ElGamal公钥密码体制简介

熊 虎

信息与软件工程学院

xionghu.uestc@gmail.com

ElGamal公钥密码体制历史

ElGamal公钥密码体制历史

ElGamal公钥加密体制原理

数字签名体制介绍

ElGamal公钥密码体制历史

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-31, NO. 4, JULY 1985

A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms

TAHER ELGAMAL, MEMBER, IEEE

Abstract—A new signature scheme is proposed, together with an implementation of the Diffie–Hellman key distribution scheme that achieves a public key cryptosystem. The security of both systems relies on the difficulty of computing discrete logarithms over finite fields.

I. Introduction

In 1976, Diffie and Hellman [3] introduced the concept of public key cryptography. Since then, several attempts have been made to find practical public key systems (see, for example, [6], [7], [9]) depending on the difficulty of solving some problems. For example, the Rives–Shamir–Adleman (RSA) system [9] depends on the difficulty of factoring large integers. This paper presents systems that rely on the difficulty of computing logarithms over finite fields.

Section II shows a way to implement the public key distribution scheme introduced by Diffie and Hellman [3] to encrypt and decrypt messages. The security of this system is equivalent to that of the distribution scheme. Section III introduces a new digital signature scheme that depends on the difficulty of computing discrete logarithms over finite fields. It is not yet proved that breaking the system is equivalent to computing discrete logarithms. Section IV develops some attacks on the signature scheme, none of which seems to break it. Section V gives some properties of the system. Section VI contains a conclusion and some remarks.

Hence both A and B are able to compute K_{AB}. But, for an intruder, computing K_{AB} appears to be difficult. It is not yet proved that breaking the system is equivalent to computing discrete logarithms. For more details refer to [3].

In any of the cryptographic systems based on discrete logarithms, p must be chosen such that $p-1$ has at least one large prime factor. If $p-1$ has only small prime factors, then computing discrete logarithms is easy (see [8]).

Now suppose that A wants to send B a message m, where $0 \le m \le p-1$. First A chooses a number k uniformly between 0 and $p-1$. Note that k will serve as the secret x_A in the key distribution scheme. Then A computes the "key"

$$K \equiv y_B^k \bmod p, \tag{1}$$

where $y_B \equiv \alpha^{x_B} \bmod p$ is either in a public file or is sent by B. The encrypted message (or ciphertext) is then the pair (c_1, c_2), where

$$c_1 = \alpha^k \bmod p \qquad c_2 = Km \bmod p \tag{2}$$

and K is computed in (1).

Note that the size of the ciphertext is double the size of the message. Also note that the multiplication operation in (2) can be replaced by any other invertible operation such as addition mod p.

The decryption operation splits into two parts. The first step is recovering K, which is easy for B since $K \equiv (\alpha^k)^{x_B}$ [illegible] mod p, and x_B is known to B only. The second step

ElGamal公钥加密体制原理

- ElGamal公钥密码体制历史
- ElGamal公钥加密体制原理
- Diffie-Hellman密钥协商
- 数字签名体制介绍
- ElGamal与RSA的区别
- ElGamal公钥密码体制现状

ElGamal公钥加密体制原理

密钥生成：

p，一个较大素数

g，Z_p^* 中的生成元

$\alpha \in Z_{p-1}, \beta = g^{\alpha} mod\ p$

p, g, β 为公钥；α 为私钥

加密：

随机生成一个秘密数 k，$k \in Z_{p-1}$ 。

$E(x,k) = (r,s)$，其中

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

$$s = x\beta^k mod\ p$$

解密：$D(r,s) = s(r^{\alpha})^{-1} mod\ p = xg^{\alpha k} g^{-\alpha k} mod\ p = x$

数字签名体制介绍

- ElGamal公钥密码体制历史
- ElGamal公钥加密体制原理
- Diffie-Hellman密钥协商
- 数字签名体制介绍
- ElGamal与RSA的区别
- ElGamal公钥密码体制现状

ElGamal - 签名

密钥生成：与加密相同.

签名：

随机产生，密钥 $k \in Z_{p-1}^{*}$。

$S(m,k)=(r,s)$，其中

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

$$s = (m - ra)k^{-1} mod(p-1)$$

即 $(m = ra + sk)$

验证：

是否 $\beta^r r^s \equiv g^m (mod\ p)$?

$$\beta^r r^s = g^{ar} g^{k(m-ra)k^{-1}} = g^{ar+(m-ra)} = g^m mod\ p$$

ElGamal - 签名

安全:

只有知道α可以签名的人，才能被β所证实。

从β求解α，或从r, m, p求解s为离散对数。

伪造的其他方式？未知。

相同的K不能重复使用。

变化:

许多变体，通过改变“签名方程”，

$$m = ra + sk$$

例如， DSA的方式:

$$m = -ra + sk$$

验证: $\beta^r g^m \equiv r^s (mod\ p) ? (\equiv g^{m+ra})$

谢谢！