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

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 $K \equiv (\alpha^k)^{x_B}$ $= \alpha^{x_B} \bmod p$, 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

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

$\{p, g, \beta\}$为公钥；α 为私钥

加密：

随机生成一个秘密数 k，$k \in Z_{p-1}$ 。

$\mathrm{Enc}(x, k) = (r, s)$，其中

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

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

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

ElGamal公钥加密体制原理

明文 x 被一个随机因素隐藏，$g^{\alpha k} \bmod p$。

DH问题：给定 g^{α}，$g^{k} \bmod p$ 什么是 $g^{\alpha k} \bmod p$？

p, g 是公开的。然后，就可以预先计算出 $g^{\alpha k} \bmod p$。

不应重复使用相同的 k。

性能：

-加密：两次取幂指数运算。

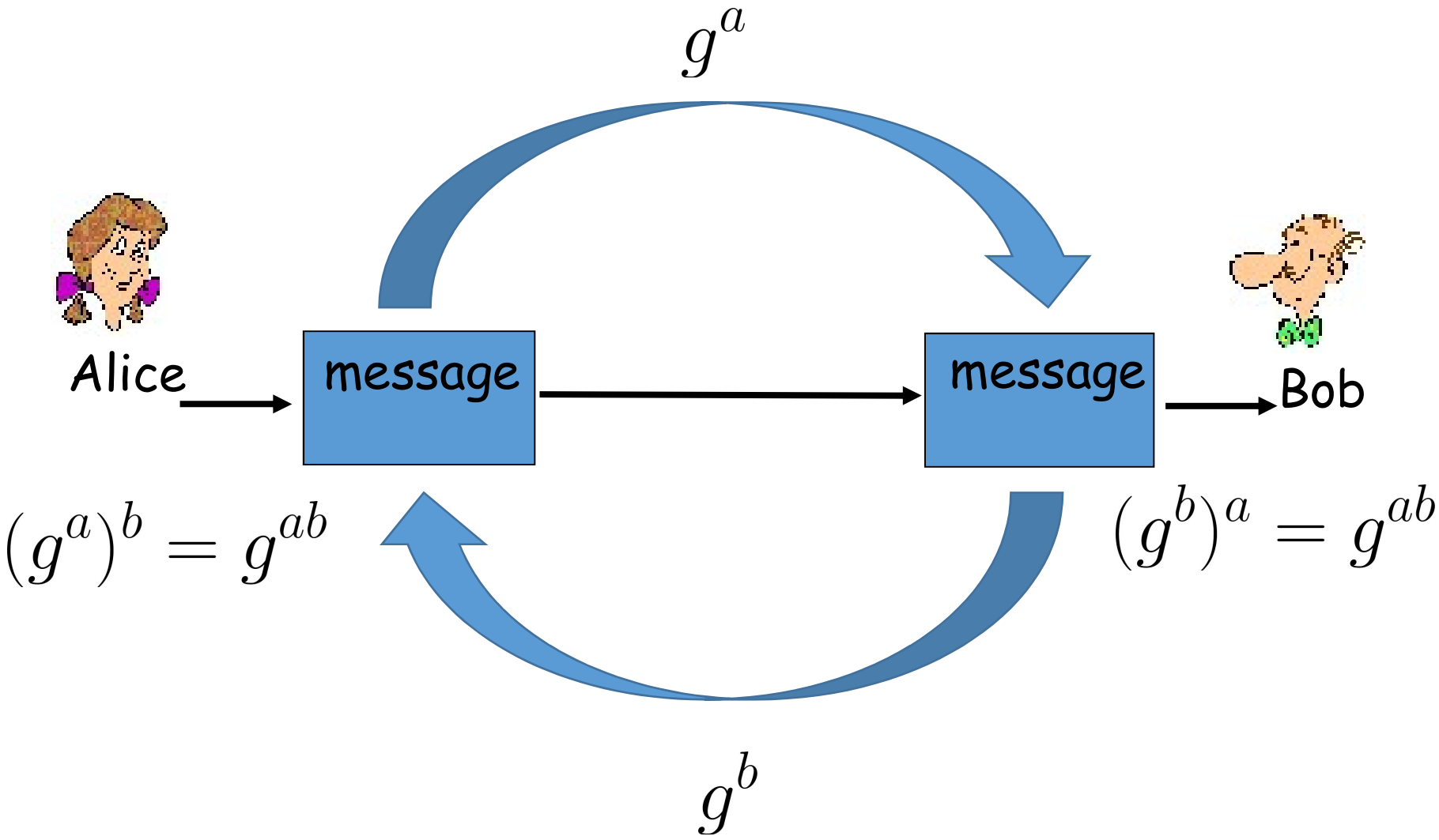
-解密：一次取幂指数运算，一次置换。

大小：密文的大小是明文的两倍大。

Diffie-Hellman密钥协商

- 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

Diffie-Hellman密钥协商



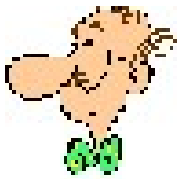
Diffie-Hellman密钥协商

Alice

message

中间人攻击

message



Bob

g^a

g^b

$(g^a)^b = g^{ab}$

$(g^b)^a = g^{ab}$

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

参数生成：与加密相同.

签名：

随机产生，密钥 $k \in Z_{p-1}^{*}$。

$\mathrm{Sign}(m,k)=(r,s)$，其中

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

$$s = (m - r\alpha)k^{-1} \bmod (p-1)$$

即 $(m = r\alpha + sk)$

验证：

是否 $\beta^r r^s \stackrel{?}{=} g^m (\bmod\ p)$ ；

$$\beta^r r^s = g^{\alpha r} g^{k(m-r\alpha)k^{-1}} = g^{\alpha r+(m-r\alpha)} = g^m \bmod p$$

ElGamal - 签名

安全:

只有知道 α 可以签名的人，才能被 β 验证。

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 不能被重复使用。

变化:

许多变体，通过改变“签名方程”，

$$m = r\alpha + sk$$

例如， DSA的方式:

$$m = -r\alpha + sk$$

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

Schnorr 签名

$q|(p-1)$ 为素数,而且, $g \in Z_p^*$ 且阶为 q。

Schnorr 群: 在 Z_P^*中， 由g产生的子群, 素数阶为 q。

$$< g >= \{1, g, g^2, \cdots, g^{q-1}\}$$

实际上: q可以比p短得多（例如:160 vs 1024比特），DLP在$< g >$ 中的强度保持不变。

Schnorr 签名

密钥生成：素数p，素数$q|(p-1)$，选取$g \in Z_p^*$且阶为 q 。
哈希函数：$H:\{0,1\}^* \to Z_q$ 。

密钥：$\alpha \in Z_q$ 是私钥；$\beta = (g^\alpha \bmod p)$ 是公钥.

签字：(r,s) 其中

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

$$r = H(M||v)$$

$$s = (k - r\alpha) \bmod q$$

验证：

$$v' = g^s \beta^r \bmod p$$

$$r = H(M||v')?$$

优点：签名长度和复杂度降低

数字签名算法(DSA)

美国国家安全局指定的数字签名标准。

思想基于ElGamal & Schnorr

专利已过期（ElGamal）

加密方案并未被指定为国家标准

争议：

ElGamal没有像RSA一样经受密码攻击分析？？？

验证开销较大

行业已经广泛部署了RSA

数字签名算法(DSA)

参数： 与Schnorr相同.

签名： (r, s) 其中

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

$$r = v \bmod q$$

$$s = (H(M) + r\alpha)k^{-1} \bmod q$$

验证：

$$v' = g^{H(M)S^{-1}} \beta^{rs^{-1}} \bmod p \quad ?$$

$$r = v' \bmod q$$

(与Schnorr比较?)

ElGamal与RSA的区别

- 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与RSA的区别

数学困难问题

公开参数设置

ElGamal公钥密码体制现状

- 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

椭圆曲线加密系统

广义离散日志问题：

对于任何群$(G,\cdot)$，对于$x \in G$，定义

$$x^n = x \cdot x \cdots x \quad (\text{n 次})$$

DLP：对于$y = x^n$，给定x, y，那么n是多少？

Zp上的椭圆曲线：

点集 $(x,y) \in Z_p \times Z_p$ 满足

$$y^2 \equiv x^3 + ax + b (\text{mod } p)$$

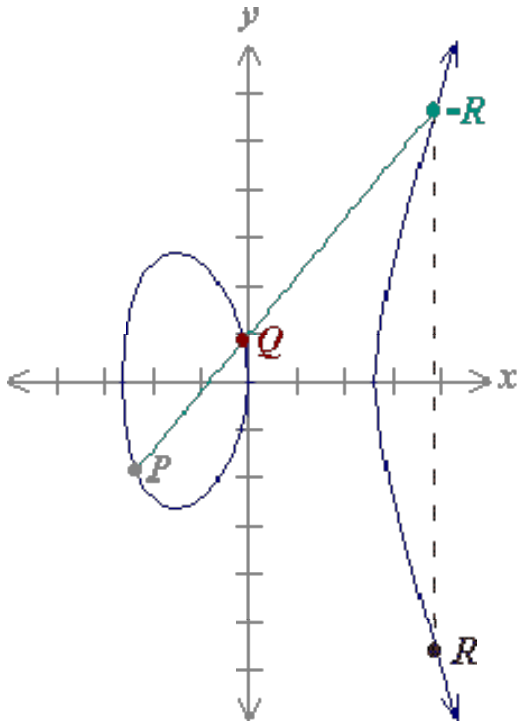
和无限远的附加点O。

群操作：$P \cdot Q$是通过$P\&Q$的线与曲线相交的位置的倒数。$P = (x,y)$的倒数被定为$P^{-1} = (x,-y)$。

明确定义，只要$4a^3 \neq -27b^2 \bmod p$。

椭圆曲线加密系统

EC例如在R^2：



P (-2.35, -1.86)

Q (-0.1, 0.836)

-R (3.89, 5.62)

R (3.89, -5.62)

$P + Q = R = (3.89, -5.62)$.

$y^2 = x^3 - 7x$

椭圆曲线加密系统

EC在有限领域的事实：

指数是有效的。

DLP很难。 其实比Z_p更难。（没有子指数算法是已知的）

因此，DH,ElGamal等可以在ECs上使用较小的密钥大小。（160位EC ~ 1024位RSA）

受限制设备（例如智能卡）比较受欢迎

优于RSA：

较小的钥匙大小

硬件紧凑

更快（用于私钥操作）

由NSA授权

谢谢！