International Journal of Cryptology Research 3(1): 27-33 (2011)

ACM Cryptographic Key Exchange for Secure Communications

Annamalai, C

Indian Institute of Technology Kharagpur

Email: anna@iitkgp.ac.in

ABSTRACT

This paper presents a new cryptographic technique for secure authenticated key exchange. For information resource transactions cryptosystem [3] plays an important role in encrypting and decrypting the messages which are sent on secure communication channels for protecting from eavesdroppers. In this research study, the ACM key exchange (a new cryptographic key exchange technique) has been introduced for secure network communication. The ACM key exchange depends primarily on ACM (Annamalai Computing Model) for both key generation and key exchange. The ACM is actually a mathematical model which enables the ACM key exchange algorithm to create secret codes. A secret code carries the secure cryptographic key from one user to another user. The secret codes are generated using 'code for signs' such as Plus Sign Code (PSC) and Minus Sign Code (MSC), and Sum of Series of Powers of two (SSP). The PSC and MSC have been used as digital numbers in the research and these codes are juxtaposed with SSP for the purpose of key exchange securely.

INTRODUCTION

Key exchange is a technique in cryptography by which the secret keys are exchanged between senders and receivers for the purposes of encryption and decryption of messages respectively. In the communication world, various key exchange techniques are being used for secure authenticated key exchange to protect from eavesdroppers. If encryption of messages is vulnerable, then eavesdroppers can gain full information over communication channels. In this research study, a new approach is introduced for efficient and secure authenticated key exchange which is named as ACM key exchange technique. The ACM key exchange uses Annamalai Computing Model based on geometric progression of powers of two [1, 2] for key generation.

ANNAMALAI COMPUTING MODEL (ACM)

The ACM (Annamalai Computing Model) is defined as a computing model based on the geometric progression of powers of two. The ACM is actually a computational technique for the purpose of finding the sum of geometric series of powers of two [1, 2]. The following theorem is named as ACM (Annamalai Computing Model).

Theorem: $\sum_{i=k}^{n-1} 2^i = 2^n - 2^k$ where $k \in \mathbf{Z}$, set of integers.

To prove the above theorem [2], we can use the following technique:

$$2^n = 2^n$$
$$2^n = 2^{n-1} + 2^{n-2} + \cdots + 2^i + \cdots + 2^k + 2^k$$
$$\sum_{i=k}^{n-1} 2^i = 2^n - 2^k$$

CODE FOR SIGNS

The ACM key exchange technique mainly uses the code for signs for creating secret codes which carry the secret keys from one party to another party. In the research study, plus sign code (PSC) and minus sign code (MSC) are used to create secret codes. For easily understanding the code for signs, here the symbols + and - are used to represent the PSC and MSC respectively. The plus sign code (+) and minus sign code (-) are juxtaposed with an unsigned number to create a secret code.

Let E be an unsigned number. Then

+E or E+ is a plus sign number
-E or E- is a minus sign number

The following examples explain the secret code.

Example 1:

Let 207 be a plus sign code and 888 an unsigned number. Then 207888 or 888207 is a plus sign number.

Let 399 be a minus sign code, then 399888 or 888399 is a minus sign number.

Example2:

Let 101 be a minus sign code and 1111 an unsigned number. Then 1011111 or 1111101 is minus sign number.

Here, plus sign and minus sign numbers are used for generation of secret codes.

ACM KEY EXCHANGE

The purpose of the ACM key exchange algorithm is to enable two parties to exchange a key securely that can be used for subsequent encryption and decryption of messages. The ACM algorithm uses Annamalai computing model $\sum_{i=k}^{n-1} 2^i = 2^n - 2^k$ primarily for generating secret code which carries the secret key from one user to another user. The secret code is the combination of a CFS (Code for Sign) and an SSP (Sum of Series of Powers of two).

Let us consider E as an SSP (Sum of Series of Powers of two). The symbols + and – can be used to represent the plus sign code (PSC) and minus sign code (MSC) respectively.

+E = (PSC)(SSP) = PSCSSP
-E = (MSC)(SSP) = MSCSSP

Here '+E' and '-E' are the secret codes used to carry the secret keys from one user to another user.

To understand the arrangement of CFS (Code for Sign) and SSP (Sum of Series of Powers of two) for secret code, Let us see the examples given below:

Examples:

Let PSC = {20, 12, 35}, MSC = {13, 31, 52} and E = {14, 30, 62}. Then,

+E = {2014, 2030, 2062, 1214, 1230, 1262, 3514, 3530, 3562}
-E = {1314, 1330, 1362, 3114, 3130, 3162, 5214, 5230, 5262}

Now, let us understand the Sum of Series of Powers of two (SSP):

Here E denotes an SSP.

Let $E = \sum_{i=k}^{n} 2^i$. Then $E = 2^n - 2^k$

That is, $2^n = 2^k + E$ and $2^k = 2^n - E$ (1)

Let g be a common key known only to both sender and receiver and p be a secret key.

Then we can rewrite (1) as $2^p = 2^g \pm E$.

That is,

(i) If p is greater than $g\,(p > g)$, then $2^p = 2^g + E$ where $E = \sum_{i=g}^{p-1} 2^i$

(ii) If p is less than $g\,(p < g)$, then $2^p = 2^g - E$ where $E = \sum_{i=p}^{g-1} 2^i$

The ACM key exchange is implemented as follows:

If user A wants to send a secret key to user B, the following procedure must be considered for efficient and secure authenticated key exchange.

1. First, users A and B must select a common key (say) g.
2. Sender A must choose a secret key (say) p which satisfies the following conditions:

   $2^p = 2^g + E$ if p is chosen greater than $g\,(p > g)$ where $E = \sum_{i=g}^{p-1} 2^i$

   OR

   $2^p = 2^g - E$ if p is chosen less than $g\,(p < g)$ where $E = \sum_{i=p}^{g-1} 2^i$

3. User A sends the secret code (-E or +E) to user B. The user B receives the secret code and calculates the secret key p in the following manners:

   Case 1:

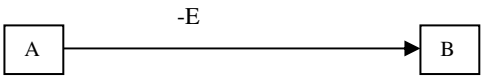


Figure 1. User A sends the secrete code (-E) to user B

As the user A has sent the secret code '-E' to user B, the secret key p must have been chosen less than g. Now, user B calculates the secret key p using –E and g which is commonly known to users A and B.

p is calculated which satisfies $2^p = 2^g - E$ where $E = \sum_{i=p}^{g-1} 2^i$

Case 2:

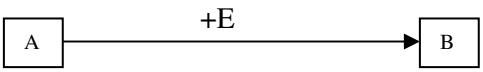


Figure 2. User A sends the secret code (+E) to user B

Since the user A has sent the secret code '+E' to user B, the secret key p must have been chosen greater than g. Now, user B calculates the secret key p using +E and g as follows:

p is found which satisfies $2^p = 2^g + E$ where $E = \sum_{i=g}^{p-1} 2^i$.

Fixing Common integer g integer (A & B selects common integer)	
User A: Key Selection & Code Generation	
Select p	$p<g$ or $p>g$
Calculate '+E'	$E = \sum_{i=g}^{p-1} 2^i \quad (p > g)$
Calculate '-E'	$E = \sum_{i=p}^{g-1} 2^i \quad (p < g)$

Figure 3 (continued): The ACM Key Exchange Algorithm

Fixing Common integer g integer (A & B selects common integer)
User B: Key Calculation
Find p if received '+E' $\quad 2^p = 2^g + \sum_{i=g}^{p-1} 2^i \quad (p > g)$
Find p if received '-E' $\quad 2^p = 2^g - \sum_{i=p}^{g-1} 2^i \quad (p < g)$

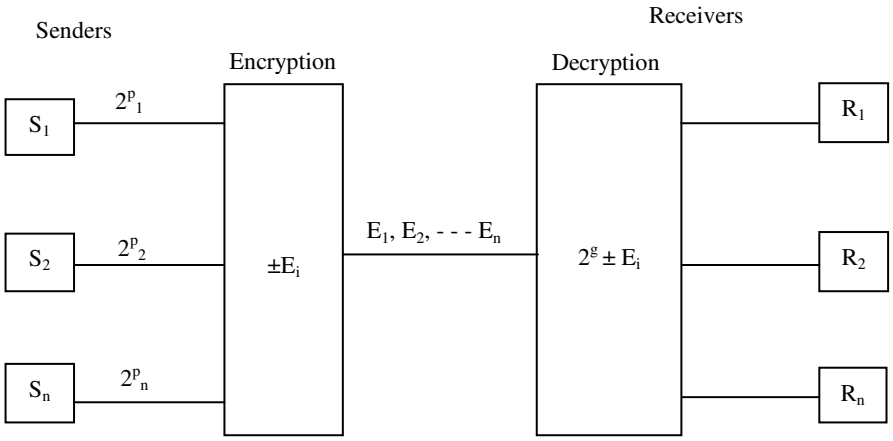
Figure 3 (continued): The ACM Key Exchange Algorithm

The ACM key exchange is a novel approach to efficient and secure authenticated key exchange. In the ACM algorithm, the common key g is known only to sender and receiver. If it is necessary, we can also exchange the common key g as the technique used of secret key p.

Let S be a set of secret codes. Then $S_i = x_i y_i$ where S_i is i^{th} secret code and x_i is i^{th} CFS and y_i is i^{th} SSP.

The following pseudocode describes the ACM algorithm for n secret codes:

```
for(i = 0;i < n;i++)
if (x[i] == PSC)
p > g
elif (x[i] == MSC)
p < g
else
wrongcode
```



CONCLUSION

In this research study, a new key exchange technique, ACM key exchange, has been introduced for efficient and secure authenticated key exchange between two parties. The ACM key exchange technique used the Annamalai computing model for the purpose of key generation. The code for signs, plus sign code and minus sign code, have been used for the purpose of juxtaposing the unsigned numbers.

REFERENCES

[1] Annamalai, C and Sasikala, P. 2009. Computational Geometric Series Model with Key Applications in Informatics, *International Journal of Computational Intelligence Research.* **5**(4): 485-499.

[2] Annamalai, C. 2009. A Novel Computational Technique for the Geometric Progression of Powers of Two. *Journal of Scientific and Mathematical Research*. **8**(1): 16-17

[3] Stallings,W. 2004. *Cryptography and Network Security: Principles and Practices,* 3rd ed. Pearson Education (S) Pte. Ltd.