Methods to Forge ElGamal Signatures and Determine Secret Key

Jing-mei Liu   Xiang-guo Cheng   Xin-mei Wang
National Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an, 710071
jmliu@mail.xidian.edu.cn   chengxiangguo@hotmail.com   xmwang@xidian.edu.cn

Abstract

We present a new method to forge ElGamal signatures with the cases that the secret key parameters of the system are not known under the chosen signature messages. The attacker can forge the signature substituting the right signature, and also attack the right secret key without depending on the computation of discrete logarithm. With the attacking probability cryptanalysis, it is found that the cryptosystem can be attacked successfully in some conditions.

Keywords: ElGamal; Signature; Cryptanalysis

1. Introduction

ElGamal designed out an inspired digital signature scheme[1,2] in 1984. Similar to the case of the ElGamal public-key cryptosystem ingenious great follow-up research and application interests which last to this day, the ElGamal signature scheme is also the origin of many further digital signature schemes which belong to the family of ElGamal-like signature schemes. The squared ElGamal signature scheme is selected as the standard of signature by NIST. ElGamal's digital signature scheme relies on the difficulty of computing discrete logarithm in the multiplicative group Z_p^*, and can therefore be broken if the computation of discrete logarithms is feasible. However, the converse has never been proved. Bleichenbacher [3] discovers the following attack if Bob would accept signatures where r is larger than p. In this paper we show that it is sometimes possible to forge signatures under the chosen cipher-texts without breaking the underlying discrete logarithm problem. With the cryptanalysis of attacking probability, it is found that the cryptosystem can be attacked with a high probability. This shows that the ElGamal signature scheme and some variants of the scheme must be used very carefully.

This paper is organized as follows. Firstly we review the ElGamal signature scheme. In Section 3 we present the cryptanalysis of ElGamal signature scheme and its attacking probability. We show that signatures can be forged under those chosen signature messages, and one method can determine the secret key of the right signer.

2. The ElGamal Signature Scheme

ElGamal's signature scheme can be described as follows.

Key Setup

To set up a user's key material, user Alice performs the following steps:

1. choose a random prime number p;
2. compute a random multiplicative generator element g of Z_p^*;
3. pick a random number $a \in Z_p^*$ as her private key;
4. compute her public key by $y \equiv g^a \bmod p$;
5. publicize p, g, y as her public key, and keep a as her private key.

Signature Generation

To create a signature of message $M \in Z_p^*$, Alice computes the Hash value $H(M)$ of M, picks a random number $k \in Z_{p-1}^*$ (i.e., k< p-1 and *gcd*(*k*; *p*-1) = 1) and creates a signature pair (r; s) where

$$r = g^k \bmod p$$

$$s = (H(M) - ar)k^{-1} \bmod (p-1)$$

(* k^{-1} can be computed using the extended Euclid's algorithm.)

Finally $Sig_k(M,k) = S = (r,s)$ is the signature pair, and Alice sends the signature $M,(r,s)$ to the receiver.

Signature Verification

Let Bob be a verifier who knows that the public-key material (p, g, y) belongs to Alice. Given a

1550-445X/06 $20.00 © 2006 IEEE

message-signature pair ($M,(r,s)$), Bob's verification procedure is as follows:

1. He computes the Hash value $H(M)$ of the message M

2. $Verify_{(g,y,p)}(M,(r,s)) = True \quad if$

$$r < p \quad and \quad y^r r^s \equiv g^{H(M)} \bmod p$$

The ElGamal signature scheme can be broken when discrete logarithms in Z_p^* can be computed. The prime p must therefore be chosen large enough to prevent the computation of discrete logarithms by the number field sieve [4] and p - 1 must contain at least one large prime factor to disable the algorithm of Pohlig and Hellman **[5].**

3.Cryptanalysis against ElGamal Signature Scheme

ElGamal signature scheme is insecure against the forgery in the case of known signature messages. The attacking difficulty of ElGamal signature scheme is based on the computation of discrete logarithm, so we innovate a new way avoiding computing the discrete logarithm to cryptanalyze this cryptosystem with different methods. More cryptanalysis of ElGamal signature scheme can refer to papers [6-10].Then malice can forge a new signature on an arbitrary message M' as follows:

Method A: Forge *r*

(1)Malice selects the right signature family $M,(r,s)$ to compute y^r using r in the right signature family $M,(r,s)$ and find which signature satisfies the following relationship that $y^r \equiv 1 \bmod p$, then the signature is determined.

(2)Compute $m = H(M')(H(M))^{-1} \bmod p$

(3)Compute $r' = r^m \bmod p$, keep $s' = s$ invariable.

Then $M',(r',s')$ is the forgery of the ElGamal signature, and it is routine to go through the following congruence:

$$y^{r'}(r')^{s'} = g^{ar^m} g^{mk(H(M)-ar)k^{-1}} \bmod p$$
$$= g^{ar^m} g^{mH(M)} g^{-arm} \bmod p$$
$$= g^{ar^m} g^{H(M')H(M)^{-1}H(M)} g^{-arm} \bmod p$$
$$= g^{ar^m} g^{H(M')} g^{-arm} \bmod p$$

because $\quad y^r \equiv 1 \bmod p \Rightarrow g^{ar} \equiv 1 \bmod p$

then $(g^{ar})^{r^{m-1}} \equiv 1 \bmod p$, $(g^{ar})^{(-m)} \equiv 1 \bmod p$

so $\quad g^{ar^m} g^{H(M')} g^{-arm} \bmod p = g^{H(M')} \bmod p$

It should be noted that this attack succeeds because of the special choice of r which avoiding the discrete logarithm problem in Z_p^*.

Method B : Forge *s*

(1)Malice selects the right signature family $M,(r,s)$ and compute y^r to find which signature satisfies the equation that $y^r \equiv 1 \bmod p$, then just the signature is determined.

(2)compute $m = H(M')(H(M))^{-1} \bmod p$

(3)compute $s' = m(H(M) - ar)k^{-1} \bmod (p-1)$, keep $r' = r \bmod p$ invariable.

Then $M',(r',s')$ is the forgery of the ElGamal signature, and it is routine to go through the following congruence:

$$y^{r'}(r')^{s'} = g^{ar} g^{mk(H(M)-ar)k^{-1}} \bmod p$$
$$= g^{ar} g^{mH(M)} g^{-arm} \bmod p$$
$$= g^{ar} g^{H(M')} g^{-arm} \bmod p$$

because $\quad y^r \equiv 1 \bmod p \Rightarrow g^{ar} \equiv 1 \bmod p$

then $\quad (g^{ar})^{(-m)} \equiv 1 \bmod p$

so $\quad g^{ar} g^{H(M')} g^{-arm} \bmod p = g^{H(M')} \bmod p$

Method C: Forge *r,s*

(1)Malice selects the right signature family $M,(r,s)$ and compute y^r to find which signature satisfies the following equation $y^r \equiv 1 \bmod p$, then just the signature is selected.

(2)compute $m = [H(M')(H(M))^{-1}]^{1/2} \bmod p$

(3)compute $\quad r' = r^m = g^{mk} \bmod p$

$$s' = m(H(M) - ar)k^{-1} \bmod (p-1)$$

Then $M',(r',s')$ is the forgery of the ElGamal signature, and it is routine to go through the following congruence:

$$y^{r'}(r')^{s'} = g^{ar^m} g^{m^2k(H(M)-ar)k^{-1}} \bmod p$$
$$= g^{ar^m} g^{m^2H(M)} g^{-arm^2} \bmod p$$
$$= g^{ar^m} g^{H(M')H(M)^{-1}H(M)} g^{-arm^2} \bmod p$$
$$= g^{ar^m} g^{H(M')} g^{-arm^2} \bmod p$$

because $\quad y^r \equiv 1 \bmod p \Rightarrow g^{ar} \equiv 1 \bmod p$

then $\quad g^{ar^m} \equiv 1 \bmod p$, $(g^{ar})^{(-m^2)} \equiv 1 \bmod p$

so $\quad g^{ar^m} g^{H(M')} g^{-arm^2} \bmod p = g^{H(M')} \bmod p$

Let us to see the attacking probability cryptanalysis of previous three attacking methods.

It can be noted that the attacking key problem is to determine $y^r = g^{ar} \equiv 1 \bmod p$, that is $(p-1) \mid ar$ using

IEEE COMPUTER SOCIETY

Fermat theorem $g^{p-1} \equiv 1 \bmod p$, g is prime to p in Z_p^*. That is $\gcd(a, p-1) \neq 1$ or $\gcd(r, p-1) \neq 1$. For a is the secret key and is an unknown quantity, so we begin the cryptanalysis with r.

Let $\{\gamma\} = \{r : r \mid p-1)\}$, then the probability of r emergence is $p(r) = 1/_{p-1-\Phi(p-1)}$, in which $\Phi(p-1)$ denotes the Euler's values of $p-1$.If one value r_i in $\{\gamma\}$ is referred, then the set $\beta_i = \{a_i, g^{a_i r_i} = 1 \bmod p\}$, $i = 1, 2, \cdots, \| \beta \|$ is determined. If the number of all the different elements in the whole sets is denoted as num, then the probability of multiplication ar which satisfies the equation $(p-1) \mid ar$ is

$$p(ar) = \frac{num}{p-1-\Phi(p-1)}.$$

Method D: Determine secret key *a*

An innovate method to forge the right ElGamal signature scheme is to attack the secret key which does little before. The process is as followed.

(1)Malice selects the right signature family $M, (r, s)$ and compute y^r to find which signature satisfies the following equation $y^r \equiv 1 \bmod p$, then the just signature is selected.

(2)Compute t in the equation $y^r = g^{ar} = g^{t(p-1)}$ according to the following method:

```
t=0;
While ( $y^r \neq 0$ ) {
    $y^r = y^r / g^{p-1}$;
    t=t+1;}
```

Because $y^r = g^{ar} \equiv 1 \bmod p$, p is a big prime, g a random multiplicative generator element of Z_p^*, and according to the Fermat theorem $g^{(p-1)} \equiv 1 \bmod p$, g is prime to p in Z_p^*, $(p-1) \mid ar$ is derived. Finally $ar = t(p-1)$, or $a = t(p-1)r^{-1}$, and the secret key is determined. Let us to see the following attacking probability cryptanalysis.

It can be noted that the attacking key problem is still to determine $y^r = g^{ar} \equiv 1 \bmod p$, that is $(p-1) \mid ar$, and $\gcd(a, p-1) \neq 1$ or $\gcd(r, p-1) \neq 1$. For a is the secret key and is an unknown quantity, so we begin the cryptanalysis with r. Let $\{\beta\} = \{r : r \mid p-1)\}$, then the probability of r emergence is $p(r) = 1/_{p-1-\Phi(p-1)}$, in which $\Phi(p-1)$ denotes the Euler's values of $p-1$. If the value r is referred, then the secret key a is determined. Therefore the probability of multiplication ar which satisfies the equation $(p-1) \mid ar$ is $p(ar) = 1/_{[p-1-\Phi(p-1)]}$.

4. Conclusions

The results presented in this paper show that ElGamal signatures can be forged in some cases without knowing the secret key. Under the case of chosen cipher-texts, the secret key can also be determined which is a challenge to ElGamal signature scheme. The attacks presented can be avoided by restricting the values of the signatures that are considered to be valid. So far the ElGamal digital signature scheme has not been broken but it has shown that the system must be used very carefully.

5. References

[1] A.B. Smith, C.D. Jones, and E.F. Roberts, “Article Title”, *Journal*, Publisher, Location, Date, pp. 1-10.

[2] Jones, C.D., A.B. Smith, and E.F. Roberts, *Book Title*, Publisher, Location, Date.

[1]Rivest.R.L, Shamir.A.,and Adleman.L.M,” A method for obtaining digital signatures and public key cryptosystems,”Communications of the ACM, Vol.21, No.2, Feb 1978, pp120-126.

[2]ElGamal, T., “ A public-key cryptosystem and a signature scheme based on discrete logarithms,’ Advances in Cryptology-CRYPTO’84 Proceedings, Springer-Verlag 1985,pp.10-18.

[3]D. Bleichenbacher. Generating ElGamal signature without knowing the secret key. In U. Maurer, editor, Advances in Cryptology Proceedings of EUROCRYPT'96, Lecture Notes in Computer Science 1070, pages 10-18. Springer-Verlag,1996.

[4]D. M. Gordon. Discrete logarithms in GF(p) using the number field sieve. SIAM,J. Disc. Math., 6(1): 124-138, February 1993.

[5]S. C. Pohlig and M. E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. Inform. Theory, IT-24: 106-110, January 1978.

[6]Yiannis Tsiounis, Moti Yung. On the Security of ElGamal Based Encryption, Springer-Verlag Volume 1431,1998, page 117

[7]Markus Jakobsson, Ari Juels. Addition of ElGamal Plaintexts**.** Springer-Verlag Volume 1976,2000, page 346

[8]Daniel Bleichenbacher.Generating ElGamal Signatures without Knowing the Secret Key**.** Springer-Verlag Volume Volume 1070,1996, page 10

[9]Lgor E. Shparlinski. On the Uniformity of Distribution of the ElGamal Signature. Springer-Verlag Volume 13, Number 1.page 9 –16.

[10]Lucas C. Ferreira, Ricardo Dahab. Optimistic Blinded-Key Signatures for ElGamal and Related Schemes. Springer-Verlag Volume 3824, 2004,page 254.