现代密码学

第四十八讲 ElGamal类签名算法

信息与软件工程学院

基于离散对数问题的数字签名方案

- ElGamal签名方案、DSS签名方案、Schnorr签名方案都是基于离散对数困难问题的签名方案。
- 秘钥产生方式的共同点
- 签名方式类似性

ElGamal签名算法---签名算法

对于消息m，首先随机选取整数k， $1 \leqslant k \leqslant p-2$ ，然后计算：

$$r = g^k \bmod p, \quad s = (h(m) - xr)k^{-1} \bmod (p-1),$$

则m的签名为(r，s)，其中h为Hash函数。

ELGamal类的签名算法---密钥生成

1、p和q是大素数，且$q \mid p-1$

2、随机选取q阶元g ，$1< g <p-1$。q，p和g公开；

3、随机选取整数x, $1 \leqslant x \leqslant q-1$，计算$y = g^x \bmod p$。

4、公钥为y，私钥为x

ELGamal类的签名算法---签名算法

对于消息m，计算签名如下。

1、计算m的Hash值$h(m)$

2、随机选取一个整数k， $1\leqslant k\leqslant q$，

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

从等式 $ak = b + cx \bmod q$ 中计算出s。

其中方程的系数a、b、c有多种选择，$\{a,b,c\} = \{r, s, h(m)\}$

则m的签名为(r, s)。

ElGamal签名算法---签名算法

对于消息m，首先随机选取整数k， $1 \leqslant k \leqslant p-2$ ，然后计算：

$$r = g^k \bmod p, \quad s = (h(m) - xr)k^{-1} \bmod (p-1),$$

则m的签名为(r, s)，其中h为Hash函数。

ELGamal类的签名算法---验证算法

接收方在收到消息m和签名(r, s)后，验证

$$g^b y^c \equiv r^a \bmod p$$

- 如果同余式成立，则(r, s)是消息m的有效签名；反之，则是无效签名。

- 表1 参数a、b、c可能的选择

$\pm r'$	$\pm s$	$h(m)$
$\pm r' h(m)$	$\pm s$	1
$\pm r' h(m)$	$\pm h(m) s$	1
$\pm h(m) r'$	$\pm r' s$	1
$\pm h(m) s$	$\pm r' s$	1

注：表中 $r' \equiv r \bmod p$

一些基于离散对数问题的签名方案

	签名方程	验证方程
①	$r'k \equiv s + h(m)x \bmod q$	$r^{r'} \equiv g^{s} y^{h(m)} \bmod p$
②	$r'k \equiv h(m) + sx \bmod q$	$r^{r'} \equiv g^{h(m)} y^{s} \bmod p$
③	$sk \equiv r' + h(m)x \bmod q$	$r^{s} \equiv g^{r'} y^{h(m)} \bmod p$
④	$sk \equiv h(m) + r'x \bmod q$	$r^{s} \equiv g^{h(m)} y^{r'} \bmod p$
⑤	$mk \equiv s + r'x \bmod q$	$r^{m} \equiv g^{s} y^{r'} \bmod p$
⑥	$mk \equiv r' + sx \bmod q$	$r^{m} \equiv g^{r'} y^{s} \bmod p$