AUTHENTICATED MULTIPLE KEY DISTRIBUTION USING SIMPLE CONTINUED FRACTION

S. Srinivasan¹, P. Muralikrishna²§, N. Chandramowliswaran³

¹,²School of Advanced Sciences
VIT University
Vellore, 632014, Tamilnadu. INDIA
³Visiting Faculty
Indian Institute of Management Indore
Indore, 453 331, INDIA

Abstract: In recent years the security of operations taking place over a computer network become very important. It is necessary to protect such actions against bad users who may try to misuse the system (e.g. steal credit card numbers, read personal mail, or impersonate other users.) Many protocols and schemes were designed to solve problem of this type. Threshold cryptography is a novel cryptographic technique sharing secret among members. It divides a secret key into multiple shares by a cryptographic operation. In this paper, we proposed a key distribution algorithm based on Simple Continued Fraction. The goal of our algorithm is to divide a secret $S$ into $\ell$ pieces $s_1 + s_2 + \cdots + s_\ell$ such that, $\ell$ pieces are necessary to reconstruct $S$, but any $m < \ell$ pieces give no information about $S$.

AMS Subject Classification: 94A60, 94A62
Key Words: simple continued fraction, shares, RSA prime

1. Introduction

Secret sharing (also called secret splitting) refers to method for distributing a
secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number, of possibly different types, of shares are combined together; individual shares are of no use on their own.

Secret sharing was invented independently by Adi Shamir [3] and George Blakley [1] in 1979. Secret sharing schemes are ideal for storing information that is highly sensitive and highly important. Examples include: encryption keys, missile launch codes and numbered bank accounts. Each of these pieces of information must be kept highly confidential, as their exposure could be disastrous, however, it is also critical that they not be lost. Traditional methods for encryption are ill-suited for simultaneously achieving high levels of confidentiality and reliability. This is because when storing the encryption key, one must choose between keeping a single copy of the key in one location for maximum secrecy, or keeping multiple copies of the key in different locations for greater reliability. Increasing reliability of the key by storing multiple copies lowers confidentiality by creating additional attack vectors; there are more opportunities for a copy to fall into the wrong hands. Secret sharing schemes address this problem, and allow arbitrarily high levels of confidentiality and reliability to be achieved.

A secure secret sharing scheme distributes shares so that anyone with fewer than \( t \) shares has no extra information about the secret than someone with 0 shares.

Consider for example the secret sharing scheme in which the secret phrase \textit{security} is divided into the shares \( se------, cu----, ri-- ,\) and \( ty.\) A person with 0 shares knows only that the password consists of eight letters. He would have to guess the password from \( 26^8 = 208 \text{ billion} \) possible combinations. A person with one share, however, would have to guess only the six letters, from \( 26^6 = 308 \text{ million} \) combinations, and so on as more persons collude. Consequently this system is not a secure secret sharing scheme, because a player with fewer than \( t \) secret-shares is able to reduce the problem of obtaining the inner secret without first needing to obtain all of the necessary shares.

2. Proposed Algorithms

Construction of the Non-Homogeneous Equation

\textbf{Definition} An expression of the form \( C_0 + \frac{1}{C_1 + \frac{1}{C_2 + \frac{1}{C_3 + \ldots \frac{1}{C_n \ldots}}}} \) where \( C_j : \)
Continued Fraction $j \geq 1$ are positive integers and $C_0$ is a non-negative integer is called a Simple Continued Fraction (SCF).

- Define $\frac{P_1}{Q_1} = \frac{C_0}{1}$
  $\frac{P_2}{Q_2} = C_0 + \frac{1}{C_1} = \frac{C_0C_1+1}{C_1}$
  $\frac{P_3}{Q_3} = C_0 + \frac{1}{C_1 + \frac{1}{C_2}} = \frac{C_0(C_1C_2+1)+C_2}{C_1C_2+1}$

- In general, we have
  $\frac{P_{n+1}}{Q_{n+1}} = C_0 + \frac{1}{C_1 + \frac{1}{C_2 + \frac{1}{\ldots + \frac{1}{C_n}}}}$ (1)

  then, $\frac{P_{n+1}}{Q_{n+1}}$ is called $(n+1)^{th}$ convergent of SCF

- Let us denote $C_0 + \frac{1}{C_1 + \frac{1}{C_2 + \frac{1}{\ldots + \frac{1}{C_n}}}}$ by $[C_0; C_1, C_2, C_3, \ldots, C_n]$ i.e., $\frac{P_{n+1}}{Q_{n+1}} = [C_0; C_1, C_2, C_3, \ldots, C_n]$ (2)

- Alternatively, we can represent SCF as the product of special $2 \times 2$ matrices over non-negative integers
  $\begin{bmatrix} C_0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} C_1 & 1 \\ 1 & 0 \end{bmatrix} \ldots \begin{bmatrix} C_n & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} P_{n+1} & P_n \\ Q_{n+1} & Q_n \end{bmatrix}$ (3)

- Taking determinant on both sides of (4), we get
  $(-1)^{n+1} = P_{n+1}Q_n - Q_{n+1}P_n$ for all $n \geq 1$ (5)

- Taking transpose of (4), we get
  $\begin{bmatrix} C_0 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} C_{n-1} & 1 \\ 1 & 0 \end{bmatrix} \ldots \begin{bmatrix} C_1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} P_{n+1} & Q_{n+1} \\ P_n & Q_n \end{bmatrix}$ (6)

- Let $R_1, R_2$ be two given very large odd primes with $R_1 < R_2$

- Represent $\frac{R_1}{R_2}$ as a SCF
  $\frac{R_1}{R_2} = C_0 + \frac{1}{C_1 + \frac{1}{C_2 + \frac{1}{\ldots + \frac{1}{C_n}}}} = [C_0; C_1, C_2, C_3, \ldots, C_n]$ (7)

- Consider the symmetric continue fraction of length $2n + 2$
  $\frac{P_{2n+2}}{Q_{2n+2}} = [C_n; C_{n-1}, C_{n-2}, \ldots, C_1, C_0, C_0; C_1, C_2, C_3, \ldots, C_n]$ (8)

  where $\frac{P_i}{Q_i}$ be the $i^{th}$ convergent of (7)

- $\frac{P_{n+1}}{Q_{n+1}} = [C_n; C_{n-1}, C_{n-2}, \ldots, C_1, C_0]$
  $\frac{P_n}{Q_n} = [C_n; C_{n-1}, C_{n-2}, \ldots, C_1]$
  $\frac{P_{n+1}}{Q_n} = [C_0; C_1, C_2, C_3, \ldots, C_n-1, C_n]$
  $\frac{Q_{n+1}}{Q_n} = [C_0; C_1, C_2, C_3, \ldots, C_{n-1}, C_n]$
Therefore
\[
\begin{bmatrix}
C_n & 1 & 0 \\
1 & 0 & 1 \\
\end{bmatrix}
\cdots
\begin{bmatrix}
C_1 & 1 & 0 \\
1 & 0 & 1 \\
\end{bmatrix}
\begin{bmatrix}
C_1 & 1 & 0 \\
1 & 0 & 1 \\
\end{bmatrix}
\begin{bmatrix}
C_1 & 1 & 0 \\
1 & 0 & 1 \\
\end{bmatrix}
\cdots
\begin{bmatrix}
C_n & 1 & 0 \\
1 & 0 & 1 \\
\end{bmatrix}
\begin{bmatrix}
P_{2n+2} & P_{2n+1} \\
Q_{2n+2} & Q_{2n+1} \\
\end{bmatrix}
= A
\]  
(8)

Clearly, \( \det(A) = (-1)^{2n+2} = 1 \)

Consider
\[
\begin{bmatrix}
C_n & 1 & 0 \\
1 & 0 & 1 \\
\end{bmatrix}
\cdots
\begin{bmatrix}
C_1 & 1 & 0 \\
1 & 0 & 1 \\
\end{bmatrix}
\begin{bmatrix}
C_1 & 1 & 0 \\
1 & 0 & 1 \\
\end{bmatrix}
\begin{bmatrix}
C_1 & 1 & 0 \\
1 & 0 & 1 \\
\end{bmatrix}
\cdots
\begin{bmatrix}
C_n & 1 & 0 \\
1 & 0 & 1 \\
\end{bmatrix}
\begin{bmatrix}
P_{n+1} & P_n \\
Q_{n+1} & Q_n \\
\end{bmatrix}
\begin{bmatrix}
P_{n+1} & Q_{n+1} \\
P_n & Q_n \\
\end{bmatrix}
\begin{bmatrix}
P_{n+1} & P_n Q_n \\
Q_{n+1} & Q_n + P_n Q_n \\
\end{bmatrix}
\begin{bmatrix}
P_{2n+2} & P_{2n+1} \\
Q_{2n+2} & Q_{2n+1} \\
\end{bmatrix}
\]
\[
P_{2n+2}Q_{2n+1} - P_{2n+1}Q_{2n+2} = 1
\]
\[
(P_{n+1}^2 + P_n^2)Q_{2n+1} = P_{2n+1}^2 + 1
\]
\[
(R_1^2 + R_2^2)Y = X^2 + 1
\]
where \( P_{n+1} = R_1, P_n = R_2, P_{2n+1} = X \) and \( Q_{2n+1} = Y \)

Here, we proposed an algorithm and its actual implementation. Our primary contribution is that, in our algorithm we discussed the key sharing by using two prime numbers and a non-homogeneous equation with two variables. The share holders can verify the validity of their shares only after reconstruction of the secret and any share holders fewer than \( \ell \), can not reconstruct the secret.

**Algorithm for Encryption**

- Choose two secret very large odd primes \( R_1, R_2 \) with \( R_1 > R_2 \)
- Construct \( x^2 + 1 = (R_1^2 + R_2^2)y \)
- Select two large RSA secret odd primes \( p \) and \( q \)
- Define \( N = pq \) then \( \phi(N) = (p - 1)(q - 1) \) where \( \phi(N) \) is Euler phi function
- Select a secret exponent \( e \) such that \( (e, \phi(N)) = 1 \) where \( 1 < e < \phi(N) \)
- For this \( e \), there is a unique \( d \) such that \( ed \equiv 1 \pmod{\phi(N)} \)
• consider \( a = (R_1^2 + R_2^2)(y + d) - (x + \phi(N))^2 \)
  \[
a = (R_1^2 + R_2^2)y - x^2 + (R_1^2 + R_2^2)d - [\phi(N)]^2 - 2x\phi(N)
  = 1 + (R_1^2 + R_2^2)d - [\phi(N)]^2 - 2x\phi(N)
  \]
  \( a \equiv (1 + (R_1^2 + R_2^2)d) \mod \phi(N) \)
  \( ae \equiv (e + (R_1^2 + R_2^2)) \mod \phi(N) \)

  \( S \equiv e \mod \phi(N) \)

  where \( S = ae - (R_1^2 + R_2^2) \)

• Here we define \( S \) is the **exponent secret**

• Represent the secret message \( m \) in the interval \([0, N - 1]\)
  with \( \gcd(m, N) = 1 \)

**Algorithm for Key Sharing**

• Consider the \( \ell \) exponent secret partition (share holders)
  \( S = s_1 + s_2 + \cdots + s_\ell \)

  Define \( Y_i \equiv m^{s_i} \mod N \) for \( 1 \leq i \leq \ell \)

  \( \prod_1^\ell Y_i \equiv m^S \mod N \)
  \( \equiv m^{s_1 + s_2 + \cdots + s_\ell} \mod N \)
  \( \equiv m^{s_1} m^{s_2} \cdots m^{s_\ell} \mod N \)

• For \( \ell \) secret share holders we can distribute \( \ell \) key’s such as \( Y_1, Y_2, \ldots, Y_\ell \)

• Sharing scheme follows from the given equations:
  \( \prod_1^\ell Y_i \equiv m^S \mod N \)
\[ \equiv m^{k\phi(N)+e} (mod N) \]
\[ \equiv m^{k\phi(N)} m^e (mod N) \]
\[ \equiv [m^{\phi(N)}]^k m^e (mod N) \]
\[ \prod \ell Y_i \equiv m^e (mod N) \]

- High Level Authentication Key manager is \( d \)
\[ (\prod \ell Y_i)^d \equiv (m^e)^d (mod N) \]
\[ (\prod \ell Y_i)^d \equiv m (mod N) \]

3. Conclusion

This paper dealt with a secret key sharing mechanism on \( \ell \) share holders. According to the algorithm, the secret can be well shared with feasible sense, it may have some performance impact when the number of share holders is accordingly increased. Our approach to secret sharing is opened a number of avenues for future work. These include research into finding schemes that will remove the restrictions on the size of \( \ell \). These schemes make it possible to store secret information in a network.

References


