Multiplicative (Non-Zero) Homomorphic CRT Secret Sharing

Shlomi Dolev and Yaniv Kleinman

July 10, 2022

Multiplicative (non-zero) Homomorphic CRT Secret Sharing
(Preliminary Version)

Shlomi Dolev, Yaniv Kleinman[*]

Ben-Gurion University of the Negev, Be'er Sheva, Israel
{dolev@cs, yanivkl@post}.bgu.ac.il

June 28, 2022

Abstract

This work suggests a new CRT-based secret sharing scheme with perfect information-theoretic security and multiplicative homomorphism. The scheme is designed to support non-zero secrets of multiplicative groups.

We will review some related works in the CRT-based secret sharing schemes and see why our scheme is innovative. Our scheme will be detailed and analyzed in this work in order to set solid foundations for future work expanding this scheme.

1 Introduction

There is a rising need for clouding storage and clouding computing. Users of the cloud services want to be sure that the providers of the service are not exposed to the data, which could be sensitive. The ongoing use of cloud computing can let companies focus on their primary goal leaving cloud providers to deal with all the storage and computing infrastructures.

Users of cloud providers need to hide sensitive data. In order to hide the data, the data can be encrypted, but there are some flaws in this scenario. First, encryption is done using a key that needs to be stored. Second, encryptions are mainly based on the hardness of computing problems, meaning brute force on keys can always solve it, rather than the ultimate perfect information security. This fact is becoming terrifying when considering the emergence of quantum computing. Third, encryption can be very time-consuming, for example, calculating powers on numbers done in RSA.

[*] Corresponding author

Besides encryption, other methods like Secret Sharing (SS) and Secure Multiparty Computations (SMC or SMPC) exist. Those methods are based on mathematical proofs that ensure the secret data is being secured as long the adversary does not have the sufficient number of shares defined by a threshold to recover the secret.

The most known secret sharing schemes are Shamir's secret sharing scheme [1], and the schemes based on the Chinese Remainder Theorem (CRT) like Asmuth-Bloom's scheme [2]. Both schemes are designed to require a threshold of t out of n shares to reconstruct the secret, where $t \leq n$ shares are enough to reconstruct the secret fully. The terminology for using such reconstruction threshold is called a *threshold scheme*.

To perform the calculation on encrypted or shared data on the cloud company's servers, we need the scheme to support mathematical operations. Such support is mainly achieved using homomorphic operations. Homomorphism is a map between two algebraic structures of the same type that preserves the operation of the structures [6]. Homomorphic operation mainly addressed by the equation: $f(x \oplus y) = f(x) \oplus f(y)$ where $'\oplus'$ is a binary mathematical operation in this case. Homomorphism is a property of the function f. Homomorphism can be limited to several operations; in this case, the scheme is only partly homomorphic.

2 Definitions

- n - The number of participants.
- t - The reconstruction threshold. State the minimum number of participants needed to reconstruct the secret.
- s - The secrecy bound. State the maximum number of participants that cannot learn any information about the secret.
- S - The secret data.
- S_i - The secret share of participant i.
- $[\cdot]_p$ - The arithmetic inside is performed in $\mathbb{Z}_p$
- U_M - The multiplicative group of integers modulo M.
- m_i - The i'th number to perform the modulus calculations with.
- m_{i+j} - The $(i+j) \pmod{n}$ number to perform the modulus calculations with.
- $\mathcal{D}$ - The secret's distribution.
- $\mathcal{S}$ - The secret domain.
- $\mathcal{S}_i$ - The participant ith shared part's domain.
- $\mathcal{A}$ - The access structure. All the qualified groups of participants that can reconstruct the secret.

The relations between the scheme factors are:

1. $1 \leq s < t \leq n$
2. The gap from s to t does not have to be one.
3. It is possible that a group of participants smaller than t could reconstruct the data.
4. It is possible that a group of participants larger than s would not learn anything about the data.

Definition 1. *Perfect Secret Sharing Scheme* should satisfy the following two conditions:

1. *Correctness*: Any qualified group of participants in $\mathcal{A}$ can reconstruct the secret.
2. *Perfect Privacy*: No unqualified group of participants in $\bar{\mathcal{A}}$ can get any information about the secret.

Definition 2. *Perfect ramp secret sharing scheme* should satisfy the following two conditions:

1. *Correctness*: Any qualified group of participants in $\mathcal{A}$ can reconstruct the secret.
2. *Perfect Ramp Privacy*: For every group of participants $G, |G| \leq s$, given a secret S with distribution $\mathcal{D}$. The distribution of the secret stays the same, meaning, the probability of the secret to be equal a specific element $S' \in \mathcal{S}$ stays the same even when knowing the data of the shared secret held by the participants of G. More formally: Given any $S' \in \mathcal{S}$:

   - $Pr[S = S'] = p$.
   - For every $S' \in \mathcal{S}$ and $S'_{i_j} \in \mathcal{S}_{i_j}, 1 \leq j \leq s$, with $1 \leq i_1 < i_2 < \cdots < i_s \leq n$, we have:

$$Pr[S = S' | S_{i_1} = S'_{i_1}, \ldots, S_{i_s} = S'_{i_s}] = p$$

3 Related Work

Some of the known SMPC homomorphic methods relevant to this research are:

Simple additive SSS – In this scheme, the sum of shared values reconstructs the secret. One such scheme has a threshold of $t = n - 1$, meaning it is an n out of n scheme. Let S be the secret, n the number of participants, and $\mathbb{Z}_p$ the field on which the calculations are being made [3].

- Distribution phase:
  The dealer choose at random the numbers $S_1, S_2, ..., S_{n-1} \in \mathbb{Z}_p$. The dealer then computes $S_n = S - \sum_{1 \leq i < n} S_i$. Finally, the dealer sends S_i to participant i for $1 \leq i \leq n$.

- Reconstruction phase:
  Let G be a group of participants gathered to reconstruct the secret. The participants compute the secret S by summing all their secret's shares.
  $RF(\bigcup_{p_i \in G} S_i) : \begin{cases} if\ |G| = n \Rightarrow S = \sum_{1 \leq i \leq n} S_i (\text{mod } p) \\ if\ |G| < n \Rightarrow \perp \end{cases}$

- Additive homomorphism:
  Let S_1 and S_2 be secrets and S_{1_i} and S_{2_i} the secrets' shares of the i'th participant. $S_1 + S_2 = \sum_{1 \leq i \leq n} S_{1_i} + \sum_{1 \leq i \leq n} S_{2_i} = \sum_{1 \leq i \leq n} S_{1_i} + S_{2_i}$. Each participant can perform $S_{1_i} + S_{2_i}$ and send the sum for the reconstruction phase. Therefore, the scheme is an additive homomorphic scheme.

Simple multiplicative homomorphic SSS – This scheme is very similar to the additive one, but in this case, the product of shared values gives the secret. Moreover, there are some restrictions; Zero or numbers that are not co-prime to p are not allowed to be used. One such scheme has a threshold of $t = n - 1$, meaning it is an n out of n scheme. Les S be the secret, n the number of participants, and U_p the group on which the calculations are being made. [5]:

- Distribution phase:
  The dealer picks $n-1$ uniformly random nonzero elements $S_i, 1 \leq i < n$, from U_p. The dealer then calculates $S_n = S \cdot (\prod_{1 \leq i < n} S_i)^{-1}$. Finally, the dealer sends S_i to participant i for $1 \leq i \leq n$.

- Reconstruction phase:
  Let G be a group of participants gathered to reconstruct the secret. The participants compute the secret S by multiplying all their secret's shares.
  $RF(\bigcup_{p_i \in G} S_i) : \begin{cases} if\ |G| = n \Rightarrow S = \prod_{1 \leq i \leq n} S_i (\text{mod } p) \\ if\ |G| < n \Rightarrow \perp \end{cases}$

- Multiplicative homomorphism:
  Let S_1 and S_2 be secrets and S_{1_i} and S_{2_i} the secrets' shares of the i'th participant. $S_1 \cdot S_2 = \prod_{1 \leq i \leq n} S_{1_i} \cdot \prod_{1 \leq i \leq n} S_{2_i} = \prod_{1 \leq i \leq n} S_{1_i} \cdot S_{2_i}$. Each participant can perform $S_{1_i} \cdot S_{2_i}$ and send the product on the reconstruction phase. Therefore, the scheme is a multiplicative homomorphic scheme. All the multiplications are correct and do not form a zero or a number with a common divider with p because U_p is a multiplicative group.

Ramp additive homomorphic SSS – [4]. This scheme is based on the ideas of Asmuth-Bloom SSS [2] as mentioned earlier in the background. The scheme is an n out of n scheme with a security factor of s, meaning that without having at least $s+1$ secret sharing parts, there is no information leak. Using such a security factor s is called a *ramp scheme.* Let S be the secret, n the number of participants, and $\mathbb{Z}_{\text{prod}}$ the group on which the calculations are being made.

- Distribution phase:
  The dealer chooses a set of integers $(\text{prod}, m_1, m_2, ..., m_n)$ such that:

  1. $m_1 < m_2 < ... < m_n$ and $S < \text{prod} = M_n = \prod_{i=1}^{n} m_i$
  2. $gcd(m_i, m_j) = 1 (\forall i \neq j)$

  The dealer randomly chooses s integers $(r_1, ..., r_s)$ in $\mathbb{Z}_{\text{prod}}$, and computes $S_{\text{mix}} = [S + \sum_{i=1}^{n} r_i]_{\text{prod}}$.
  The dealer computes and distributes share set of each participant i:

  $$S_i = (S_{\text{mix}} (\text{mod } m_i), r_1 (\text{mod } m_{i+1}), \ldots, r_s (\text{mod } m_{i+s}))$$

- Reconstruction phase:
  Let G be a group of participants gathered to reconstruct the secret. The participants compute the secret S by solving the CRT equations.

$$RF\begin{pmatrix} \bigcup\limits_{p_i \in G} S_{i,0} \\ \bigcup\limits_{p_i \in G} S_{i,1} \\ \ldots \\ \bigcup\limits_{p_i \in G} S_{i,s} \end{pmatrix} : \begin{cases} if\ |G| = n : \begin{pmatrix} S_{\text{mix}} = CRT[S_{1,0}, ..., S_{n,0}]_{\text{prod}} \\ \\ r_1 = CRT[S_{1,1}, ..., S_{n,1}]_{\text{prod}} \\ \ldots \\ r_s = CRT[S_{1,s}, ..., S_{n,s}]_{\text{prod}} \\ \end{pmatrix} \\ \qquad \Rightarrow S = [S_{\text{mix}} - \sum_{i=1}^{s} r_i]_{\text{prod}} \\ if\ s+1 \leq |G| < n \Rightarrow partial\ information \\ if\ |G| < s+1 \Rightarrow \perp \end{cases}$$

- Additive homomorphism:
  Let S_1 and S_2 be secrets. $S_{1_{\text{mix}}}, r_{1_1}, ..., r_{1_s}$ are the blinded secret and all the blinding randoms of S_1. $S_{2_{\text{mix}}}, r_{2_1}, ..., r_{2_s}$ are the blinded secret and all the blinding randoms of S_2. Each participant i has the secret shares of each blinded secret and blinding randoms:
  $S_{1_{mix_i}}, r_{1_{1_i}}, ..., r_{1_{s_i}}, S_{2_{mix_i}}, r_{2_{1_i}}, ..., r_{2_{s_i}}$.
  Now we will show that this scheme is additive homomorphic:
  $S_1 + S_2 = S_{1_{\text{mix}}} - \sum_{1 \leq j \leq s} r_{1_j} + S_{2_{\text{mix}}} - \sum_{1 \leq j \leq s} r_{2_j} = S_{1_{\text{mix}}} + S_{2_{\text{mix}}} - \sum_{1 \leq j \leq s} r_{1_j} + r_{2_j}$. Each participant can perform $S_{1_{mix_i}} + S_{2_{mix_i}}$ and $r_{1_{j_i}} + r_{2_{j_i}}$ for each $1 \leq j \leq s$ and send the sum of all the needed parts to the reconstruction phase, where using a CRT solver algorithm. Therefore, the scheme is an additive homomorphic scheme.

4 Motivation for the new scheme

In this work, we want to introduce a new SSS with the feature of multiplicative homomorphism. There are already schemes that allow homomorphic multiplication, one of them found in the related work Section(3). However our scheme can be extended to support more features, such as threshold reconstruction and additive homomorphism, under some disclaimers.

5 Method explanation

The scheme is an n out of n scheme with a security factor of s, meaning that without having at least $s+1$ secret sharing parts, there is no information leak. Using such a security factor s is called a *ramp scheme*. Let $S \in U_{\text{prod}}$ be the secret, n the number of participants, and U_{prod} the group in which the calculations are being made.

- Distribution phase:
  The dealer chooses a set of pairwise co-primes $m_1, m_2, ..., m_n$ and calculate $\text{prod} = \prod_{1\le i\le n} m_i$ such that:

  1. $m_1 < m_2 < ... < m_n$ and $S < \text{prod} = M_n$
  2. $\gcd(m_i, m_j) = 1, \forall i \neq j$

  The dealer randomly chooses s integers $r_1, ..., r_s$ in U_{prod}, and computes $S_{\text{mix}} = [S \cdot \prod_{1\le i\le s} r_i]_{\text{prod}}$ The dealer computes and distributes share set of each participant $1 \le i \le n$:

$$S_i = (S_{\text{mix}}(\text{mod } m_i), r_1(\text{mod } m_{i+1}), \ldots, r_s(\text{mod } m_{i+s}))$$

- Reconstruction phase:
  Let G be a group of participants gathered to reconstruct the secret. The participants compute the secret S by solving the CRT equations, following the steps of the reconstruction function:

$$RF\begin{pmatrix}\bigcup_{p_i\in G} S_{i,0}\\ \bigcup_{p_i\in G} S_{i,1}\\ ...\\ \bigcup_{p_i\in G} S_{i,s}\end{pmatrix} : \begin{cases} if\ |G| = n : \begin{pmatrix} S_{\text{mix}} = CRT[S_{1,0}, ..., S_{n,0}]_{\text{prod}}\\ r_1 = CRT[S_{1,1}, ..., S_{n,1}]_{\text{prod}}\\ ...\\ r_s = CRT[S_{1,s}, ..., S_{n,s}]_{\text{prod}}\end{pmatrix}\\ \qquad \Rightarrow S = [S_{\text{mix}} \cdot \prod_{i=1}^{s} r_i^{-1}]_{\text{prod}}\\ if\ s+1 \le |G| < n \Rightarrow partial\ information\\ if\ |G| < s+1 \Rightarrow \perp \end{cases}$$

5.1 Auxiliary claims

Corollary 1. *Given the multiplicative group $A = U_{m_1 \cdot m_2 \cdot \dots \cdot m_n} = U_{M_n}$ there is an isomorphism to the direct product of M_n pairwise co-primes dividers, meaning $B = U_{m_1} \times U_{m_2} \times ... \times U_{m_n}$.*

Proof. Let's define $f : A \to B$ in the following way:

$$f(\alpha) = \langle \alpha (\text{mod } m_1), \alpha (\text{mod } m_2), ..., \alpha (\text{mod } m_n) \rangle \tag{1}$$

We need to show that $f(\alpha_1 \cdot \alpha_2) = f(\alpha_1) \cdot f(\alpha_2)$.

$$f(\alpha_1 \cdot \alpha_2) = \langle (\alpha_1 \cdot \alpha_2)(\text{mod } m_1), (\alpha_1 \cdot \alpha_2)(\text{mod } m_2), ..., (\alpha_1 \cdot \alpha_2)(\text{mod } m_n) \rangle \tag{2}$$

$$\begin{aligned} f(\alpha_1) \cdot f(\alpha_2) = \langle \alpha_1 (\text{mod } m_1), \alpha_1 (\text{mod } m_2), ..., \alpha_1 (\text{mod } m_n) \rangle \cdot \\ \langle \alpha_2 (\text{mod } m_1), \alpha_2 (\text{mod } m_2), ..., \alpha_2 (\text{mod } m_n) \rangle = \\ \langle (\alpha_1 \cdot \alpha_2)(\text{mod } m_1), (\alpha_1 \cdot \alpha_2)(\text{mod } m_2), ..., (\alpha_1 \cdot \alpha_2)(\text{mod } m_n) \rangle \end{aligned} \tag{3}$$

The last equality in Equation(3) is achieved by the definition of multiplication in a direct product. □

Corollary 2. *Define $M_n = m_1 \cdot m_2 \cdot \dots \cdot m_n$ where $m_1, m_2, \dots, m_n$ are pairwise co-primes. Given element $\alpha \in A = U_{M_n}$ of a finite group:*
$\forall \gamma \in U_{M_n}, \exists \beta \in U_{m_n}$ s.t. $\alpha \cdot \beta = \gamma$. Meaning that all elements can be the product of α and another element in the group.

Proof. Given $\alpha \in U_{M_n}$, let's assume in contradiction that there is an element $\gamma_1 \in U_{M_n}$ such that: $\alpha \cdot \beta \neq \gamma_1, \forall \beta \in U_{m_n}$. We know that U_{M_n} is a multiplicative group so every multiplication of elements in the group form an element in the group. Since the source and the domain of the multiplication are of the same finite size, there is at least one element $\gamma_2 \in U_{M_n}$ such that:

$$\alpha \cdot \beta_1 = \alpha \cdot \beta_2 = \gamma_2, \beta_1 \neq \beta_2 \tag{4}$$

The element α has an inverse α^{-1} because U_{M_n} is a group. Applying α^{-1} on Equation (4) we get: $\alpha^{-1} \cdot \alpha \cdot \beta_1 = \alpha^{-1} \cdot \alpha \cdot \beta_2 = \alpha^{-1} \cdot \gamma \Rightarrow$
$\beta_1 = \beta_2 = \alpha^{-1} \cdot \gamma$ in contrast to $\beta_1 \neq \beta_2$ which means that our assumption was incorrect: $\nexists \gamma_1 \in U_{M_n}, \forall \beta \in U_{m_n}$ s.t. $\alpha \cdot \beta \neq \gamma_1 \Rightarrow \forall \gamma \in U_{M_n}, \exists \beta \in U_{m_n}$ s.t. $\alpha \cdot \beta = \gamma$. □

Corollary 3. *Let G be a finite group. Given two elements $g_1, g_2 \in G$ chosen randomly, uniformly and independently. The multiplication $g_1 \cdot g_2 = g\prime \in G$ is a randomly, uniformly element of G.*

Proof. We need to show that each $g\prime$ can be chosen with the same probability, which means $\frac{1}{|G|}$.

$$Pr[g_1 \cdot g_2 = g'] = Pr[\bigcup_{g_0 \in G} \{g_1 = g_0, g_2 = g_0^{-1} \cdot g'\}] =^1$$

$$\sum_{g_0 \in G} Pr[g_1 = g_0, g_2 = g_0^{-1} \cdot g'] =^2$$

$$\sum_{g_0 \in G} Pr[g_1 = g_0] Pr[g_2 = g_0^{-1} g\prime] =^3 \sum_{g_0 \in G} \frac{1}{|G|} \cdot \frac{1}{|G|} = |G| \cdot \frac{1}{|G|^2} = \frac{1}{|G|}$$

The 1 equality is achieved by the fact that each event of $g_0 \in G$ are different.
The 2 equality is achieved because of the independence of g_1 and g_2.
The 3 equality is achieved because g_1 and g_2 are chosen randomly uniformly. □

Corollary 4. *Let G be a finite group. Given two elements $g_1, g_2 \in G$ where g_1 is taken from a uniformly distribution and g_2 is from some distribution $\mathcal{D}$. g_1 and g_2 are chosen independently. The multiplication $g_1 \cdot g_2 = g\prime \in G$ is a randomly, uniformly element of G.*

Proof. Same proof as Corollary(3), until equality 3.

$$Pr[g_1 \cdot g_2 = g'] = \cdots = \sum_{g_0 \in G} Pr[g_1 = g_0] Pr[g_2 = g_0^{-1} g\prime] =^3 \frac{1}{|G|}$$

The 3 equality is achieved as g_0 goes over all elements in G, same goes with g_0^{-1} as each element has a different inverse. So finally when going over all elements in G we receive that each element g' has the same probability. □

5.2 Correctness

In order to use a scheme, one must know that the scheme is always correct.

Theorem 1. *The multiplicative scheme can always be reconstructed given a group of participants $G \in \mathcal{A}$.*

Proof. Given a group of participants $G \in \mathcal{A}$. The scheme is of threshold $t = n - 1$, meaning $|G| = n$. The correctness of this scheme relays on the fact that all elements in U_{M_n} have an inverse. Each $r_i, 1 \leq i \leq s$ can be reconstructed from the n shares of its modulus using CRT as $r_i \in U_{M_n}$ and CRT can reconstruct numbers to it's product of modulus pairwise co-primes equations meaning one solution in $\mathbb{Z}_{M_n}$ because all the modulus are the pairwise co-primes factors of M_n. After reconstructing $r_i, \forall 1 \leq i \leq s$, we can calculate r_i^{-1}. That is the reason why we *must* take the randoms from U_{M_n} and not from $\mathbb{Z}_{M_n}$. To get the secret we calculate:

$$S_{\text{mix}} \cdot \prod_{i=1}^{s} r_i^{-1} = S \cdot \prod_{i=1}^{s} r_i \cdot \prod_{i=1}^{s} r_i^{-1} = S$$

That can be done because multiplication is associative in U_{M_n}. □

5.3 Multiplicative Homomorphism

Theorem 2. *The multiplicative scheme is multiplicatively homomorphic.*

Proof. To show that the scheme is multiplicative homomorphic, we will show that when taking k secrets, distributing them, multiplying as shares on the participants side and finally reconstructing the result, the result will be correct.
Let n be the number of participants, k the number of secrets and s the secrecy bound.

- Let $S_1, S_2, \ldots, S_k \in U_{M_n}$ be secrets that the user want to know later their product.

- Apply the distribution phase of the scheme on each secret. Note that $S_{i_j}, 1 \leq i \leq k, 1 \leq j \leq n$ is the part of the $S_i, 1 \leq i \leq k$ secret held by the j'th participant. Calculating:
  $S_{1_1} = (S_{1_{\text{mix}}} (\text{mod } m_1), r_{1_1} (\text{mod } m_2), \ldots, r_{1_s} (\text{mod } m_{s+1}))$
  $\ldots$
  $S_{k_1} = (S_{k_{\text{mix}}} (\text{mod } m_1), r_{k_1} (\text{mod } m_2), \ldots, r_{k_s} (\text{mod } m_{s+1}))$
  $S_{1_2} = (S_{1_{\text{mix}}} (\text{mod } m_2), r_{1_1} (\text{mod } m_3), \ldots, r_{1_s} (\text{mod } m_{s+2}))$
  $\ldots$
  $S_{k_2} = (S_{k_{\text{mix}}} (\text{mod } m_2), r_{k_1} (\text{mod } m_3), \ldots, r_{k_s} (\text{mod } m_{s+2}))$
  $\ldots$
  $S_{1_n} = (S_{1_{\text{mix}}} (\text{mod } m_n), r_{1_1} (\text{mod } m_1), \ldots, r_{1_s} (\text{mod } m_s))$
  $\ldots$
  $S_{k_n} = (S_{k_{\text{mix}}} (\text{mod } m_n), r_{k_1} (\text{mod } m_1), \ldots, r_{k_s} (\text{mod } m_s))$

- Multiply all shares of each participant - this operation can be done by the participants themselves as needed:
  $S_{\text{res}_1} = (\prod_{1 \leq i \leq k} S_{i_{\text{mix}}} (\text{mod } m_1), \ldots, \prod_{1 \leq i \leq k} r_{i_s} (\text{mod } m_{s+1}))$
  $S_{\text{res}_2} = (\prod_{1 \leq i \leq k} S_{i_{\text{mix}}} (\text{mod } m_2), \ldots, \prod_{1 \leq i \leq k} r_{i_s} (\text{mod } m_{s+2}))$
  $\ldots$
  $S_{\text{res}_n} = (\prod_{1 \leq i \leq k} S_{i_{\text{mix}}} (\text{mod } m_n), \ldots, \prod_{1 \leq i \leq k} r_{i_s} (\text{mod } m_s))$

- Reconstructing all the results of products shares in order to find the result of the product of all secrets $S_{\text{res}} = \prod_{1 \leq i \leq k} S_i$:

  $S_{\text{res}_{\text{mix}}} = CRT[S_{\text{res}_{1_0}} (\text{mod } m_1), \ldots, S_{\text{res}_{n_0}} (\text{mod } m_n)]_{M_n}$
  $r_{\text{res}_1} = CRT[r_{\text{res}_{1_1}} (\text{mod } m_2), \ldots, r_{\text{res}_{n_1}} (\text{mod } m_1)]_{M_n}$
  $\ldots$
  $r_{\text{res}_s} = CRT[r_{\text{res}_{1_s}} (\text{mod } m_{s+1}), \ldots, r_{\text{res}_{n_s}} (\text{mod } m_s)]_{M_n}$

  Each CRT equation has all the pairwise co-prime modulus $m_i, 1 \leq i \leq n$ results, meaning that the numbers are reconstructed perfectly in modulo $\mathbb{Z}_{M_n}$. Also The calculations are correct from Corollary 1.

□

5.4 Security Analysis

Since we want to use the scheme to store and make operations on secret data, we want to ensure that the scheme holds the security properties we need.

Theorem 3. *The multiplicative scheme is a Perfect ramp secret sharing scheme and is a perfect secret sharing scheme in case $s = n - 1$.*

For the simplicity of notation and sizes, we will use $m_i, \forall 1 \leq i \leq n$ as primes and not the general case of pairwise co-primes. To get some *intuition* we will start by analyzing the basic case of $s = 1$. The domain of S_{mix} and r_1 is U_{M_n} and the size of the domain is $|U_{M_n}| = \varphi(M_n) = \prod_{1 \leq i \leq n} \varphi(m_i)$.
For any elements $r'_1, S'_{\text{mix}}, S' \in U_{M_n}$, we have:
$Pr[r_1 = r'_1] = \frac{1}{\varphi(M_n)}$ as r_1 is randomly uniformly chosen.
$Pr[S = S'] = p$ as S is chosen from some distribution $\mathcal{D}$.
$Pr[S_{\text{mix}} = S'_{\text{mix}}] = \frac{1}{\varphi(M_n)}$ as r_1 is randomly uniformly chosen, and the secret S is of some distribution, based on Corollary 4.

The probabilities of r_1 and S_{mix} to be equal to r'_1 and S'_{mix}, respectively, do change knowing some i'th participant data since $s = 1$:

- $Pr[r_1 = r'_1 | r_1 (\text{mod } m_{i+1}) = r'_1 (\text{mod } m_{i+1})] = \frac{1}{\frac{\varphi(M_n)}{\varphi(m_{i+1})}} = \frac{\varphi(m_{i+1})}{\varphi(M_n)}$[1],
- $Pr[S_{\text{mix}} = S'_{\text{mix}} | S_{\text{mix}} (\text{mod } m_i) = S'_{\text{mix}} (\text{mod } m_i)] = \frac{1}{\frac{\varphi(M_n)}{\varphi(m_i)}} = \frac{\varphi(m_i)}{\varphi(M_n)}$.

Yet, we claim that the conditional probability of the secret S to be equal to S' does not change:

$$\begin{aligned} Pr[S = S' | \quad & r_1 (\text{mod } m_{i+1}) = r'_1 (\text{mod } m_{i+1}), \\ & S_{\text{mix}} (\text{mod } m_i) = S'_{\text{mix}} (\text{mod } m_i)] \quad = p \end{aligned} \tag{5}$$

[1] same as a secret shared in Mignotte's scheme, which is the equivalence class of $r_1 (\text{mod } m_{i+1})$

In fact, S_{mix} has $\varphi(M_n)^2$ options to be calculated, and all the $\varphi(M_n)$ options to be formed to. The options left for participant i as possible results of S_{mix} are $\frac{\varphi(M_n)}{\varphi(m_{i+1})}$. Also, r_1 has $\varphi(M_n)$ options to be chosen from, so each option left for participant i can be from $\frac{\varphi(M_n)}{\varphi(m_i)}$ options.

The participant then can also calculate $[r_1^{-1}]_{M_n}$ for every r_1 in his options because M_n is known. Calculating the number of options to get S we have $\frac{\varphi(M_n)}{\varphi(m_i)} \cdot \frac{\varphi(M_n)}{\varphi(m_{i+1})} = \varphi(M_n) \cdot \prod_{1 \leq j \leq n, j \neq i, i+1} \varphi(m_j)$ options.

From Corollary 1 we know that $U_{M_n} \cong U_{m_1} \times U_{m_2} \times ... \times U_{m_n}$ and we can also say that $U_{M_n/m_i} \cong U_{m_1} \times ... \times U_{m_{i-1}} \times U_{m_{i+1}} \times ... \times U_{m_n}$ for every i. Therefore when multiplying all elements in U_{M_n/m_i} with all elements in $U_{M_n/m_{i+1}}$ we get all the elements in U_{M_n}. Since r_1 and S_{mix} act as randomly chosen elements in U_{M_n}, each option of $S \in U_{m_n}$ **has the same amount of appearances** from all the $\varphi(M_n) \cdot \prod_{j \neq i, i+1} \varphi(m_j)$ options calculated by the participant, and exactly $\prod_{j \neq i, i+1} \varphi(m_j)$ calculations each. Therefore the scheme is perfect ramp security for $s = 1$.

Proof. Let G be a group of curious participants gathered to reconstruct the secret or leak some information about it, $|G| \leq s$.

Given $S_{\text{mix}}, r_1, \ldots, r_s \in U_{M_n}$, The domain of $S_{\text{mix}}, r_1, \ldots, r_s$ is U_{M_n} and the size of the domain is $|U_{M_n}| = \varphi(M_n) = \prod_{1 \leq i \leq n}(m_i - 1)$ (The Euler function in case M_n is the product of primes from degree 1).
For each element $r'_1, \ldots, r'_s, S'_{\text{mix}}, S' \in U_{M_n}$ the probabilities of $r_1, \ldots, r_s, S_{\text{mix}}$ and S to be equal accordingly are:
$Pr[r_1 = r'_1] = \frac{1}{\varphi(M_n)}$ as r_1 is randomly uniformly chosen.
...
$Pr[r_s = r'_s] = \frac{1}{\varphi(M_n)}$ as r_s is randomly uniformly chosen.
$Pr[S = S'] = p$ as S is chosen from some distribution $\mathcal{D}$.
$Pr[S_{\text{mix}} = S'_{\text{mix}}] = \frac{1}{\varphi(M_n)}$ as $r_1, \ldots, r_s$ are randomly uniformly chosen, and the secret S is of some distribution, based on Corollary 3 with induction That can be applied and Corollary 4.

The probabilities of $r_1, \dots, r_s$ and S_{mix} to be equal to $r'_1, \dots, r'_s$ and S'_{mix} respectively, do change knowing the information held by the group $G = \{i_1, \dots, i_s\}, 1 \leq i_1 < \cdots < i_s \leq n$:

$$Pr[r_1 = r'_1 | r_1 (\text{mod } m_{i_1+1}) = r'_1 (\text{mod } m_{i_1+1}), \dots, r_1 (\text{mod } m_{i_s+1}) = r'_1 (\text{mod } m_{i_s+1})] =$$

$$\frac{1}{\frac{\varphi(M_n)}{\prod_{i \in G} \varphi(m_{i+1})}} = \frac{\prod_{i \in G} \varphi(m_{i+1})}{\varphi(M_n)}$$

$$\dots$$

$$Pr[r_s = r'_s | r_s (\text{mod } m_{i_1+s}) = r'_s (\text{mod } m_{i_1+s}), \dots, r_s (\text{mod } m_{i_s+s}) = r'_s (\text{mod } m_{i_s+s})] =$$

$$\frac{1}{\frac{\varphi(M_n)}{\prod_{i \in G} \varphi(m_{i+s})}} = \frac{\prod_{i \in G} \varphi(m_{i+s})}{\varphi(M_n)}$$

$$Pr[S_{\text{mix}} = S'_{\text{mix}} | S_{\text{mix}} (\text{mod } m_{i_1}) = S'_{\text{mix}} (\text{mod } m_{i_1}), \dots, S_{\text{mix}} (\text{mod } m_{i_s}) = S'_{\text{mix}} (\text{mod } m_{i_s})] =$$

$$\frac{1}{\frac{\varphi(M_n)}{\prod_{i \in G} \varphi(m_i)}} = \frac{\prod_{i \in G} \varphi(m_i)}{\varphi(M_n)}$$

Yet, we claim that the conditional probability of the secret S to be equal to S' does not change:

$$Pr[S = S' | r_1(\text{mod } m_{i_1+1}) = r'_1(\text{mod } m_{i_1+1}), \ldots, r_1(\text{mod } m_{i_s+1}) = r'_1(\text{mod } m_{i_s+1}),$$

$$\ldots, r_s(\text{mod } m_{i_1+s}) = r'_s(\text{mod } m_{i_1+s}), \ldots, r_s(\text{mod } m_{i_s+s}) = r'_s(\text{mod } m_{i_s+s}),$$

$$S_{\text{mix}}(\text{mod } m_{i_1}) = S'_{\text{mix}}(\text{mod } m_{i_1}), \ldots, S_{\text{mix}}(\text{mod } m_{i_s}) = S'_{\text{mix}}(\text{mod } m_{i_s})] =^* p$$

In fact we know that $s < n$ and therefore, we know that each modulo of $\varphi(m_{i_j}), \forall 1 \leq j \leq s$ does not appear n times in different equations. Hence the total amount of valid options for S to be calculated by the group G is:

$$\prod_{1 \leq j \leq s} \frac{\varphi(M_n)}{\prod_{i \in G} \varphi(m_{i+j})} \cdot \frac{\varphi(M_n)}{\prod_{i \in G} \varphi(m_i)} = \frac{\varphi(M_n)^{s+1}}{(\prod_{1 \leq j \leq s} \prod_{i \in G} \varphi(m_{i+j})) \cdot (\prod_{i \in G} \varphi(m_i))}$$

$$\leq^{**} \frac{\varphi(M_n)^{s+1}}{\varphi(M_n)^s}$$

** Since $s < n$, than $\varphi(m_i), \forall 1 \leq i \leq n$ appear at most s times.

As in the intuition part, based on Corollary 1, it is possible to show that the distribution of S does not change, even when knowing the information of the group G, and each element in $S' \in U_{M_n}$ stays with the same probability that S is equal to it. Therefore the scheme is perfect ramp security for any $s < n$.

The choice of $s = n - 1$ yields a perfect secret sharing scheme according to Definition 1 as $\forall G \notin \mathcal{A}$ there is no information leak. □

6 References

[1] Adi Shamir, How to share a secret, Communications of the ACM (Volume 22, Issue 11, 01 November 1979), 612–613.

[2] C. Asmuth, J. Bloom, A modular approach to key safeguarding, IEEE Transactions on Information Theory (Volume: 29, Issue: 2, Mar 1983) 208 - 210.

[3] Yildirim, İsmail Fatih, SecurePL: A compiler and toolbox for practical and easy secure multiparty computation, Sabanci University (Spring, 2008).

[4] Oğuzhan Ersoy, Thomas Brochmann Pedersen, Emin Anarim, Homomorphic extensions of CRT-based secret sharing, Discrete Applied Mathematics (Volume 285, 15 October 2020) 317-329.

[5] Dor Bitan, Shlomi Dolev, Optimal-Round Preprocessing-MPC of Polynomials over Non-Zero Inputs via Distributed Random Matrix, Association for Computing Machinery (Vol. 1, No. 1, November 2020).

[6] Stanley Burris, H.P. Sankappanavar, A Course in Universal Algebra (2012).

[7] Leslie G. Valiant, Why is Boolean complexity theory difficult?, Proceedings of the London Mathematical Society Symposium on Boolean function complexity (1992), 84–94.