Taylor & Francis
Taylor & Francis Group

Systems Science & Control Engineering
An Open Access Journal

ISSN: (Print) 2164-2583 (Online) Journal homepage: http://www.tandfonline.com/loi/tssc20

# Authenticated key distribution using given set of primes for secret sharing

N. Chandramowliswaran, S. Srinivasan & P. Muralikrishna

*Systems Science & Control Engineering: An Open Access Journal*, 2015
Vol. 3, 106–112, http://dx.doi.org/10.1080/21642583.2014.985803



# Authenticated key distribution using given set of primes for secret sharing

N. Chandramowliswaran[a*], S. Srinivasan[b] and P. Muralikrishna[b]

[a]*Department of Applied Sciences, ITM University, Gurgaon-122017, Haryana, India;* [b]*School of Advanced Sciences, VIT University, Vellore – 632014, India*

(*Received 16 November 2013; accepted 1 November 2014*)

In recent years, *Chinese remainder theorem* (CRT)-based function sharing schemes are proposed in the literature. In this paper, we study systems of two or more linear congruences. When the moduli are pairwise coprime, the main theorem is known as the CRT, because special cases of the theorem were known to the ancient Chinese. In modern algebra the CRT is a powerful tool in a variety of applications, such as cryptography, error control coding, fault-tolerant systems and certain aspects of signal processing. Threshold schemes enable a group of users to share a secret by providing each user with a share. The scheme has a threshold $t+1$ if any subset with cardinality $t+1$ of the shares enables the secret to be recovered. In this paper, we are considering $2t$ prime numbers to construct $t$ share holders. Using the $t$ share holders, we split the secret $S$ into $t$ parts and all the $t$ shares are needed to reconstruct the secret using CRT.

**Keywords:** key distribution; Chinese remainder theorem; Pell's equation; graceful labeling

*AMS Classification*: 94A60; 94A62; 05C78

## 1. Introduction

A threshold scheme enables a secret to be shared among a group of $\ell$ members providing each member with a share. The scheme has a threshold $t+1$ if any subset with cardinality $t+1$ out of the $\ell$ shares enables the secret to be recovered. We will use the notation $(t+1,\ell)$ to refer to such a scheme. Ideally, in a $(t+1)$ threshold scheme, $t$ shares should not give any information on the secret. We will discuss later how to express this information. In the 1980s, several algebraic constructions of $(t+1,\ell)$ threshold schemes were proposed.

Key distribution is a central problem in cryptographic systems, one of the nicest ones is the idea of secret sharing, originally suggested by Blakley (1979). Somewhat surprisingly, Shamir was able to construct a very efficient such scheme for any $n$ and $t$ without relying on any cryptographic assumptions. Such schemes are called $t$ out of $n$ secret sharing schemes. An $n$ out of $n$ schemes is a scheme where all $n$ shares are needed to reconstruct, and if even one share is missing then there is absolutely no information about the secret. Secret sharing was invented independently by Shamir (1979) and Blakley (1979).

A number of common mathematical techniques in signal processing and data transmission have as their common basis an earliest number-theoretic theorem known as the *Chinese remainder theorem* (CRT). The scope of problems to which this applies is very wide. It includes cryptography, error control coding, fault-tolerant systems and certain aspects of signal processing. In this paper, we present three new centralized group key management protocols based on the CRT. By shifting more computing load onto the key server we optimize the number of re-key broadcast messages, user-side key computation, and number of key storages. It is attracted much attention in the research community and a number of schemes have been proposed, including many encryption schemes and signature schemes (Lu & Li, 2013).

The CRT can also be used in secret sharing, there are two secret sharing schemes that make use of the CRT, *Mignotte's* and *Asmuth-Bloom's* Schemes see in Mignotte (1983) and Asmuth and Bloom (1983). They are threshold secret sharing schemes, in which the shares are generated by reduction modulo the integers $m_i$, and the secret is recovered by essentially solving the system of congruences using the CRT (Apostol (1976)).

THEOREM 1.1 (CRT) *Suppose that $m_1, m_2, \ldots, m_r$ are pairwise relatively prime positive integers, and let $a_1, a_2, \ldots, a_r$ be integers. Then the system of congruences, $x \equiv a_i \pmod{m_i}$ for $1 \le i \le r$, has a unique solution modulo $M = m_1 \times m_2 \times \ldots \times m_r$, which is given by: $x \equiv a_1M_1y_1 + a_2M_2y_2 + \ldots + a_rM_ry_r \pmod{M}$, where $M_i = M/m_i$ and $y_i \equiv (M_i)^{-1} \pmod{m_i}$ for $1 \le i \le r$.*

All types of secret key sharing considered in this paper mainly uses factorization difficulty and discrete log

*Corresponding author. Email: ncmowli@hotmail.com

problem difficulty. Here, we propose three secret sharing scheme among $t$ shares. The motivation for the use of secret key sharing scheme is that, it gives confidence to the source node or the owner about the genuinely participating shares in the network. Here, a key is transmitted or shared among the multiple share holders in the network that are under the process of encryption and decryption. The objective is to maintain the genuineness of the nodes that are present in the network. Here, the shares are properly distributed by choosing $2t$ prime numbers and then it is shared to their corresponding nodes for which it is generated.

## 2. Main result

In this section we give key distribution theorem and algorithms. The proposed system involves a design of a pre-distribution algorithm using a deterministic approach. A key pre-distribution algorithm using number theory with high connectivity, high resilience and memory requirements is being designed by implementing a deterministic approach. Most of the related technical terms and definitions appear in Mignotte (1983), Muralikrishna, Srinivasan, and Chandramowliswaran (2013), Okamoto and Tanaka (1989) and Muralikrishna et al. (2013). The others can be found in text books such as Apostol (1976), Berlekamp (1968), Blakley (1979), and Koblitz (1994).

In this section, we give three distinct novel secret sharing schemes. Consider the three very large odd primes $p, q$ and $r$ with $(q^{r-1} + r^{q-1}) \not\equiv 0 \pmod p$, $(r^{p-1} + p^{r-1}) \not\equiv 0 \pmod q$ and $(p^{q-1} + q^{p-1}) \not\equiv 0 \pmod r$. To accomplish our first secret key sharing scheme, we adopt the following theorem.

THEOREM 2.1 *Let $S$ be the given secret and $N = pqr$ where $p, q$ and $r$ are distinct large odd primes. Define three secret shareholders $Y_1, Y_2, Y_3$ as follows: $Y_1 \equiv (-Sk_1p(q^{r-1} + r^{q-1})) \pmod N$, $Y_2 \equiv (-Sk_2q(p^{r-1} + r^{p-1})) \pmod N$ and $Y_3 \equiv (-S(k_3r(p^{q-1} + q^{p-1}) + 1)) \pmod N$ then $S = Y_1 + Y_2 + Y_3 \pmod N$*

In order to prove the proposed theorem, we regard a Lemma 2.2, as the secret key information.

LEMMA 2.2 *Let $p, q$ and $r$ be three given distinct odd primes. Then there exist integers $k_1, k_2$ and $k_3$ such that*

$$k_1p(q^{r-1} + r^{q-1}) + k_2q(p^{r-1} + r^{q-1}) + k_3r(p^{q-1} + q^{p-1}) + 2 \equiv 0 \pmod{pqr}.$$

*Proof* Define: $X = (p^{q-1} + q^{p-1}) + (p^{r-1} + r^{p-1}) + (q^{r-1} + r^{q-1}) - 2$. Then

$$X \equiv (q^{r-1} + r^{q-1}) \pmod p$$
$$X \equiv (p^{r-1} + r^{p-1}) \pmod q \quad \text{and}$$
$$X \equiv (p^{q-1} + q^{p-1}) \pmod r.$$

By CRT, the above system of congruences has exactly one solution modulo the product $pqr$.

Define $M = pqr$ then $M_p = M/p = qr, M_q = M/q = pr$ and $M_r = M/r = pq$.

Since $(M_p, p) = 1$, then there is a unique $M_p'$ such that $M_pM_p' \equiv 1 \pmod p$.

Similarly there are unique $M_q'$ and $M_r'$ such that $M_qM_q' \equiv 1 \pmod q$ and $M_rM_r' \equiv 1 \pmod r$.

Consider

$$X \equiv ((p^{q-1} + q^{p-1})M_rM_r' + (p^{r-1} + r^{p-1})M_qM_q' + (q^{r-1} + r^{q-1})M_pM_p') \pmod{pqr}$$

that is,

$$\begin{aligned}
&p^{q-1} + q^{p-1} + p^{r-1} + r^{p-1} + q^{r-1} + r^{q-1} - 2\\
&\quad \equiv ((p^{q-1} + q^{p-1})M_rM_r' + (p^{r-1} + r^{p-1})M_qM_q'\\
&\qquad + (q^{r-1} + r^{q-1})M_pM_p') \pmod{pqr}\\
&\qquad - 2 \equiv ((p^{q-1} + q^{p-1})(M_rM_r' - 1) + (p^{r-1} + r^{p-1})\\
&\qquad \times (M_qM_q' - 1) + (q^{r-1} + r^{q-1})(M_pM_p' - 1))\\
&\qquad \times \pmod{pqr}.
\end{aligned}$$

Thus

$$k_1p(q^{r-1} + r^{q-1}) + k_2q(p^{r-1} + r^{q-1}) + k_3r(p^{q-1} + q^{p-1}) + 2 \equiv 0 \pmod{pqr}. \qquad \blacksquare$$

*Proof of Theorem 2.1* By the above Lemma 2.2, we have

$$\begin{aligned}
&k_1p(q^{r-1} + r^{q-1}) + k_2q(p^{r-1} + r^{q-1}) + k_3r(p^{q-1} + q^{p-1})\\
&\quad + 2 \equiv 0 \pmod N.\\
&1 \equiv (-(k_1p(q^{r-1} + r^{q-1})) - (k_2q(p^{r-1} + r^{q-1}))\\
&\quad - (k_3r(p^{q-1} + q^{p-1}) + 1)) \pmod N.
\end{aligned}$$

Thus $S = Y_1 + Y_2 + Y_3 \pmod N$. $\blacksquare$

The following three examples motivating us to write nice secret sharing algorithms

*Example 1* Secret Key Sharing using Quadratic Polynomials

*Step 1* Define $P(x) = \ell_1x^2 + \ell_2x + \ell_3$ (secret) where $\ell_i \in \mathbb{Z}^+$, $i \in \{1, 2, 3\}$
Let $\lambda$ be a positive integer with $P(\lambda) = \ell_1\lambda^2 + \ell_2\lambda + \ell_3 = \mu$ (say)

*Step 2* Define $Q(x) = P(x) - \mu$ then $Q(\lambda) = 0$

*Step 3* Let $s$ is the given secret. Find integers $a, b, c, d, e, f\ ,\ g, , h, r$ satisfying $\ell_1x^2 + \ell_2x + (\ell_3 - \mu + s) = \alpha[a(1 + x)^2 + b(1 + x) + c] +$

$\beta[d(1+x)^2+e(1+x)+f]+\gamma[g(1+x)^2+h(1+x)+r]$ with

$$\begin{vmatrix} a & d & g \\ 2a+b & 2d+e & 2g+h \\ a+b+c & d+e+f & g+h+r \end{vmatrix} = \pm 1.$$

*Step* 4 Compare the coefficients on both sides we get,

$$\alpha a+\beta d+\gamma g=\ell_1$$
$$\alpha(2a+b)+\beta(2d+e)+\gamma(2g+h)=\ell_2$$
$$\alpha(a+b+c)+\beta(d+e+f)+\gamma(g+h+r)=\ell_3-\mu+s.$$

*Step* 5

$$\begin{pmatrix} a & d & g \\ 2a+b & 2d+e & 2g+h \\ a+b+c & d+e+f & g+h+r \end{pmatrix}\begin{pmatrix}\alpha\\ \beta\\ \gamma\end{pmatrix} = \begin{pmatrix}\ell_1\\ \ell_2\\ \ell_3-\mu+s\end{pmatrix},$$

where

$$\begin{pmatrix} a & d & g \\ 2a+b & 2d+e & 2g+h \\ a+b+c & d+e+f & g+h+r \end{pmatrix} \in GL_3(\mathbb{Z}),$$

where $GL_3(\mathbb{Z})$ be the set of all $3\times 3$ matrices of integer coefficients with determinant is $\pm 1$

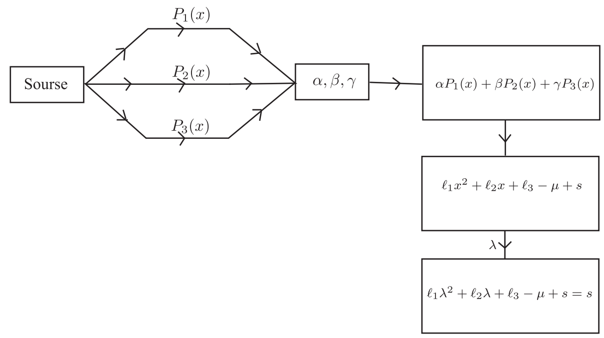
*Step* 6

$$\begin{pmatrix}\alpha\\ \beta\\ \gamma\end{pmatrix} = \begin{pmatrix} a & d & g \\ 2a+b & 2d+e & 2g+h \\ a+b+c & d+e+f & g+h+r \end{pmatrix}^{-1} \times \begin{pmatrix}\ell_1\\ \ell_2\\ \ell_3-\mu+s\end{pmatrix},$$

where $\alpha,\beta$ and $\gamma$ are uniquely solved by the above information

*Step* 7 Select three secret share holders $P_1, P_2$ and $P_3$

$$P_1 \longleftrightarrow ax^2+(2a+b)x+(a+b+c)=P_1(x)$$
$$P_2 \longleftrightarrow dx^2+(2d+e)x+(d+e+f)=P_2(x)$$
and
$$P_3 \longleftrightarrow gx^2+(2g+h)x+(g+h+r)=P_3(x)$$




*Example 2* Secret Key Sharing using Finite Groups

*Step* 1 Let $\mathcal{P}=2p^r+1$ and $\mathcal{Q}=2q^s+1$, where $\mathcal{P},\mathcal{Q},p$ and $q$ are very large odd primes (which is kept secret).
*Step* 2 Let $N=\mathcal{P}\mathcal{Q}$
*Step* 3 Define $G=\{1\le x\le N \mid (x,N)=1\}$
*Step* 4 Let $\times_N$ be the multiplication modulo $N$. Clearly $(G,\times_N)$ forms a finite group with $O(G)=\phi(N)=4p^rq^s$
*Step* 5 Let $s$ (given secret) be the element of $G$
*Step* 6 From finite group theory, any map $\Psi$, $g\longmapsto g^m$ is always an *automorphism of G*, if $(m,O(G))=1$
*Step* 7 Let $m=\ell_1+\ell_2+\cdots+\ell_t$.
Consider $s=x^m$

$$s=x^{\ell_1+\ell_2+\cdots+\ell_t}$$
$$s=x^{\ell_1}x^{\ell_2}\cdots x^{\ell_t}$$
$$s=y_1y_2\cdots y_t,$$

where $y_i=x^{\ell_i} \pmod N$, $1\le i\le t$ be the individual share holders.

*Example 3* Secret Key Sharing using affine number theoretic functions

*Step* 1 Let $S=\{a_k \mid 1\le k\le N\}$ be the given set of distinct positive integers
*Step* 2 $\sum_{k=1}^N a_k=P$, where $P$ is very large *odd* prime
*Step* 3 Clearly, $(\prod_{j=1}^N a_j, P)=1$ and $(a_j, P-a_j)=1, \forall j$, $1\le j\le N$
*Step* 5 Denote $\{0,1,2,\ldots,\prod_{j=1}^N a_j-1\}=[0,\prod_{j=1}^N a_j-1]$, then
Define $f_P:[0,\prod_{j=1}^N a_j-1]\xrightarrow[\text{onto}]{1-1}[0,\prod_{j=1}^N a_j-1]$ such that for each $x\in[0,\prod_{j=1}^N a_j-1]$, $f_P(x)=Px+t \pmod{\prod_{j=1}^N a_j}$ where $t\in[0,\prod_{j=1}^N a_j-1]$
*Step* 6 Define $f_{a_j}:[0,P-a_j-1]\xrightarrow[\text{onto}]{1-1}[0,P-a_j-1]$ such that for each $y\in[0,P-a_j-1]$ $f_{a_j}(y)=a_jy+b_j \pmod{P-a_j}$ where $b_j\in[0,P-a_j-1]$

*Step* 7 Define $g_{a_j} : [0, a_j - 1] \xrightarrow[\text{onto}]{1-1} [0, a_j - 1]$ such that for each $z \in [0, a_j - 1]$ $g_{a_j}(z) = (P - a_j)z + c_j \pmod{a_j}$ where $c_j \in [0, a_j - 1]$

*Step* 8 Define $Y_j = g_{a_j}(z) = (P - a_j)w + d_j \pmod{a_j}$, $w \in [0, a_j - 1]$ and $\forall j$, $j\{1, 2, \ldots, N\}$ with $(a_r, a_s) = 1, \forall s,\ r \in \{1, 2, \ldots, N\}$.
Solve $w$ uniquely mod $\prod_{j=1}^{N} a_j$

*Step* 9 Let $S = f_P(w) = Pw + t \pmod{\prod_{j=1}^{N} a_j}$ be the given secret

## 3. Algorithms

ALGORITHM 1 *By means of our first secret key sharing scheme, we execute the following hierarchy.*

*Step* 1 *Consider* $\{p_i, q_i : i \in \{1, 2, \ldots, t\}\}$ *be the given distinct secrete odd primes*

*Step* 2 *Let* $N_i = p_i q_i$

*Step* 3 *Pick* $a_i$ *such that* $(a_i, N_i) = 1$

*Step* 4 *Choose the positive integers* $e_i$ *such that* $(e_i, (p_i - 1)(q_i - 1)) = 1$

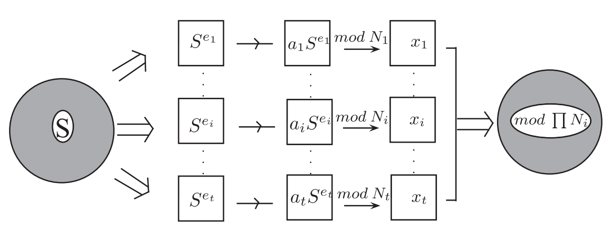
*Step* 5 *Select a common secret* $S$ *such that* $(S, N_i) = 1, i \in \{1, 2, \ldots, t\}$

*Step* 6 *Define* $x_i, i \in \{1, 2, \ldots, t\}$ *by* $N_i y_i^2 + 1 = x_i^2$ *where* $x_i, y_i$ *be the least positive integer solution of* $N_i y^2 + 1 = x^2$

*Step* 7 *For each* $i$, $1 \leq i \leq t$ *then construct* $x_i \equiv a_i S^{e_i} \pmod{N_i}$

*Step* 8 *Solve* $S$ *uniquely under* $(\bmod \prod N_i)$ $i \in \{1, 2 \ldots, t\}$ *using CRT*

*Step* 9 *S is the common secret shared by the each share holder* $x_i$, $i \in \{1, 2, \ldots, t\}$




The following proposition asserts that algorithm 2 is a nontrivial secret share holders.

PROPOSITION *Let* $P, Q$ *be given very large odd primes with the following conditions*

(*i*) *P does not divides* $x_2$ *and* $y_2$

(*ii*) *Q does not divides* $x_1$ *and* $y_1$

(*iii*) $2y_1^2 \not\equiv -1 \pmod{Q}$ *and* $2y_2^2 \not\equiv -1 \pmod{P}$

*where* $x_1, y_1, x_2, y_2, x_3$ *and* $y_3$ *satisfy* $y_1^2 - Px_1^2 = 1$ $y_2^2 - Qx_2^2 = 1$ $y_3^2 - PQx_3^2 = 1$ *and* $1 \equiv ((y_1y_2y_3)^2 + (-P(x_1y_2y_3)^2) + (-Q(x_2y_1y_3)^2)) \pmod{PQ}$ *gives non-degenerate key sharing.*

ALGORITHM 2 *Construction of Secret sharing by two odd primes P and Q*

*Step* 1 *Let* $P, Q$ *be given very large odd primes*

*Step* 2 *Define* $N = PQ$

*Step* 3 *Consider the following Pell's equations*

$$Px^2 + 1 = y^2 \quad (1)$$

$$Qx^2 + 1 = y^2 \quad (2) \quad \text{and}$$

$$PQx^2 + 1 = y^2 \quad (3).$$

*Step* 4 *Let* $(x_1, y_1), (x_2, y_2)$ *and* $(x_3, y_3)$ *be the least positive integral solution of* (1), (2) *and* (3) (*i.e.*) $Px_1^2 + 1 = y_1^2$, $Qx_2^2 + 1 = y_2^2$ *and* $PQx_3^2 + 1 = y_3^2$

$$y_1^2 - Px_1^2 = 1 \quad (1)'$$

$$y_2^2 - Qx_2^2 = 1 \quad (2)'$$

$$y_3^2 - PQx_3^2 = 1 \quad (3)'.$$

*Step* 5 $1 = (y_1^2 - Px_1^2)(y_2^2 - Qx_2^2)(y_3^2 - PQx_3^2)$

$$1 \equiv (y_1^2 - Px_1^2)(y_2^2 - Qx_2^2)y_3^2 \pmod{PQ}$$

$$1 \equiv (y_1^2y_2^2 - Px_1^2y_2^2 - Qx_2^2y_1^2)y_3^2 \pmod{PQ}$$

$$1 \equiv ((y_1y_2y_3)^2 - P(x_1y_2y_3)^2 - Q(x_2y_1y_3)^2) \times \pmod{PQ}$$

$$1 \equiv ((y_1y_2y_3)^2 + (-P(x_1y_2y_3)^2) + (-Q(x_2y_1y_3)^2)) \pmod{PQ}.$$

*Step* 6 *Select a secret* $S$ *such that* $(S, PQ) = 1$

*Step* 7

$$S = (S(y_1y_2y_3)^2 + (-PS(x_1y_2y_3)^2) + (-QS(x_2y_1y_3)^2)) \pmod{PQ}.$$

*Step* 8 $Y_1, Y_2$ *and* $Y_3$ *are secret share holders, where* $Y_1 = S(y_1y_2y_3)^2 \pmod{PQ}$,

$$Y_2 = (-PS(x_1y_2y_3)^2) \pmod{PQ} \quad \text{and}$$

$$Y_3 = (-QS(x_2y_1y_3)^2) \pmod{PQ}.$$

ALGORITHM 3 *Extension of Algorithm 2 for three odd primes* $P, Q$ *and* $R$

*Step* 1 *Let* $P, Q$ *and* $R$ *be given very large odd primes*

*Step* 2 *Consider the following Pell's equations*

$$Px^2 + 1 = y^2 \quad (1)$$

$$Qx^2 + 1 = y^2 \quad (2)$$

$$PQx^2 + 1 = y^2 \quad (3)$$

$$Rx^2 + 1 = y^2 \quad (4)$$

$$PRx^2 + 1 = y^2 \quad (5)$$

$$QRx^2 + 1 = y^2 \quad (6) \quad \text{and}$$

$$PQRx^2 + 1 = y^2 \quad (7).$$

*Step 3* *Let* $(x_i, y_i)$ *be the least positive integral solution of* (1)–(7)

$$Px_1^2 + 1 = y_1^2 \quad (1)$$

$$Qx_2^2 + 1 = y_2^2 \quad (2)$$

$$PQx_3^2 + 1 = y_3^2 \quad (3)$$

$$Rx_4^2 + 1 = y_4^2 \quad (4)$$

$$PRx_5^2 + 1 = y_5^2 \quad (5)$$

$$QRx_6^2 + 1 = y_6^2 \quad (6) \quad \text{and}$$

$$PQRx_7^2 + 1 = y_7^2 \quad (7).$$

*Step 4*

$$1 = (y_1^2 - Px_1^2)(y_2^2 - Qx_2^2)(y_3^2 - PQx_3^2)(y_4^2 - Rx_4^2) \times (y_5^2 - PRx_5^2)(y_6^2 - QRx_6^2)(y_7^2 - PQRx_7^2)$$

*that is,* $(y_1^2 - Px_1^2)(y_2^2 - Qx_2^2)(y_3^2 - PQx_3^2)(y_4^2 - Rx_4^2)(y_5^2 - PRx_5^2)(y_6^2 - QRx_6^2)y_7^2 \equiv 1 \pmod{PQR}$

*Step 5*

*Step A* : $(y_1^2 - Px_1^2)(y_6^2 - QRx_6^2) \pmod{PQR} \equiv y_1^2y_6^2 - Px_1^2y_6^2 - QRy_1^2x_6^2 \pmod{PQR}$

*Step B* : $(y_3^2 - PQx_3^2)(y_5^2 - PRx_5^2) \pmod{PQR} \equiv y_3^2y_5^2 - PQx_3^2y_5^2 - PRy_3^2x_5^2 \pmod{PQR}$

*Step C* : $(y_2^2 - Qx_2^2)(y_4^2 - Rx_4^2) \pmod{PQR} \equiv y_2^2y_4^2 - Qx_2^2y_4^2 - Ry_2^2x_4 - QRx_2^2x_4^2 \pmod{PQR}$

*Step 6* *Combining Step A and Step C, we have the following*

$$\begin{aligned}
&(y_1^2 - Px_1^2)(y_6^2 - QRx_6^2)(y_2^2 - Qx_2^2)(y_4^2 - Rx_4^2) \\
&\times \pmod{PQR} \equiv y_1^2y_2^2y_4^2y_6^2 - Qx_2^2y_1^2y_4^2y_6^2 \\
&\quad - Rx_4^2y_1^2y_2^2y_6^2 + QRx_2^2x_4^2y_1^2y_6^2 - Px_1^2y_2^2y_4^2y_6^2 \\
&\quad + PQx_1^2x_2^2y_4^2y_6^2 + PRx_1^2x_4^2y_2^2y_6^2 \\
&\quad - QRx_6^2y_1^2y_2^2y_4^2 + Q^2Rx_2^2x_6^2y_1^2y_4^2 \\
&\quad + QR^2x_4^2x_6^2y_1^2y_2^2 \\
&\quad - Q^2R^2x_2^2x_4^2x_6^2y_1^2 \pmod{PQR}.
\end{aligned}$$

*Step 7* *Now include Step B, we have*

$$\begin{aligned}
&y_1^2y_2^2y_3^2y_4^2y_5^2y_6^2 - Qx_2^2y_1^2y_3^2y_4^2y_5^2y_6^2 \\
&\quad - Rx_4^2y_1^2y_2^2y_3^2y_5^2y_6^2 + QRx_2^2x_4^2y_1^2y_3^2y_5^2y_6^2 \\
&\quad - Px_1^2y_2^2y_3^2y_4^2y_5^2y_6^2 + PQx_1^2x_2^2y_3^2y_4^2y_5^2y_6^2 \\
&\quad + PRx_1^2x_4^2y_2^2y_3^2y_5^2y_6^2 - QRx_6^2y_1^2y_2^2y_3^2y_4^2y_5^2 \\
&\quad + Q^2Rx_2^2x_6^2y_1^2y_3^2y_4^2y_5^2 + QR^2x_4^2x_6^2y_1^2y_2^2y_3^2y_5^2 \\
&\quad - Q^2R^2x_2^2x_4^2x_6^2y_1^2y_3^2y_5^2 - PQx_3^2y_1^2y_2^2y_4^2y_5^2y_6^2 \\
&\quad + PQ^2x_2^2x_3^2y_1^2y_4^2y_5^2y_6^2 + P^2Qx_1^2x_3^2y_2^2y_4^2y_5^2y_6^2 \\
&\quad + P^2Q^2x_1^2x_2^2x_3^2y_4^2y_5^2y_6^2 - PRx_5^2y_1^2y_2^2y_3^2y_4^2y_6^2 \\
&\quad + PR^2x_4^2x_5^2y_1^2y_2^2y_3^2y_6^2 + P^2Rx_1^2x_5^2y_2^2y_3^2y_4^2y_6^2 \\
&\quad - P^2R^2x_1^2x_4^2y_2^2y_3^2y_5^2y_6^2 \\
&\equiv 1 \pmod{PQR}.
\end{aligned}$$

*Step 8* *Let S be the given secret with* $P, Q$ *and R does not divide S*

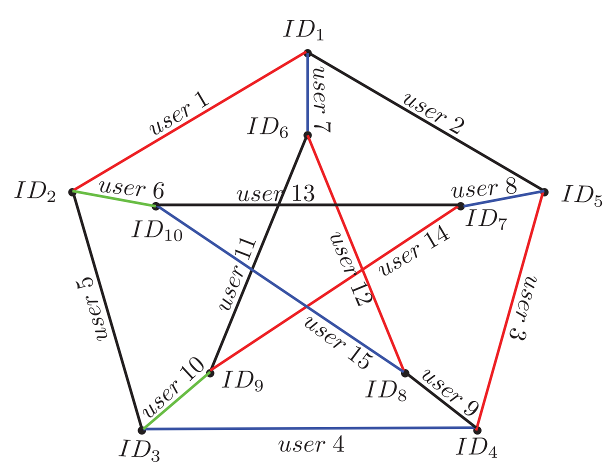
*Step 9* *Let*

$$\begin{aligned}
&t_1 = y_1^2y_2^2y_3^2y_4^2y_5^2y_6^2, \quad t_2 = -Qx_2^2y_1^2y_3^2y_4^2y_5^2y_6^2, \\
&t_3 = -Rx_4^2y_1^2y_2^2y_3^2y_5^2y_6^2, \quad t_4 = QRx_2^2x_4^2y_1^2y_3^2y_5^2y_6^2, \\
&t_5 = -Px_1^2y_2^2y_3^2y_4^2y_5^2y_6^2, \quad t_6 = PQx_1^2x_2^2y_3^2y_4^2y_5^2y_6^2, \\
&t_7 = PRx_1^2x_4^2y_2^2y_3^2y_5^2y_6^2, \quad t_8 = -QRx_6^2y_1^2y_2^2y_3^2y_4^2y_5^2 \\
&t_9 = Q^2Rx_2^2x_6^2y_1^2y_3^2y_4^2y_5^2, \quad t_{10} = QR^2x_4^2x_6^2y_1^2y_2^2y_3^2y_5^2, \\
&t_{11} = -Q^2R^2x_2^2x_4^2x_6^2y_1^2y_3^2y_5^2, \quad t_{12} = -PQx_3^2y_1^2y_2^2y_4^2y_5^2y_6^2, \\
&t_{13} = PQ^2x_2^2x_3^2y_1^2y_4^2y_5^2y_6^2, \quad t_{14} = P^2Qx_1^2x_3^2y_2^2y_4^2y_5^2y_6^2, \\
&t_{15} = P^2Q^2x_1^2x_2^2x_3^2y_4^2y_5^2y_6^2, \quad t_{16} = -PRx_5^2y_1^2y_2^2y_3^2y_4^2y_6^2, \\
&t_{17} = PR^2x_4^2x_5^2y_1^2y_2^2y_3^2y_6^2, \quad t_{18} = P^2Rx_1^2x_5^2y_2^2y_3^2y_4^2y_6^2 \text{ and} \\
&t_{19} = -P^2R^2x_1^2x_4^2y_2^2y_3^2y_5^2y_6^2
\end{aligned}$$

*then, the 19 secret share holders are* $Y_i = t_iS$ *where* $1 \leq i \leq 19$

*Step 10* $\sum_{j=1}^{19} Y_j \equiv S \pmod{PQR}$.

*Example 4* Managing the shortage of Login ID Problems in Petersen Networks . The other terminology not defined here can be found in Balakrishnan and Ranganathan (2000)



(1) There are 10 Login ID and 15 users in the given network
(2) Any two Login IDs can be utilized by at most one user
(3) Every Login ID is used by exactly three users
(4) Represent the Login IDs by the nodes (vertices) of the graph $G$
(5) If there is a user-$j$ using Login IDs $\text{Log ID}_r$ and $\text{Log ID}_s$, then join them by an edge

$$Log\ ID_r \overset{user\ j}{\bullet\!\!-\!\!-\!\!-\!\!-\!\!-\!\!-\!\!\bullet} Log\ ID_s$$

(6) If the two users have a common Login ID then they are conflict users, otherwise non-conflict users. For example, Conflict users: user-1, user-2 and user-7, they have common Login ID $\text{Log ID}_1$ and Non-Conflict users: user-2, user-5 and user-9
(7) Define $V(G) = \{v_i = \text{Log ID}_i \mid 1 \leq i \leq 10\}$
Define $E(G) = \{k = \text{user}\,k \mid 1 \leq k \leq 15\}$
(8) Define $f\ (v_i) = f\ \ (\text{Log ID}_i) = \sigma(i)$, where $\sigma$ is a permutation on the set of numbers $\{1, 2, \ldots, 10\}$. This $\sigma(i)$ is given for each $\text{Log ID}_i$
(9) Now define the graceful labeling $g$ on the set $\{\sigma(1), \sigma(2), \ldots, \sigma(10)\}$

$$g : \{\sigma(i) : 1 \leq i \leq 10\} \longrightarrow \{0, 1, 2, \ldots, q-1, q\}.$$

Suppose

$$Log\ ID_r \overset{user\ j}{\bullet\!\!-\!\!-\!\!-\!\!-\!\!-\!\!-\!\!\bullet} Log\ ID_s$$

$$g[\text{user}\,j\,] = \mid g(\sigma(r)) - g(\sigma(s)) \mid \in \{1, 2, \ldots, q\}$$

where $1 \leq r,\ s \leq 10,\ r \neq s$
(10) $g : E(G) \longrightarrow \{1, 2, \ldots, q\}$
(11) $g$ is kept secret, but $g[\text{user}\,j\,]$ is given for each user $j$
(12) $g[\text{user}\,j\,]$ is called user-ID

$$Log\ ID_r \overset{user\ j}{\bullet\!\!-\!\!-\!\!-\!\!-\!\!-\!\!-\!\!\bullet} Log\ ID_s$$

$(\sigma(r), \sigma(s))$ are two Login IDs for the user $j$
(13) Entire Network is kept secret
(14) $\mathcal{P} : V(G) \longrightarrow \{p_1, p_2, \ldots, p_{10}\}$ where $p_i, 1 \leq i \leq 10$ are distinct odd primes with $q < \min\{p_i\},\ 1 \leq i \leq 10,\ q < p_j \forall j$ ($\mathcal{P}$ is kept secret)

$$\begin{array}{ccc} Log\ ID_r & \overset{user\ j}{\bullet\!\!-\!\!-\!\!-\!\!-\!\!-\!\!-\!\!\bullet} & Log\ ID_s \\ & \updownarrow & \\ \sigma(r) \longleftarrow & known & \longrightarrow \sigma(s) \end{array}$$

$g[\text{user}\,j\,]$ is known $1 \leq j\ \leq 15$
(15) Define $e_j\ :\ \ (e_j, (p_r - 1)(p_s - 1)) = 1\ \ (e_j$ kept secret)
(16) Define $m_j\ \equiv (g[\text{user}\,j\,])^{e_j} \pmod{p_r p_s}$ $\mathcal{P}[\text{LogID}_r] = p_r, \mathcal{P}[\text{Log ID}_s] = p_s,\ 1 \leq r,\ s \leq 10, r \neq s$
(17) Decompose the user (edges) into subset of Non-Conflict users (set of Independent Edges)
(18)

$$\begin{aligned}
&A = \{\text{user-2, user-5, user-9, user-11, user-13}\} : \\
&\quad \text{user-2} \longleftrightarrow \{\text{Log ID}_1,\ \text{Log ID}_5\} \\
&\quad \text{user-5} \longleftrightarrow \{\text{Log ID}_2,\ \text{Log ID}_3\} \\
&\quad \text{user-9} \longleftrightarrow \{\text{Log ID}_4,\ \text{Log ID}_8\} \\
&\quad \text{user-11} \longleftrightarrow \{\text{Log ID}_6,\ \text{Log ID}_9\} \\
&\quad \text{user-13} \longleftrightarrow \{\text{Log ID}_7,\ \text{Log ID}_10\} \\
&B = \{\text{user-1, user-3, user-12, user-14}\} : \\
&\quad \text{user-1} \longleftrightarrow \{\text{Log ID}_1,\ \text{Log ID}_2\} \\
&\quad \text{user-3} \longleftrightarrow \{\text{Log ID}_5,\ \text{Log ID}_4\} \\
&\quad \text{user-12} \longleftrightarrow \{\text{Log ID}_6,\ \text{Log ID}_8\} \\
&\quad \text{user-14} \longleftrightarrow \{\text{Log ID}_7,\ \text{Log ID}_9\} \\
&C = \{\text{user-4, user-7, user-8, user-15}\} : \\
&\quad \text{user-4} \longleftrightarrow \{\text{Log ID}_3,\ \text{Log ID}_4\} \\
&\quad \text{user-7} \longleftrightarrow \{\text{Log ID}_1,\ \text{Log ID}_6\} \\
&\quad \text{user-8} \longleftrightarrow \{\text{Log ID}_5,\ \text{Log ID}_7\} \\
&\quad \text{user-15} \longleftrightarrow \{\text{Log ID}_8,\ \text{Log ID}_10\} \\
&D = \{\text{user-6, user-10}\} : \\
&\quad \text{user-6} \longleftrightarrow \{\text{Log ID}_2,\ \text{Log ID}_10\} \\
&\quad \text{user-10} \longleftrightarrow \{\text{Log ID}_3,\ \text{Log ID}_9\}
\end{aligned}$$

(19) Define congruences equations for the set $A, B, C$ and $D$ as follows

$$\begin{aligned}
x &\equiv m_2 \pmod{p_1 p_5} \\
x &\equiv m_5 \pmod{p_2 p_3} \\
x &\equiv m_9 \pmod{p_4 p_8} \\
x &\equiv m_{11} \pmod{p_6 p_9} \\
x &\equiv m_{13} \pmod{p_7 p_{10}}
\end{aligned}$$

$x$ has a unique solution $\pmod{p_1 p_2 \cdots p_{10}}$

Thus $x$ is the common secret shared by the group *A Non-Conflict users*

$$\begin{aligned}
y &\equiv m_1 \pmod{p_1 p_2} \\
y &\equiv m_3 \pmod{p_4 p_5} \\
y &\equiv m_{12} \pmod{p_6 p_8} \\
y &\equiv m_{14} \pmod{p_7 p_9}
\end{aligned}$$

$y$ has a unique solution $\pmod{p_1 p_2 p_4 p_5 p_6 p_7 p_8 p_9}$

Thus $y$ is the common secret shared by the group *B Non-Conflict users*

$$z \equiv m_4 \pmod{p_3 p_4}$$
$$z \equiv m_7 \pmod{p_1 p_6}$$
$$z \equiv m_8 \pmod{p_5 p_7}$$
$$z \equiv m_{15} \pmod{p_8 p_{10}}$$

$z$ has a unique solution $(\mathrm{mod}\, p_1 p_3 p_4 p_5 p_6 p_7 p_8 p_{10})$
Thus $z$ is the common secret shared by the group *C Non-Conflict users*

$$w \equiv m_6 \pmod{p_2 p_{10}}$$
$$w \equiv m_{10} \pmod{p_3 p_9}$$

$w$ has a unique solution $(\mathrm{mod}\, p_2 p_3 p_9 p_{10})$

Thus $w$ is the common secret shared by the group *D Non-Conflict users*

## 4. Conclusion

In the proposed system we only focused on protecting the group key information broadcasted from the Dealer to all the share holders in the group and the group guarantees the confidentiality authentication of the key generated. This confirms that the protocol is secure for both inside and outside attack. In this paper, an algorithm is proposed for secure key sharing. This method can be used for factorization of positive integer $N$. The proposed tool is more efficient key distribution algorithm used for a secret code, since it involves more number of prime numbers. The technique used in this paper for secret sharing is to split the secret into different primes 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 and it leads a opening of new developments in the field of cryptosystems

**Disclosure statement**

No potential conflict of interest was reported by the authors.

## References

Apostol, T. M. (1976). *Introduction to analytic number theory*. Springer.

Asmuth, C., & Bloom, J. (1983). A modular approach to key safeguarding. *IEEE Transactions on Information Theory*, *29*, 208–210.

Balakrishnan, R., & Ranganathan, K. (2000). *A textbook of graph theory*. Berlin: Springer.

Berlekamp, E. R. (1968). *Algebraic coding theory*. New York, NY: McGraw-Hill.

Blakley, G. R. (1979). *Safeguarding cryptographic keys*. Proceedings of the National Computer Conference, AFIPS Press, Monval, NJ, Vol. 48, pp. 313–317.

Koblitz, N. (1994). *A course in number theory and cryptography* (2nd ed.). New York: Springer-Verlag.

Lu, Y., & Li, J. (2013). Constructing paring-free certificate-based encryption. *International Journal of Innovative Computing Information and Control*, *9*(11), 4509–4518.

Mignotte, M. (1983). *How to share a secret*. Advances in Cryptology – Eurocrypt'82, LNCS, Vol. 149, Springer-Verlag, pp. 371–375.

Muralikrishna, P., Srinivasan, S., & Chandramowliswaran, N. (2013). Secure schemes for secret sharing and key distribution using Pell's equation. *International Journal of Pure and Applied Mathematics*, *85*(5), 933–937.

Okamoto, E., & Tanaka, K. (1989). Key distribution system based on identification information. *IEEE Journal on Selected Areas in Communications*, *7*(4), 481–485.

Schneier, B. (1996). *Applied cryptography* (2nd ed.). New York: J. Wiley & Sons, Inc.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, *22*(11), 612–613.

Srinivasan, S., Muralikrishna, P., & Chandramowliswaran, N. (2013). Authenticated multiple key distribution using simple continued fraction. *International Journal of Pure and Applied Mathematics*, *87*(2), 349–354.