Hang Lung Mathematics Awards
Vol. 2 (2006), pp. 155–193

AN INVESTIGATION IN SECRET SHARING

TEAM MEMBERS
Ho-Kwan Lee, Kin-Shing Lo, Chi Wong[1]

SCHOOL
Fung Kai Liu Man Shek Tong Secondary School

Abstract. The aim of this project is to study the problem of Threshold Scheme. After reading the book "In Code: A Mathematical Journey"[1] written by Sarah Flannery, we found an interesting problem. When 11 persons keep a secret and any 6 of them are allowed to open it, we need 462 locks and each person needs 252 keys. As the author gives the answer without explanation, we are interested in Threshold Scheme. We call this problem the Key Distribution scheme "KD Scheme". Afterwards, we think about how the Chinese Remainder Theorem (CRT) works to implement the Threshold Scheme. We call it "CRT Scheme". As CRT requires some pairwisely prime (prp) numbers, we create algorithms to generate prp numbers. The results of this report include:

1. Solving the KD scheme completely.
2. Constructing the CRT Scheme.
3. Comparing the CRT Scheme with the KD scheme.
4. Constructing a set of prp numbers by the method of $\{M \pm 1\} \cup \{M + p_i\}$.
5. Constructing a set of prp numbers by the "Sieve of PRP Numbers".
6. Making a conjecture that the maximum number of prp numbers within the range $[s, s + k]$ is approximately equal to $\pi(k)$.

1. Introduction

Secret Sharing and Threshold Scheme

In cryptography, there is a way that distributes a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can only be opened when the shares are combined together. Individual shares are of no use on their own. This way is called Secret Sharing.

Alice, Bob and Claire are the captains of a restaurant. They share the

[1]This work is done under the supervision of the authors' teacher, Mr. Ka-Wo Leung.

customer's tips at the end of each month. One day, the manager buys a tips box and suggests that two of them could open it to divide the tips into 3 equal parts. (If only one can open the box, it is not secure enough. But, if all three are required to open the box, it is too trouble when one leaves the restaurant.) This problem is called $(2,3)-$Threshold Scheme.

Generally speaking, when a secret is divided into n pieces (called shadows) given the following two conditions:

1. Availability: Any t shadows or more can together open the secret
2. Confidentiality: Any $(t-1)$ shadows or less cannot together open the secret

The problem is called $(t,n)-$Threshold Scheme, or abbreviated TS(t,n) hereafter.

Then, the manager locks the tips box with 3 locks, named L_1, L_2 and L_3. Alice holds a key for L_1 and L_2 only. Bob for L_1 and L_3 while Claire for L_2 and L_3. Since any two of them have a full set of keys to all 3 locks, the condition of Availability is satisfied. As each of them holds only 2 keys, the condition of Confidentiality is satisfied. We call the above way the Key Distribution Scheme, abbreviated KD(t,n) or "KD Scheme" hereafter.

When we try to solve the problem of KD Scheme, we need to answer the following questions. How many locks are needed? How many keys does each person need? How are the keys distributed?

Chinese Remainder Theorem Scheme (CRT Scheme)

Afterwards, we think about how the Chinese Remainder Theorem (CRT) works to implement the Threshold Scheme. We call it CRT(t,n) or "CRT Scheme".

We ask ourselves questions about CRT Scheme. how does the CRT Scheme work? What conditions must be satisfied? What conditions should be satisfied to ensure a secure CRT Scheme? How can the degree of security be measured? How is the CRT Scheme compared with the KD Scheme?

Finding Pairwise Relatively Prime (PRP) Numbers

As CRT Scheme requires some pairwise relatively prime (prp) numbers, we need to find enough prp numbers. We then create two useful algorithms

to generate prp numbers. They are as follows:

1. The method of $\{M \pm 1\} \cup \{M + p_i\}$
2. Sieve of PRP Numbers

In our project, some algorithms failed and the above two succeeded. In the investigation process, we found the crucial tool to analyze whether two numbers are relatively prime. It is the prime factor function, which is a set-valued function.

An interesting conjecture

Once we obtained the Sieve of PRP Numbers, we tested the method with different sets of $(k + 1)$ consecutive integers and saw what would happen. For different values of s and k, we tried to find the maximum number of prp numbers within the range of $[s, s + k]$. We made a conjecture that the maximum number of prp numbers within the range $[s, s + k]$ is approximately equal to $\pi(k)$. We guessed the Sieve of Eratosthenes and the Inclusion-Exclusion Principle would help in proving this conjecture.

2. Key Distribution Scheme (KD Scheme)

Investigation direction

$\mathrm{TS}(t, n)$ is well defined for $1 \leqslant t \leqslant n$. When $\mathrm{TS}(t, n)$ is well defined, we mark a solid dot at (t, n). Otherwise, we mark a hollow dot. Then we have Figure 1. Our aim is to solve the KD Scheme for all solid dots in Figure 1.

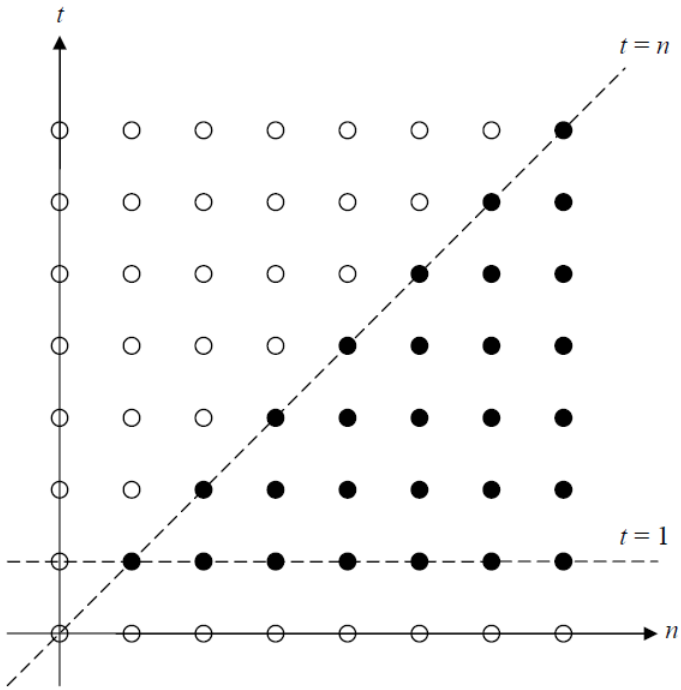


FIGURE 1

Notations used

We use m locks to protect the secret and distribute different keys to the n persons.

Persons \ Locks	L_1	L_2	L_3	...	L_j	...	L_m
P_1	K_{11}	K_{12}	K_{13}				
P_2	K_{21}	K_{22}	K_{23}				
P_3	K_{31}	K_{32}	K_{33}				
$\vdots$							
P_i					K_{ij}		
$\vdots$							
P_n							K_{mn}

$$K_{ij} = \begin{cases} 1 & \text{if } P_i \text{ has a key for } L_j \text{ and can open the lock} \\ 0 & \text{if } P_i \text{ does not have a key for } L_j \text{ and cannot open the lock} \end{cases}$$

The two trivial solutions

When $t = 1$, the solution is trivial. We use only 1 lock and give keys for the locks to the n persons. Mathematically, the solution is $m = 1$ and $K_{11} = K_{21} = \ldots = K_{n1} = 1$.

When $t = n$, the solution is trivial, too. The n persons use their locks to protect the secret and keep their keys without giving to the others. Mathematically, the solution is $m = n$ and $K_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$.

The first few non-trivial solutions

From Figure 1, we know that the next step is to solve KD(2,3), KD(2,4), KD(3,4), etc.

A solution of KD(2,3):

$m = 3$

	L_1	L_2	L_3
P_1	0	1	1
P_2	1	0	1
P_3	1	1	0

A solution of KD(2,4):

$m = 3$

	L_1	L_2	L_3	L_4
P_1	0	1	1	1
P_2	1	0	1	1
P_3	1	1	0	1
P_4	1	1	1	0

After the above solution, we can make a conclusion for KD$(2, n)$. $m = n$ and $K_{ij} = \begin{cases} 0 & \text{if } i = j \\ 1 & \text{if } i \neq j \end{cases}$.

Graphically, the solution is:

	L_1	L_2	...	L_j	...	L_m
P_1	0	1	1	1	1	1
P_2	1	0	1	1	1	1
$\vdots$	1	1	$\ddots$	...	...	1
P_i	1	1	$\vdots$	$\ddots$	...	1
$\vdots$	1	1	$\vdots$	$\vdots$	$\ddots$	1
P_n	1	1	1	1	1	0

Since each lock L_j can only block one person, any two-person group can open all the locks. The condition of Availability is satisfied. As each person P_i cannot open the lock L_i, the condition of Confidentiality is satisfied.

A mistaken solution to KD(3,4) gives a clue to the general solution

One of our teammates gives a mistaken solution of KD(3,4) as follows:

$m = 5$

	L_1	L_2	L_3	L_4	L_5
P_1	0	1	1	0	1
P_2	0	0	1	1	0
P_3	1	0	0	0	1
P_4	1	1	0	1	0

When we use the condition of Confidentiality to verify his solution, we need to ask whether all two-person groups are blocked by a lock. We find that P_1–P_4 group is not blocked by any locks, and they can steal the secret. How can we modify it?

Can we add more "0"s in a column?

No, otherwise, one of the columns has 3 "0"s. The lock will block a three-person group. The condition of Availability will be violated.

Can we add one more column which blocks the P_1-P_4 group to open it?

Yes, we guess it is the only way and will be proved later.

Then the solution of KD(3,4) comes:

$m = 6$

	L_1	L_2	L_3	L_4	L_5	L_6
P_1	0	1	1	0	1	0
P_2	0	0	1	1	0	1
P_3	1	0	0	0	1	1
P_4	1	1	0	1	0	0

Trying the KD(3,5) first

- We cannot have a column of 3 "0"s, because of the condition of Availability.
- We must count all two-person groups. A column of 2 "0"s corresponds to the group to satisfy the condition of Confidentiality.

Then the solution of KD(3,5) comes:

$m = {}_5C_2 = 10$

	L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8	L_9	L_{10}
P_1	0	0	0	0	1	1	1	1	1	1
P_2	0	1	1	1	0	0	0	1	1	1
P_3	1	0	1	1	0	1	1	0	0	1
P_4	1	1	0	1	1	0	1	0	1	0
P_5	1	1	1	0	1	1	0	1	0	0

The fundamental solution to KD(t, n)

- Each lock has a column of $(t-1)$ "0"s. (Availability)
- The locks consist of all different $(t-1)$-number combination of "0"s. (Confidentiality)
- When choosing $(t-1)$ numbers from 1 to n, there are ${}_nC_{t-1}$ ways of choosing. Therefore, there are ${}_nC_{t-1}$ locks.

Mathematically, the fundamental solution can be rewritten as:

- For all j, $\sum_{i=1}^{n} K_{ij} = n - t + 1$
- For all $a_1, a_2, \ldots, a_{i-1}$, there exists j such that

$$K_{ij} = \begin{cases} 0 & \text{if } i = a_1 \text{ or } a_2 \text{ or } \ldots \text{ or } a_{i-1} \\ 1 & \text{otherwise} \end{cases}$$

- $m = {}_nC_{t-1}$

Prove that the fundamental solution to KD(t, n) satisfies the conditions of Availability and Confidentiality

Availability:

Each lock consists of $(t-1)$ "0"s only.
For any t-person group, all locks could be opened by at least one person.

Confidentiality:

The locks consist of all different $(t-1)$-number combination of "0"s.
For any $(t-1)$-person group, there is a lock which could not be opened by all the $(t-1)$ persons.

Is the fundamental solution to KD(t, n) simple enough?

- Can a lock have a column of t "0"s or more?
  No, it violates the condition of Availability.

- Can we delete any lock?
  No, or if you do that, the corresponding $(t-1)$-person group is not blocked by any lock and the condition of Confidentiality is violated.

- Can we add any locks?
  Yes, but
  1. the lock must have $(t-1)$ "0"s or less,
  2. the lock is redundant.

- Can a lock have a column of $(t-2)$ "0"s or less?
  Yes, but the lock must be redundant.

Therefore, you may add some locks to the fundamental solution, provided that each lock consists of $(t-1)$ "0"s or less. Also, the locks added are redundant.

Properties of the fundamental solution to KD(t, n)

Number of locks	$= {}_nC_{t-1}$
Number of keys for each lock	$= n - t + 1$
Total number of keys	$= (n - t + 1){}_nC_{t-1}$
Number of keys for each person	$= \dfrac{(n - t + 1){}_nC_{t-1}}{n}$
	$= \dfrac{(n - t + 1)}{n} \cdot \dfrac{n!}{(n - t + 1)!(t - 1)!}$
	$= \dfrac{(n - 1)!}{(n - t)!(t - 1)!)}$
	$= {}_{n-1}C_{t-1}$

3. The Chinese Remainder Theorem (CRT)

From some websites[2, 3], we learn the Chinese Remainder Theorem.

Given a set of simultaneous congruence, $x = y_i \pmod{m_i}$ for $i = 1, 2, \ldots, t$ and with the condition that the m_i are pairwise relatively prime (prp). There exist a unique solution for $0 \leqslant x \leqslant \prod_{i=1}^{t} m_i - 1$.

4. The Chinese Remainder Theorem Scheme (CRT Scheme)

CRT Scheme

For the secret number x, we take the congruence as follows:

$y_i = x \mod m_i$ for $i = 1, 2, \ldots, n$
with m_i are prp and $m_1 < m_2 < \cdots < m_n$

The y_i are the shadows with the following two conditions:

1. Availability: Any t values or more can together uniquely reconstruct x.
2. Confidentiality: Any $(t - 1)$ values of y_i or less cannot together uniquely reconstruct x.

The problem is abbreviated CRT(t, n) or CRT Scheme hereafter.

Notation used

For convenience, we make definitions as follow:

- $m_i = \{2, 3, 5, 7, 11, \ldots\}$ refers $m_1 = 2$, $m_2 = 3$, etc.
- n_x refers to the number of possible values of x, equivalently, $0 \leqslant x \leqslant n_x - 1$.
  Similarly, n_{y_i} refers to the number of possible values of y_i, equivalently, $0 \leqslant y_i \leqslant n_{y_i} - 1$.

The first trial – CRT(2,3)

As m_i are prp, we take the first 3primes m_i, that is $m_i = \{2, 3, 5\}$. We have:

x	y_1	y_2	y_3
0	0	0	0
1	1	1	1
2	0	2	2
3	1	0	3
4	0	1	4
5	1	2	0
6	0	0	1
7	1	1	2
⋮	⋮	⋮	⋮

If $0 \leqslant x \leqslant 6$, the condition of Availability is violated. The worst case would be $y_1 = y_2 = 0$. In such case, we cannot determine $x = 0$ or 6.

If $0 \leqslant x \leqslant 4$, the condition of Confidentiality is violated since $x = y_3$.

Therefore, we need $0 \leqslant x \leqslant 5$, or $n_x = 6$.

We noticed that, in such case, y_3 knows much about x. When $1 \leqslant y_3 \leqslant 4$, $x = y_3$. Only when $y_3 = 0$, we need to guess whether $x = 0$ or 5. Surely it is not secure enough.

A better way for CRT(2,3)

As 3 consecutive integers staring from an odd are prp (see appendices A and B), we can take $m_i = \{101, 102, 103\}$.

If $n_x > 101 \times 102$, the condition of Availability is violated.

If $n_x \leqslant 103$, the condition of Confidentiality is violated.

Therefore, $103 < n_x \leqslant 101 \times 102$.

Surely if n_x is just slightly greater than 103, we need very few guess to obtain x from y_3.

When we took $n_x = 101 \times 102$, the average number of possible values of x corresponding to a value of y_3 is $\dfrac{101 \times 102}{103} \approx 100$.

Therefore,

$$\text{Larger } m_i \Rightarrow \text{ more secure CRT Scheme} \tag{1}$$

Another CRT(2,3)

Take $m_i = \{101, 102, 10301\}$ which is a set of prp numbers. Since $10301 < n_x \leqslant 101 \times 102$, $n_x = 10302$.

The average number of possible values of x corresponding to a value of y_3 is $\dfrac{101 \times 102}{10301} \approx 1$.

It is less secure than CRT(2,3) which $m_i = \{101, 102, 103\}$.

Therefore,

$$\text{Closer } m_i \Rightarrow \text{ more secure CRT Scheme} \tag{2}$$

A general solution to CRT(2,3)

We take $m_i = \{2n-1, 2n, 2n+1\}$. To satisfy the condition of Availability and Confidentiality, we have $m_3 < n_x \leqslant m_1 m_2$.

If n is large enough, the average number of possible values of x corresponding to a value of y_i is $\dfrac{n_x}{m_i} \leqslant \dfrac{m_1 m_2}{m_3} = \dfrac{(2n-1)(2n)}{2n+1} \approx 2n = m_2$.

Trying the CRT(3,5)

As m_i are prp, we take the first 5 primes m_i, that is, $m_i = \{2, 3, 5, 7, 11\}$.

We have:

x	y_1	y_2	y_3	y_4	y_5
0	0	0	0	0	0
1	1	1	1	1	1
⋮	⋮	⋮	⋮	⋮	⋮
59	1	2	4	3	4
60	0	0	0	4	5
61	1	1	1	5	6
⋮	⋮	⋮	⋮	⋮	⋮
76	0	1	1	6	10
77	1	2	2	0	0
78	0	0	3	1	1

If $n_x > 60$, the condition of Availability is violated. The worst case would be $y_1 = y_2 = y_3 = 0$. In such case, we cannot determine $x = 0$ or 60.

If $n_x \leqslant 77$, the condition of Confidentiality is violated since $x = (22y_4 + 56y_5) \mod 77$. Contradiction occurs! $77 < n_x \leqslant 60$ implies $77 < 60$ which is false.

A feasible way for CRT(3,5)

We take $m_i = \{4, 5, 7, 9, 11\}$. To satisfy the condition of Availability and Confidentiality, we have $9 \times 11 < n_x \leqslant 4 \times 5 \times 7$.

When we take $n_x = 4 \times 5 \times 7$, the average number of possible values of x corresponding to a pair of values of y_4 and y_5 is $\dfrac{4 \times 5 \times 7}{9 \times 11} \approx 1.4$. What does it mean?

When $0 \leqslant x \leqslant 40$, $x = (55y_4 + 45y_5) \mod 99$ or $[(55y_4 + 45y_t) \mod 99] + 99$. Number of possible values of $x = 2$.

When $41 \leqslant x \leqslant 99$, $x = (55y_4 + 45y_5) \mod 99$. Number of possible values of $x = 1$.

Then the average number of possible values of x corresponding to a pair of values of y_4 and y_5 is $\dfrac{41 \times 2 + 58}{41 + 58} = \dfrac{4 \times 5 \times 7}{9 \times 11} \approx 1.4$.

Changing 4 to 8, to form another feasible way for CRT(3,5)

We take $m_i = \{5, 7, 8, 9, 11\}$. To satisfy the condition of Availability and Confidentiality, we have $9 \times 11 < n_x \leqslant 5 \times 7 \times 8$.

When we take $n_x = 5 \times 7 \times 8$, the average number of possible values of x corresponding to a pair of values of y_4 and y_5 is $\dfrac{5 \times 7 \times 8}{9 \times 11} \approx 2.8$.

The case with $m_i = \{5, 7, 8, 9, 11\}$ is more secure than the one with $m_i = \{4, 5, 7, 9, 11\}$.

It is another example to show (2): Closer $m_i \Rightarrow$ more secure CRT Scheme.

The general case – CRT(t,n)

To satisfy the condition of Availability and Confidentiality, we have

$$\underbrace{m_{n-t+2}m_{n-t+3}}_{(t-1)\text{ factors}} \cdots m_n < n_x \leqslant \underbrace{m_1 m_2 \cdots m_t}_{t\text{ factors}}$$

or

$$\prod_{i=n-t+2}^{n} m_i < n_x \leqslant \prod_{i=1}^{t} m_i.$$

In order to have a more secure CRT Scheme, take $n_x = \prod_{i=1}^{t} m_i$.

The average number of possible values of x corresponding to $(t-1)$ values of y_i is

$$\begin{aligned} \frac{n_x}{\text{product of } (t-1) \text{ different } m_i} &\geqslant \frac{\prod_{i=1}^{t} m_i}{\prod_{i=n-t+2}^{n} m_i} \\ &= \frac{\text{product of } t \text{ smallest } m_i}{\text{product of } (t-1) \text{ largest } m_i} \\ &\geqslant \frac{m_1^t}{m_n^{t-1}}. \end{aligned}$$

Because of the following two conditions for a more secure CRT Scheme,

(1) larger $m_i \Rightarrow$ more secure CRT Scheme, and
(2) closer $m_i \Rightarrow$ more secure CRT Scheme,

we assume that m_i are large enough and close to one another. We let $m_i \approx m$, and have the average number of possible values of x corresponding to $(t-1)$ values of $y_i \approx \dfrac{m^t}{m^{t-1}} = m$.

5. Secret Sharing Model and Comparison between KD Scheme and CRT Scheme

Secret Sharing Model

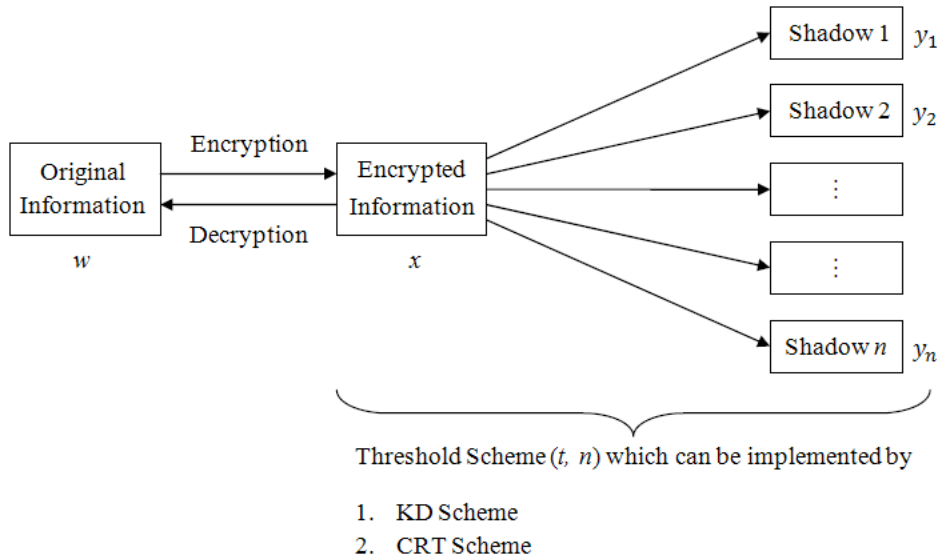


FIGURE 2

Assumptions:

1. The original information is encrypted to get the encrypted information.
2. The encrypted information is divided into n shadows to implement the Threshold Scheme (t, n).
3. The encryption, decryption and Threshold Scheme algorithms are public.
4. The entire encrypted information can result the entire original information.
5. Only part of the encrypted information is not sufficient to get any part of the original information.

The aim of this project is to study the problem of Threshold Scheme. The above assumption is to ensure that insufficient number of shadows cannot obtain any part of the original information.

An analogy to the Secret Sharing Model

A computer consists of 5 harddisks. We have a secret letter and encrypt it to a file. We divided the encrypted file into 5 shadows and store them separately in each harddisk. Once any 3 of them are in good condition, we can get back the encrypted file and decrypted it to read the secret letter. If we just store the encrypted file in one harddisk, it is not secure enough. If we store the encrypted file in all harddisks, it wastes storage spaces. After trading off between security and space saving, we may need the Threshold Scheme (t, n).

Degree of Security

We define the following indices:

1. Carrying Portion
   $= \alpha$
   $$= \frac{\text{maximum number of bits of a shadow}}{\text{number of bits of the encrypted information}}$$
   The range of α is $\frac{1}{t} \leqslant \alpha \leqslant 1$ ($\alpha = 1$ if and only if $t = 1$) and the ideal value of α is $\frac{1}{t}$.
2. Threshold Security
   $= \beta$
   $$= \frac{\text{minimum number of missing bits for } (t-1) \text{ shadows}}{\text{number of bits of the encrypted information}}$$
   $$= 1 - \frac{\text{maximum number of bits of } (t-1) \text{ shadows}}{\text{number of bits of the encrypted information}}$$
   The range of β is $0 < \beta \leqslant \frac{1}{t}$ and the ideal value of β is $\frac{1}{t}$.

Analysis on KD Scheme

When 11 persons keep a secret and any 6 of them are allowed to open it, we need 462 locks and each person needs 252 keys. If any 5 of them try to open the secret, there is a lock to block their way.

If a piece of encrypted information has 462 bits, and distributes the bits according to the KD(6,11). Each shadow has 252 bits. Any 6 of the shadows are allowed to get all the bits. Any 5 of them together have 1 bit missing.

We consider the general case KD(t, n). For every ${}_nC_{t-1}$ bits, each shadow has ${}_{n-1}C_{t-1}$ bits. Any t of the shadows are allowed to get all the bits. Any $(t-1)$ of them together miss 1 bit.

Therefore,

$$\alpha = \frac{{}_{n-1}C_{t-1}}{{}_nC_{t-1}} = \frac{(n-1)!}{(n-t)!(t-1)!} \cdot \frac{(n-t+1)!(t-1)!}{n!} = \frac{n-t+1}{n}$$

and

$$\beta = \frac{1}{{}_nC_{t-1}}.$$

Since $\alpha = \dfrac{n-t+1}{n} = \dfrac{1}{t} + (t-1)\left(\dfrac{1}{t} - \dfrac{1}{n}\right)$ (see appendix G) and $\beta = \dfrac{1}{{}_nC_{t-1}} = \dfrac{1}{t + \displaystyle\sum_{i=1}^{n} {}_iC_{t-2}}$ (see appendix H), α and β differ from the ideal values by significant amounts for the non-trivial cases $2 \leqslant t \leqslant n-1$.

Analysis on CRT Scheme

Let $\gamma_i = \dfrac{\log_2(m_i)}{\log_2(m_n)}$ and $n_x = \prod_{i=1}^{t} m_i$.

$$\alpha = \frac{\log_2(n_{y_n})}{\log_2(n_x)} = \frac{\log_2(m_n)}{\log_2\left(\prod_{i=1}^{t} m_i\right)} = \frac{\log_2(m_n)}{\sum_{i=1}^{t} \gamma_i \log_2(m_n)} = \frac{1}{\sum_{i=1}^{t} \gamma_i}$$

Therefore,

$$\frac{1}{t\gamma_t} < \alpha < \frac{1}{t\gamma_1}.$$

$$\begin{aligned}
\beta &= 1 - \frac{\log_2\left(\prod_{i=n-t+2}^{n} n_{y_i}\right)}{\log_2(n_x)} \\
&= 1 - \frac{\log_2\left(\prod_{i=n-t+2}^{n} m_i\right)}{\log_2\left(\prod_{i=1}^{t} m_i\right)} \\
&= 1 - \frac{\sum_{i=n-t+2}^{n} \gamma_i \log_2(m_n)}{\sum_{i=1}^{t} \gamma_i \log_2(m_n)} \\
&= 1 - \frac{\sum_{i=n-t+2}^{n} \gamma_i}{\sum_{i=1}^{t} \gamma_i}
\end{aligned}$$

Therefore,

$$1 - \frac{t-1}{t\gamma_1} < \beta < 1 - \frac{(t-1)\gamma_{n-t+2}}{t\gamma_t}.$$

If the condition that m_i are very close to one another holds, or equivalently γ_i are very close to 1, α and β are very close to the ideal values.

Comparison between KD Scheme and CRT Scheme

	Carrying Portion α	Threshold Security β
Range	$\frac{1}{t} \leqslant \alpha \leqslant 1$ ($\alpha = 1$ if and only if $t = 1$)	$0 < \beta \leqslant \frac{1}{t}$
Ideal Value	$\frac{1}{t}$	$\frac{1}{t}$
KD Scheme	$\frac{1}{t} + \frac{(t-1)(n-t)}{nt}$	$\frac{1}{t + \sum_{i=t}^{n-1} {}_iC_{t-2}}$
CRT Scheme	$< \frac{1}{t\gamma_1}$	$> 1 - \frac{t-1}{t\gamma_1}$

6. Finding Pairwise Relatively Prime (PRP) numbers

Investigation Background

As CRT Scheme requires some pairwise relatively prime (prp) numbers, we need to find enough prp numbers. In order to obtain a secure CRT Scheme, we need to:

1. make m_i as large as required, and
2. pack m_i as close to one another as possible.

If we need only 3 prp numbers, it is as easy as taking 3 consecutive integers starting from an odd (see Appendices A and B). Therefore, we need methods to generate 4 or more prp numbers.

Can we simply take prime numbers m_i?

No, by the Prime Number Theorem[4, 5], we can find fewer prime numbers around a larger number. It means the above two conditions contradict each other if we simply take prime numbers m_i. Instead of taking prime numbers as m_i, we hope to create algorithms to generate enough prp numbers.

A failed trial

We have taken $m_i = \{4, 5, 7, 9, 11\}$ or $\{5, 7, 8, 9, 11\}$. We guess that m_i has the form of $p_i^{\alpha_i}$ but they are not close to one another for large numbers.

The first light of the morning comes

The set of prp numbers $m_i = \{5, 7, 8, 9, 11\}$ is better than $m_i = \{4, 5, 7, 9, 11\}$ since the numbers in the first set are larger and closer to one another. We let $N = 5$ and m_i becomes $\{N, N+2, N+3, N+4, N+6\}$. We found that if $2 \nmid N$ and $3 \nmid N$, the set of numbers $\{N, N+2, N+3, N+4, N+6\}$ are prp.

Proof.

$(N, N+2) = (N, 2) = 1$ or 2.	Since $2 \nmid N$, N and $N+2$ are relatively prime.
$(N, N+3) = (N, 3) = 1$ or 3.	Since $3 \nmid N$, N and $N+3$ are relatively prime.
$(N, N+4) = (N, 4) = 1$, 2 or 4.	Since $2 \nmid N$, N and $N+4$ are relatively prime.
$(N, N+6) = (N, 6) = 1$, 2, 3 or 6.	Since $2 \nmid N$ and $3 \nmid N$, N and $N+6$ are relatively prime.
$(N+2, N+3) = (N+2, 1) = 1$.	$N+2$ and $N+3$ are relatively prime.
$(N+2, N+4) = (N+2, 2) = (N, 2) = 1$ or 2.	Since $2 \nmid N$, $N+2$ and $N+4$ are relatively prime.
$(N+2, N+6) = (N+2, 4) = 1$, 2 or 4.	Since $2 \nmid N$, $N+2$ and $N+6$ are relatively prime.
$(N+3, N+4) = (N+3, 1) = 1$.	$N+3$ and $N+4$ are relatively prime.
$(N+3, N+6) = (N+3, 3) = (N, 3) = 1$ or 3.	Since $3 \nmid N$, $N+3$ and $N+6$ are relatively prime.
$(N+4, N+6) = (N+4, 2) = (N, 2) = 1$ or 2.	Since $2 \nmid N$, $N+4$ and $N+6$ are relatively prime.

□

We change the above proof to the following table:

The gcd of two numbers

N	$(N,2)$	$(N,3)$	$(N,4)$	$(N,6)$
	$N+2$	1	$(N,2)$	$(N+2,4)$
		$N+3$	1	$(N,3)$
			$N+4$	$(N,2)$
				$N+6$

We modify the above table to get the below one:
(p,r) refers to "$N \mod p = r$ is false $\Leftrightarrow$ the corresponding two numbers are relatively prime"

N	$(2,0)$	$(3,0)$	$(2,0)$	$(2,0)$ $(3,0)$
	$N+2$	nil	$(2,0)$	$(2,0)$
		$N+3$	nil	$(3,0)$
			$N+4$	$(2,0)$
				$N+6$

Explanation: ($N \mod 2 \neq 0$ and $N \mod 3 \neq 0$) $\Leftrightarrow$ N and $N+6$ are relatively prime.

Since we are going to find a set of prp numbers, write down $(2,0)$ 6 times is redundant. We simplify the above table by this way. If the conditions appear more than once, we can just write down the first appearance.

Then we have the following tables:

Table of Necessary and Sufficient Conditions for Relatively Prime
(p,r) refers to $N \mod p \neq r$

N	$(2,0)$	$(3,0)$		
	$N+2$			
		$N+3$		
			$N+4$	
				$N+6$

Table of Case Rejected
(p,r) refers to $N \mod p \neq r$

p	r
2	0
3	0

Explanation:

- The condition that N and $N+2$ are relatively prime $\Leftrightarrow$ $N \mod 2 \neq 0$.

- When the set $\{N, N+2\}$ is changed to $\{N, N+2, N+3\}$, we need to add a condition $N \mod 3 \neq 0$ to maintain the set to be prp.
- No more conditions are needed when the set is changed from $\{N, N+2, N+3\}$ to $\{N, N+2, N+3, N+4\}$.
- $N \mod 2 \neq 0$ and $N \mod 3 \neq 0 \Leftrightarrow \{N, N+2, N+3, N+4, N+6\}$ are prp.

Can we add $N+7$?

Table of Necessary and Sufficient Conditions for Relatively Prime
(p, r) refers to $N \mod p \neq r$

N	$(2,0)$	$(3,0)$			$(7,0)$
	$N+2$				$(5,3)$
		$N+3$			$(2,1)$
			$N+4$		$(3,2)$
				$N+6$	nil
					$N+7$

Table of Case Rejected
(p, r) refers to $N \mod p \neq r$

p	r
2	0
3	0

$N+3$ and $N+7$ are relatively prime $\Leftrightarrow N \mod 2 \neq 1$
N and $N+2$ are relatively prime $\Leftrightarrow N \mod 2 \neq 0$
Since $(N \mod 2)$ have only 2 possible values, which are 0 or 1, we cannot add $N+7$.

7. The Method of $\{M \pm 1\} \cup \{M + p_i\}$

If we need only 5 or less prp numbers, it is as easy as taking 3 consecutive integers starting from an odd (see appendices A and B) or using $\{N, N+2, N+3, N+4, N+6\}$ with $2 \nmid N$ and $3 \nmid N$. Therefore, we want to create algorithms to generate n prp numbers, where $n \geqslant 6$.

Adding more numbers

Performing the above steps up to $N + 102$, we have the Table of Necessary and Sufficient Conditions for Relative Prime (see appendix C) and the Table of Case Rejected (see appendix D).

Observation

We found in the Table of Case Rejected (see appendix D) that $r \neq p - 1$. Therefore,

$$\begin{aligned} & N \mod p = p - 1 \text{ for } p \in \mathbb{P} \cap [2, 71] \\ \Rightarrow\ & \text{the set } \{N, N + 2, \ldots, N + 102\} \text{ are prp.} \end{aligned}$$

($\mathbb{P}$ denotes the set of prime numbers.)

Let $N = M - 1$, we have

$$p \mid M \Leftrightarrow (M - 1) \mod p = p - 1 \Leftrightarrow N \mod p = p - 1$$

and $\{N, N + 2, N + 3, N + 4, \ldots, N + 102\} = \{M - 1, M + 1, M + 2, M + 3, \ldots, M + 101\}$.

Therefore,

$$\begin{aligned} & p \mid M \text{ for } p \in \mathbb{P} \cap [2, 71] \\ \Rightarrow\ & \text{the set } \{M - 1, M + 1, M + 2, M + 3, \ldots, M + 101\} \text{ are prp.} \end{aligned}$$

We observe that the set $\{M - 1, M + 1, M + 2, M + 3, \ldots, M + 101\}$ has the form of $\{M \pm 1\} \cup \{M + p_i\}$.

The Prime Factor Function

We define that $\mathrm{pf}(x) =$ the set of prime factors of x.

Example: $\mathrm{pf}(1) = \varnothing$, $\mathrm{pf}(6) = \{2, 3\}$, $\mathrm{pf}(64) = \{2\}$, $\mathrm{pf}(168) = \{2, 3, 7\}$.

An important lemma: a, b are relatively prime $\Leftrightarrow \mathrm{pf}(a) \cap \mathrm{pf}(b) = \varnothing$ (see appendix E)

Three methods

We guess the form of $\{M \pm 1\} \cup \{M + p_i\}$ can be a set of prp numbers, but we think that it is too complicated to find a proof at the very beginning. So, we try some easier methods before it. The methods we try are as follow:

1. $\{M + p_i\}$ for $i = 1, 2, \ldots, n$
2. $\{M\} \cup \{M + p_i\}$ for $i = 1, 2, \ldots, n-1$
3. $\{M \pm 1\} \cup \{M + p_i\}$ for $i = 1, 2, \ldots, n-2$

1. The method of $\{M + pi\}$

Let $p_i =$ some odd primes, for $i = 1, 2, \ldots, n$, such that $p_1 < p_2 < \ldots < p_n$.

We proposed that

$$\begin{aligned} & p \mid M \text{ for all } p \in \mathbb{P} \cap \left[2, \frac{p_n - p_1}{2}\right] \\ \Rightarrow\ & \{M + p_i\} \text{ is a set of } n \text{ prp numbers for } i = 1, 2, \ldots, n. \end{aligned}$$

Prove that $M + p_i$ and $M + p_j$ are relatively prime for $i < j$.

Proof.

$$\begin{aligned} & (M, M + p_i) = (M, p_i) = 1 \text{ or } p_i \\ \Rightarrow\ & \mathrm{pf}(M) \cap \mathrm{pf}(M + p_i) = \varnothing \text{ or } \{p_i\} \end{aligned} \tag{3}$$

Since

$$\begin{aligned} \mathrm{pf}(p_j - p_i) &= \{2\} \cup \mathrm{pf}\left(\frac{p_j - p_i}{2}\right) \\ &\subset \mathbb{P} \cap \left[2, \frac{p_j - p_i}{2}\right] \\ &\subset \mathbb{P} \cap \left[2, \frac{p_n - p_1}{2}\right] \\ &\subset \mathrm{pf}(M), \end{aligned}$$

we have

$$\mathrm{pf}(p_j - p_i) \subset \mathrm{pf}(M). \tag{4}$$

Since

$$\begin{aligned} (p_i, p_j) = 1 &\Rightarrow (p_i, p_j - p_i) = 1 \\ &\Rightarrow \mathrm{pf}(p_i) \cap \mathrm{pf}(p_j - p_i) = \varnothing \\ &\Rightarrow \{p_i\} \cap \mathrm{pf}(p_j - p_i) = \varnothing, \end{aligned}$$

we have

$$\mathrm{pf}(p_j - p_i) = \varnothing. \tag{5}$$

By (3), (4) and (5), with reference to Figure 3,

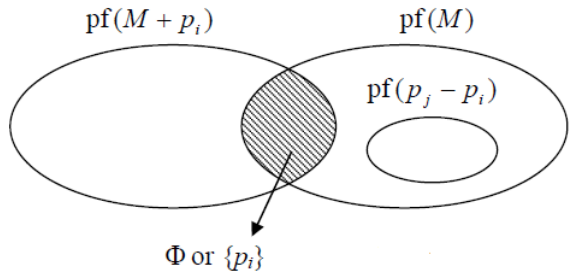


FIGURE 3

we have

$$\begin{aligned} & \operatorname{pf}(M+p_i) \cap \operatorname{pf}(p_j - p_i) = \varnothing \\ \Rightarrow\ & (M+p_i, p_j - p_i) = 1 \\ \Rightarrow\ & (M+p_i, M+p_i+p_j-p_i) = 1 \\ \Rightarrow\ & (M+p_i, M+p_j) = 1 \\ \Rightarrow\ & M+p_i \text{ and } M+p_j \text{ are relatively prime.} \end{aligned}$$

Therefore, we proved that

$$\begin{aligned} & p \mid M \text{ for all } p \in \mathbb{P} \cap \left[2, \frac{p_n - p_1}{2}\right] \\ \Rightarrow\ & \{M+p_i\} \text{ is a set of } n \text{ prp numbers for } i = 1, 2, \ldots, n. \end{aligned}$$ □

2. The method of $\{M\} \cup \{M + p_i\}$

Let p_i = some odd primes, for $i = 1, 2, \ldots, n-1$, such that $p_1 < p_2 < \ldots < p_{n-1}$.

We proposed that

$$\begin{aligned} & p \mid M \text{ for all } p \in \mathbb{P} \cap \left[2, \frac{p_{n-1} - p_1}{2}\right] \text{ and } p_i \nmid M \text{ for } i = 1, 2, \ldots, n-1 \\ \Rightarrow\ & \{M\} \cup \{M+p_i\} \text{ is a set of } n \text{ prp numbers for } i = 1, 2, \ldots, n-1. \end{aligned}$$

Proof. M and $M + p_i$ are relatively prime since $(M, M + p_i) = (M, p_i) = 1$. (Since $p_i \nmid M$.) $M + p_i$ and $M + p_j$ are relatively prime for $i < j$. It is proved in the method of $\{M + p_i\}$.

Therefore, we proved that

$$p \mid M \text{ for all } p \in \mathbb{P} \cap \left[2, \frac{p_{n-1} - p_1}{2}\right] \text{ and } p_i \nmid M \text{ for } i = 1, 2, \ldots, n-1$$
$$\Rightarrow \{M\} \cup \{M + p_i\} \text{ is a set of } n \text{ prp numbers for } i = 1, 2, \ldots, n-1.$$

□

We notice that $p_1 > \frac{p_{n-1} - p_1}{2}$, otherwise $p_1 \in \mathbb{P} \cap \left[2, \frac{p_{n-1} - p_1}{2}\right] \Rightarrow p_1 \mid M$ which contradicts with $p_1 \nmid M$. Equivalently, we have $p_{n-1} < 3p_1$ and $\frac{p_{n-1} - p_1}{2} < \frac{3p_1 - p_1}{2} = p_1$.

Therefore, we have

$$p \mid M \text{ for all } p \in \mathbb{P} \cap [2, p_1) \text{ and } p \nmid M \text{ for all } p \in \mathbb{P} \cap [p_1, 3p_1)$$
$$\Rightarrow \{M\} \cup \{M + p_i\} \text{ is a set of } n \text{ prp numbers for } i = 1, 2, \ldots, n-1.$$

Some examples:

M	$M + p_i$
$2k$	$2k+3$, $2k+5$
$6k$	$6k+5$, $6k+7$, $6k+13$
$30k$	$30k+7$, $30k+11$, $30k+13$, $30k+17$, $30k+19$

where $p \nmid k$ for all $p \in \mathbb{P} \cap [p_1, 3p_1)$

We find that the difference between M and $M + p_1$ becomes bigger when we need more prp numbers.

3. The method of $\{M \pm 1\} \cup \{M + p_i\}$

Let p_i = the $(i+1)$-th prime, for $i = 1, 2, \ldots, n-2$, that is $p_1 = 3$, $p_2 = 5$, $p_3 = 7$, $p_4 = 11$, …, etc.

We proposed that

$$p \mid M \text{ for all } p \in \mathbb{P} \cap \left[2, \frac{p_{n-2} + 1}{2}\right]$$
$$\Rightarrow \{M \pm 1\} \cup \{M + p_i\} \text{ is a set of } n \text{ prp numbers for } i = 1, 2, \ldots, n-2.$$

Proof. Prove that $M-1$ and $M+1$ are relatively prime.

$$\begin{aligned} & 2 \mid M \\ \Rightarrow\ & M-1 \text{ and } M+1 \text{ are consecutive odds.} \\ \Rightarrow\ & M-1 \text{ and } M+1 \text{ are relatively prime (see appendix B).} \end{aligned}$$

Prove that $M \pm 1$ and $M + p_i$ are relatively prime.

$$\begin{aligned} & M \pm 1 \text{ and } M \text{ are consecutive integers} \\ \Rightarrow\ & M \pm 1 \text{ and } M \text{ are relatively prime (see appendix A)} \\ \Rightarrow\ & \mathrm{pf}(M \pm 1) \cap \mathrm{pf}(M) = \varnothing \end{aligned} \tag{6}$$

Since

$$\begin{aligned} \mathrm{pf}(p_i \mp 1) =& \{2\} \cup \mathrm{pf}\left(\frac{p_i \mp 1}{2}\right) \\ \subset& \mathbb{P} \cap \left[2, \frac{p_i \mp 1}{2}\right] \\ \subset& \mathbb{P} \cap \left[2, \frac{p_{n-2}+1}{2}\right] \\ \subset& \mathrm{pf}(M), \end{aligned}$$

we have

$$\mathrm{pf}(p_i \mp 1) \subset \mathrm{pf}(M) \tag{7}$$

By (6) and (7), with reference to Figure 4,

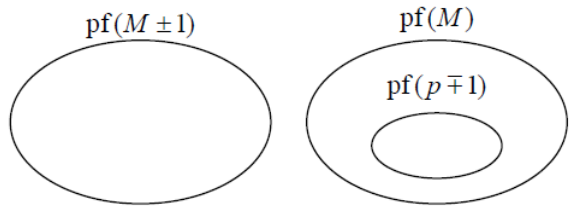


FIGURE 4

we have

$$\begin{aligned} & \mathrm{pf}(M \pm 1) \cap \mathrm{pf}(p_i \mp 1) = \varnothing \\ \Rightarrow\ & (M \pm 1, p_i \mp 1) = 1 \\ \Rightarrow\ & (M \pm 1, (M \pm 1) + (p_i \mp 1)) = 1 \\ \Rightarrow\ & (M \pm 1, M + p_i) = 1 \\ \Rightarrow\ & M \pm 1 \text{ and } M + p_i \text{ are relatively prime.} \end{aligned}$$

$M+p_i$ and $M+p_j$ are relatively prime for $i<j$. Since $\mathbb{P}\cap\left[2,\frac{p_{n-2}-p_1}{2}\right]\subset \mathbb{P}\cap\left[2,\frac{p_{n-2}+1}{2}\right]$, it is proved in the method of $\{M+p_i\}$.

Therefore, we proved that

$$p \mid M \text{ for all } p\in\mathbb{P}\cap\left[2,\frac{p_{n-2}+1}{2}\right]$$
$$\Rightarrow \{M\pm 1\}\cup\{M+p_i\} \text{ is a set of } n \text{ prp numbers for } i=1,2,\ldots,n-2.$$

□

Comparing the methods

$\{M\pm 1\}\cup\{M+p_i\}$ is the best. It needs only $(n-2)$ primes. The difference between the largest and smallest prp numbers is minimum. The condition for M is not as complicated as $\{M\}\cup\{M+p_i\}$.

Alternative expression
We define that $x\# = \prod(\mathbb{P}\cap[1,x])$.

Example: $2\# = 2$, $3\# = 2\times 3$, $4\# = 2\times 3$, $5\# = 2\times 3\times 5$, $16\# = 2\times 3\times 5\times 7\times 11\times 13$.

Therefore, $\{M\pm 1\}\cup\{M+p_i\}_{i=1,2,\ldots,n-2}$ is a set of n prp numbers where $M=k\left[\left(\frac{p_{n-2}+1}{2}\right)\#\right]$, $k\in\mathbb{Z}^+$.

8. The Sieve of PRP Numbers

An observation

When filling up the Table of Necessary and Sufficient Conditions for Relatively Prime (see appendix C), we found that the requirement of two numbers to be relatively prime is directly related to the prime factor of their difference.

The theorem involved

Given: a and b are two distinct integers with $b>a$. Let $b-a=d\leqslant k$.

Define: $\Omega(x,k) = \mathrm{pf}(x) \cap [1,k]$.

To prove: a and b are relatively prime $\Leftrightarrow \Omega(a,k) \cap \Omega(b,k) = \varnothing$.

Proof.

$$
\begin{aligned}
& a \text{ and } b \text{ are relatively prime} \\
\Leftrightarrow\ & (a,d) = (a,a+d) = (a,b) = 1 \\
\Leftrightarrow\ & a \text{ and } b \text{ are relatively prime} \\
\Leftrightarrow\ & \mathrm{pf}(a) \cap \mathrm{pf}(d) = \varnothing \quad \text{(see appendix E)} \\
\Leftrightarrow\ & \mathrm{pf}(a) \cap \mathrm{pf}(d) \cap [1,k] = \varnothing \quad (\mathrm{pf}(d) = \mathrm{pf}(d) \cap [1,k]) \\
\Leftrightarrow\ & \mathrm{pf}(a) \cap \mathrm{pf}(a+d) \cap [1,k] = \varnothing \\
& (\mathrm{pf}(a) \cap \mathrm{pf}(d) = \mathrm{pf}(a) \cap \mathrm{pf}(a+d) \text{ (see appendix F))} \\
\Leftrightarrow\ & \mathrm{pf}(a) \cap [1,k] \cap \mathrm{pf}(b) \cap [1,k] = \varnothing \\
\Leftrightarrow\ & \Omega(a,k) \cap \Omega(b,k) = \varnothing
\end{aligned}
$$

□

An example of the Sieve of PRP Numbers

We are going to pick up prp numbers within the range of $[51079, 51100]$.

The following table show the value of $m \mod p$ where $m \in [51079, 51100]$ and $p \in \mathbb{P} \cap [1, 51100 - 51079]$.

m \ p	2	3	5	7	11	13	17	19
51079	1	1	4	0	4	6	2	11
51080	0	2	0	1	5	7	3	12
51081	1	0	1	2	6	8	4	13
51082	0	1	2	3	7	9	5	14
51083	1	2	3	4	8	10	6	15
51084	0	0	4	5	9	11	7	16
51085	1	1	0	6	10	12	8	17
51086	0	2	1	0	0	0	9	18
51087	1	0	2	1	1	1	10	0
51088	0	1	3	2	2	2	11	1
51089	1	2	4	3	3	3	12	2
51090	0	0	0	4	4	4	13	3
51091	1	1	1	5	5	5	14	4
51092	0	2	2	6	6	6	15	5
51093	1	0	3	0	7	7	16	6
51094	0	1	4	1	8	8	0	7
51095	1	2	0	2	9	9	1	8
51096	0	0	1	3	10	10	2	9
51097	1	1	2	4	0	11	3	10
51098	0	2	3	5	1	12	4	11
51099	1	0	4	6	2	0	5	12
51100	0	1	0	0	3	1	6	13

Then we choose some numbers m to form the following table:

m	51079	51081	50182	51083	51085	51089	51091	51097
$\Omega(m, 21)$	$\{7\}$	$\{3\}$	$\{2\}$	$\varnothing$	$\{5\}$	$\varnothing$	$\varnothing$	$\{11\}$

Therefore, $\{51079, 51081, 50182, 51083, 51085, 51089, 51091, 51097\}$ is set of 8 prp numbers.

The Sieve of PRP Numbers

We are going to pick up prp numbers within the range of $[s, s+k]$.

1. Tabulate the value of $m \mod p$ where $m \in [s, s+k]$ and $p \in \mathbb{P} \cap [1, k]$
2. Pick up the value of m_i such that $\Omega(m_i, k)$ are disjoint sets.

9. An Interesting Conjecture

We were afraid that it is not possible to pick up enough number of prp numbers within the range of $[s, s+k]$ by the Sieve of PRP Numbers. Therefore, we tested the Sieve of PRP Numbers with different sets of $(k+1)$ consecutive integers and saw what would happen. The Excel files are attached with this report.

k	no. of prp	$\pi(k)$
20	7	8
	9	
	9	
	9	
	8	
	9	
	9	
	10	
	8	
	9	
50	16	15
	14	
	15	
	15	
	14	
	15	
	18	
	15	
	16	
	17	

k	no. of prp	$\pi(k)$
100	22	25
	23	
	24	
	24	
	26	
	24	
	23	
	23	
	26	
	23	
200	42	46
	41	
	38	
	43	
	37	
	43	
	41	
	38	
	45	
	40	

We found an interesting result that the maximum number of prp numbers within the range $[s, s+k]$ is approximately equal to $\pi(k)$. We made a conjecture that the maximum number of prp numbers within the range $[s, s+k]$ is approximately equal to $\pi(k)$. We guessed the Sieve of Eratosthenes and

the Inclusion-Exclusion Principle would help in proving this conjecture but could not prove it or disprove it before the deadline of this report.

10. Summary and Conclusions

Key Distribution Scheme

$\mathrm{KD}(t, n)$ has solutions and it is useful for hardware configuration. But if we use it to distribute bits to implement $\mathrm{TS}(t, n)$, it is much apart from the ideal case.

Chinese Remainder Theorem Scheme

If we use $\mathrm{CRT}(t, n)$ to implement $\mathrm{TS}(t, n)$, $\mathrm{CRT}(t, n)$ is nearly ideal provided that we can find n prp numbers such that the prp numbers are

1. as large as required, and
2. as close to one another as possible.

Finding Pairwise Relatively Prime (PRP) Numbers

We have two ways to generate prp numbers. They are as follows:

- If we need only 3 prp numbers, take 3 consecutive integers starting from an odd.
- If we need only 5 prp numbers, use $\{N, N+2, N+3, N+4, N+6\}$ with $2 \nmid N$ and $3 \nmid N$.
- The method of $\{M \pm 1\} \cup \{M + p_i\}$: it is useful to find very close prp numbers.
- Sieve of PRP Numbers: it is useful to find prp numbers within a specific range.
  We made a conjecture that the maximum number of prp numbers within the range $[s, s+k]$ is approximately equal to $\pi(k)$.

Appendix A. Two consecutive integers are relatively prime

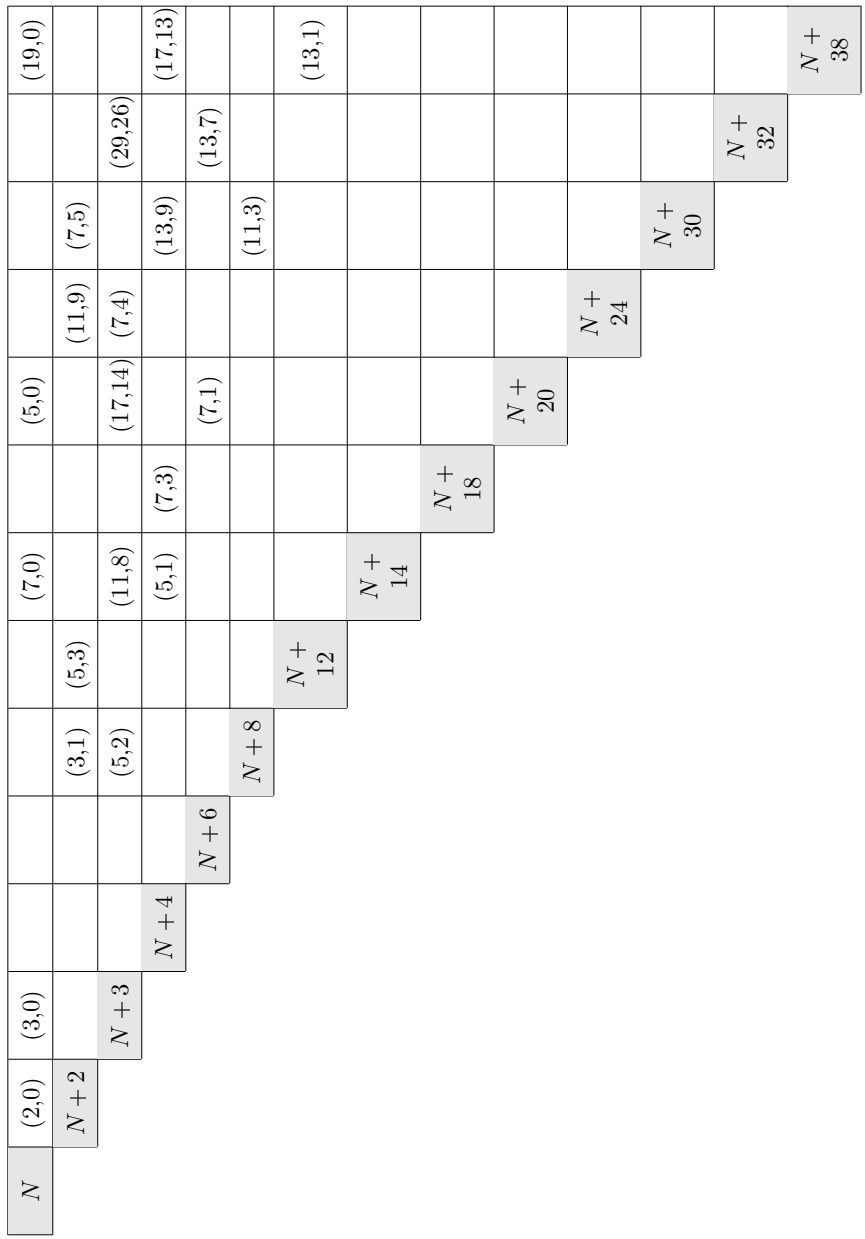
Proof. By using $(a, b) = (a, b-a)$, we have $(n, n+1) = (n, 1) = 1$. Therefore n and $n+1$ are relatively prime. □

Appendix B. Two consecutive odds are relatively prime

Proof. By using $(a, b) = (a, b - a)$, we have $(n, n + 2) = (n, 2)$. As n is odd, $(n, 2) = 1$. Therefore n and $n + 2$ are relatively prime. □

Appendix C. The table of Necessary and Sufficient Conditions for Relatively Prime up to N+102

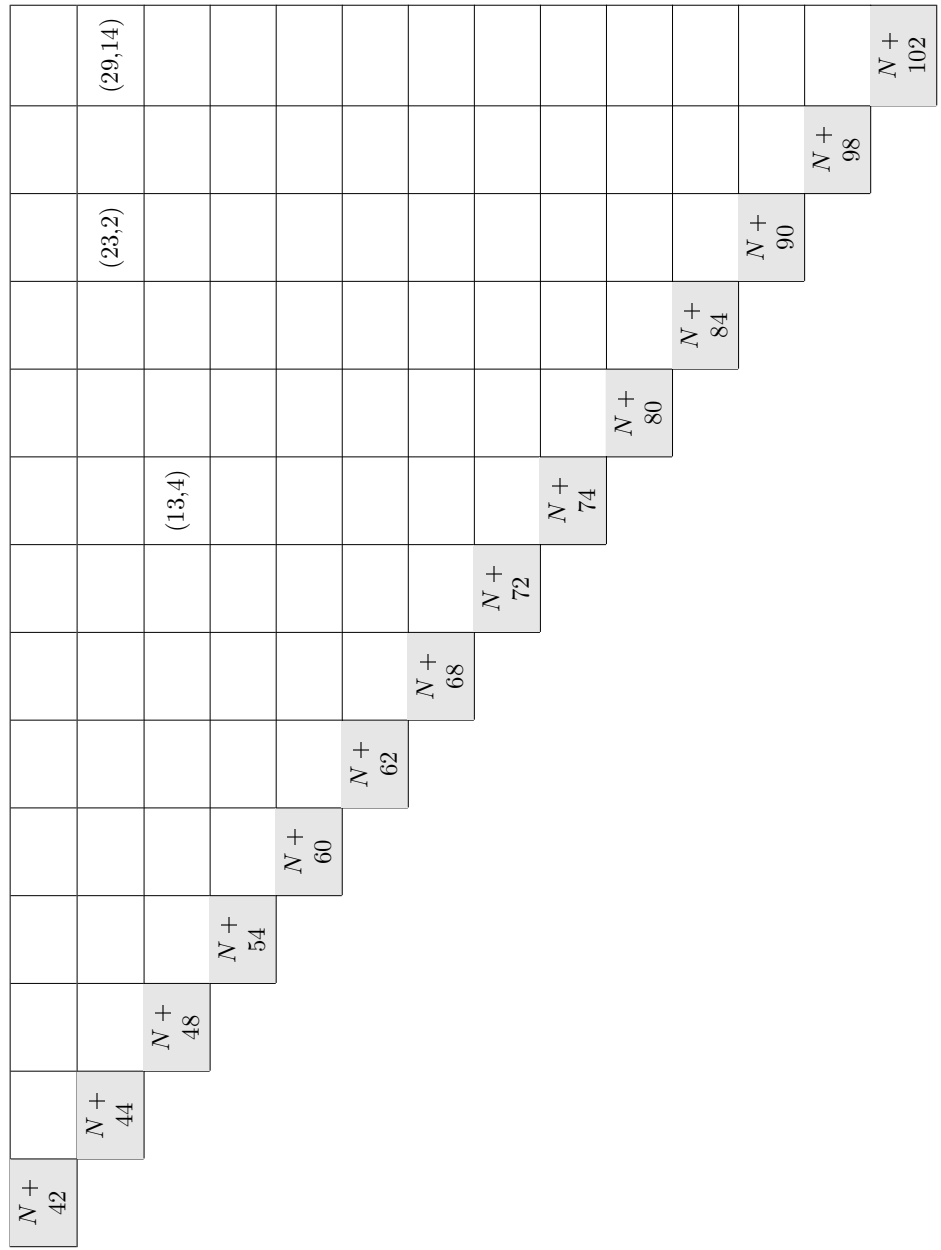
Part 1/3



Part 2/3

N	$N+42$	$N+44$	$N+48$	$N+54$	$N+60$	$N+62$	$N+68$	$N+72$	$N+74$	$N+80$	$N+84$	$N+90$	$N+98$	$N+102$
$N+2$		(11,0)				(31,0)	(17,0)		(37,0)					
$N+3$			(23,21)	(13,11)	(29,27)						(41,39)			
$N+4$	(13,10)	(41,38)			(19,16)	(59,56)		(23,20)	(71,68)					
$N+6$	(19,15)		(11,7)			(29,25)						(43,39)	(47,43)	
$N+8$		(19,13)					(31,25)	(11,5)	(17,11)	(37,31)			(23,17)	
$N+12$	(17,9)			(23,15)	(13,5)						(19,11)	(41,33)		(47,39)
$N+14$				(7,2)					(31,19)	(17,5)			(43,31)	
$N+18$			(17,3)		(23,9)			(29,15)				(19,5)		
$N+20$		(13,8)				(11,4)				(31,13)				
$N+24$	(11,2)							(13,6)						(41,21)
$N+30$						(19,14)							(37,13)	(13,2)
$N+32$							(19,8)						(17,4)	
$N+38$				(11,1)										
					(11,6)						(23,8)			

Part 3/3


N + 42
N + 44
N + 48
N + 54
N + 60
N + 62
N + 68
N + 72
N + 74
N + 80
N + 84
N + 90
N + 98
N + 102
(29,14)
(23,2)
(13,4)

Appendix D. Table of Case Rejected up to $N+102$

p	r
2	0
3	0, 1
5	0, 1, 2, 3
7	0, 1, 2, 3, 4, 5
11	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
13	1, 2, 4, 5, 6, 7, 8, 9, 10, 11
17	0, 3, 4, 5, 9, 11, 13, 14
19	0, 5, 8, 11, 13, 14, 15, 16
23	2, 8, 9, 15, 17, 20, 21
29	14, 15, 25, 26, 27
31	0, 13, 19, 25
37	0, 13, 31
41	21, 33, 38, 39
43	31, 39
47	39, 43
59	56
71	68

Appendix E. a, b are relatively prime $\Leftrightarrow$ $\mathbf{pf}(a)\cap\mathbf{pf}(b) = \varnothing$

Proof.

$$
\begin{aligned}
& a, b, \text{ are not relatively prime} \\
\Leftrightarrow\ & \text{there exists } p \text{ such that } p \mid a \text{ and } p \mid b \\
\Leftrightarrow\ & p \in \mathrm{pf}(a) \text{ and } p \in \mathrm{pf}(b) \\
\Leftrightarrow\ & \mathrm{pf}(a) \cap \mathrm{pf}(b) \neq \varnothing
\end{aligned}
$$

Therefore,

$$a, b, \text{ are relatively prime} \Leftrightarrow \mathrm{pf}(a) \cap \mathrm{pf}(b) = \varnothing. \qquad \square$$

Appendix F. $\mathbf{pf(a)\cap pf(d)=pf(a)\cap pf(a+d)}$

Proof.

$$\begin{aligned}
& p \in \mathrm{pf}(a) \cap \mathrm{pf}(d) \\
\Leftrightarrow\ & p \in \mathrm{pf}(a) \text{ and } p \in \mathrm{pf}(d) \\
\Leftrightarrow\ & p \in \mathbb{P} \text{ and } p \mid a \text{ and } p \mid d \\
\Leftrightarrow\ & p \in \mathbb{P} \text{ and } p \mid a \text{ and } p \mid a+d \\
\Leftrightarrow\ & p \in \mathrm{pf}(a) \text{ and } p \in \mathrm{pf}(a+d) \\
\Leftrightarrow\ & p \in \mathrm{pf}(a) \cap \mathrm{pf}(a+d)
\end{aligned}$$

Therefore,

$$\mathrm{pf}(a) \cap \mathrm{pf}(d) = \mathrm{pf}(a) \cap \mathrm{pf}(a+d). \qquad \square$$

Appendix G. $\boldsymbol{\alpha = \dfrac{n-t+1}{n} = \dfrac{1}{t} + (t-1)\left(\dfrac{1}{t} - \dfrac{1}{n}\right)}$

Proof.

$$\begin{aligned}
\alpha &= \frac{n-t+1}{n} \\
&\quad \text{(this expression is useful in calculating } \alpha\text{)} \\
&= \frac{1}{t} + \frac{nt - t^2 + t - n}{nt} \\
&= \frac{1}{t} + \frac{(t-1)(n-t)}{nt} \\
&= \frac{1}{t} + (t-1)\left(\frac{1}{t} - \frac{1}{n}\right) \\
&\quad \text{(this expression is useful in finding how much } \alpha \text{ is greater than } \frac{1}{t}\text{)} \square
\end{aligned}$$

Appendix H. $\boldsymbol{{}_nC_{t-1} = t + \sum_{i=1}^{n-1} {}_iC_{t-2}}$ is true for $\boldsymbol{n \geqslant t}$.

Proof. When $n = t$, the statement is true.

Assume that ${}_kC_{t-1} = t + \sum_{i=t}^{k-1} {}_iC_{t-2}$.

$$\begin{aligned} {}_{k+1}C_{t-1} &= {}_kC_{t-1} + {}_kC_{t-2} \\ &= t + \sum_{i=t}^{k-1} {}_iC_{t-2} + {}_kC_{t-2} \\ &= t + \sum_{i=t}^{k} {}_iC_{t-2} \end{aligned}$$

Therefore,

$${}_nC_{t-1} = t + \sum_{i=t}^{n-1} {}_iC_{t-2} \text{ is true for } n \geqslant t. \qquad \square$$

REFERENCES

[1] Flannery, S., *In Code : A Mathematical Journey*, New York : Workman Pub, 2001.
[2] *Chinese Remainder Theorem*, Wolfram Research, Inc., http://mathworld.wolfram.com/ChineseRemainderTheorem.html.
[3] *Chinese Remainder Theorem*, Wikipedia, http://en.wikipedia.org/wiki/Chinese_remainder_theorem.
[4] *Prime Number Theorem*, Wolfram Research, Inc., http://mathworld.wolfram.com/PrimeNumberTheorem.html.
[5] *Prime Number Theorem*, Wikipedia, http://en.wikipedia.org/wiki/Prime_number_theorem.

Reviewer's Comments

The reviewer has only comments on the wordings, which have been amended in this paper.