it with the actual $c=a+b+k$ and checks whether $a=a'$ and $b=b'$.

(iii). If the entered values are correct, then the system proceeds further, otherwise it indicates incorrect input and prompts the user for authentic shares, subject to a maximum of two trials.

IV. Accessing process of the locker

(i). The control system computes $\alpha \equiv {}_2F_1\left(a,b;c;1\right) \pmod{k}$ and send it to the manager through a secure channel.

(ii). The manager receives α' and enters α' and if both α and α' are matched then the locker is accessible for the customer and exit.

7 Block Diagram

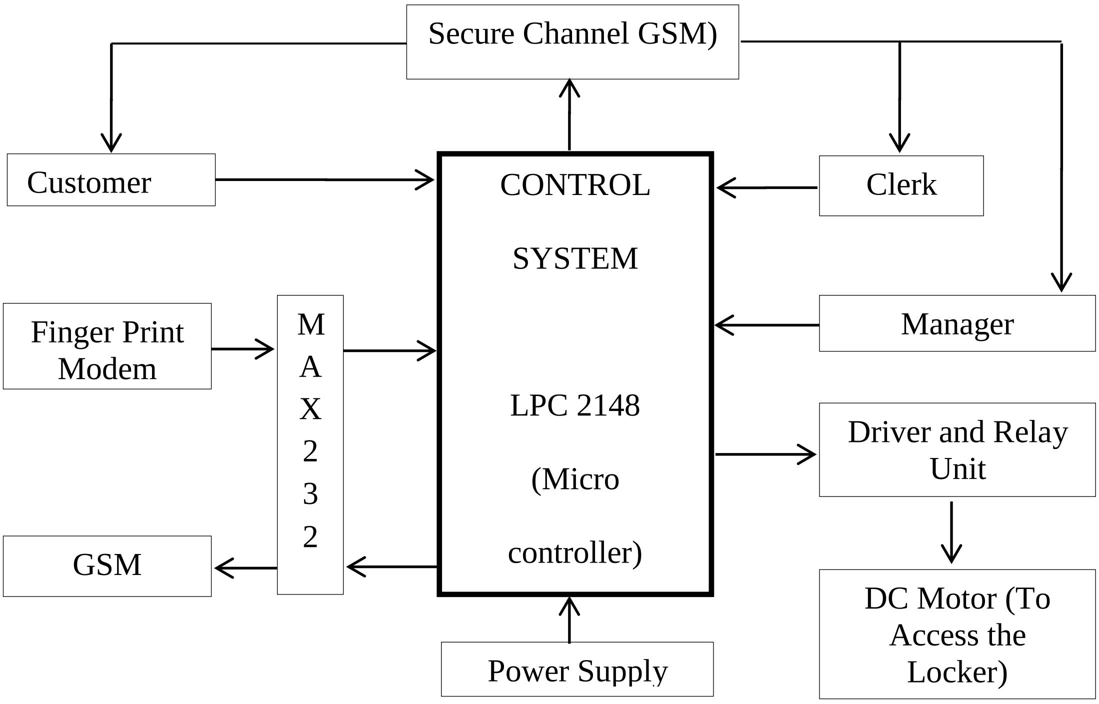

Figure 2: Block diagram for locker security.

8 Illustration

As the number of lockers in a branch is less than 150 we take c to be such that $1 \le c \le 200$ and so the shares a, b are such that $1 \le a,b \le 200$. Assume that the randomly chosen k is 3, a=90 , b=10 and c=103. After scanning the finger print of the customer, the customer is given his share 90 and the clerk his share

10. The control system checks whether c=90+10+3. Note that c=103 and k=3 are hidden from the bank branch. After receiving the shares of the customer and the clerk, the control system proceeds to compute $\alpha \equiv {}_2F_1(a,b;c;1) \pmod{k} \equiv 2 \pmod{3}$.The value $\alpha = 2$ is sent to the manager. The manager enters this value ($\alpha = 2$), the locker door opens up for the customer. Thus this system is very secure as it cannot be opened by the customer without the help of the manager and the clerk and the manager and the clerk alone cannot open without the customer.

References

[1] W.N. Bailey, Generalized Hypergeometric series, Cambridge, England: University Press, 1935.

[2] J. Benolah, J. Leichter, Generalized secret sharing and monotone functions, Advances in cryptology-CRYPTO'88, S. Goldwasser, Ed., Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, Vol.403, 1989.

[3] G.R. Blakley, Safeguarding cryptography keys, AFIPS 1979, National Computer Conference, Vol.48, 1979, 313-317.

[4] M.J. Collins, A Notes on Ideal Tripartite Access Structures. Cryptology ePrint Archive, Report 2002/193, http://eprint.iacr.org/2002/193.

[5] G.H. Hardy, Hypergeometric series, ch-7 in Ramanujan: Twelve Lectures on subjects suggested by His Life and Work, 3rd ed., New York: Chelsea, (1999), 101-112.

[6] M. Ito, A. Saito, T. Nishizeki, Secret Sharing Scheme realizing general access structure, IEEE Globecom Conference, 1987, 99-102.

[7] N. Koblitz, A course in Number Theory and Cryptography, Springer, 1994.

[8] A.J. Menezes, P.C. Oorschot Van, S.A. Vanstoon, Handbook of Applied Cryptography, CRC Press, USA, 1997.

[9] M. Mignotte, How to share a secret, Cryptography, Workshop Proceedings, Lecture Notes in Computer Science, Vol.149, Springer – Verlag, 1983.

[10] C. Padro, G. Saez, Secret Sharing Schemes with bipartite access structure, IEEE Transactions for Information Theory Vol.46, 2000, 2596-2604.

[11] P.D. Seymour, On secret-sharing matroids, Journal of Combinatorial Theory Vol.56, 1992, 69-73.

[12] A. Shamir, How to share a secret, Communications of ACM, Vol.22, 1979.

[13] D.R. Stinson, Decomposition construction for secret-sharing schemes, IEEE transactions for Information Theory, Vol.140, 1994, 118-125.

[14] M.K. Viswanath, K.P. Vidya, Pollard's rho Split Knowledge Scheme, K.G. Subramanian, K. Rangarajan and Madhavan Mukund, Editors, Formal Models, Languages and Applications, Series in Machine Perception and Artificial Intelligence, Vol.66, World Scientific Publishing, 2006, 378-389.

Received: June 7, 2014