AN EFFICIENT PUBLIC KEY ENCRYPTION SCHEME USING SHARED SECRETS

Sattar J Aboud
The University for Graduate Studies
Faculty of IT
Amman - Jordan
sattar_aboud@yahoo.com

ABSTRACT

This paper describes the combination of Shamir secret sharing method with the trap door characteristics of discrete logarithm mod a large prime number as employed in the Diffie-Hellman exchange scheme. The purpose of this combination is to protect the privacy of the numbers held by the parties of the shared secret, while at the same time authorizing them to broadcast data in the clear which when published by adequate of the parties enables authorization of the transaction for instance t out of n signers for the cheque.

Key words**:** *Public key encryption, Shared Secret, Discrete logarithm, Diffie-Hellman Scheme.*

1. Introduction

Secret sharing schemes permit a set of parties to share a piece of private data in such a way that just authorized subgroup of the parties can find out the secret. However, the unauthorized subgroup is not capable to recover the secret. The group of all authorized subset is named the access structure. Secret sharing methods have numerous practical uses. For example, they can be employed to control the access to a protected, so only an authorized subgroup of bank workers can open it by grouping their shares together and rebuilding the secret combination which unlocks the protected.

The predominantly attractive type of secret sharing methods comprises threshold schemes with a set of n parties. Their access structure contains all subgroup of t or more parties. These schemes are named t out of n threshold methods or just (t,n) methods. Threshold schemes are originally invented by Shamir [1]. The important key regarding the understanding of a secret sharing scheme for a random access structure was considered by many researchers [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13], they recommended various solutions for building such systems.

Shamir secret sharing method [1] suggests a method of distributing a secret number between numerous parties. Simply after some minimum number of parties cooperates can the secret number be rebuild. The Diffie-Hellman public key distribution method presents a technique for two parties to agree on a secret number among them [14], while all their exchanges are transmitted over a public way. In this paper we discuss the combination of Shamir secret sharing scheme with the trap door characteristics of discrete logarithm of a large prime number as employed in the Diffie-Hellman secret number exchange scheme. The object of this combination is to preserve the secrecy of the numbers held by the members of the shared secret, whilst at the same time permitting them to send information in the clear which, when issued by sufficient of the individuals enables authorization of transaction [15, 16, 17] for example t out of n signers for a cheque.

The concept of the suggested method is considered in section 2, the descriptions of the scheme and an example of the applications is analyzed in section 3. Section 4 presents a number of comments and notes concerning the scheme proposed.

2. The Proposed Scheme

The polynomial of degree n in one parameter is entirely distinct when $n+1$ a point in which it ranges specified. This is factual if the coefficients related to some fields and in specific to the $GF(p)$ of integer mod a prime number p. If these points are (x_i, z_i), for $i = 1,...,n+1$, the number of z according to

the number of x is specified by the Lagrange interpolation theorem:

$$z = \sum_{i=1}^{n+1} w_i * z_i \bmod p \quad (1)$$

Such that

$$w_i = \prod_{j=1}^{n+1} (x - x_j)/(x_i - x_j) \bmod p \text{ , } for$$

$$i = 1,...,n+1 \text{ Where } j \neq i \quad (2)$$

In this suggested method the ordinates x are public key and since w_i base only on them, these are also public. It must be noticed that w_i is resulting by numerical operations, p and x are also members of the field $GF(p)$, i.e. are both integers. The divisions needed in their derivation are achieved by employing the Euclidean method [18]. The ordinates z on the other hand, are remained secret by the parties and by no means straight sent by them. Instead they are employed as key exponents to raise certain public base value h to various powers to give a new set of values s. This exponentiation is performed by mod operation with another prime number q, the base value h and the out comings $s's$ are consequently members of the field $GF(q)$.

$$\text{So } s_i = h^{z_i} \bmod q \quad (3)$$

The exponentiations possibly accomplished efficiently employing the repeated square and multiply algorithm [19], which is commonly employed in public key encryption, and illustrated for instance by Rivest Shamir and Adleman [20]. While in the Diffie-Hellman public key distributed algorithm given q is a well selected prime knowledge of h, q and the $s's$ does not disclose the related $z's$ because logarithm mod a well selected prime is a computationally difficult to solve. The prime numbers p and q are selected so that both are connected to each other by the following formula:

$$q = g * p + 1 \quad (4)$$

When p is selected as a prime number, g is handily chosen from the sorting order of even numbers $2,4,6,...$ is the least positive integer which produces q prime. This relationship has two aims:

1. To ensure that $q-1$ have a large prime factor which is an essential condition for guarantee that logarithm mod q is computationally difficult to solve. The well known method is shanks method [4] which requires $o(\sqrt{q})$ operations to achieve the logarithm.

2. To offer a technique of efficiently achieving the operations among the exponents needed by formula (1) via performing on the matching s numbers. Additions among z values are substituted by multiplications among s values. Multiplications of z values by known key multipliers w_i are substituted by raising the s values to the power of these public multipliers. To achieve this properly, it is essential to limit the range of base integer h as follows:

$$h = a^g \bmod q, \quad for \quad 2 \leq a \leq q-1 \quad and$$

$$h \neq 1 \quad (5)$$

By Fermat's Theorem:

$$a^{q-1} \equiv 1 \bmod q \quad for \ any \quad a \neq v \bmod q \quad (6)$$

Hence

$$h^p = (a^g)^p = a^{(q-1)} = 1 = h^v \bmod q \quad (7)$$

$$i.e. \quad h^p = h^v \bmod q \quad (8)$$

The exponents of h act as integer mod p It perhaps noted that this constraint still allows selection of $p-1$ is another possibility working numbers for h. If h is raised correspondingly to the power of every part of formula (1) the following relationship is computed.

$$s = h^z = h^{(\sum_{i=1}^{n+1} w_i * z_i)} = \prod_{i=1}^{n+1} h^{(w_i * z_i)}$$

$$= \prod_{i=1}^{n+1} (h^{z_i})^{w_i} \quad (9)$$

$$i.e. \qquad s = \prod_{i=1}^{n+1} s_i^{\,w_i} \bmod q \quad (10)$$

Formula (10) is a relationship among $n+2$ different $s's$ every of which is resulting from one of the $n+2$ matching $z's$ which demonstrate the relationship given in formula (1) Every participant provided with a sum of $n+2$ numbers of s can test if formula (10) is

achieved. When it is achieved, then the $n+2$ numbers of s and therefore their providers are real.

3. Authorization of the transaction

Assume that a minimum number of t signers out of a total of n signers are needed to authorize a cheque. Then a polynomial of degree $2*t-1$ is secretly created. Let the bank is concerned with one point while every signer is concerned with two points on this polynomial. Next employing the same base value t authorizers must both provide the bank with two s integer numbers. The bank can create one s integer number itself providing a sum of $2*t+1$. These are enough for the bank to test achievement with formula (10). As soon as $2*t+1$ is perceived, s numbers are accepted, and any additional s values can be computed from them, so that the same base number should not be employed for a different operation. To avoid this it is recommended that the base value must include in certain methods a date and time stamp.

Example

This example demonstrates the idea of the scheme is suggested, creation of small prime numbers to show the standard of operation. In reality a number of 150 or more decimal digits should be employed. Assume that a minimum of 2 signers from the total of 5 are wanted to sign a cheque. Select $p=29$ prime and then compute $q=g*p+1=59$ also is prime, with $g=2.$ suppose a program is employed to choose a private polynomial of degree 3 with coefficient in $GF(29)$. Assume it chooses:

$$z=5*x^3+8*x^2+9*x+3 \bmod 29 \quad (11)$$

Next chooses 11 ordinates x two for every of the five authorizing parties and one for the bank. It computes secretly from formula (11) the matching ordinates using the multiplicative inverse [21, 22] which is as follows:

Participant	x	z
P_{1a}	7	27
P_{1b}	3	5
P_{2a}	4	23
P_{2b}	5	3
P_{3a}	8	15
P_{3b}	2	6
P_{4a}	12	14
P_{4b}	9	27
P_{5a}	16	26
P_{5b}	6	4
Bank	17	5

The program provides every participant with information of each one's x values and every participant independently with his private z values. It then removes its memory to erase the polynomial coefficients it has selected. Assume that participant 2 and 5 agree to authorize an operation. They determine with the bank a value $a=13$, connected with the operation, and from it compute the base value as follows:

$$\begin{aligned} h &= a^g \bmod q \\ &= 13^2 \bmod 59 \\ &= 51 \end{aligned} \quad (12)$$

Every one send to the bank two values (x,s), such that $s=51^z \bmod 59$ and z is a private ordinate according to the ordinate x. The bank also computes it's s as follows:

Participant	**suffix**	x	z	s
P_{2a}	1	4	23	17
P_{2b}	2	5	3	19
P_{5a}	3	16	26	28
P_{5b}	4	6	4	25
Bank		17	5	36

Employing the received ordinate data the bank computes by the formula (12) the w_i numbers according to its ordinate.

$$w_1=\frac{(5-12)*(17-16)*(17-6)}{(4-5)*(4-16)*(4-6)}=\frac{16}{5}=16*6=9$$

$$w_2=\frac{(17-4)*(17-16)*(17-6)}{(5-4)*(5-16)*(5-6)}=\frac{27}{11}=27*8=13$$

$$w_3=\frac{(17-4)*(17-5)*(17-6)}{(16-4)*(16-5)*(16-6)}=\frac{5}{15}=5*2=10$$

$$w_4=\frac{(17-4)*(17-5)*(17-16)}{(6-4)*(6-5)*(6-16)}=\frac{11}{9}=11*13=27$$

The bank then computes from formula (10) the number of it's s as provided by the four accepted $s's$ to obtain:

$$\begin{aligned} s &= 17^9 * 19^{13} * 28^{10} * 25^{27} \bmod 59 \\ &= 25*57*22*27 \bmod 59 \\ &= 36 \end{aligned}$$

Since this agrees with its own inside created m number, the bank considers the transaction as authorized. As soon as this specific base number is employed, its future use is no longer private. The z values though keep their privacy and perhaps used again with another base value.

4. Discussion

In this method we assumed that the private z values are physically saved in the participants stations. This provides the scheme in danger with secured stations, therefore it perhaps convenient to have certain mnemonic system to allow participants to remember their private keys.

It is probable for one participant to masquerade as another. So it is essential that all authorizing stations trust one another, if not one authorizing station may acquire a benefit by creating it seems that a new authorized a transaction rather than itself. Alternatives of the Shamir secret sharing method are studied by Denning [23, 24, 25], which have their similarities in the scheme examined. These give better authority to certain participants than others. It is potential to change the scheme to employ polynomials in many variables. This can give benefits of overview in practical completion and of expanding the possible uses of the system.

5. Conclusions

This paper described the Shamir secret sharing scheme with the trap door characteristics of discrete logarithm mod an appropriate large prime as employed in the Diffie-Hellman secret exchange scheme. This combination permits participant's elements of a shared secret number are transmitted over a public means in a concealed type, so that the privacy of the elements and full of the shared number are protected. This denotes that the same private number can be employed repeatedly, on upcoming events. This scheme can be employed in many circumstances needing the operation of t participants from n. The case is given viewing that the scheme can be employed to authorize a transaction for instance signing a cheque.

References

[1] Shamir A. "How to Share a Secret", *Communications of the ACM*, vol. 22, pp.612-613, 1079

[2] Blakley G, "Safeguarding Cryptography Keys", *in Proceeding of AFIPS 1979 National Computer Conference,* vol. 48, pp. 313-317, 1979

[3] Chaum, D. "Computer Systems Establishment, Maintained, and Trusted by Mutually Suspicious Groups", tech. rep., Memorandum No. UCB/ERL M/79/10, University of California, Berkeley, CA, Feb. 1979.

[4] Ito M, Saito, A. and Nishizeki, T. "Secret Sharing Scheme Realizing General Access Structure", *in Proceeding IEEE Global Telecomm. Conference Globecom '87,* pp. 99-102, Washington: IEEE Communications Soc. Press, 1987.

[5] Benaloh J. and Leichter J., "Generalized Secret Sharing and Monotone Functions", *in Advances in Cryptology, Proceeding of CRYPTO '88, vol. 403 of Lecture Notes in Computer Science*, pp 27-35, Springer-Verlag, 1990.

[6] Simmons G., "How to Really Share a Secret", *in Advances in Cryptology – Proceedings of CRYPTO '88, vol. 403 of Lecture Notes in Computer Science,* pp. 390-448, Springer-Verlag, 1990.

[7] Simmons G., "Robust Shared Secret Schemes or How to be Sure You Have the Right Answer Even Though You Don't Know the Question", *in 18th Annual Conference on Numerical Mathematics and Computing,* Vol. 68 of Congresses Numeratiun, (Manitoba, Canada), pp. 215-248, Winnipeg, 1989.

[8] Simmons G., "Propositioned Shared Secret and Shared Control Schemes", *in Advances in Cryptology, Proceedings of EUROCRYPT '89,* vol. 434 of Lecture Notes in Computer Science, pp. 436-467, Springer-Verlag, 1990.

[9] Simmons G., "The Consequences of trust in Shared Secret Schemes", *Advances in Cryptology EUROCRYPT '93, Lecture Notes in Computer Science*, pp. 448-452, 1994.

[10] Stinson D. "An Explication of Secret Sharing Schemes", *Design Codes and Cryptography,* vol. 2, pp. 357-390, 1992

[11] Bertilsson M.and Ingemarsson I., "A construction of Practical Secret Sharing Schemes Using Linear Block Codes"

Advances in Cryptology, AUSCRYPT'92, Lecture Notes in Computer Science, pp. 67-79, 1993.

[12] Jackson W., Martin K., and O'Keefe C., "Efficient Secret Sharing Without a Mutually Trusted Authority" *Advances in Cryptology, EUROCRYPT '95, Lecture Notes in Computer Science,* pp.183-193, 1995

[13] Charnes C., Martin K, Pieprzyk J.and Ssfavi-Naini R., "Remarks on the Multiple Assignment Secret Sharing Scheme" *Information and Communications Security, ICIS '97, Lecture Notes in Computer Science,* pp.72-80, 1997

[14] Diffie w. and Hellman M. "New Directions in Cryptography", *IEEE Transactions on Information Theory,* IT-22, 1976

[15] Ammar M, and Musbah M, "Verification of Signatures of Bank Checks at very Low Resolutions and Noisy Images", *Applied Science University Journal*, Jordan, 2003.

[16] Ammar M, and Mousbah M. "A High Efficiency Method for Automatic Signature Verification", *Patent No. 09/453730, 2/12/1999,* USA, 2002.

[17] Musbah A, and Ammar M. "Function Structure and Operation of a Modern System for Authentication of Signatures of Bank Checks", *Pak. Information Technology Journal* 4(1), 2005, pp. 96-105.

[18] Trappe W and Washington L, "Introduction to Cryptography with Code Theory", 2nd edition Prentice Hall, 2006.

[19] Menezenes, P. van Oorschot and Vanstone S., "Handbook of Applied Cryptography", ARC Press, 1997

[20] R. Rivest, A. Shamir, and Adelman L., "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", *Communication of the ACM* 21, 2, 1978, 120-126.

[21] Aboud S., "Baghdad Method for Calculating Multiplicative Inverse", International *Conference on Information Technology,* Las Vegas, Nevada, USA, 2004, pp. 816-819.

[22] Aboud S. "Fraction – Integer Method (FIM) for Calculating Multiplicative Inverse", *Journal of Systemic, Cybernetics and Informatics,* Volume 2, Number 5, 2005, USA.

[23] Denning D. "Cryptography and Data Security", *Addison Wesley*, 1982.

[24] Kaliaperumal S. "Securing authentication and Privacy in ad hoc partitioned networks", *Applications and the Internet Workshops, Proceedings of 2003 Symposium on, IEEE*, 27-31 Jan. 2003, pp. 354-357.

[25] Stinson D. "Cryptography Theory and Practice," CRC 3rd 2006, pp. 117-149.