



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

A decorative graphic consisting of several horizontal blue bars of varying lengths, located to the left of the title.

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。
- 密钥产生方式的共同点
- 签名方式类似性

A decorative graphic consisting of several horizontal blue lines of varying lengths, stacked vertically, is positioned to the left of the title.

ElGamal 签名算法---签名算法

对于消息 m ，首先随机选取整数 k ， $1 \leq k \leq p-2$ ，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。

A decorative blue horizontal bar with a series of parallel lines is positioned to the left of the title.

ELGamal类的签名算法---密钥生成

- 1、 p 和 q 是大素数，且 $q|p-1$
- 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 ， $1 \leq x \leq q-1$ ，计算 $y = g^x \bmod p$ 。
- 4、公钥为 y ，私钥为 x

A decorative graphic consisting of several horizontal blue bars of varying lengths, located to the left of the title.

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 ， $1 \leq k \leq q$ ，

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

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) 。

A decorative blue horizontal bar with a series of parallel lines is positioned to the left of the title.

ElGamal 签名算法---签名算法

对于消息 m ，首先随机选取整数 k ， $1 \leq k \leq p-2$ ，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。

A decorative blue horizontal bar with a series of parallel lines is positioned to the left of the title.

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

$$g^b y^c \equiv r^a \pmod{p}$$

- 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 $r' \equiv r \pmod{p}$

一些基于离散对数问题的签名方案

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