TWMS J. App. and Eng. Math. V.11, Special Issue, 2021, pp. 63-74

KEY DISTRIBUTION USING GRAPHS FOR SECRET SHARING

RISHABH MALHOTRA[1], N. CHANDRAMOWLISWARAN [2], §

Abstract. Key distribution for secret sharing is the core important aspect of any secure cryptosystem, the threshold scheme enables a secret key to be shared among p members in which each member holds a part of the secret key. In recent years, many works have been done on constructing $(t+1, l)$ threshold schemes using different algebraic aspects of the mathematics. In this paper, we discuss certain aspects of key sharing using *Graph Theory* and *Strongly co-prime integers* to present techniques which manage the sharing of keys equally amongst the users keeping the security of the system intact.

Keywords: Key Distribution, Chinese Remainder Theorem, Asymmetric Graph, Strongly co-prime integers, Graceful Labelling
AMS Subject Classification: 94A60; 94A62; 05C78

1. Introduction

A cryptosystem consists of an encryption/decryption algorithm and a key. The algorithm, along with the key, encrypts the message M to get the encrypted text $Enc(M)$. In order to secure the cryptosystem, the sharing of the secret keys needs to safe guarded. Secret sharing/key distribution is the procedure of assigning a secret amongst a class, each of whom is given a share of the secret. When different types of shares are merged together then only the secret can be retrieved; individual shares are of no use on their own.

In 1979, Blakley suggested an idea of Key Sharing using the concept of Guarding Keys [4]. Shamir later presented a secret sharing scheme based on Lagrange's polynomial interpolation [1]. The Chinese Remainder Theorem has been used widely in secret sharing schemes, Mignotte Scheme [8], Asmuth-Bloom Scheme use the threshold key sharing technique where the secret are created by reduction modulo the integers [2]. Tao Feng, Jiaqi Guo proposed a new access control model which uses Linear Secret Sharing Scheme [12]. Sorin Iftene also proposed a secret sharing scheme using the CRT with its application in multi-authority key sharing scheme [11].

Key management deals with the generation, exchange, storage, and application of keys. The Key Exchange protocols should mantain the following compliance domains [5]:

1. Confidentiality - The secret key should be accesible only to the authorised user.
2. Integrity - The code of the key should not be altered by some third person.

[1] Amity Institute of Information and Technology, Amity University Rajasthan, India.
e-mail: rish.malhotra1996@gmail.com; ORCID: https://orcid.org/0000-0002-7178-3458.
[2] Amity University Haryana, India.
e-mail: ncmowli@hotmail.com; ORCID: https://orcid.org/0000-0002-9828-777X.
§ Manuscript received: October 15, 2019; accepted: April 2, 2020.
TWMS Journal of Applied and Engineering Mathematics, V.11, Special Issue

3. Availability - The key should be available for use at the required time, that is, some malicious user must not be able to destroy the key.

Keys are the most crucial asset for any cryptosystem, and hence are prone to many cyber attacks. A side channel leak or a human error (like social hacking) may lead to the destruction of the whole cryptosystem, leading the organisation's data to a breach. In order to add another layer of security, the keys are usually stored in pieces, the procedure to store the keys in such a manner is called *threshold scheme*.

1.1. **Threshold Scheme.** When storing the encryption key, one must decide on 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. Raising genuineness or authenticity of the key by storing numerous replicas at various positions lowers secrecy by providing more chances for a copy to fall into the wrong hands. Secret sharing strategy deals with this issue, and allows effective secrecy and authenticity to be attained. A secure secret sharing strategy assigns $t - shares$ so that any person with $(t-1) - shares$ has no additional knowledge about the secret than someone with $0 - shares$.

If a person with $(t-1) - shares$ is able to lower the problem of attaining the inner secret without first needing to recover all of the significant portions, the network is not secure enough. More generally, (n, k) secret sharing is the problem of distributing the secret key S among n people so that no *k-1* of them have any information about S but k of them can determine S [6, 7].

For record, we would like to mention the Chinese Remainder Theorem

Theorem 1.1 (CRT) Suppose that $m_1, m_2, ..., m_r$ are pairwise relatively prime positive integers, and let $a_1, a_2, ..., a_r$ be integers. Then the system of congruences, $x \equiv a_i (\text{mod } m_i))$ for $1 \leq i \leq r$, has a unique solution *modulo* $M = m_1 \times m_2 \times ... \times m_r$, which is given by: $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_r M_r y_r (\text{mod } M)$, where $M_i = M/m_i$ and $y_i \equiv (M_i)^{-1} (\text{mod } m_i)$ for $1 \leq i \leq r$.

2. Key Sharing Using Mutually Co-Prime Integers

One of the major challanges in the key management system is related to the *scalability* of the system. A large number of encryption keys with a support system running among multiple databases might consume a lot of space in the network and hence time.

The proposed system involves a design of pre-distribution algorithm using a deterministic approach. This algorithm uses Graph Theory and Number Theory with high connectivity, high resilience and memory requirement.

Theorem 2.1 Consider three very large mutually co-prime positive integers a, b, c such that

$$a^{\phi(b)} + b^{\phi(a)} \not\equiv 0 (\text{mod } c)$$
$$a^{\phi(c)} + c^{\phi(a)} \not\equiv 0 (\text{mod } b)$$
$$b^{\phi(c)} + c^{\phi(b)} \not\equiv 0 (\text{mod } a)$$

Let S be the given secret and $N = abc$ where a, b and c are mutually co-prime positive integers and ϕ is the *Euler's Phi Function*. Define three secret shareholders Y_1, Y_2, Y_3 as

follows:

$Y_1 \equiv (-Sk_1a(b^{\phi(c)} + c^{\phi(b)}))(\text{mod } N)$
$Y_2 \equiv (-Sk_2b(a^{\phi(c)} + c^{\phi(a)}))(\text{mod } N)$
$Y_3 \equiv (-S\left[k_3c(a^{\phi(b)} + b^{\phi(a)}) + 1\right])(\text{mod } N)$

then $S = Y_1 + Y_2 + Y_3(\text{mod } N)$

Theorem 2.2 Let a, b, c, d are mutually co-prime positive integers. Then there exist integers k_1, k_2, k_3, k_4 such that
$k_1a\left[b^{\phi(cd)} + c^{\phi(bd)} + d^{\phi(bc)}\right] + k_2b\left[a^{\phi(cd)} + c^{\phi(ad)} + d^{\phi(ac)}\right] + k_3c\left[a^{\phi(bd)} + b^{\phi(ad)} + d^{\phi(ab)}\right] + k_4d\left[a^{\phi(bc)} + b^{\phi(ac)} + c^{\phi(ab)}\right] + 6 \equiv 0(\text{mod } abcd)$

Proof

Define $X = b^{\phi(cd)} + c^{\phi(bd)} + d^{\phi(bc)} + a^{\phi(cd)} + c^{\phi(ad)} + d^{\phi(ac)} + a^{\phi(bd)} + b^{\phi(ad)} + d^{\phi(ab)} + a^{\phi(bc)} + b^{\phi(ac)} + c^{\phi(ab)} - 6$

$X \equiv b^{\phi(cd)} + c^{\phi(bd)} + d^{\phi(bc)}(\text{mod } a)$
$X \equiv a^{\phi(cd)} + c^{\phi(ad)} + d^{\phi(ac)}(\text{mod } b)$
$X \equiv a^{\phi(bd)} + b^{\phi(ad)} + d^{\phi(ab)}(\text{mod } c)$
$X \equiv a^{\phi(bc)} + b^{\phi(ac)} + c^{\phi(ab)}(\text{mod } d)$

By the CRT, we have

$X \equiv (b^{\phi(cd)} + c^{\phi(bd)} + d^{\phi(bc)})M_aM'_a + (a^{\phi(cd)} + c^{\phi(ad)} + d^{\phi(ac)})M_bM'_b + (a^{\phi(bd)} + b^{\phi(ad)} + d^{\phi(ab)})M_cM'_c + (a^{\phi(bc)} + b^{\phi(ac)} + c^{\phi(ab)})M_dM'_d$

Therefore, there exist integers k_1, k_2, k_3, k_4 such that
$k_1a(b^{\phi(cd)} + c^{\phi(bd)} + d^{\phi(bc)}) + k_2b(a^{\phi(cd)} + c^{\phi(ad)} + d^{\phi(ac)}) + k_3c(a^{\phi(bd)} + b^{\phi(ad)} + d^{\phi(ab)}) + k_4d(a^{\phi(bc)} + b^{\phi(ac)} + c^{\phi(ab)}) + 6 \equiv 0(\text{mod } abcd)$

The theorems can be generalised to the following lemmas

Lemma 2.1 Let S be the given secret and $N = pqr$ where p, q, r are distinct large prime numbers. Define three secret shareholders Y_1, Y_2, Y_3 as:
$Y_1 \equiv (-Sk_1p(q^{\phi(r-1)} + r^{\phi(q-1)}))(\text{mod } N), Y_2 \equiv (-Sk_2q(p^{\phi(r-1)} + r^{\phi(p-1)}))(\text{mod } N), Y_3 \equiv (-Sk_3r(p^{\phi(q-1)} + q^{\phi(p-1)}))(\text{mod } N)$ then $S = Y_1 + Y_2 + Y_3(\text{mod } N)$

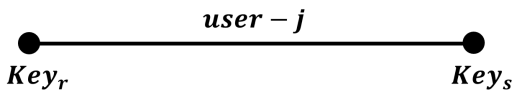
Lemma 2.2 Let p, q and r be the three given distinct odd primes. Then there exist integers k_1, k_2, k_3 such that:
$k_1p(q^{r-1} + r^{q-1}) + k_2q(p^{r-1} + r^{p-1}) + k_3r(p^{q-1} + q^{p-1}) + 2 \equiv 0(\text{mod } pqr)$

Theorem 2.3 For any positive integer $k \geq 2$, there exist $k + \frac{k(k-1)}{2}$ share holders, sharing the common secret S.
[10]

3. Key Sharing using Graph Theory

N. Chandramowliswaran et al [9] presented a technique to manage this situation using a *Peterson Graph*. Here, we extend the scheme to implement on ***Asymmetric Graph with 25 vertices*** [3].
Asymmetric Graph is an undirected graph which has no non-trivial symmetries.

1. Consider a graph G, where the vertices represent the keys and the edges represent users of the network.



If 2 users share a common key, they are called **conflict users**, otherwise **non-conflict users**.

2. Define
$V(G) = \{V_i = Key_i : 1 \leq i \leq m\}$
$E(G) = \{k = user - k : 1 \leq k \leq n\}$
where m and n are the total number of keys and users respectively.

3. Define $f(v_i) = f(Key_i) = \sigma(i)$ where σ is a permutation on the set of numbers $\{1, 2, ..., m\}$. This $\sigma(i)$ is given for each Key_i

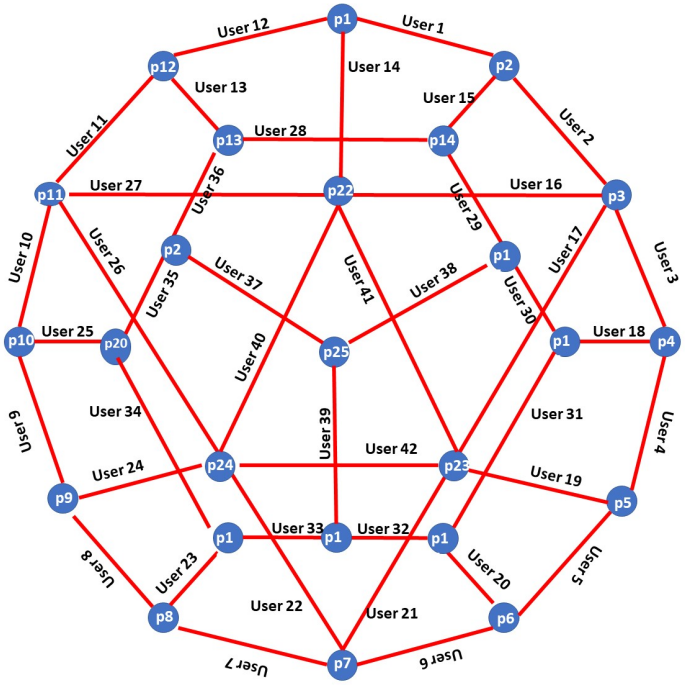
4. Now define the *graceful labelling* g on the set $\{\sigma(1), \sigma(2), ..., \sigma(m)\}$
$g : \{\sigma(i) : 1 \leq i \leq m\} \to \{0, 1, 2, ..., q-1, q\}$
Suppose $g[userj] = |g(\sigma(r)) - g(\sigma(s))| \in \{1, 2, ..., q\}$
g is kept secret, but $g[userj]$ is given for each user j
Entire network is also kept secret.

5. Define
$\mathcal{P} : V(G) \to \{p_1, p_2, ..., p_i\}$ where p_i are distinct odd primes.
$e_j : gcd(e_j, (p_r - 1), (p_s - 1)) = 1$
$m_j \equiv (g[user - j])^{e_j} (mod p_r p_s)$
$\mathcal{P}, e_j$ are kept secret.

6. Decompose the user (edges) into subset of Non Conflict users (set of Independent Edges) and hence define the congruence equations for the sets.

7. The solution of the congruence relations (via Chinese Remainder Theorem) would be the common secret shared by the each set of non conflict users.

3.1. **Asymmetric Graph.** We take an undirected graph with 25 vertices and 42 edges. It has odd number of vertices, therefore we cannot obtain a perfect matching or 1-factor for this graph because perfect matching is a graph containing $n/2$ edges where n is the no. of vertices. Now, we are using this graph as a network where the nodes are the keys and the edges are the users. For each vertex, we assign a large prime number $p_1, p_2, p_3, ..., p_{25}$ and for edges we are using numbers i.e. $1, 2, 3, ..., 42$.



1. Given system has 25 keys and 42 users. Every user can use at most two keys. Here the distribution is not symmetric i.e. some keys are used by 5 users, some are used by 4 users and some are used by 3 users. Represent the Keys by the nodes (vertices) of the graph G and users by the edges.

2. Set of non-conflict users

$M_1 = \{user1, user3, user5, user7, user9, user11, user28, user31, user34\}$
$M_2 = \{user2, user4, user6, user8, user10, user12, user29, user32, user35\}$
$M_3 = \{user13, user15, user17, user18, user20, user22, user23, user25\}$
$M_4 = \{user16, user21, user30, user33, user36\}$
$M_5 = \{user14, user19, user24, user37\}$
$M_6 = \{user38, user40\}$
$M_7 = \{user39, user42\}$
$M_8 = \{user26, user41\}$

3. Define

$V(G) = \{V_i = Key_i : 1 \leq i \leq 25\}$
$E(G) = \{k = user - k : 1 \leq k \leq 42\}$
$f(v_i) = f(Key_i) = \sigma(i)$ where σ is a permutation on the set of numbers $\{1, 2, ..., 25\}$. For each Key we have a different $\sigma(i)$ This $\sigma(i)$ is given for each Key_i

4. Let $g(userk) = |g(\sigma(r)) - g(\sigma(s))| \in \{1, 2, ..., q\}$, where $1 \leq r, s \leq 25, r \neq s$ be the graceful labeling on the set $\{\sigma(1), \sigma(2), ..., \sigma(25)\}$.

5. For each user, we define $g(userk)$ such that $g : E(G) \to \{1, 2, ..., q\}$ which is kept confidential.

$g(userk)$ is the user id, user k has two keys i.e $\sigma(r), \sigma(s)$ and the entire network is kept secret.

6. $\mathcal{P} : V(G) \to \{p_1, p_2, ..., p_{25}\}$ where $p_i, 1 \leq i \leq 25$ are distinct large odd primes with with $q < min(p_i), q < p_k$ for all $k(1 \leq k \leq 42)$.

7. Let us assume a prime e_k such that $gcd(e_k, (p_r-1), (p_s-1))$ and $m_k \equiv (g\,[user - k])^{e_k} (\text{mod}\, p_r p_s)$ $P(Key_r) = p_r, P(Key_s) = p_s$.

8. Now, the user set is broken apart into different sets of non-conflict users.
$user1 \leftrightarrow \{Key_1, Key_2\}$
$user3 \leftrightarrow \{Key_3, Key_4\}$
$user5 \leftrightarrow \{Key_5, Key_6\}$
$user7 \leftrightarrow \{Key_7, Key_8\}$
$user9 \leftrightarrow \{Key_9, Key_{10}\}$
$user11 \leftrightarrow \{Key_{11}, Key_{12}\}$
$user28 \leftrightarrow \{Key_{13}, Key_{14}\}$
$user31 \leftrightarrow \{Key_{16}, Key_{17}\}$
$user34 \leftrightarrow \{Key_{19}, Key_{20}\}$

Now, defining the congruence equations for M_1

$A \equiv n_1 (\text{mod}\ p_1 p_2)$
$A \equiv n_3 (\text{mod}\ p_3 p_4)$
$A \equiv n_5 (\text{mod}\ p_5 p_6)$
$A \equiv n_7 (\text{mod}\ p_7 p_8)$
$A \equiv n_9 (\text{mod}\ p_9 p_{10})$
$A \equiv n_{11} (\text{mod}\ p_{11} p_{12})$
$A \equiv n_{28} (\text{mod}\ p_{13} p_{14})$
$A \equiv n_{31} (\text{mod}\ p_{16} p_{17})$
$A \equiv n_{34} (\text{mod}\ p_{19} p_{20})$

Now, we can say (using the Chinese Remainder Theorem) that, A has a distinct solution $(\text{mod}\ (p_1 \cdot p_2 ... p_{20}))$.

Therefore, M_1 non conflict users share the common secret A.

Similarly, for M_2

$user2 \leftrightarrow \{Key_2, Key_3\}$
$user4 \leftrightarrow \{Key_4, Key_5\}$
$user6 \leftrightarrow \{Key_6, Key_7\}$
$user8 \leftrightarrow \{Key_8, Key_9\}$
$user10 \leftrightarrow \{Key_{10}, Key_{11}\}$
$user12 \leftrightarrow \{Key_{12}, Key_1\}$
$user29 \leftrightarrow \{Key_{20}, Key_{21}\}$
$user32 \leftrightarrow \{Key_{14}, Key_{15}\}$

$user35 \leftrightarrow \{Key_{17}, Key_{18}\}$

Defining the congruence equations for M_2

$B \equiv n_2 (\text{mod } p_2 p_3)$
$B \equiv n_4 (\text{mod } p_4 p_5)$
$B \equiv n_6 (\text{mod } p_6 p_7)$
$B \equiv n_8 (\text{mod } p_8 p_9)$
$B \equiv n_{10} (\text{mod } p_{10} p_{11})$
$B \equiv n_{12} (\text{mod } p_{12} p_1)$
$B \equiv n_{29} (\text{mod } p_{20} p_{21})$
$B \equiv n_{32} (\text{mod } p_{14} p_{15})$
$B \equiv n_{35} (\text{mod } p_{17} p_{18})$

B has a distinct solution (mod $(p_1 \cdot p_2 ... p_{21})$).
Therefore, M_2 non conflict users share the common secret B.

For M_3

$user13 \leftrightarrow \{Key_{12}, Key_{13}\}$
$user15 \leftrightarrow \{Key_2, Key_{14}\}$
$user17 \leftrightarrow \{Key_3, Key_{23}\}$
$user18 \leftrightarrow \{Key_4, Key_{16}\}$
$user20 \leftrightarrow \{Key_6, Key_{17}\}$
$user22 \leftrightarrow \{Key_7, Key_{24}\}$
$user23 \leftrightarrow \{Key_8, Key_{19}\}$
$user25 \leftrightarrow \{Key_{10}, Key_{20}\}$
$user27 \leftrightarrow \{Key_{11}, Key_{22}\}$

Defining congruence equations for M_3

$C \equiv n_{13} (\text{mod } p_{12} p_{13})$
$C \equiv n_{15} (\text{mod } p_2 p_{14})$
$C \equiv n_{17} (\text{mod } p_3 p_{23})$
$C \equiv n_{18} (\text{mod } p_4 p_{16})$
$C \equiv n_{20} (\text{mod } p_6 p_{17})$
$C \equiv n_{22} (\text{mod } p_7 p_{24})$
$C \equiv n_{23} (\text{mod } p_8 p_{19})$
$C \equiv n_{25} (\text{mod } p_{10} p_{20})$
$C \equiv n_{27} (\text{mod } p_{11} p_{22})$

C has a distinct solution (mod $(p_2 \cdot p_3 \cdot p_4 \cdot p_6 \cdot p_7 \cdot p_8 \cdot p_{10} \cdot p_{11} \cdot p_{12} \cdot p_{13} \cdot p_{14} \cdot p_{16} \cdot p_{17} \cdot p_{19} \cdot p_{20} \cdot p_{22} \cdot p_{23} \cdot p_{24})$).
Therefore, M_3 non conflict users share the common secret C.

For M_4

$user16 \leftrightarrow \{Key_{22}, Key_3\}$
$user21 \leftrightarrow \{Key_7, Key_{23}\}$

$user30 \leftrightarrow \{Key_{15}, Key_{16}\}$
$user33 \leftrightarrow \{Key_{18}, Key_{19}\}$
$user36 \leftrightarrow \{Key_{21}, Key_{13}\}$

Defining congruence equations for M_4

$D \equiv n_{16}(\text{mod } p_{22}p_3)$
$D \equiv n_{21}(\text{mod } p_7p_{23})$
$D \equiv n_{30}(\text{mod } p_{15}p_{16})$
$D \equiv n_{33}(\text{mod } p_{18}p_{19})$
$D \equiv n_{36}(\text{mod } p_{21}p_{13})$

D has a distinct solution (mod $(p_3 \cdot p_7 \cdot p_{13} \cdot p_{15} \cdot p_{16} \cdot p_{18} \cdot p_{19} \cdot p_{21} \cdot p_{22} \cdot p_{23})$)
Therefore, M_4 non conflict users share the common secret D.

For M_5

$user14 \leftrightarrow \{Key_1, Key_{22}\}$
$user19 \leftrightarrow \{Key_5, Key_{23}\}$
$user24 \leftrightarrow \{Key_9, Key_{24}\}$
$user37 \leftrightarrow \{Key_{21}, Key_{25}\}$

Defining congruence equations for M_5

$E \equiv n_{14}(\text{mod } p_1p_{22})$
$E \equiv n_{19}(\text{mod } p_5p_{23})$
$E \equiv n_{24}(\text{mod } p_9p_{24})$
$E \equiv n_{37}(\text{mod } p_{21}p_{25})$

E has a distinct solution (mod $(p_1 \cdot p_5 \cdot p_9 \cdot p_{21} \cdot p_{22} \cdot p_{23} \cdot p_{24} \cdot p_{25})$)
Therefore, M_5 non conflict users share the common secret E.

For M_6

$user38 \leftrightarrow \{Key_{15}, Key_{25}\}$
$user40 \leftrightarrow \{Key_{22}, Key_{24}\}$

Defining congruence equations for M_6

$F \equiv n_{38}(\text{mod } p_{15}p_{25})$
$F \equiv n_{40}(\text{mod } p_{22}p_{24})$

F has a distinct solution (mod $(p_{15} \cdot p_{22} \cdot p_{24} \cdot p_{25})$)
Therefore, M_6 non conflict users share the common secret F.

For M_7

$user39 \leftrightarrow \{Key_{18}, Key_{25}\}$

$user42 \leftrightarrow \{Key_{23}, Key_{24}\}$

Defining congruence equations for M_6

$G \equiv n_{39} (\text{mod } p_{18}p_{25})$
$G \equiv n_{40} (\text{mod } p_{23}p_{24})$

G has a distinct solution (mod $(p_{18} \cdot p_{23} \cdot p_{24} \cdot p_{25})$)
Therefore, M_7 non conflict users share the common secret G.

For M_8

$user26 \leftrightarrow \{Key_{11}, Key_{24}\}$
$user41 \leftrightarrow \{Key_{22}, Key_{23}\}$

Defining congruence equations for M_8

$H \equiv n_{26} (\text{mod } p_{11}p_{24})$
$H \equiv n_{41} (\text{mod } p_{22}p_{23})$

H has a distinct solution (mod $(p_{11} \cdot p_{22} \cdot p_{23} \cdot p_{24})$)
Therefore, M_8 non conflict users share the common secret H.

4. Secret Sharing using Strongly co-prime integers and CRT

We also use certain theorems based on strongly co-prime integers. A pair of co-prime positive integers m, n is said to be strongly ϕ co-prime if:

$$gcd(m, n) = gcd(m, \phi(n)) = gcd(\phi(m), n) = 1$$

Where $\phi(x)$ is Euler's Totient Function. It is defined as the number of positive integers $\leq x$ that are relatively prime to x.

Lemma: Let p, q, r be three given distinct odd primes. Assume p, q, r to be mutually strongly co-prime. Then, there exist integers k_1, k_2, k_3 such that $k_1 p\left[(q-1)^{r-1} + (r-1)^{q-1}\right] + k_2 q\left[(r-1)^{p-1} + (p-1)^{r-1}\right] + k_3 r\left[(p-1)^{q-1} + (q-1)^{p-1}\right] + 4 \equiv 0 (\text{mod } pqr)$

Proof: Consider three VERY LARGE odd primes p, q, r with $p < q < r$. Now, we require that they must be strongly co-prime.
$gcd(p, \phi(q)) = 1$ (1)
$gcd(\phi(p), q) = 1$ (2)
$gcd(p, \phi(r)) = 1$ (3)
$gcd(\phi(p), r) = 1$ (4)
$gcd(q, \phi(r)) = 1$ (5)
$gcd(\phi(q), r) = 1$ (6)

The conditions 2, 4 & 6 say that
$gcd(p-1, q) = gcd(p-1, r) = gcd(q-1, r) = 1$

The condition is valid since $p < q < r$

Now, the conditions $1, 3$ & 5 say that
$gcd(p, q-1) = gcd(p, r-1) = gcd(q, r-1) = 1$

This is equivalently

$r \not\equiv 1(\text{mod } q)$
$r \not\equiv 1(\text{mod } p)$
$q \not\equiv 1(\text{mod } p)$

Define $Y = (p-1)^{q-1} + (q-1)^{p-1} + (p-1)^{r-1} + (r-1)^{p-1} + (q-1)^{r-1} + (r-1)^{q-1} - 4$

Since $q \not\equiv 1(\text{mod } p)$, we have $(q-1)^{p-1} \equiv 1(\text{mod } p)$.
Since $r \not\equiv 1(\text{mod } p)$, we have $(r-1)^{p-1} \equiv 1(\text{mod } p)$.
Since q, r are odd primes, we have $(p-1)^{q-1} \equiv 1(\text{mod } p), (p-1)^{r-1} \equiv 1(\text{mod } p)$

Therefore $Y \equiv (q-1)^{r-1} + (r-1)^{q-1}(\text{mod } p)$

Similarly $Y \equiv (r-1)^{p-1} + (p-1)^{r-1}(\text{mod } q)$
$Y \equiv (p-1)^{q-1} + (q-1)^{p-1}(\text{mod } r)$

Now, we apply the Chinese Remainder Theorem for the above mentioned simultaneous congruences. We have a unique solution for $Y(\text{mod } pqr)$

Define $M = pqr$

$M_p = M/p = qr$
$M_q = M/q = pr$
$M_r = M/r = pq$

Since, $gcd(M_p, p) = 1$, there is a unique $M_p^{'}$ such that $M_p M_p^{'} \equiv (\text{mod } p)$
Similarly, $M_q M_q^{'} \equiv (\text{mod } q)$
and, $M_r M_r^{'} \equiv (\text{mod } r)$

Now, by the CRT we must have
$Y \equiv \left[(q-1)^{r-1} + (r-1)^{q-1}\right] M_p M_p^{'} + \left[(r-1)^{p-1} + (p-1)^{r-1}\right] M_q M_q^{'} +$
$\left[(p-1)^{q-1} + (q-1)^{p-1}\right] M_r M_r^{'}(\text{mod } pqr)$

So, we can say that
$Y = \left[(p-1)^{q-1} + (q-1)^{p-1}\right] + \left[(p-1)^{r-1} + (r-1)^{p-1}\right]$
$+ \left[(q-1)^{r-1} + (r-1)^{q-1}\right] - 4 \equiv Y \equiv \left[(q-1)^{r-1} + (r-1)^{q-1}\right] M_p M_p^{'} +$
$\left[(r-1)^{p-1} + (p-1)^{r-1}\right] M_q M_q^{'} + \left[(p-1)^{q-1} + (q-1)^{p-1}\right] M_r M_r^{'}(\text{mod } pqr)$

Therefore, $-4 \equiv \left[(q-1)^{r-1} + (r-1)^{q-1}\right] (M_p M_p^{'} - 1) + \left[(r-1)^{p-1} + (p-1)^{r-1}\right] (M_q M_q^{'} -$
$1) + \left[(p-1)^{q-1} + (q-1)^{p-1}\right] (M_r M_r^{'} - 1)(\text{mod } pqr)$

Now,

$M_pM_p^{'} = k_1p$ for some integer k_1
$M_qM_q^{'} = k_2q$ for some integer k_2
$M_rM_r^{'} = k_3p$ for some integer k_3

Therefore, we have:

$k_1p\left[(q-1)^{r-1}+(r-1)^{q-1}\right]+k_2q\left[(r-1)^{p-1}+(p-1)^{r-1}\right]+k_3r\left[(p-1)^{q-1}+(q-1)^{p-1}\right]+4 \equiv 0(\text{mod } pqr)$

Now, we set up the *Secret Sharing Scheme* with the following setup:

Step 1.
Choose $p, q, r(p < q < r)$ VERY LARGE odd primes and keep them private.

Step 2.
p, q, r are stronlgy co-prime.

Step 3.
$(q-1)^{r-1}+(r-1)^{q-1} \not\equiv 0(\text{mod } p)$
$(q-1)^{r-1}+(r-1)^{q-1} \not\equiv 0(\text{mod } p)$
$(q-1)^{r-1}+(r-1)^{q-1} \not\equiv 0(\text{mod } p)$

Step 4.
Set $N = pqr$

In this type of Secret Key Sharing, we use Factorization Difficulty and Discrete Log Difficulty

1. Let S be the given secret.
2. The three secret shareholders receive Y_1, Y_2, Y_3. (They are computed Modulo pqr)
3. Compute

$Y_1 \equiv -Sk_1p\left[(q-1)^{r-1}+(r-1)^{q-1}\right] (\text{mod } N)$
$Y_2 \equiv -Sk_2q\left[(r-1)^{p-1}+(p-1)^{r-1}\right] (\text{mod } N)$
$Y_3 \equiv -S\left\{k_3r\left[(p-1)^{q-1}+(q-1)^{p-1}\right]+3\right\} (\text{mod } N)$

Now, $S = Y_1 + Y_2 + Y_3$

5. Conclusion and Future Work

The proposed scheme focuses on securing the key(s) broadcasted amongst the users and guarantees the authentication. The protocol is secure for both internal and external attacks. The technique used in this paper for secret sharing is to split the secret amongst a network of users and send it to the participating share holders in the network. Also, it is not able to decode the secret without the knowledge of all shares and any attacker cannot identify if any one share is missing. Hence forth one can use it for various network protocols. The techniques use analytical discrete mathematics amalgamated with theoretical computer science in order to achieve high order space-time compatibility.

The technique can be extended to the development of new algorithms based on the decomposition of vertices.

References

[1] Adi Shamir (1979), How to share a secret, Communications of the ACM, 22, No.11, 612-613.
[2] Asmuth, C., Bloom, J. (1983). A modular approach to key safeguarding. IEEE Transactions on Information Theory, 29, 208–210.
[3] Balakrishnan, R., Ranganathan, K. (2000). A textbook of graph theory. Berlin: Springer.
[4] Blakley, G. R. (1979) Safeguarding cryptographic keys, Proceedings of the National Computer Conference, 48 , 313-317.
[5] C. Banerjee, S. K. Pandey (2009) Software Security Rules: SDLC Perspective, International Journal of Computer Science and Information Security, Vol. 6, No.1
[6] Gaurav Gupta, Sangeet Srivastava and N. Chandramowliswaran (2015) Combinatorial conditions for secret sharing for Public Key Cryptography
[7] Lein Harna, Changlu Linb (2010) Strong (n, t, n) verifiable secret sharing scheme Information Sciences 180, 3059–3064
[8] Mignotte, M. (1983), How to share a secret, Lecture Notes in Computer Science, Vol.149, pp.371-375. (Pubitemid 15443646)
[9] N. Chandramowliswaran, S. Srinivasan, P. Muralikrishna (2015) Authenticated key distribution using given set of primes for secret sharing, Systems Science & Control Engineering, 3:1, 106-112
[10] S. Srinivasan, P. Muralikrishna, N. Chandramowliswaran (2014) Secret Key Distribution Technique Using Theory of Numbers, Italian Jouranl of Pure And Applied Mathematics, N. 32-2014 (325-328)
[11] Sorin Iftene (2007) General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting Electronic Notes in Theoretical Computer Science 186, 67–84
[12] Tao Feng, Jiaqi Guo (2018) A New Access Control System Based on CP-ABE in Named Data Networking, International Journal of Network Security, Vol.20, No.4, PP.710-720

Rishabh Malhotra graduated in Mathematics from Amity University Haryana, India in 2014. He is pursuing his Masters degree in Cyber Security from Amity University Rajasthan, India. His research interests focus mainly on Cryptography and Key Sharing.

N. Chandramowliswaran received his Ph. D degree in 1996 from Indian Institute of Technology, Delhi, India. He did his Ph.D. degree in the major research project entitled "Automorphisms of certain relatively free groups and one relator groups". His area of interest includes Graph Theory, Group Algebra, Real Analysis, Cryptology, Combinatorics. He has more than two decades of teaching and research experience.