A New Multiple Key Cipher and an Improved Voting Scheme

Colin Boyd
Communications Research Group
Department of Electrical Engineering
University of Manchester, Manchester, M13 9PL, UK

1. Introduction

At Eurocrypt 88 [1] we introduced the notion of a multiple key cipher and illustrated it with an example based on RSA which we called "multiple key RSA". In this paper we consider another multiple key cipher also based on a well known cryptographic function, exponentiation in a prime field. The important difference from multiple key RSA is that this function does not possess the trapdoor property. At the end of [1] we speculated that such functions may have useful applications and here we give as one illustration a new voting scheme.

One of the applications of multiple key RSA given in [1] was a simple voting scheme. Although that scheme allowed voters to verify that their votes were counted while maintaining anonymity with respect to other voters, it did not maintain anonymity of voting from the "government" or vote-issuing authority. Indeed, we suggested, as had others [5], that the two properties that voters could only vote once, and that votes were anonymous to the authority, were incompatible. However, at the same conference Chaum [3] proved us wrong with a counterexample.

As an application of our new multiple key cipher we give an improved version of our voting scheme which also has the property that Chaum's has. It could equally be implemented with multiple key RSA.

2. Multiple Key Ciphers

In [1] we defined a Multiple Key Cipher (MKC) to be an abelian group of transformations of some message space, M. In a particular application a set of transformations (parametrised by a set of keys) k1, k2, ...kn are chosen so that

k1 o k2 o ... o kn = identity(M).

The keys are distributed to the authorised users and then messages of the form k1 o k2 o ... o kj(M) can be written by a set of users possessing keys k1, k2, ... kj and read by a set of users possessing k(j+1), k(j+2), ..., kn, or their product.

With the trapdoor property it is not feasible to calculate inverses in the group of keys without knowledge of the trapdoor. The applications described in [1] exploited this property of multiple key RSA. Next we examine a MKC without this property.

3. The new MKC

The new MKC is simply that defined by the group of exponentiation transformations in a prime field with exponent prime to p-1. The message space is equal to the integers in the same field. This function has received much attention in modern cryptography starting with Diffie and Hellman's well known public key distribution scheme [6]. This MKC can properly be called a generalisaton of the cryptosystem proposed by Pohlig and Hellman in [8]. The important difference between this function and multiple key RSA, is the absence of a trapdoor. Thus if a is a known key defining the transformation

M |-> M**a mod p

then the inverse transformation with exponent b is easily

calculated by solving

$a.b \equiv 1 \bmod p-1.$

What can we say about the security of the multiple key cipher? Clearly a known plaintext attack is no harder than the discrete logarithm problem. In view of this we should certainly choose the prime p carefully as suggested by [8], for example $p = 2p'+1$ for some prime p'. According to the arguments from [8], a large number of plaintext/ciphertext pairs should not give an attacker any advantage.

Before going on to the main application we briefly mention that this MKC can also be used for schemes such as the selective distribution scheme from [1] if the keys are hidden from the users by tamperproofing.

In the selective distribution scheme each user has all keys except a single one which distinguishes the user. In order to distribute to a particular set of users the centre encrypts with exactly those keys that distinguish the users who are not to receive the information.

4. The improved Voting Scheme

As in Chaum's scheme [3] we assume the existence of a voting authority who will faithfully carry out elections and issue valid voting slips to every authorised voter exactly once. We assume the existence of some universally publicised large (enough) prime p so that it is universally accepted that the discrete logarithm problem in the field of integers modulo p is hard.

4.1 Choosing the parameters

In the first stage the voting authority selects three complementary keys a,b, and c. For example the first two can be chosen randomly (but coprime to p-1) and then the third selected so that

$a.b.c = 1 \bmod p-1.$

One of these keys, say a, is then made public for the purposes of this particular election. Note that there is a sufficient supply of numbers prime to p-1 as estimated in [8]; for example, when $p = 2p'+1$ the proportion of such numbers is about a half.

A primitive element e of the group of transformations prime to p-1 is also published. It may be a universal element for all elections as well as p.

4.2 Registration Phase

At the next stage each voter registers for the election by forming a block M consisting of a component of redundancy, a component of randomness and his voting intention. (Here is the crux of the difference between this scheme and our former scheme, in that there the block was formed by the authority.) The component of redundancy should be the same for all voters and could either be fixed for all elections or should be broadcast together with the key a during the first stage of the election. It should be large enough that random encryptions should have negligible chance of containing it.

The component of randomness should be chosen uniquely by the user for that particular vote. However it should also be chosen so that the whole voting block M is prime to p-1. As mentioned above this condition is easily satisfied and the randomness component needs to be large enough to ensure that many tries are possible until it can be satisfied. The voter's voting intention

may be specified in a selected number of bits depending on the number of possible outcomes of the election.

The voter now performs two encryptions on M before sending it to the authority for registration. First the voter forms

B = e**M mod p.

Then the voter "blinds" B [2]. This may be done by splitting the public key a as follows. The voter selects a1 at random (but prime to p-1) and then calculates a2 such that

a1.a2 = a mod p-1.

B is encrypted with a1 by the voter and sent to the authority. Thus

e**(M.a1) = B**a1 mod p

is sent to the authority. The point of the double encryption is to guarantee anonymity since all votes will be an exponentiation of e by a random power prime to p-1. In order to reduce computation M.a1 mod p-1 can be calculated first and then a single exponentiation is required.

The authority will require authentication of the user's identity which may be done in several ways which we do not consider here. The authority records the fact that the voter has registered in order that no voter may vote twice, and encrypts the voting block with the secret key b and returns B**(a1.b) mod p to the voter.

4.3 Voting Phase

Each voter completes his vote by encrypting the returned block

with a2 to form

((B**a1)**b)**a2 mod p = B**ab mod p.

and returning it anonymously to the authority together with the original block M. This may need to be done using a completely untraceable protocol such as that defined by Chaum in [4] in order to ensure that the vote is not traced.

The authority will encrypt the received anonymous block with c to recover the plaintext block. It will also check that B = e**M mod p. If the redundancy condition is satisfied then the authority will accept the vote. Note that in order to preserve anonymity all voters should register their votes before any voter returns an anonymous vote. The authority will publish all plain voting blocks with the result of the election. Each voter may then check that his random number is present to verify that his vote is counted. In order that voters may be able to distinguish their votes, the number of possible randomness components should be large in comparison with the number of voters. All identical votes are discarded by the authority to avoid repeat voting. If the randomness element is large enough this will result in disenfranchisment of any voters only with negligible probability.

5. Security of the Scheme

We consider the security of the scheme from two aspects. Firstly the difficulty of discovering the voting intentions of any voter, and secondly the difficulty to any voter of cheating to make more than one vote.

5.1 Anonymity of Votes

When considering the anonymity of voters we assume that during

the voting phase there is a perfectly untraceable protocol which allows the voter to deliver the vote to the authority. Then the only information available to the authority or any other entity in order to discover voters' intentions is the set of messages passed in the registration phase and the set of published votes. It is impossible for any entity to associate any published vote with any registered vote since the registered votes are all random exponentiations of e by a number prime to p-1. Therefore any registered vote could take the value of any other registered vote if the public key a had been split by the voter in a different way. Thus anonymity of votes is unconditionally guaranteed.

5.2 Forgery of Votes

Attempts to forge votes may be made both by legitimate voters who want to vote more than once and by outsiders who wish to influence the outcome. Forgers may try to break the system completely by finding the authority's secret keys or they may try to forge votes without finding the keys. In addition they may want to forge votes without even knowing their values in order to simply disrupt the election.

In order to forge a vote it must be possible to convince the authority that the forged vote delivered in the final phase is a registered vote. This means that the redundancy condition must be satisfied. Thus the forger must be able to construct a pair (M,e**(M.ab)) with M satisfying the redundancy condition.

For an outsider to discover the secret authority key he must use the random (X,X**b) pairs exchanged in the registration phase to find b, or the (M,e**(M.a.b)) pairs sent in the voting phase. In other words he must solve the discrete logarithm problem for this instance. For an insider to find b he may also have a (X,X**b) pair with X chosen during the registration phase. This

is obviously related to the discrete logarithm problem and is equivalent to finding the key for the Pohlig-Hellman cryptosystem with a chosen plaintext attack.

To forge a particular vote (including random number) means finding a M,e**(M.a.b) pair which is equivalent to breaking the Pohlig-Hellman cryptosystem without finding the secret key. However care must be taken to avoid attacks based on the multiplicative property of exponentiation. Thus for all integers k, if M,e**(M.a.b) is a valid pair then so is kM,e**(M.a.b)k. Therefore the redundancy condition should be chosen so that this is not possible.

6. Variations

As already mentioned the scheme could equally be implemented with multiple key RSA. In order to give further confidence in the difficulty of forging votes, one variation that might bear further investigation is to use multiple key RSA but with a modulus as defined by McCurley in [7] and then with 16 as the primitive element it follows that finding the key for an observer is equivalent to factoring the modulus as well as solving the discrete logarithm for the factors of the modulus.

A more radical variation is to dispense with the primitive element e and instead make each voting block M be a primitive element by suitable adjustment to the random part. (Checking this condition is harder than checking M is prime to p-1 but is straightforward if p-1 = 2p'.) Then M ** a1 mod p is sent by the voter to the authority who returns M ** a1.b mod p. Finally M ** ab mod p is delivered anonymously in the voting phase. This has the advantage that the vote does not have to be sent in cleartext since it is recovered completely by the authority. This variation may well be more secure against forgery since no plaintext/ciphertext pairs with the redundancy condition may be obtained.

7. Acknowledgement

I am grateful for the resources of the Data Security Laboratory, British Telecom, where I was when this work was started.

8. References

[1] C.A.Boyd, Some Applications of Multiple Key Ciphers, Proceedings of Eurocrypt 88, Springer-Verlag, 1988.

[2] D.L.Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Comm.ACM, 24,2,(1981), 84-88.

[3] D.L.Chaum, Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA, Proceedings of Eurocrpyt 88, Springer-Verlag, 1988.

[4] D.L.Chaum, The Dining Cryptographers Problem, Journal of Cryptology, 1,1,(1988), 65-75.

[5] J.D.Cohen & M.J.Fischer, A Robust and Verifiable Cryptographically Secure Election Scheme, Proceedings of IEEE Conference on Foundations of Computer Science, 1985.

[6] W.Diffie & M.Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, IT-22,6,1976.

[7] K.S.McCurley, A Key Distribution System Equivalent to Factoring, Journal of Cryptology, 1,2,(1988), 95-105.

[8] S.C.Pohlig & M.Hellman, An Improved Algorithm for Computing Logarithms over GF(p) and Its Cryptographic Significance, IEEE Transactions on Information Theory, IT-24,1,1978.