Secret sharing using the Chinese remainder theorem

Secret sharing consists of recovering a secret *S* from a set of shares, each containing partial information about the secret. The Chinese remainder theorem (CRT) states that for a given system of simultaneous congruence equations, the solution is unique in some **Z**/*n***Z**, with $n > 0$ under some appropriate conditions on the congruences. Secret sharing can thus use the CRT to produce the shares presented in the congruence equations and the secret could be recovered by solving the system of congruences to get the unique solution, which will be the secret to recover.

1 Secret sharing schemes: several types

Main article: Secret sharing

There are several types of secret sharing schemes. The most basic types are the so-called threshold schemes, where only the cardinality of the set of shares matters. In other words, given a secret *S*, and *n* shares, any set of *t* shares is a set with the smallest cardinality from which the secret can be recovered, in the sense that any set of *t-1* shares is not enough to give *S*. This is known as a threshold access structure. We call such schemes (*t*,*n*) threshold secret sharing schemes, or *t*-out-of-*n* scheme.

Threshold secret sharing schemes differ from one another by the method of generating the shares, starting from a certain secret. The first ones are Shamir's threshold secret sharing scheme, which is based on polynomial interpolation in order to find *S* from a given set of shares, and George Blakley's geometric secret sharing scheme, which uses geometric methods to recover the secret *S*. Threshold secret sharing schemes based on the CRT are due to Mignotte and Asmuth-Bloom, they use special sequences of integers along with the CRT.

2 Chinese remainder theorem

Main article: Chinese remainder theorem

Let $k \geqslant 2, m_1, ..., m_k \geqslant 2$, and $b_1, ..., b_k \in \mathbf{Z}$. The system of congruences

$$\begin{cases} x \equiv & b_1 \bmod m_1 \\ & \vdots \\ x \equiv & b_k \bmod m_k \end{cases}$$

has solutions in **Z** if and only if $b_i \equiv b_j \bmod (m_i, m_j)$ for all $1 \leqslant i, j \leqslant k$, where (m_i, m_j) denotes the greatest common divisor (GCD) of *mi* and *mj*. Furthermore, under these conditions, the system has a unique solution in **Z**/*n***Z** where $n = [m_1, ..., m_k]$, which denotes the least common multiple (LCM) of $m_1, ..., m_k$.

3 Secret sharing using the CRT

Since the Chinese remainder theorem provides us with a method to uniquely determine a number *S* modulo *k*-many relatively prime integers $m_1, m_2, ..., m_k$, given that $S < \prod_{i=1}^{k} m_i$, then, the idea is to construct a scheme that will determine the secret *S* given any *k* shares (in this case, the remainder of *S* modulo each of the numbers *mi*), but will not reveal the secret given less than *k* of such shares.

Ultimately, we choose *n* relatively prime integers $m_1 < m_2 < ... < m_n$ such that *S* is smaller than the product of any choice of *k* of these integers, but at the same time is greater than any choice of *k-1* of them. Then the shares $s_1, s_2, ..., s_n$ are defined by $s_i = S \bmod m_i$ for $i = 1, 2, ..., n$. In this manner, thanks to the CRT, we can uniquely determine *S* from any set of *k* or more shares, but not from less than *k*. This provides the so-called threshold access structure.

This condition on *S* can also be regarded as

$$\prod_{i=n-k+2}^{n} m_i < S < \prod_{i=1}^{k} m_i.$$

Since *S* is smaller than the smallest product of *k* of the integers, it will be smaller than the product of any *k* of them. Also, being greater than the product of the greatest $k - 1$ integers, it will be greater than the product of any $k - 1$ of them.

There are two Secret Sharing Schemes that utilize essentially this idea, Mignotte's and Asmuth-Bloom's Schemes, which are explained below.

3.1 Mignotte's threshold secret sharing scheme

As said before, Mignotte's threshold secret sharing scheme uses, along with the CRT, special sequences of integers called the (*k*,*n*)-Mignotte sequences which consist of *n* integers, pairwise coprime, such that the product of the smallest *k* of them is greater than the product of the $k-1$ biggest ones. This condition is crucial because the scheme is built on choosing the secret as an integer between the two products, and this condition ensures that at least *k* shares are needed to fully recover the secret, no matter how they are chosen.

Formally, let $2 \leq k \leq n$ be integers. A (*k*,*n*)-Mignotte sequence is a strictly increasing sequence of positive integers $m_1 < \cdots < m_n$, with $(m_i, m_j) = 1$ for all $1 \leq i < j \leq n$, such that $m_{n-k+2} \cdots m_n < m_1 \cdots m_k$. We call this range the authorized range. We build a (*k*,*n*)-threshold secret sharing scheme as follows: We choose the secret *S* as a random integer in the authorized range. We compute, for every $1 \leq i \leq n$, the reduction modulo *mi* of *S* that we call *si*, these are the shares. Now, for any *k* different shares $s_{i_1}, \ldots, s_{i_k}$, we consider the system of congruences:

$$\begin{cases} x \equiv & s_{i_1} \bmod m_{i_1} \\ & \vdots \\ x \equiv & s_{i_k} \bmod m_{i_k} \end{cases}$$

By the Chinese remainder theorem, since $m_{i_1}, \ldots, m_{i_k}$ are pairwise coprime, the system has a unique solution modulo $m_{i_1} \cdots m_{i_k}$. By the construction of our shares, this solution is nothing but the secret *S* to recover.

3.2 Asmuth-Bloom's threshold secret sharing scheme

This scheme also uses special sequences of integers. Let $2 \leq k \leq n$ be integers. We consider a sequence of pairwise coprime positive integers $m_0 < ... < m_n$ such that $m_0.m_{n-k+2}...m_n < m_1...m_k$. For this given sequence, we choose the secret S as a random integer in the set $\mathbf{Z}/m_0\mathbf{Z}$.

We then pick a random integer α such that $S + \alpha.m_0 < m_1...m_k$. We compute the reduction modulo *mi* of $S + \alpha.m_0$, for all $1 \leq i \leq n$, these are the shares $I_i = (s_i, m_i)$. Now, for any *k* different shares $I_{i_1}, ..., I_{i_k}$, we consider the system of congruences:

$$\begin{cases} x \equiv & s_{i_1} \bmod m_{i_1} \\ & \vdots \\ x \equiv & s_{i_k} \bmod m_{i_k} \end{cases}$$

By the Chinese remainder theorem, since $m_{i_1}, ..., m_{i_k}$ are pairwise coprime, the system has a unique solution S_0 modulo $m_{i_1}...m_{i_k}$. By the construction of our shares, the secret S is the reduction modulo m_0 of S_0.

It is important to notice that the Mignotte (*k*,*n*)-threshold secret-sharing scheme is not perfect in the sense that a set of less than *k* shares contains some information about the secret. The Asmuth-Bloom scheme is perfect: α is independent of the secret S and

$$\left.\begin{matrix} \prod_{i=n-k+2}^{n} m_i \\ \alpha \end{matrix}\right\} < \frac{\prod_{i=1}^{k} m_i}{m_0}$$

Therefore α can be any integer modulo

$$\prod_{i=n-k+2}^{n} m_i.$$

This product of $k-1$ moduli is the largest of any of the n choose $k-1$ possible products, therefore any subset of $k-1$ equivalences can be any integer modulo its product, and no information from S is leaked.

3.3 Example

The following is an example on the Asmuth-Bloom's Scheme. For practical purposes we choose small values for all parameters. We choose *k=3* and *n=4*. Our pairwise coprime integers being $m_0 = 3, m_1 = 11, m_2 = 13, m_3 = 17$ and $m_4 = 19$. They satisfy the Asmuth-Bloom required sequence because $3 \cdot 17 \cdot 19 < 11 \cdot 13 \cdot 17$.

Say our secret S is 2. Pick $\alpha = 51$, satisfying the required condition for the Asmuth-Bloom scheme. Then $2+51 \cdot 3 = 155$ and we compute the shares for each of the integers 11, 13, 17 and 19. They are respectively 1, 12, 2 and 3. We consider one possible set of 3 shares: among the 4 possible sets of 3 shares we take the set {1,12,2} and show that it recovers the secret S=2. Consider the following system of congruences:

$$\begin{cases} x \equiv & 1 \bmod 11 \\ x \equiv & 12 \bmod 13 \\ x \equiv & 2 \bmod 17 \end{cases}$$

To solve the system, let $M = 11 \cdot 13 \cdot 17$. From a constructive algorithm for solving such a system, we know that a solution to the system is $x_0 = 1 \cdot e_1 + 12 \cdot e_2 + 2 \cdot e_3$, where each *ei* is found as follows:

By Bézout's identity, since $(m_i, M/m_i) = 1$, there exist positive integers *ri* and *si*, that can be found using the Extended Euclidean algorithm, such that $r_i.m_i + s_i.M/m_i = 1$. Set $e_i = s_i \cdot M/m_i$.

From the identities $1 = 1 \cdot 221 - 20 \cdot 11 = (-5) \cdot 187 + 72 \cdot 13 = 5 \cdot 143 + (-42) \cdot 17$, we get that $e_1 = 221, e_2 = -935, e_3 = 715$, and the unique solution modulo $11 \cdot 13 \cdot 17$ is 155. Finally, $S = 155 \equiv 2 \mod 3$.

4 See also

- Secret Sharing
- Shamir's Secret Sharing Scheme
- Chinese remainder theorem
- Access Structure

5 References

- Oded Goldreich, Dana Ron and Madhu Sudan, Chinese Remaindering with Errors, IEEE Transactions on Information Theory, Vol. 46, No. 4, July 2000, pages 1330-1338.
- C.A. Asmuth and J. Bloom. A modular approach to key safeguarding. IEEE Transactions on Information Theory, IT-29(2):208-210, 1983.
- Sorin Iftene. General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting. Electronic Notes in Theoretical Computer Science (ENTCS). Volume 186, (July 2007). Pages 67–84. Year of Publication: 2007. ISSN 1571-0661.
- Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to Algorithms, Second Edition. MIT Press and McGraw-Hill, 2001. ISBN 0-262-03293-7. Section 31.5: The Chinese remainder theorem, pages 873-876.
- Ronald Cramer. Basic Secret Sharing (Lectures 1-2), Class Notes. October 2008, version 1.1.

6 External links

- http://www.cryptolounge.org/wiki/Ronald_Cramer

7 Text and image sources, contributors, and licenses

7.1 Text

- **Secret sharing using the Chinese remainder theorem** *Source:* https://en.wikipedia.org/wiki/Secret_sharing_using_the_Chinese_remainder_theorem?oldid=701997522 *Contributors:* GünniX, SmackBot, Myasuda, David Eppstein, Yugsdrawkcabeht, Vlsergey, Sun Creator, Addbot, Luckas-bot, Yobot, CryptoBm, Erik9bot, TLange, Jannaston, DarthCrypt, Tohecz, Marc renault and Anonymous: 9

7.2 Images

7.3 Content license