On Key Distribution and Authentication in Mobile Radio Networks

Choonsik Park, Kaoru Kurosawa, Tatsuaki Okamoto† and Shigeo Tsujii

Department of Electrical and Electronic Engineering,
Faculty of Engineering, Tokyo Institute of Technology
2-12-1 O-okayama, Meguro-ku, Tokyo, 152 Japan
Email: parkcs@ss.titech.ac.jp

† NTT Network Information Systems Laboratories,
Nippon Telegraph and Telephone Corporation
1-2356, Take, Yokosuka-shi, Kanagawa-ken, 238-03 Japan

Abstract. Mobile communication networks need public key cryptosystems that offer both low computation cost and user authentication. Tatebayashi et al. showed such a key distribution protocol for such networks at CRYPTO'89 based on low exponent RSA. This paper shows that their protocol is not secure. We also present a new secure and efficient key distribution protocol.

1 Introduction

Security in digital mobile communication systems has two major characteristics that must be be achieved, low computation cost and user authentication. Theoretically, A(lice) and B(ob) who have never met can share a cryptographic key by using a public key cryptosystem. The disadvantage of current public key cryptosystems is that encryption and decryption take too long. This disadvantage is serious in mobile communication networks because each user has very small computational power. The user authentication problem is also important to avoid charges of fraudulent usage. Another property of mobile communication networks, which is a good news for us, is that each user communicates with each other through a network center. Our goal is to design a public key cryptosystem for such networks that realizes both low computation cost and user authentication.

Until recently, however, only slight attention has been paid to this problem. The key distribution protocol shown by Tatebayashi et al.[1] at the 1989 CRYPTO conference is the only product known to the authors.

This paper first shows that their protocol is not secure. In the protocol of [1], A and B send initial information to the network center by using a low exponent RSA. However, we show that B can find the secret of A, needed for user authentication, easily by using this low exponent property. We then present a new key distribution protocol which realizes both low computation cost and user authentication by introducing a simple nonlinear function.

T. Helleseth (Ed.): Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 461-465, 1994.

Our technical contribution is as follows. Hastad [3] showed that we can solve the following simultaneous equations,

$$(\alpha_i X + \beta_i)^3 = c_i \pmod{N_i}, (i = 1, \cdots, 7),$$

for X in polynomial time if $\gcd(N_i, N_j) = 1$ for $i \neq j$ and if the number of equations is seven. Our analysis of [1] shows that we can obtain the following simultaneous equations,

$$(\alpha_i X + \beta_i)^3 = c_i \pmod{N}.$$

Since N is common for each i, Hastad's attack cannot be applied. We show a method for this problem which finds X in polynomial time if the number of equations is three. We propose a key distribution protocol which is secure for both attacks.

o denotes concatenation. $|X|$ denotes the bit length of X.

2 Review of Tatebayashi et al.'s scheme

The key distribution scheme of [1] was developed in the following process. First, network center C generates an RSA cryptosystem $e = 3$. Let

$$E(M) = M^3 \bmod N (= pq),$$

where N is the public key of C and p, q are the secret keys of C. Suppose that A and B want to share a key K. X and Y are opponents.

2.1 KDP1

Their basic protocol KDP1 is as follows.
[KDP1]

1. A chooses a random number r_1 and computes $Z_a = E(r_1)$.
   A sends Z_a to C.
2. B chooses a key K randomly and computes $Z_b = E(K)$.
   B sends Z_b to C.
3. C decrypts Z_a and Z_b. It computes $u = r_1 + K \bmod N$.
   C send u to A.
4. A computes the key K as $K = u - r_1 \bmod N$.

2.2 Simmons attack

Simmons showed one attack on KDP1.
[Simmons' attack]

1. X and Y monitor Z_b.
2. X chooses a random number R and computes $Z_x = E(R)$.
   X sends Z_x to C.
3. Y sends Z_b to C.
4. C then sends $u' = R + K \bmod N$ to X.
5. X can compute from u' and R the key K of A and B.

2.3 User authentication

We should also consider the problem of user authentication because it is important to avoid charges of fraudulent usage. To eliminate this problem, KDP1 can be modified as follows. Let f be a pseudorandom function which is the secret of C. Let ID_a and ID_b be the identity of A and B, respectively. In the preprocessing stage, C computes

$$S_a = f(ID_a), \quad S_b = f(ID_b)$$

C sends S_a to A secretly. Similarly, C sends S_b to B secretly.
[KDP1*]

1. A chooses a random number r_1 and computes $Z_a = E(S_a \circ r_1)$.
   A sends Z_a and ID_a to C.
2. B chooses a key K randomly and computes $Z_b = E(S_b \circ K)$.
   B sends Z_b and ID_b to C.
3. C decrypts Z_a and Z_b. It checks that $S_a = f(ID_a)$ and $S_b = f(ID_b)$.
   It the check passes, C computes $u = r_1 + K$ and send u to A.
4. A computes the key K as $K = u - r_1$.

It is easy to see that Simmons' attack can also be applied to KDP1*.

2.4 KDP2

Finally, Tatebayashi et al. developed the following protocol KDP2 which uses timestamps to avoid Simmons' attack.
[KDP2]

1. A chooses a random number r_1 and computes $Z_a = E(T_a \circ S_a \circ r_1)$, where T_a is A's timestamp information.
   A sends Z_a and his identity ID_a to the center C.
2. C decrypts the ciphertext and verifies the identity of A and the timestamp information. C then calls B.
3. B chooses a key K randomly and computes $Z_b = E(T_b \circ S_b \circ K)$, where T_b is B's timestamp information.
   B sends Z_b and his identity ID_b to the center C.
4. C checks T_b and S_b. C then computes $u = r_1 + K$ and sends u to A.
5. A computes K as $K = u - r_1$.

3 Attack on KDP2

This section shows that KDP2[1] is not secure. Actually, we show that B can find A's secret information S_a if B executes KDP2 with A three times.

After repeating KDP2 three times, B obtains

$$Z_{a_i} = E(T_{a_i} \circ S_a \circ r_{1_i}), \quad u_i = r_{1_i} + K_i, \quad (i = 1, 2, 3)$$

by listening to the conversation between A and the center C. B then gets

- r_{1i} from u_i and K_i.
- T_{ai} because it is the time at which A sends Z_{ai} to C.

The unknown constant is only S_a. Suppose that

$$|r_{1i}| = l, \quad |S_a| + |r_{1i}| = m,$$

Z_{ai} is written as follows.

$$\begin{aligned}(T_{a1} \times 2^m + S_a \times 2^l + r_{11})^3 &= Z_{a1} \ (\bmod N) \\ (T_{a2} \times 2^m + S_a \times 2^l + r_{12})^3 &= Z_{a2} \ (\bmod N) \\ (T_{a3} \times 2^m + S_a \times 2^l + r_{13})^3 &= Z_{a3} \ (\bmod N)\end{aligned}$$

Let $X_a = S_a \times 2^l$ and $Y_i = T_{ai} \times 2^m + r_{1i}$. We then obtain

$$\begin{aligned}X_a^3 + 3X_a^2 \times Y_1 + 3 \times (Y_1)^2 \times X_a &= Z_{a1} - (Y_1)^3 \ (\bmod N), \\ X_a^3 + 3X_a^2 \times Y_2 + 3 \times (Y_2)^2 \times X_a &= Z_{a2} - (Y_2)^3 \ (\bmod N), \\ X_a^3 + 3X_a^2 \times Y_3 + 3 \times (Y_3)^2 \times X_a &= Z_{a3} - (Y_3)^3 \ (\bmod N).\end{aligned}$$

The only unknown constant is X_a. We can view the above equations as linear simultaneous equations on X_a^3, X_a^2 and X_a. B can easily solve these equations in polynomial time. B can compute S_a from the solution X_a.

This attack works even if T_a, S_a and r_1 are interleaved. It also works for $E(M) = M^e \bmod N$ if e is small.

Similarly, A can find the secret information S_b of B because KDP2 is symmetric for A and B.

4 Proposed scheme

The reason why our attack succeeds is that B can obtain r_{1i} (A can obtain K_i) from the equation

$$u_i = r_{1i} + K_i. \tag{1}$$

We can prevent our attack if we introduce a nonlinear function h and modify eq.(1) as follows.

$$u_i = h(r_{1i}) + h(K_i).$$

For example, the following simple h is enough.

$$h(x_1 \circ x_2) = x_1 + x_2 \bmod 2^{l/2}$$

where $|x_1| = |x_2| = l/2$ and $\circ$ denotes concatenation.

It is information theoretically impossible to determine x_1 and x_2 from $x_1 + x_2$. Based on this observation, we propose a key distribution protocol as follows.

(E is the public key of the center. See the beginning of section 2.)

1. A chooses random numbers (r_1, r_2) such that $|r_1| = |r_2| = l/2$ and computes $Z_a = E(T_a \circ S_a \circ r_1 \circ r_2)$, where T_a is A's timestamp information.
   A sends Z_a and his identity ID_a to the center C.

2. C decrypts the ciphertext and verifies the identity of A and the timestamp information. C then calls B.
3. B chooses (K_1, K_2) randomly and computes $Z_b = E(T_b \circ S_b \circ K_1 \circ K_2)$, where T_b is B's timestamp information.
   B sends Z_b and his identity ID_b to the center C.
4. C checks T_b and S_b. C then computes $u = r_1 + r_2 + K_1 + K_2 \mod 2^{l/2}$ and send u to A.
5. The session key is given by $K = K_1 + K_2 \mod 2^{l/2}$. A computes K as $K = u - r_1 - r_2 \mod 2^{l/2}$.

We can use the Rabin cryptosystem instead of RSA because the plaintext has a special data structure.

Security

Suppose that the proposed protocol is executed I times. Let the ith parameters be $Z_{ai}, T_{ai}, r_{1i}, r_{2i}, Z_{bi}, T_{bi}, K_{1i}$ and K_{2i}. B knows that

$$Z_{ai} = E(T_{ai} \circ S_a \circ r_{1i} \circ r_{2i}).$$

He knows the values of Z_{ai}, T_{ai} and $r_{1i} + r_{2i} \pmod{2^{l/2}}$ by monitoring A's communication. However, he cannot know $r_{1i} \circ r_{2i}$. ($\circ$ denotes concatenation.) Therefore, what B can have is the following type of equations,

$$(\alpha_i X + Y_i + \beta_i)^3 = c_i \pmod{N}, (i = 1, \cdots, I),$$

where $X = S_a, Y_i = r_{1i} \circ r_{2i}$, $\alpha_i = 2^l$, $\beta_i = T_{ai} \times 2^{(l+|S_a|)}, c_i = Z_{ai}$. Here, X and Y_i are unknown variables. α_i, β_i and c_i are known values.

Then, the number of equations is I and that of unknown variables is $I + 1$. Hence, B cannot find $X(= S_a)$. Similarly, A cannot find S_b.

References

1. Tatebayashi, M., Matsuzaki, N., Newman, Jr., D.B.: Key Distribution Protocol for Digital Mobile Communication Systems. Advances in Cryptology. Proceedings of Crypto'89 (1989) 324-334
2. Moore, J. H.: Protocol Failures in Cryptosystems. Proc. of IEEE, Vol.76, No.5 (1988) 594-602
3. Hastad,J.: On using RSA with Low exponent in a public key network. Advances in Cryptology, Proceedings of Crypto'85 (1985)403-408
4. Simmons,G.J.: A 'weak' privacy protocol using the RSA cryptoalgorithm. Cryptologia, Vol.7 (1983) 180-182
5. Beller,M.J. Chang,L.F., Yacobi,Y. : Privacy and Authentication on a Portable Communication System. IEEE GLOBECOM '91 conference (1991) 1922 - 1927