Threshold cryptosystems

Yvo Desmedt *Yair Frankel*
EE & CS Department
University of Wisconsin-Milwaukee
Milwaukee, WI 53201

Abstract. *In a society oriented cryptography it is better to have a public key for the company (organization) than having one for each individual employee [Des88]. Certainly in emergency situations, power is shared in many organizations. Solutions to this problem were presented [Des88], based on [GMW87], but are completely impractical and interactive. In this paper practical non-interactive public key systems are proposed which allow the reuse of the shared secret key since the key is not revealed either to insiders or to outsiders.*

1 Introduction

When a society oriented cryptosystem is used, an individual should be able to send an encrypted message to an organization without knowing the public key for every person within the receiving company. The destination organization should also be able to set up its own security policy to determine who can read the messages it receives. The cryptosystem must be designed such that the sender cannot circumvent the security policy, and the individual can send the message without knowing the policy [Des88].

Societies are organized in a multi-level structure [Sim88]. Organizations in a group oriented society must consider many issues when determining its security policy. Companies which are organized in a hierarchical structure (*e.g.*, board of directors, supervisors, executives) may require fewer individuals to read the messages if they are at a higher level. The security policy might also require that a specific number of individuals work together in order to be able to read the message.

Certainly when public key systems are used, it is not appropriate to use threshold schemes to determine the key. Otherwise all the individuals who work together can determine the key, or the one who receives all shares (shadows) may keep the key. This would be terrible in a public key system since modifying a public key is more difficult than modifying a secret key in a conventional system.

We propose a method in which every organization has a *single* public key. However for anyone within the company to read the message, they must get "enough" people with the appropriate number of shadows to calculate the message. Some of the earlier

solutions [Des88,GMW87] to this problem require an impractical ping-pong protocol. A solution using clerks is discussed in [Fra89]. This method modifies the decryption process of RSA by requiring each of the multiple clerks to do a partial calculation. The use of clerks, however, is not very robust. In our solution, which is practical and non-interactive (see Figure 1 and 2), the receiving company will allow all of its employees to view the ciphertext. Each shareholder will calculate their "partial result" separately and transmit the result to a designated individual. The designated individual will be able to decrypt the message using these partial results.

2 Background

To obtain the above we will adapt the ElGamal [ElG85] public key cryptosystem to meet our needs. This cryptosystem's security is based on the discrete log problem. (For an overview of the security of discrete logarithm, see [BvOV88,IBV85,Odl84]). It will be proven that even $t-1$ shadows are not sufficient for the calculation of the plaintext; and the system will also give no information on what the key is until t individuals act in collusion, both under the assumption that the ElGamal system is secure.

2.1 Threshold schemes

A (t,n) threshold scheme [Bla79,Sha79] does not reveal a secret S unless any t out of n participants, or *shadowholders*, work together. Each participant i will have a unique shadow K_i which he/she must keep secret. When any $t-1$ shadowholders work together, they can *not* receive any information about the secret S. In this way, a secret can be shared by many people. If a share is burned in a fire or someone forgets his/her shadow, there should be enough shareholders to recover the secret. In our system, a *modified shadow* is a result after making certain computations on the shadow. These modified shadows must also be secret. Let us explain the concept of a modified shadow with an example.

A (t,n) threshold scheme (see also [Den82]) based on Lagrange interpolation was developed by Shamir [Sha79]. To implement it, a polynomial f of degree $t-1$ is chosen in a field such that $f(0)$ will equal the secret S. Each of the shadowholders i will be given a secret $K_i = f(i)$. The reconstruction of the polynomial can be done with any subset B of t shadows, $K_{\pi_B(1)}, K_{\pi_B(2)}, \ldots, K_{\pi_B(t)}$ (for a given subset B of t out of n, $\pi_B : B \rightarrow \{1,2,\cdots,n\}$ and $|B| = t$). Hereto the following is calculated where the field corresponds to $GF(p)$:

$$f(x) = \sum_{s=1}^{t} K_{\pi_B(s)} \prod_{j=1, j\neq s}^{t} \frac{(x - x_{\pi_B(j)})}{(x_{\pi_B(s)} - x_{\pi_B(j)})} \pmod{p},$$

where the x_i are public. The *modified shadows* $a_{\pi_B(i)}$ in our scheme are computed such that $a_{\pi_B(s)} = K_{\pi_B(s)} \prod_{j=1, j\neq s}^{t} \frac{(0 - x_{\pi_B(j)})}{(x_{\pi_B(s)} - x_{\pi_B(j)})} \pmod{p}$. Giving away the modified shadows $a_{\pi_B(s)}$ to others has the same effect as giving away the shadows $K_{\pi_B(s)}$. It

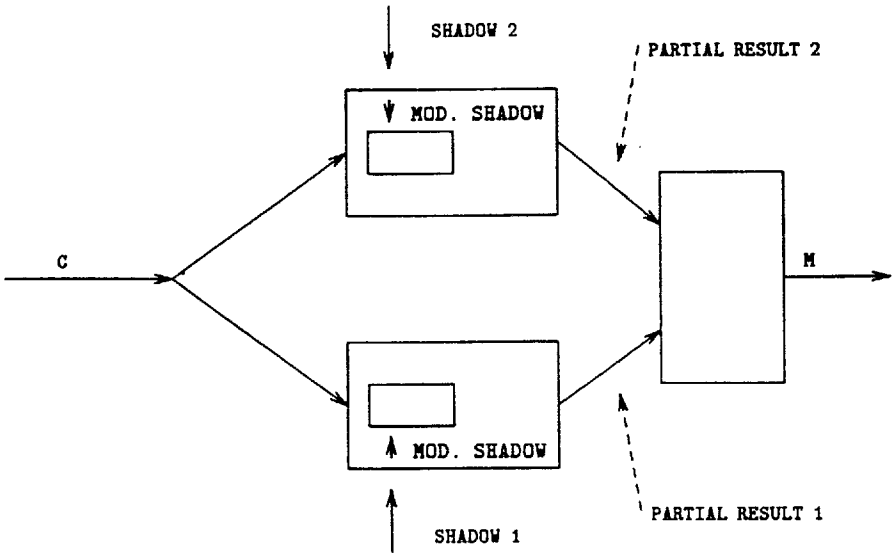

FIGURE 1. Our non-interactive solution

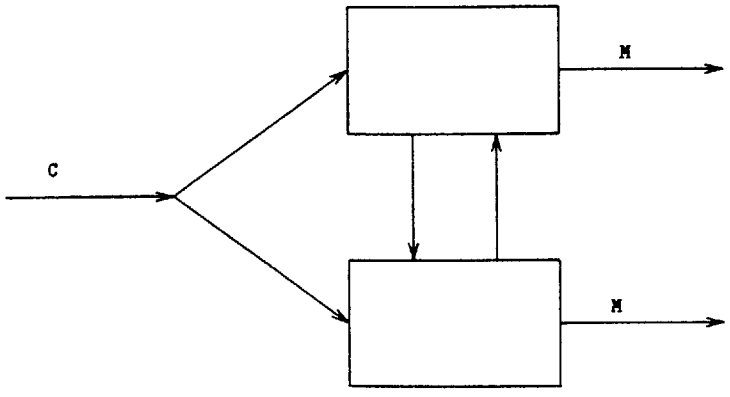

FIGURE 2. The impractical interactive solution

is imperative that each of the participant's modified shadow has the same security protection as the actual shadow.

2.2 ElGamal cryptosystem

The ElGamal cryptosystem is a public key extension of [DH76]. Its security is based on the discrete log problem. To use this cryptosystem, an element g (which should be a generator) is chosen in a finite field F_q. A trusted source will generate a random integer a within the the range $0 < a < q - 1$. Before destroying its copy of a, the trusted source will supply the company with the a as its private key and publish g^a as the public key. To transmit the message M, the sender will create a random integer k and send the tuple $C = (g^k, Mg^{ak})$. To decrypt the message, the receiver needs only raise g^k to the power a. The multiplicative inverse g^{-ak} of this result will be multiplied with the second entry of the tuple, Mg^{ak}, to get the message M.

3 Solutions

Both of the methods, which will be described to solve the problem, are implemented with the ElGamal cryptosystem. Each approach, however, will use a different threshold scheme to calculate a modified shadow for each participant. The modified shadow and the ciphertext will be used to get a *partial result* which is transmitted to a designated individual. This person will receive all the partial results and be able to calculate the message by using multiplication. In one of the approaches, any subset B of t individuals can perform the required operations.

3.1 The basic idea

Lets first modify the set-up phase in the ElGamal scheme. The one who has chosen the secret decryption key will give each shadowholder a shadow of a, where a is the secret decryption key in the ElGamal scheme. Once each shadowholder has his shadow a_i, the center can blow itself up. The encryption phase remains the same as described in 2.2. Let us now explain how decryption is performed.

Unless stated otherwise all the calculations to be performed in this section will be done in F_q. When a message is received, any subset B of t participants $\pi_B(s)$ will calculate their modified shadow $a_{\pi_B(s)}$ using threshold schemes explained in Section 3.2 and 3.3. The sum of these modified shadows will be congruent to the secret a mod $\phi(q)$ (a as in Section 2.1). Each $\pi_B(s)$ will then raise g^k by $-a_{\pi_B(s)}$ to get $g'_{\pi_B(s)}$ as their *partial result*. These partial results will be transmitted to the designated individual. To get M, the designated individual needs to multiply each of the $g'_{\pi_B(s)}$ together. This result g^{-ak} is multiplied with the second entry of the ciphertext (Mg^{ak}) to get the message M. An example using a $(3, n)$ threshold is given below. Let $\pi_B(1) = 1$, $\pi_B(2) = 2$, and $\pi_B(3) = 3$ such that $a_1 + a_2 + a_3 = a$ mod $\phi(n)$. Each of the participants will transmit their $g'_{\pi_B(s)}$ to a designated individual. That individual will perform the

following calculation:

$$\begin{aligned} Mg^{ak}\prod_{i=1}^{3} g'_{\pi_B(i)} &= Mg^{ak}g^{k(-a_1-a_2-a_3)} \\ &= Mg^{ak}g^{-ak} \\ &= M. \end{aligned}$$

To make this algorithm truly non-interactive, have each individual send $(g^{kK_{\pi_B(i)}}, \pi_B(i))$ to the designated individual. That individual can now exponentiate the first tuple by $\prod_{j=1,j\neq s}^{t} \frac{(0-x_{\pi_B(j)})}{(x_{\pi_B(s)}-x_{\pi_B(j)})}$ to generate $g^{ka_{\pi_B(i)}}$.

3.2 Using Lagrange interpolation for modified shadow generation

If q is a prime, then the calculations of the exponents is performed $\bmod\phi(q)$, which isn't a prime (except when $q = 3$ in which case we are not interested). This implies that Lagrange interpolation for calculating the modified shadows will not work. So choosing $q = 2^l$ is a solution *if* $q - 1$ is a *Mersenne prime* that is large enough. We, therefore, will perform the ElGamal system in $GF(2^l)$ where "depending on the level of security that is desired, it seems that the fields $GF(2^n)$ to be used ought to have n large, no smaller than 800 and preferably at least 1500" [Odl84, p. 226](*i.e.*, $l = 1,279$ or 2,203). The Lagrange interpolation will be done in Z_{q-1} where $q-1$ is a prime. The modified shadows $a_{\pi_B(s)}$ will be generated by each person as described in Section 2.1.

3.3 Using a geometry based threshold

Another (t, n) threshold scheme which can be used in our system is based on geometry. All n individuals in the organization are given a plane $s_{i,1}x_1 + s_{i,2}x_2 + \cdots + s_{i,t}x_t = K_i$ whose slope is public. These planes are created in such a manner that the intersection of t of them is at a secret point $S = [x_1, x_2, \ldots, x_t]$. The secret $a \bmod \phi(q)$ is the sum of the intersection coordinates. Each individual in the company will have their public $1 \times t$ matrix representing slope of their plane. During initialization a trusted center will multiply each $1 \times t$ slope matrix with the $t \times 1$ matrix to obtain each secret threshold K_i. Then the center will distribute each K_i to the correct individual i before destroying itself. To use the system, a subset B of t people generate each a $t \times t$ matrix T_B by putting each of their slope matrices on top of each other. The following relation holds:

$$\begin{vmatrix} s_{\pi_B(1),1} & \cdots & s_{\pi_B(1),t} \\ & \vdots & \\ s_{\pi_B(t),1} & \cdots & s_{\pi_B(t),t} \end{vmatrix} * \begin{vmatrix} x_1 \\ \vdots \\ x_t \end{vmatrix} = \begin{vmatrix} K_{\pi_B(1)} \\ \vdots \\ K_{\pi_B(t)} \end{vmatrix}.$$

Once the T_B matrix has been generated, it is inverted. To calculate the intersection one needs only to compute $S = T_B^{-1}K_B$. But this cannot be done in a straight forward manner since the entries in K_B are secret. As in the case of Lagrange interpolation, it is possible to calculate a modified shadow which will be used to determine the

partial result. This is done by having the participant who supplied $K_{\pi_B(i)}$ determine his modified shadow $a_{\pi_B(i)} = \sum_{r=1}^{t} K_{\pi_B(i)} s'_{\pi_B(r),\pi_B(i)} \bmod \phi(q)$ where $s'_{\pi_B(r),\pi B(i)}$ are from the T_B^{-1} matrix. For example, the person who supplied the $K_{\pi_B(2)}$ will multiply that value with each element in second column of T_B^{-1} and then add them all up to get his/her modified threshold. It is easy to see the the sum of all the modified thresholds will be congruent to a.

This method will only work if the matrix T_B is in $GL_t(R)$, thus has an inverse. The probability that a randomly chosen matrix is invertible is: $|GL_t(R)|$ / $|M_t(R)|$. If $R = Z_p$ where p is prime, then the above ratio is $(1 - \frac{1}{p})(1 - \frac{1}{p^2}) \cdots (1 - \frac{1}{p^n})$ (See [Kob87]). When the prime is large, this probability is high enough to insure that the matrix will be invertible. This implies that if q is a prime and the n planes are chosen randomly (by the center during initialization), there is a large probability that t users are not able to invert T_B and are unable to perform their job. In some cases, when excluding some collisions is not detrimental, this method is advantageous. If special planes are used, the above can be avoided. These are easy to generate if t and n are small. If ElGamal is used in $GF(2^l)$ with $2^l - 1$ a Mersenne prime, there is no problem.

4 Enhancements

There are two enhancements given which will increase the security and practicality of this scheme.

4.1 Avoiding Galois fields

Peralta has made the following suggestion to us to avoid the use of Galois fields for executing the ElGamal cryptosystem. Since $\phi(n)$ is even, use g^2 rather then g.

In more general terms, if we drop in this text the requirement that g is a generator, then our solution presented in previous paragraphs (using Lagrange) always works when Elgamal is executed in any (finite) *group* as long as the order of g (ord(g)) is a prime.

If ElGamal is done in a group and ord(g) = RS where S does not contain any factors less than n, it will always work when using g^R instead of g and when Lagrange is done mod S. This is true because ord(g^R) = S and the only inverses that must be calculated are those of $(x_i - x_j)$, which are between $-n$ and n since $0 < x_i, x_j \leq n$.

4.2 Anonymity

If in an organization the shadowholders are known to each other, the temptation for t of them to collude could be irresistible. As a result, they would find the secret key of the company, which will be continued to be used. To increase security, only pseudonyms of the shadowholders are known to outsiders. The shadowholders are then going to send their partial results in an untraceable way [Cha81,Cha88]. Anonymous threshold is evidently applicable in other situations. Other obvious measures can be

used to increase security such as using local organized encryption (using local public key system).

5 Proof of security

To prove its security we will use the concept of zero-knowledge [GMR89]. We only need the simulatability concept and not the interactive proof part. In our system, we have the following participants: a sender, a receiver and t shadowholders. Let us take a subset, V, and call those participants not in this subset P. Given a legitimate pair (message, ciphertext), we will prove that the interaction between the participants in P and the participants in V can be simulated (to be more precise, the probability distribution of the views can be simulated). To illustrate let us take an example in which P corresponds with one of the shadowholders. Because k is known (sender of message is part of V), it is trivial to simulate the interaction between P and V.

Informally, this implies that "no" extra information is leaked about $a_{\pi_B(s)}$ than $g^{ka_{\pi_B(s)}}$. If the discrete logarithm is hard, then the calculation of the modified shadow will also be hard.

6 Failures with RSA

The implementation of the Lagrange threshold scheme was modified and another one presented, in order to allow each person to calculate, on his own, the modified shadows. Other attempts to use the same approach with RSA failed mainly because $\phi(n)$ has to remain secret.

Lagrange interpolation cannot be used since $\phi(n)$ is even and calculations mod $\phi(n)$ does not form a field. Given persons i and j it can happen that $(i-j)$ is even and therefore not invertible. There is no way of selecting the number i in order for each person to get around this difficulty. The Chinese remainder interpolation method [AB80] is not possible since $\phi(n)$ must be revealed. Other methods using projective geometry cannot be used since all t individuals must provide their shadows to a designated person who will do the required calculation. The secret, however, will be known to that person.

7 Conclusion

We have shown a practical non-interactive scheme which allows an organization to use a public key system, yet still require t out of n people work together to read the message. Our scheme uses the ElGamal cryptosystem and modified threshold schemes to solve many of the problems associated with a group oriented society.

Recently we have been able to come up with a threshold signature scheme. This is a signature system where the signature can be verified by anyone knowing the public key of the signing company. To generate a signature requires t out of n individuals

and one interaction. The scheme is partially based on [GQ88].

ACKNOWLEDGMENTS

We wish to thank René Peralta for his suggestion given in Section 4.1. We thank Andrew Odlyzko for a discussion about $|GL_t(R)|/|M_t(R)|$ and Jean-Jacques Quisquater for pointing out his paper on signatures, discussed in the conclusion.

8 REFERENCES

[AB80] C. Asmuth and J. Bloom. A modular approach to key safeguarding. Technical report, Math Dept., Texas A & M Univ., College Station, Tx., 1980.

[Bla79] G. R. Blakley. Safeguarding cryptographic keys. In *Proc. Nat. Computer Conf. AFIPS Conf. Proc.*, pages 313–317, 1979. vol.48.

[BvOV88] I. F. Blake, P. C. van Oorschot, and S. Vanstone. Complexity issues for public key cryptography. In J. K. Skwirzynski, editor, *Performance Limits in Communication, Theory and Practice, NATO ASI Series E: Applied Sciences–Vol. 142*, pages 75–97. Kluwer Academic Publishers, 1988. Proceedings of the NATO Advanced Study Institute Il Ciocco, Castelvecchio Pascoli, Tuscany, Italy, July 7–19, 1986.

[Cha81] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–88, February 1981.

[Cha88] D. Chaum. The dining cryptographers problem: unconditional sender and recipient untraceability. *Journal of Cryptology*, 1(1):65–75, 1988.

[Den82] D. E. R. Denning. *Cryptography and Data Security.* Addison – Wesley, Reading, Mass., 1982.

[Des88] Y. Desmedt. Society and group oriented cryptography : a new concept. In C. Pomerance, editor, *Advances in Cryptology, Proc. of Crypto'87 (Lecture Notes in Computer Science 293)*, pages 120–127. Springer-Verlag, 1988. Santa Barbara, California, U.S.A., August 16–20.

[DH76] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT–22(6):644–654, November 1976.

[ElG85] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory*, 31:469–472, 1985.

[Fra89] Y. Frankel. A practical protocol for large group oriented networks. Presented at Eurocrypt'89, Houthalen, Belgium, to appear in: Advances in Cryptology. Proc. of Eurocrypt'89 (Lecture Notes in Computer Science), Springer–Verlag, April 1989.

[GMR89] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *Siam J. Comput.*, 18(1):186–208, February 1989.

[GMW87] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *Proceedings of the Nineteenth ACM Symp. Theory of Computing, STOC*, pages 218 - 229, May 25–27, 1987.

[GQ88] L. C. Guillou and J. J. Qisquater. A "pardoxical" identity–based signature scheme resulting from zero–knowledge. Presented at Crypto'88, Santa Barbara, California, U.S.A., to appear in: Advances in Cryptology. Proc. of Crypto'88 (Lecture Notes in Computer Science), Springer–Verlag, August 1988.

[IBV85] R.C.. Mullin I.F. Blake, R. Fuji-Hara and S.A. Vanstone. Computing logrithms in a finite field of characteristic two. *SIAM J. Alg. Disc. Meth.*, 5:276–285, 1985.

[Kob87] N. Koblitz. *A Course in Number Theory and Cryptology.* Springer–Verlang, 1987.

[Odl84] A. M. Odlyzko. Discrete logs in a finite field and their cryptographic significance. In N. Cot T. Beth and I. Ingemarsson, editors, *Advances in Cryptology, Proc. of Eurocrypt'84 (Lecture Notes in Computer Science 209)*, pages 224–314. Springer–Verlag, 1984. Paris, France April 1984.

[Sha79] A. Shamir. How to share a secret. *Commun. ACM*, 22:612 - 613, November 1979.

[Sim88] G. J. Simmons. How to (really) share a secret. Presented at Crypto'88, Santa Barbara, California, U.S.A., to appear in: Advances in Cryptology. Proc. of Crypto'88 (Lecture Notes in Computer Science), Springer–Verlag, August 1988.