(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102487321 B
(45)授权公告日 2014.07.02

(21)申请号 201010578298.6
(22)申请日 2010.12.03
(73)专利权人 航天信息股份有限公司
地址 100097 北京市海淀区杏石口路甲18号
(72)发明人 张庆胜
(74)专利代理机构 北京科龙寰宇知识产权代理有限责任公司 11139
代理人 孙皓晨 朱世定
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/30(2006.01)

(56)对比文件
CN 101018125 A,2007.08.15,
CN 1505313 A,2004.06.16,

审查员 薛玮

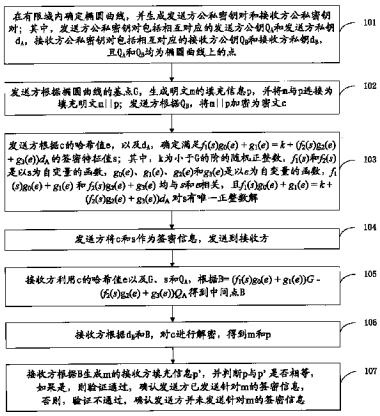
权利要求书4页 说明书13页 附图2页

(54)发明名称

一种签密方法和系统

(57)摘要

本发明涉及一种签密方法和系统。该签密方法包括：在有限域内确定椭圆曲线，生成包括相对应的Q_A、d_A的发送方公私密钥对和包括相对应的Q_B、d_B的接收方公私密钥对，Q_A、Q_B均为椭圆曲线的点；发送方根据椭圆曲线的基点G，生成明文m的填充信息p，将m与p连为m||p后，根据Q_B将其加密为密文c；确定满足$f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$的s，k为小于G的阶的随机正整数，$f_1(s)g_0(e)+g_1(e)$和$f_2(s)g_2(e)+g_3(e)$均与s、e相关，且$f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$对s有唯一正整数解；发送方将c和s作为签密信息发送到接收方；接收方利用c的哈希值e及G、s、Q_A，根据$B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$得到B；根据$d_B$和B对c解密得到m和p；根据B生成m的接收方填充信息p'；判断p与p'是否相等来验证发送方是否发送了针对m的签密信息。利用本发明能提高保密和认证的运算效率。



CN 102487321 B

1. 一种签密方法，其特征在于，该方法包括：

在有限域内确定椭圆曲线，并生成发送方公私密钥对和接收方公私密钥对；其中，所述发送方公私密钥对包括相互对应的发送方公钥 Q_A 和发送方私钥 d_A，所述接收方公私密钥对包括相互对应的接收方公钥 Q_B 和接收方私钥 d_B，且 Q_A 和 Q_B 均为所述椭圆曲线上的点；所述椭圆曲线的基点记为 G；

发送方根据 G，生成明文 m 的填充信息 p，并将 m 与 p 连接为填充明文 m||p；发送方根据 Q_B，将 m||p 加密为密文 c；

发送方根据 c 的哈希值 e，以及 d_A，确定满足 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 的签密特征值 s；其中，k 为小于 G 的阶的随机正整数，$f_1(s)$ 和 $f_2(s)$ 是以 s 为自变量的函数，$g_0(e)$、$g_1(e)$、$g_2(e)$ 和 $g_3(e)$ 是以 e 为自变量的函数，$f_1(s)g_0(e)+g_1(e)$ 和 $f_2(s)g_2(e)+g_3(e)$ 均与 s 和 e 相关，且 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 对 s 有唯一正整数解；

发送方将 c 和 s 作为签密信息，发送到接收方；

接收方利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；

接收方根据 d_B 和 B，对 c 进行解密，得到 m 和 p；

接收方根据 B 生成 m 的接收方填充信息 p'；

接收方判断 p 与 p'是否相等，如果是，则验证通过，确认发送方已发送针对 m 的签密信息，否则，验证不通过，确认发送方并未发送针对 m 的签密信息。

2. 根据权利要求 1 所述的方法，其特征在于，在生成发送方公私密钥对和接收方公私密钥对之后，该方法进一步包括：将 Q_A 与发送方的身份信息相对应、将 Q_B 与接收方的身份信息相对应，发送到证书管理机构；

所述证书管理机构判断所述发送方的身份信息是否真实，如果是，则生成发送方的数字证书发布到目录服务协议 LDAP 服务器上；其中，所述发送方的数字证书包括 Q_A 和发送方的身份信息；

所述证书管理机构判断所述接收方的身份信息是否真实，如果是，则生成接收方的数字证书发布到 LDAP 服务器上；其中，所述接收方的数字证书包括 Q_B 和接收方的身份信息；

则在发送方根据 Q_B，将 m||p 加密为密文 c 之前，该方法进一步包括：发送方从所述 LDAP 服务器上获得 Q_B；

在接收方利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B 之前，该方法进一步包括：接收方从所述 LDAP 服务器上获得 Q_A。

3. 根据权利要求 1 所述的方法，其特征在于，

发送方根据 Q_B，将 m||p 加密为密文 c 的方法为：发送方随机从小于 G 的阶的正整数中选定 k；将 k 与 Q_B 进行标量乘运算，得到形式为 (k_1, k_2) 的数组；利用 k_1 将 m||p 加密为密文 c；

接收方根据 d_B 和 B，对 c 进行解密，得到 m 和 p 的方法为：接收方将 d_B 与 B 进行标量乘运算，获得形式为 (k_1, k_2) 的数组；利用 k_1 对 c 进行解密，得到 m 和 p；

则该方法进一步包括：接收方将 k_1 和所述签密信息发送到仲裁方；所述仲裁方根

据 k_1 对 c 进行解密，得到 m 和 p；仲裁方利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；仲裁方根据 B 生成 m 的仲裁方填充信息 p”；仲裁方判断 p 与 p” 是否相等，如果是，则验证通过，确认发送方已发送针对 m 的签密信息，否则，验证不通过，确认发送方并未发送针对 m 的签密信息；

或，

发送方根据 Q_B，将 m||p 加密为密文 c 的方法为：发送方随机从小于 G 的阶的正整数中选定 k；将 k 与 Q_B 进行标量乘运算，得到形式为 (k_1, k_2) 的数组；利用 k_2 将 m||p 加密为密文 c；

接收方根据 d_B 和 B，对 c 进行解密，得到 m 和 p 的方法为：接收方将 d_B 与 B 进行标量乘运算，获得形式为 (k_1, k_2) 的数组；利用 k_2 对 c 进行解密，得到 m 和 p；

则该方法进一步包括：接收方将 k_2 和所述签密信息发送到仲裁方；所述仲裁方根据 k_2 对 c 进行解密，得到 m 和 p；仲裁方利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；仲裁方根据 B 生成 m 的仲裁方填充信息 p”；仲裁方判断 p 与 p” 是否相等，如果是，则验证通过，确认发送方已发送针对 m 的签密信息，否则，验证不通过，确认发送方并未发送针对 m 的签密信息。

4. 根据权利要求 3 所述的方法，其特征在于，发送方随机从小于 G 的阶的正整数中选定 k 之后，发送方根据所述椭圆曲线的基点 G，生成明文 m 的填充信息 p 的方法为：发送方将 k 与所述椭圆曲线的基点 G 进行标量乘运算，得到填充点 M；根据 M 生成明文 m 的填充信息 p。

5. 根据权利要求 1、2 或 3 所述的方法，其特征在于，

生成发送方公私密钥对的方法为：随机从小于 G 的阶的正整数中选取 d_A 作为发送方私钥；将 d_A 与 G 进行标量乘运算，生成发送方公钥 Q_A；

和 / 或，

生成接收方公私密钥对的方法为：随机从小于 G 的阶的正整数中选取 d_B 作为接收方私钥；将 d_B 与 G 进行标量乘运算，生成接收方公钥 Q_B。

6. 根据权利要求 1、2 或 3 所述的方法，其特征在于，所述有限域为大素数域或二元域。

7. 根据权利要求 1、2 或 3 所述的方法，其特征在于，G 的阶为素数，且其二进制比特位数大于 160。

8. 根据权利要求 1、2 或 3 所述的方法，其特征在于，$f_1(s)$ 的函数式为 $f_1(s)=s$；和 / 或，$f_2(s)$ 的函数式为 $f_2(s)=s$。

9. 一种签密系统，其特征在于，该系统包括：曲线与密钥生成模块、签密模块、解密与验证模块，其中，

所述曲线与密钥生成模块用于，在有限域内确定椭圆曲线，并生成发送方公私密钥对和接收方公私密钥对；其中，所述发送方公私密钥对包括相互对应的发送方公钥 Q_A 和发送方私钥 d_A，所述接收方公私密钥对包括相互对应的接收方公钥 Q_B 和接收方私钥 d_B，且 Q_A 和 Q_B 均为所述椭圆曲线上的点；将所述椭圆曲线的基点 G 和 G 的阶发送到所述签密模块；将 G 发送到所述解密与验证模块；

所述签密模块用于，根据 G 生成明文 m 的填充信息 p，并将 m 与 p 连接为填充明文 m||p；根据 Q_B 将 m||p 加密为密文 c；根据 c 的哈希值 e，以及 d_A，确定满足 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 的签密特征值 s；其中，k 为小于 G 的阶的随机正整数，

$f_1(s)$ 和 $f_2(s)$ 是以 s 为自变量的函数，$g_0(e)$、$g_1(e)$、$g_2(e)$ 和 $g_3(e)$ 是以 e 为自变量的函数，$f_1(s)g_0(e)+g_1(e)$ 和 $f_2(s)g_2(e)+g_3(e)$ 均与 s 和 e 相关，且 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 对 s 有唯一正整数解；将 c 和 s 作为签密信息，发送到解密与验证模块；

所述解密与验证模块用于，利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；根据 d_B 和 B，对 c 进行解密，得到 m 和 p；根据 B 生成 m 的接收方填充信息 p'；判断 p 与 p' 是否相等。

10. 根据权利要求 9 所述的系统，其特征在于，该系统进一步包括数字证书模块；

所述曲线与密钥生成模块进一步用于，将 Q_A 与发送方的身份信息相对应、将 Q_B 与接收方的身份信息相对应，发送到所述数字证书模块；

所述数字证书模块用于，判断所述发送方的身份信息是否真实；生成发送方的数字证书发布到自身的服务器上，所述发送方的数字证书包括 Q_A 和发送方的身份信息；判断所述接收方的身份信息是否真实；生成接收方的数字证书发布到自身的服务器上，所述接收方的数字证书包括 Q_B 和接收方的身份信息；

则所述签密模块进一步用于，从所述数字证书模块的服务器上获得 Q_B；

所述解密与验证模块进一步用于，从所述数字证书模块的服务器上获得 Q_A。

11. 根据权利要求 9 所述的系统，其特征在于，该系统进一步包括仲裁模块；

所述签密模块用于，随机从小于 G 的阶的正整数中选定 k；将 k 与 Q_B 进行标量乘运算，得到形式为 (k_1, k_2) 的数组；利用 k_1 将 m||p 加密为密文 c；

所述解密与验证模块用于，将 d_B 与 B 进行标量乘运算，获得形式为 (k_1, k_2) 的数组；利用 k_1 对 c 进行解密，得到 m 和 p；将 k_1 和所述签密信息发送到所述仲裁模块；

则所述仲裁模块用于，根据 k_1 对 c 进行解密，得到 m 和 p；利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；根据 B 生成 m 的仲裁方填充信息 p"；判断 p 与 p" 是否相等；

或，

所述签密模块用于，随机从小于 G 的阶的正整数中选定 k；将 k 与 Q_B 进行标量乘运算，得到形式为 (k_1, k_2) 的数组；利用 k_2 将 m||p 加密为密文 c；

所述解密与验证模块用于，将 d_B 与 B 进行标量乘运算，获得形式为 (k_1, k_2) 的数组；利用 k_2 对 c 进行解密，得到 m 和 p；将 k_2 和所述签密信息发送到所述仲裁模块；

则所述仲裁模块用于，根据 k_2 对 c 进行解密，得到 m 和 p；利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；根据 B 生成 m 的仲裁方填充信息 p"；判断 p 与 p" 是否相等。

12. 根据权利要求 11 所述的系统，其特征在于，所述签密模块用于，将 k 与所述椭圆曲线的基点 G 进行标量乘运算，得到填充点 M；根据 M 生成明文 m 的填充信息 p。

13. 根据权利要求 9、10 或 11 所述的系统，其特征在于，所述曲线与密钥生成模块用于，随机从小于 G 的阶的正整数中选取 d_A 作为发送方私钥；将 d_A 与 G 进行标量乘运算，生成发送方公钥 Q_A；随机从小于 G 的阶的正整数中选取 d_B 作为接收方私钥；将 d_B 与 G 进行标量乘运算，生成接收方公钥 Q_B。

14. 根据权利要求 9、10 或 11 所述的系统，其特征在于，所述有限域为大素数域或二元域。

15. 根据权利要求 9、10 或 11 所述的系统，其特征在于，G 的阶为素数，且其二进制比特位数大于 160。

16. 根据权利要求 9、10 或 11 所述的系统，其特征在于，$f_1(s)$ 的函数式为 $f_1(s)=s$；和/或，$f_2(s)$ 的函数式为 $f_2(s)=s$。

一种签密方法和系统

技术领域

[0001] 本发明涉及计算机应用领域，特别是涉及一种签密方法和系统。

背景技术

[0002] 在计算机应用领域中，保密和认证是最重要的问题之一。现有技术常用加密手段达到保密的目的，用数字签名的手段达到认证的目的，即计算机之间在传输数据时，通常需要对这些数据进行加密，以防止发生泄密事件，同时，为了防止数据发送方与接收方之间发生数据传输责任方面的纠纷、并防止第三方假冒发送方向接收方传输数据，发送方在发送加密数据的同时，还要向接收方发送数字签名，以供接收方根据该数字签名来确认发送方确实发送了该加密数据，这有效防止了发送方否认发送过数据、接收方否认接收到正确的数据以及第三方假冒发送方等事件的发生。

[0003] 现有技术中，明文数据从发送方传输到接收方的过程要同时满足保密和认证的要求，因而发送方需要将明文数据加密后的密文和数字签名同时发送给接收方。这样，发送方在发送密文和数字签名之前，要进行明文加密和生成数字签名两项工作。现有技术中，加密和生成数字签名是采用两套算法先后进行的，虽然二者的先后顺序可以颠倒，但发送方必须按照两套算法运算完毕才能获得密文和数字签名，因此，现有技术进行保密和认证的运算效率比较低。

发明内容

[0004] 本发明所要解决的技术问题是提供一种签密方法和系统，能提高保密和认证的运算效率。

[0005] 本发明解决上述技术问题的技术方案如下：一种签密方法，该方法包括：

[0006] 在有限域内确定椭圆曲线，并生成发送方公私密钥对和接收方公私密钥对；其中，所述发送方公私密钥对包括相互对应的发送方公钥 Q_A 和发送方私钥 d_A，所述接收方公私密钥对包括相互对应的接收方公钥 Q_B 和接收方私钥 d_B，且 Q_A 和 Q_B 均为所述椭圆曲线上的点；所述椭圆曲线的基点记为 G；

[0007] 发送方根据 G，生成明文 m 的填充信息 p，并将 m 与 p 连接为填充明文 m||p；发送方根据 Q_B，将 m||p 加密为密文 c；

[0008] 发送方根据 c 的哈希值 e，以及 d_A，确定满足 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 的签密特征值 s；其中，k 为小于 G 的阶的随机正整数，$f_1(s)$ 和 $f_2(s)$ 是以 s 为自变量的函数，$g_0(e)$、$g_1(e)$、$g_2(e)$ 和 $g_3(e)$ 是以 e 为自变量的函数，$f_1(s)g_0(e)+g_1(e)$ 和 $f_2(s)g_2(e)+g_3(e)$ 均与 s 和 e 相关，且 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 对 s 有唯一正整数解；

[0009] 发送方将 c 和 s 作为签密信息，发送到接收方；

[0010] 接收方利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；

[0011] 接收方根据 d_B 和 B，对 c 进行解密，得到 m 和 p；

[0012] 接收方根据 B 生成 m 的接收方填充信息 p'；

[0013] 接收方判断 p 与 p'是否相等，如果是，则验证通过，确认发送方已发送针对 m 的签密信息，否则，验证不通过，确认发送方并未发送针对 m 的签密信息。

[0014] 本发明的有益效果是：本发明中，发送方公私密钥对中的发送方公钥 Q_A 和发送方私钥 d_A，以及接收方公私密钥对中的接收方公钥 Q_B 和接收方私钥 d_B 分别相互对应，且 Q_A 和 Q_B 均为椭圆曲线上的点，发送方可利用椭圆曲线的基点 G 生成明文 m 的填充信息 p，提供给接收方来验证发送方确实发送了针对 m 的签密信息，发送方在将 m 和 p 连接为填充明文 m||p 后，即可根据 Q_B 将 m||p 加密为密文 c，这样，发送方用椭圆曲线签密的方法实现了明文数据的保密和认证工作；发送方利用 c 的哈希值 e 和 d_A 确定出满足 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 的签密特征值 s，并将 c 和 s 作为签密信息发送给接收方之后，接收方即可利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B，然后根据 d_B 和 B 对 c 进行解密，从而得到明文信息 m 和填充信息 p，接着，接收方可根据 B 生成 m 的接收方填充信息 p'，通过判断 p 与 p' 是否相等，即可实现认证过程，因此，本发明中，发送方可以利用椭圆曲线签密方法一次性实现对明文 m 进行加密得到密文 c 和验证用的填充信息 p，从而实现保密和认证功能，相对于现有技术先后执行两套算法来实现保密和认证功能，本发明大大提高了保密和认证的运算效率。

[0015] 在上述技术方案的基础上，本发明还可以做如下改进：

[0016] 进一步，在生成发送方公私密钥对和接收方公私密钥对之后，该方法进一步包括：将 Q_A 与发送方的身份信息相对应、将 Q_B 与接收方的身份信息相对应，发送到证书管理机构；

[0017] 所述证书管理机构判断所述发送方的身份信息是否真实，如果是，则生成发送方的数字证书发布到目录服务协议 LDAP 服务器上；其中，所述发送方的数字证书包括 Q_A 和发送方的身份信息；

[0018] 所述证书管理机构判断所述接收方的身份信息是否真实，如果是，则生成接收方的数字证书发布到 LDAP 服务器上；其中，所述接收方的数字证书包括 Q_B 和接收方的身份信息；

[0019] 则在发送方根据 Q_B，将 m||p 加密为密文 c 之前，该方法进一步包括：发送方从所述 LDAP 服务器上获得 Q_B；

[0020] 在接收方利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B 之前，该方法进一步包括：接收方从所述 LDAP 服务器上获得 Q_A。

[0021] 进一步，发送方根据 Q_B，将 m||p 加密为密文 c 的方法为：发送方随机从小于 G 的阶的正整数中选定 k；将 k 与 Q_B 进行标量乘运算，得到形式为 (k_1, k_2) 的数组；利用 k_1 将 m||p 加密为密文 c；

[0022] 接收方根据 d_B 和 B，对 c 进行解密，得到 m 和 p 的方法为：接收方将 d_B 与 B 进行标量乘运算，获得形式为 (k_1, k_2) 的数组；利用 k_1 对 c 进行解密，得到 m 和 p；

[0023] 则该方法进一步包括：接收方将 k_1 和所述签密信息发送到仲裁方；所述仲裁方根据 k_1 对 c 进行解密，得到 m 和 p；仲裁方利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)$

$g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；仲裁方根据 B 生成 m 的仲裁方填充信息 p”；仲裁方判断 p 与 p” 是否相等，如果是，则验证通过，确认发送方已发送针对 m 的签密信息，否则，验证不通过，确认发送方并未发送针对 m 的签密信息；

[0024] 或，

[0025] 发送方根据 Q_B，将 m||p 加密为密文 c 的方法为：发送方随机从小于 G 的阶的正整数中选定 k；将 k 与 Q_B 进行标量乘运算，得到形式为 (k_1, k_2) 的数组；利用 k_2 将 m||p 加密为密文 c；

[0026] 接收方根据 d_B 和 B，对 c 进行解密，得到 m 和 p 的方法为：接收方将 d_B 与 B 进行标量乘运算，获得形式为 (k_1, k_2) 的数组；利用 k_2 对 c 进行解密，得到 m 和 p；

[0027] 则该方法进一步包括：接收方将 k_2 和所述签密信息发送到仲裁方；所述仲裁方根据 k_2 对 c 进行解密，得到 m 和 p；仲裁方利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；仲裁方根据 B 生成 m 的仲裁方填充信息 p”；仲裁方判断 p 与 p” 是否相等，如果是，则验证通过，确认发送方已发送针对 m 的签密信息，否则，验证不通过，确认发送方并未发送针对 m 的签密信息。

[0028] 进一步，发送方随机从小于 G 的阶的正整数中选定 k 之后，发送方根据所述椭圆曲线的基点 G，生成明文 m 的填充信息 p 的方法为：发送方将 k 与所述椭圆曲线的基点 G 进行标量乘运算，得到填充点 M；根据 M 生成明文 m 的填充信息 p。

[0029] 进一步，生成发送方公私密钥对的方法为：随机从小于 G 的阶的正整数中选取 d_A 作为发送方私钥；将 d_A 与 G 进行标量乘运算，生成发送方公钥 Q_A；

[0030] 和 / 或，

[0031] 生成接收方公私密钥对的方法为：随机从小于 G 的阶的正整数中选取 d_B 作为接收方私钥；将 d_B 与 G 进行标量乘运算，生成接收方公钥 Q_B。

[0032] 进一步，所述有限域为大素数域或二元域。

[0033] 进一步，G 的阶为素数，且其二进制比特位数大于 160。

[0034] 进一步，$f_1(s)$ 的函数式为 $f_1(s)=s$；和 / 或，$f_2(s)$ 的函数式为 $f_2(s)=s$。

[0035] 本发明还提出了一种签密系统，该系统包括：曲线与密钥生成模块、签密模块、解密与验证模块，其中，

[0036] 所述曲线与密钥生成模块用于，在有限域内确定椭圆曲线，并生成发送方公私密钥对和接收方公私密钥对；其中，所述发送方公私密钥对包括相互对应的发送方公钥 Q_A 和发送方私钥 d_A，所述接收方公私密钥对包括相互对应的接收方公钥 Q_B 和接收方私钥 d_B，且 Q_A 和 Q_B 均为所述椭圆曲线上的点；将所述椭圆曲线的基点 G 和 G 的阶发送到所述签密模块；将 G 发送到所述解密与验证模块；

[0037] 所述签密模块用于，根据 G 生成明文 m 的填充信息 p，并将 m 与 p 连接为填充明文 m||p；根据 Q_B 将 m||p 加密为密文 c；根据 c 的哈希值 e，以及 d_A，确定满足 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 的签密特征值 s；其中，k 为小于 G 的阶的随机正整数，$f_1(s)$ 和 $f_2(s)$ 是以 s 为自变量的函数，$g_0(e)$、$g_1(e)$、$g_2(e)$ 和 $g_3(e)$ 是以 e 为自变量的函数，$f_1(s)g_0(e)+g_1(e)$ 和 $f_2(s)g_2(e)+g_3(e)$ 均与 s 和 e 相关，且 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 对 s 有唯一正整数解；将 c 和 s 作为签密信息，发送到解密与验证模块；

[0038] 所述解密与验证模块用于，利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)$

$g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；根据 d_B 和 B，对 c 进行解密，得到 m 和 p；根据 B 生成 m 的接收方填充信息 p'；判断 p 与 p' 是否相等。

[0039] 进一步，该系统包括数字证书模块；

[0040] 所述曲线与密钥生成模块进一步用于，将 Q_A 与发送方的身份信息相对应、将 Q_B 与接收方的身份信息相对应，发送到所述数字证书模块；

[0041] 所述数字证书模块用于，判断所述发送方的身份信息是否真实；生成发送方的数字证书发布到自身的服务器上，所述发送方的数字证书包括 Q_A 和发送方的身份信息；判断所述接收方的身份信息是否真实；生成接收方的数字证书发布到自身的服务器上，所述接收方的数字证书包括 Q_B 和接收方的身份信息；

[0042] 则所述签密模块进一步用于，从所述数字证书模块的服务器上获得 Q_B；

[0043] 所述解密与验证模块进一步用于，从所述数字证书模块的服务器上获得 Q_A。

[0044] 进一步，该系统包括仲裁模块；

[0045] 所述签密模块用于，随机从小于 G 的阶的正整数中选定 k；将 k 与 Q_B 进行标量乘运算，得到形式为 (k_1, k_2) 的数组；利用 k_1 将 m||p 加密为密文 c；

[0046] 所述解密与验证模块用于，将 d_B 与 B 进行标量乘运算，获得形式为 (k_1, k_2) 的数组；利用 k_1 对 c 进行解密，得到 m 和 p；将 k_1 和所述签密信息发送到所述仲裁模块；

[0047] 则所述仲裁模块用于，根据 k_1 对 c 进行解密，得到 m 和 p；利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；根据 B 生成 m 的仲裁方填充信息 p"；判断 p 与 p" 是否相等；

[0048] 或，

[0049] 所述签密模块用于，随机从小于 G 的阶的正整数中选定 k；将 k 与 Q_B 进行标量乘运算，得到形式为 (k_1, k_2) 的数组；利用 k_2 将 m||p 加密为密文 c；

[0050] 所述解密与验证模块用于，将 d_B 与 B 进行标量乘运算，获得形式为 (k_1, k_2) 的数组；利用 k_2 对 c 进行解密，得到 m 和 p；将 k_2 和所述签密信息发送到所述仲裁模块；

[0051] 则所述仲裁模块用于，根据 k_2 对 c 进行解密，得到 m 和 p；利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；根据 B 生成 m 的仲裁方填充信息 p"；判断 p 与 p" 是否相等。

[0052] 进一步，所述签密模块用于，将 k 与所述椭圆曲线的基点 G 进行标量乘运算，得到填充点 M；根据 M 生成明文 m 的填充信息 p。

[0053] 进一步，所述曲线与密钥生成模块用于，随机从小于 G 的阶的正整数中选取 d_A 作为发送方私钥；将 d_A 与 G 进行标量乘运算，生成发送方公钥 Q_A；随机从小于 G 的阶的正整数中选取 d_B 作为接收方私钥；将 d_B 与 G 进行标量乘运算，生成接收方公钥 Q_B。

[0054] 进一步，所述有限域为大素数域或二元域。

[0055] 进一步，G 的阶为素数，且其二进制比特位数大于 160。

[0056] 进一步，$f_1(s)$ 的函数式为 $f_1(s)=s$；和 / 或，$f_2(s)$ 的函数式为 $f_2(s)=s$。

附图说明

[0057] 图 1 为本发明提供的签密方法的流程图；

[0058] 图 2 为本发明提供的签密系统的结构图。

具体实施方式

[0059] 以下结合附图对本发明的原理和特征进行描述，所举实例只用于解释本发明，并非用于限定本发明的范围。

[0060] 图 1 为本发明提供的签密方法的流程图。如图 1 所示，该方法包括 ：

[0061] 步骤 101 ：在有限域内确定椭圆曲线，并生成发送方公私密钥对和接收方公私密钥对 ；其中，发送方公私密钥对包括相互对应的发送方公钥 Q_A 和发送方私钥 d_A，接收方公私密钥对包括相互对应的接收方公钥 Q_B 和接收方私钥 d_B，且 Q_A 和 Q_B 均为椭圆曲线上的点。

[0062] 本步骤中生成的发送方公私密钥对和接收方公私密钥对，是用于供发送方对明文数据进行加密、供接收方对密文进行解密以及对发送方是否发送了针对 m 的签密信息进行认证的。其中，发送方可利用接收方公私密钥对中的接收方公钥 Q_B 和发送方公私密钥对中的发送方私钥 d_A，对明文数据 m 进行加密、产生 m 的填充信息 p 以供接收方验证发送方确实发送了针对 m 的签密信息，并产生签密特征值 s 以供接收方解密 ；接收方可利用发送方公私密钥对中的发送方公钥 Q_A 和接收方公私密钥对中的接收方私钥 d_B，对密文 c 进行解密得到明文数据 m 和填充信息 p，并生成 m 的接收方填充信息 p’，以与 p 进行比较从而验证发送方是否发送了针对 m 的签密信息。

[0063] 发送方公私密钥对中的 Q_A 和 d_A 是相互对应的，接收方公私密钥对中的 Q_B 和 d_B 也是相互对应的，这两个对应关系可以实现如下的功能 ：发送方利用 Q_B 对明文 m 和填充信息 p 连接后的填充明文 m||p 加密所得到的密文 c，可由接收方利用 d_B 对其解密从而得到 m 和 p ；发送方利用 d_A 确定签密特征值 s，接收方即可利用 s 和 Q_A 获得中间点 B，从而对 c 进行解密以及生成 m 的接收方填充信息 p’，实现对发送方是否发送了针对 m 的签密信息进行验证。

[0064] 本发明采用的技术为椭圆曲线签密技术，这意味着本发明中，发送方公私密钥对中的 Q_A 和接收方公私密钥对中的 Q_B 均为在有限域内确定的椭圆曲线上的点。其中，有限域可以为大素数域，记为 F（p），p 为大素数域 F 的参数，有限域也可以为二元域，记为 F_{2^m}，m 为二元域 F 的参数。这样，有限域 F 上的椭圆曲线记为 E（F），该椭圆曲线是一条由离散的点组成的封闭曲线，其离散性和封闭性具体表现为 ：该椭圆曲线上有阶为 n 的点 G，对于闭区间 [1,n-1] 内的任一正整数 k，其与点 G 进行标量乘运算之后所得到的新的点仍在该椭圆曲线 E（F）上。数学原理已证明，对于已知的 E（F）上的点 G 以及 G 与某一小于其阶 n 的正整数 k 进行标量乘运算所得到的另外一点 Q，要确定正整数 k 是极其困难的，而本发明利用椭圆曲线签密技术来保证数据传输的安全性的依据，也就在于定义在椭圆曲线上的离散点的求 k 问题的难解性。有数据表明，按现在的计算机技术水平，在密钥长度为 1024 位的情况下，要破解现有技术所采用的 RSA 密钥，需要上千年的计算时间，而要破解本发明所采用的建立在有限域内的椭圆曲线上的发送方公钥和接收方公钥，需要更长的时间，因此，可以认为本发明所采用的椭圆曲线签密技术是非常安全的。

[0065] 以有限域为大素数域 F（p）的情况为例，说明在有限域内确定椭圆曲线的方法 ：

[0066] 在大素数域 F（p）中，椭圆曲线的方程为 $y^2=x^3+ax+b$，其中，x 和 y 分别为椭圆曲线上的点的横坐标和纵坐标，该椭圆曲线基点为 G，G 的坐标为 (G_x,G_y)，G 的阶为 n。要确定一条椭圆曲线，只需确定该椭圆曲线的方程即可，因此，在大素数域 F（p）中确定椭圆曲线 $y^2=x^3+ax+b$，只需确定 p、a、b、G_x、G_y 和 n 这几个参数即可。

[0067] 本发明给出大素数域中的椭圆曲线的一组参数如下，这些参数均为十六进制参数，且长度均为 256 比特：

[0068] p=FFFFFFFF0000000100000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFF；

[0069] a=FFFFFFFF0000000100000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFC；

[0070] b=5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B；

[0071] G_x=6B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C296；

[0072] G_y=4FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5；

[0073] n=FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551。

[0074] 当然，椭圆曲线的这些参数也可以设置为其他数值，各参数的二进制比特位的长度也可以设置为其他长度，并且其长度也可以相互不同，只需满足该椭圆曲线的基点 G 的阶 n 为素数，且 n 的二进制比特位数大于 160 即可。

[0075] 在有限域为二元域的情况下，确定椭圆曲线的方法也为通过确定该椭圆曲线的参数来确定该椭圆曲线，与大素数域下确定椭圆曲线的区别仅在于，二元域下所确定的椭圆曲线的参数与大素数域下的不同，在二元域下的椭圆曲线的参数已在数学领域成为公知常识，也包括该椭圆曲线的基点 G，该基点 G 也有阶 n，其他参数在此不做赘述。

[0076] 步骤 102：发送方根据椭圆曲线的基点 G，生成明文 m 的填充信息 p，并将 m 与 p 连接为填充明文 m||p；发送方根据 Q_B，将 m||p 加密为密文 c。

[0077] 这里，明文 m 为发送方实际要发送的数据。

[0078] 发送方根据椭圆曲线的基点 G，可以生成 m 的填充信息 p，p 用于供接收方验证发送方是否发送了针对 m 的签密信息，另外，p 也可以用于与 m 连接为填充明文 m||p，以保证 m||p 加密后得到的密文 c 的长度符合规定。

[0079] 发送方根据 Q_B 将 m||p 加密为密文 c，这样，接收方就可以根据与 Q_B 对应的 d_B，对密文 c 进行解密得到 m 和 p，同时，由于利用 Q_B 来推得 d_B 是极其困难的，因此，即使 c 在传输中被第三方截获，没有获得 d_B 的第三方也不可能将 c 解密，这也就保证了本发明中传输的信息的安全性。

[0080] 发送方根据 Q_B 将 m||p 加密为密文 c 的方法可以为对称密钥算法，也可以为非对称密钥算法。

[0081] 步骤 103：发送方根据 c 的哈希值 e，以及 d_A，确定满足 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 的签密特征值 s；其中，k 为小于 G 的阶的随机正整数，$f_1(s)$ 和 $f_2(s)$ 是以 s 为自变量的函数，$g_0(e)$、$g_1(e)$、$g_2(e)$ 和 $g_3(e)$ 是以 e 为自变量的函数，$f_1(s)g_0(e)+g_1(e)$ 和 $f_2(s)g_2(e)+g_3(e)$ 均与 s 和 e 相关，且 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 对 s 有唯一正整数解。

[0082] 这里，发送方对步骤 102 所得到的密文 c 进行哈希运算，得到 c 的哈希值 e，然后利用自身保存的 d_A，来确定满足方程 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 的签密特征值 s，s 是作为发送方所发送的签密信息的一部分发送给接收方的，用于供接收方生成中间点 B，从而进一步利用 B 来对 c 解密和生成 m 的接收方填充信息 p’ 以验证发送方是否发送了针对 m 的签密信息。

[0083] 利用 d_A 来确定 s，可以保证接收方利用 Q_A 获得中间点 B，由于利用 Q_A 来确定 d_A 是极其困难的，因此，本发明中的密钥也是安全的。

[0084] $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 对 s 有唯一正整数解，可以保证本步骤中确定的 s 是唯一的，从而也就保证了步骤 104 向接收方发送的签密信息的唯一性，因而接收方在利用 s 确定 B 的过程是唯一的，不会发生得到两个以上的 s 造成接收方无法确定 B，进而无法解密和验证的问题。

[0085] 在 G 的阶记为 n 的情况下，k 为小于 G 的阶的随机正整数，意味着 k 为闭区间 [1，n-1] 内的正整数，且 k 为随机在该闭区间内选取的，本发明在小于 G 的阶的正整数中随机选取 k，有利于保证本步骤所确定的 s 为外部不可知的，这也有利于本发明中的密钥和信息的安全性。

[0086] 本发明中，$f_1(s)$ 和 $f_2(s)$ 是以 s 为自变量的函数，$g_0(e)$、$g_1(e)$、$g_2(e)$ 和 $g_3(e)$ 是以 e 为自变量的函数。

[0087] $f_1(s)g_0(e)+g_1(e)$ 和 $f_2(s)g_2(e)+g_3(e)$ 均与 s 和 e 相关，可以保证任何第三方都不可能冒充发送方，向接收方发送伪造的明文 m_0，从而有利于本发明中的数据和密钥的安全性。可以用反证法来对这一结论加以证明：

[0088] 设 $f_1(s)g_0(e)+g_1(e)$ 为与 s、e 无关，则该式即可看做是与 s、e 无关的常量 l，将 $l=f_1(s)g_0(e)+g_1(e)$ 代入方程 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$，可得

[0089] $$l=k+(f_2(s)g_2(e)+g_3(e))d_A \quad (1)$$

[0090] 设有第三方截获了发送方发送给接收方的签密信息，即第三方获得了密文 c 和签密特征值 s，并且该第三方企图冒充发送方，将伪造的明文 m_0 加密为密文 c_0 后替换发送方发送给接收方的密文 c，则该第三方根据椭圆曲线的基点 G 生成 m_0 的填充信息 p_0，并且将 m_0 和 p_0 连接为填充明文 $m_0||p_0$ 后，对其加密得到密文 c_0，然后通过哈希运算得到 c_0 的哈希值 e_0；这样，第三方只需要计算得到关于 c_0 的签密特征值 s_0，即可实现冒充发送方向接收方发送伪造明文 m_0 的目标；

[0091] 式（1）中，k 为一小于基点 G 的阶的随机正整数，在发送方将签密信息发出的情况下，k 已为一定值，l 也为常量，因此，l 与 k 相减所得的差值也为常量，这种情况下，第三方虽然不可能获得式（1）中的发送方私钥 d_A，但由于该式对于发送方所发送的签密信息（c，s）以及第三方所发送的伪造签密信息（c_0，s_0）都是成立的，因此，有下式成立：

[0092] $$f_2(s_0)g_2(e_0)+g_3(e_0)=f_2(s)g_2(e)+g_3(e)) \quad (2)$$

[0093] 式（2）中，第三方可以确定 s、c 的哈希值 e 以及 e_0，这样，第三方根据式（2）即可确定伪造的签密特征值 s_0；

[0094] 这样，第三方就可以用伪造的签密信息（c_0，s_0）替换发送方发送的签密信息（c，s）发送给接收方，从而使发送方发送的签密信息丢失，这严重影响了发送方数据的安全，因此，前述 $f_1(s)g_0(e)+g_1(e)$ 与 s、e 无关的假设是不可行的，$f_1(s)g_0(e)+g_1(e)$ 必须与 s 和 e 相关，才能保证本发明的数据安全性。

[0095] 同理，$f_2(s)g_2(e)+g_3(e)$ 也必须与 s 和 e 相关，不再重复证明。

[0096] 步骤 104：发送方将 c 和 s 作为签密信息，发送到接收方。

[0097] 这里，发送方将 c 和 s 作为签密信息发送到接收方，接收方可以利用该签密信息，解密得到明文 m，并对发送方是否发送了针对 m 的签密信息进行验证。

[0098] 步骤 105：接收方利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B。

[0099] 这里，接收方在步骤 104 中接收到 c 和 s 组成的签密信息后，可以计算得到 c 的哈希值 e，然后利用 e、G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B，进而在后续步骤中利用 B 对 c 解密得到 m 和 p，并利用 B 获得接收方填充信息 p'，进而利用 p 和 p' 来验证发送方是否发送了针对 m 的签密信息。

[0100] 计算 B 的公式 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 是与步骤 103 中确定 s 的方程 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 相对应的。

[0101] 步骤 106 :接收方根据 d_B 和 B，对 c 进行解密，得到 m 和 p。

[0102] 这里，接收方利用 d_B 和 B，即可对 c 进行解密，解密的运算为与步骤 102 中根据 Q_B 将 m||p 加密为密文 c 的运算的逆运算，解密得到 m||p，根据发送方和接收方对于填充信息 p 的长度约定，从解密得到的 m||p 中分离出 m 和 p。

[0103] 步骤 107 :接收方根据 B 生成 m 的接收方填充信息 p'，并判断 p 与 p' 是否相等，如果是，则验证通过，确认发送方已发送针对 m 的签密信息，否则，验证不通过，确认发送方并未发送针对 m 的签密信息。

[0104] 这里，接收方在步骤 106 中解密得到明文 m 之后，还要对发送方是否发送了针对 m 的签密信息进行验证，如果验证通过，则说明接收方所收到的签密信息确实为发送方所发出的，且该签密信息为针对 m 的签密信息，同时，本步骤也可以确定发送方的具体身份，即在存在多个发送方的情况下，接收方可以利用本步骤精确确定每一个签密信息的发送方，另外，本步骤验证通过后，接收方就可以根据收到的明文进行相应的操作，并防止发送方否认曾经发送过该签密信息。进一步地，该验证通过，也意味着接收方不能否认自身已收到该签密信息，而且也可以证明该签密信息不是由任何第三方所伪造传输过来的。

[0105] 接收方是利用在步骤 106 中解密得到的 p 和本步骤中生成的 m 的接收方填充信息 p' 来验证发送方是否发送了针对 m 的签密信息的，如果二者相等，则验证通过，说明发送方确实发送了针对 m 的签密信息，并且该签密信息在传输过程中并未被篡改，如果二者不相等，则验证不通过，可以确认发送方并未发送针对 m 的签密信息，这种情况下，有可能是发送方所发送的针对 m 的签密信息在发送到接收方之前被篡改过，也有可能是发送方所发送的信息并非针对 m 的签密信息，在这种情况下，接收方不能根据收到的签密信息进行下一步的操作。

[0106] 接收方是根据 B 生成 m 的接收方填充信息 p' 的，其方法与步骤 102 中发送方根据 G 生成 p 的方法相同。

[0107] 由此可见，本发明中，发送方公私密钥对中的发送方公钥 Q_A 和发送方私钥 d_A，以及接收方公私密钥对中的接收方公钥 Q_B 和接收方私钥 d_B 分别相互对应，且 Q_A 和 Q_B 均为椭圆曲线上的点，发送方可利用椭圆曲线的基点 G 生成明文 m 的填充信息 p，提供给接收方来验证发送方确实发送了针对 m 的签密信息，发送方在将 m 和 p 连接为填充明文 m||p 后，即可根据 Q_B 将 m||p 加密为密文 c，这样，发送方用椭圆曲线签密的方法实现了明文数据的保密和认证工作 ；发送方利用 c 的哈希值 e 和 d_A 确定出满足 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 的签密特征值 s，并将 c 和 s 作为签密信息发送给接收方之后，接收方即可利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B，然后根据 d_B 和 B 对 c 进行解密，从而得到明文信息 m 和填充信息 p，接着，接收方可根据 B 生成 m 的接收方填充信息 p'，通过判断 p 与 p' 是否相等，即可实现认证过程，因此，本发明中，发

送方可以利用椭圆曲线签密方法一次性实现对明文 m 进行加密得到密文 c 和验证用的填充信息 p，从而实现保密和认证功能，相对于现有技术先后执行两套算法来实现保密和认证功能，本发明大大提高了保密和认证的运算效率。

[0108] 本发明中，在步骤 101 生成发送方公私密钥对和接收方公私密钥对之后，该方法进一步包括：将 Q_A 与发送方的身份信息相对应、将 Q_B 与接收方的身份信息相对应，发送到证书管理机构；

[0109] 证书管理机构判断发送方的身份信息是否真实，如果是，则生成发送方的数字证书发布到目录服务协议 LDAP 服务器上；其中，发送方的数字证书包括 Q_A 和发送方的身份信息；

[0110] 证书管理机构判断接收方的身份信息是否真实，如果是，则生成接收方的数字证书发布到 LDAP 服务器上；其中，接收方的数字证书包括 Q_B 和接收方的身份信息；

[0111] 则在发送方根据 Q_B，将 m||p 加密为密文 c 之前，该方法进一步包括：发送方从 LDAP 服务器上获得 Q_B；

[0112] 在接收方利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B 之前，该方法进一步包括：接收方从 LDAP 服务器上获得 Q_A。

[0113] 这里，证书管理机构是作为验证发送方和接收方的身份信息、并存储、发布 Q_A 和 Q_B 的中立的第三方诚信机构而存在的，其判断发送方或接收方的身份信息为真实的情况下，将 Q_A 或 Q_B 发送到 LDAP 服务器上，可以起到存储和公示 Q_A 和 Q_B 的作用，任何机构和个人都可以访问 LDAP 服务器来获得 Q_A 和 Q_B。如果证书管理机构判断发送方或接收方的身份信息为虚假信息，则不会将 Q_A 或 Q_B 发布到其 LDAP 服务器上，因而其他机构或个人也无法获得 Q_A 或 Q_B，从而无法与发送方或接收方进行通信，这样，证书管理机构也就起到了保证发送方和接收方诚信的作用。

[0114] 步骤 102 中，发送方根据 Q_B，将 m||p 加密为密文 c 的方法可以为：发送方随机从小于 G 的阶的正整数中选定 k；将 k 与 Q_B 进行标量乘运算，得到形式为 (k_1, k_2) 的数组；利用 k_1 将 m||p 加密为密文 c；

[0115] 步骤 106 中，接收方根据 d_B 和 B，对 c 进行解密，得到 m 和 p 的方法为：接收方将 d_B 与 B 进行标量乘运算，获得形式为 (k_1, k_2) 的数组；利用 k_1 对 c 进行解密，得到 m 和 p；

[0116] 则该方法进一步包括：接收方将 k_1 和签密信息发送到仲裁方；仲裁方根据 k_1 对 c 进行解密，得到 m 和 p；仲裁方利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；仲裁方根据 B 生成 m 的仲裁方填充信息 p”；仲裁方判断 p 与 p”是否相等，如果是，则验证通过，确认发送方已发送针对 m 的签密信息，否则，验证不通过，确认发送方并未发送针对 m 的签密信息。

[0117] 由此可见，本发明中，发送方是采用对称密钥算法对 m||p 进行加密得到密文的，在加密和解密的过程中所使用的密钥相同，均为 k 与 Q_B 标量乘运算得到的形式为 (k_1, k_2) 的数组中的前一项 k_1。

[0118] 当然，加密和解密用的密钥也可以为该数组中的第二项 k_2，这样，步骤 102 中，发送方根据 Q_B，将 m||p 加密为密文 c 的方法为：发送方随机从小于 G 的阶的正整数中选定 k；将 k 与 Q_B 进行标量乘运算，得到形式为 (k_1, k_2) 的数组；利用 k_2 将 m||p 加密为密文 c；

[0119] 步骤 106 中，接收方根据 d_B 和 B，对 c 进行解密，得到 m 和 p 的方法为：接收方将 d_B

与 B 进行标量乘运算，获得形式为（k_1，k_2）的数组；利用 k_2 对 c 进行解密，得到 m 和 p；

[0120] 则该方法进一步包括：接收方将 k_2 和签密信息发送到仲裁方；仲裁方根据 k_2 对 c 进行解密，得到 m 和 p；仲裁方利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；仲裁方根据 B 生成 m 的仲裁方填充信息 p”；仲裁方判断 p 与 p”是否相等，如果是，则验证通过，确认发送方已发送针对 m 的签密信息，否则，验证不通过，确认发送方并未发送针对 m 的签密信息。

[0121] 由于 k 是发送方随机从小于 G 的阶的正整数中选定的，因此，发送方之外的任何机构或个人都无法获知 k 的值，也就无法获得加密和解密用的密钥，这有利于保证本发明的密钥和信息的安全。

[0122] 另外，本发明还提供了中立的仲裁方，用于防范和解决发送方和接收方之间的纠纷。由于接收方将自身所得到的密钥以及签密信息发送给了仲裁方，因此，仲裁方可以根据该密钥对密文 c 独立进行解密，得到 m 和 p，并独立生成仲裁方填充信息 p”，以与自身独立获得的 p 进行比较，从而独立验证发送方是否发送了针对 m 的签密信息，这样，在发送方和接收方之间存在纠纷和争议的情况下，中立的仲裁方就可以利用自身独立得到的数据来对二者的争议和纠纷进行仲裁。

[0123] 本发明中，发送方随机从小于 G 的阶的正整数中选定 k 之后，步骤 102 中发送方根据椭圆曲线的基点 G，生成明文 m 的填充信息 p 的方法为：发送方将 k 与椭圆曲线的基点 G 进行标量乘运算，得到填充点 M；根据 M 生成明文 m 的填充信息 p。

[0124] 发送方根据 M 生成 p 的方法在现有技术中已有很多论述，在此不做赘述。

[0125] 步骤 101 中，生成发送方公私密钥对的方法可以为：随机从小于 G 的阶的正整数中选取 d_A 作为发送方私钥；将 d_A 与 G 进行标量乘运算，生成发送方公钥 Q_A；

[0126] 同样，生成接收方公私密钥对的方法可以为：随机从小于 G 的阶的正整数中选取 d_B 作为接收方私钥；将 d_B 与 G 进行标量乘运算，生成接收方公钥 Q_B。

[0127] 这里，由于 d_A 和 d_B 均为随机从小于 G 的阶的正整数中选取的，因此，发送方之外的任何机构或个人都无法获知 d_A，接收方之外的任何机构或个人也都无法获知 d_B，只要发送方和接收方不泄露，d_A 和 d_B 是永远不会泄露的，这保证了本发明中的密钥安全。

[0128] 本发明中，公钥 Q_A 和 Q_B 分别为相应的私钥 d_A 和 d_B 与 G 进行标量乘运算得到，因此，Q_A 与 d_A、以及 Q_B 与 d_B 之间是有步骤 101 所述的对应关系的。

[0129] 本发明中，有限域为大素数域的情况下，椭圆曲线的基点 G 的阶为素数，且其二进制比特位数大于 160，这符合国际标准对椭圆曲线签密技术的要求，有利于保证密钥和数据的安全。

[0130] 步骤 103 和步骤 105 中的 $f_1(s)$ 的函数式的较佳实施例为 $f_1(s)=s$。

[0131] 同样，$f_2(s)$ 的函数式的较佳实施例为 $f_2(s)=s$。

[0132] 本发明中，$f_1(s)$ 和 $f_2(s)$ 的函数式分别设置为 $f_1(s)=s$ 和 $f_2(s)=s$，这是符合要求的 $f_1(s)$ 和 $f_2(s)$ 的函数式的最简洁表达式，采用该实施例，有利于进一步提高本发明的运算效率。

[0133] 现有技术中，发送方除了向接收方发送密文之外，还要发送数字签名，以供接收方进行验证，这样，发送方向接收方所发送的数据通常包括三部分内容，可用（c，r，s）的形式来表征，其中，c 表示密文，其二进制比特位数与明文 m 大致相同；r 和 s 均为发送方和接收

方之间约定的有关数据加解密和签名验证方面的特征参数，二者的二进制比特位数大致相同，约等于基点的阶的长度。因此，现有技术中，发送方所发送的数据包的总长度约为基点的阶的长度的两倍与明文 m 的长度相加所得的和。

[0134] 本发明中，发送方向接收方发送的签密信息可用(c,s)的形式来表征，比现有技术少发送了一个参数，其中，密文 c 的长度也与明文 m 的长度大致相同，而 s 的长度也与椭圆曲线的基点的阶的长度大致相同，因此，本发明中发送方所发送的数据包的总长度仅为基点的阶的长度与明文 m 的长度相加所得的和，由此可见，由于本发明中发送方可以比现有技术少发送一个特征参数，因而本发明中发送方发送的数据的长度远远小于现有技术。

[0135] 由于本发明中发送方所发送的数据的长度远远小于现有技术，因此，本发明能够提高发送方与接收方之间的通信效率，在发送方与接收方之间的通信带宽比较窄的情况下，本发明有利于提高通信的速度，同时，与现有技术相比，在发送方所发送的数据长度相同的情况下，本发明能节省通信所使用的带宽，并节省存储数据所占用的存储空间。

[0136] 图 2 为本发明提供的签密系统的结构图。如图 2 所示，该系统包括：曲线与密钥生成模块 201、签密模块 202、解密与验证模块 203，其中，

[0137] 曲线与密钥生成模块 201 用于，在有限域内确定椭圆曲线，并生成发送方公私密钥对和接收方公私密钥对；其中，发送方公私密钥对包括相互对应的发送方公钥 Q_A 和发送方私钥 d_A，接收方公私密钥对包括相互对应的接收方公钥 Q_B 和接收方私钥 d_B，且 Q_A 和 Q_B 均为椭圆曲线上的点；将椭圆曲线的基点 G 和 G 的阶发送到签密模块 202；将 G 发送到解密与验证模块 203；

[0138] 签密模块 202 用于，根据 G 生成明文 m 的填充信息 p，并将 m 与 p 连接为填充明文 m||p；根据 Q_B 将 m||p 加密为密文 c；根据 c 的哈希值 e，以及 d_A，确定满足 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 的签密特征值 s；其中，k 为小于 G 的阶的随机正整数，$f_1(s)$ 和 $f_2(s)$ 是以 s 为自变量的函数，$g_0(e)$、$g_1(e)$、$g_2(e)$ 和 $g_3(e)$ 是以 e 为自变量的函数，$f_1(s)g_0(e)+g_1(e)$ 和 $f_2(s)g_2(e)+g_3(e)$ 均与 s 和 e 相关，且 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 对 s 有唯一正整数解；将 c 和 s 作为签密信息，发送到解密与验证模块 203；

[0139] 解密与验证模块 203 用于，利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；根据 d_B 和 B，对 c 进行解密，得到 m 和 p；根据 B 生成 m 的接收方填充信息 p'；判断 p 与 p' 是否相等。

[0140] 由此可见，曲线与密钥生成模块 201 所生成的发送方公私密钥对中的发送方公钥 Q_A 和发送方私钥 d_A，以及接收方公私密钥对中的接收方公钥 Q_B 和接收方私钥 d_B 分别相互对应，且 Q_A 和 Q_B 都为椭圆曲线上的点，签密模块 202 可利用椭圆曲线的基点 G 生成明文 m 的填充信息 p，提供给解密与验证模块 203 对发送方是否发送了针对明文 m 的签密信息进行验证，签密模块 202 在将 m 和 p 连接为填充明文 m||p 后，即可根据 Q_B 将 m||p 加密为密文 c，这样，签密模块 202 用椭圆曲线签密的方法实现了明文数据的保密和认证工作；签密模块 202 利用 c 的哈希值 e 和 d_A 确定出满足 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 的签密特征值 s，并将 c 和 s 作为签密信息发送给解密与验证模块 203 之后，解密与验证模块 203 即可利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B，然后根据 d_B 和 B 对 c 进行解密，从而得到明文信息 m 和填充信息 p，接着，解密与验证模块 203 可根据 B 生成 m 的接收方填充信息 p'，通过判断 p 与 p' 是否相等，即可

实现认证过程，因此，本发明中，签密模块 202 可以利用椭圆曲线签密技术一次性实现对明文 m 进行加密得到密文 c 和验证用的填充信息 p，从而实现保密和认证功能，相对于现有技术先后执行两套算法来实现保密和认证功能，本发明大大提高了保密和认证的运算效率。

[0141] 该系统进一步包括数字证书模块；则

[0142] 曲线与密钥生成模块 201 进一步用于，将 Q_A 与发送方的身份信息相对应、将 Q_B 与接收方的身份信息相对应，发送到数字证书模块；

[0143] 数字证书模块用于，判断发送方的身份信息是否真实；生成发送方的数字证书发布到自身的服务器上，发送方的数字证书包括 Q_A 和发送方的身份信息；判断接收方的身份信息是否真实；生成接收方的数字证书发布到自身的服务器上，接收方的数字证书包括 Q_B 和接收方的身份信息；

[0144] 则签密模块 202 进一步用于，从数字证书模块的服务器上获得 Q_B；

[0145] 解密与验证模块 203 进一步用于，从数字证书模块的服务器上获得 Q_A。

[0146] 这里，数字证书模块可以作为验证发送方和接收方的身份信息、存储和发布 Q_A 和 Q_B 的中立的第三方模块，从而保证本发明中发送方和接收方身份信息的真实性。

[0147] 本发明中，该系统进一步包括仲裁模块；

[0148] 签密模块 202 可以用于，随机从小于 G 的阶的正整数中选定 k；将 k 与 Q_B 进行标量乘运算，得到形式为 (k_1, k_2) 的数组；利用 k_1 将 m||p 加密为密文 c；

[0149] 解密与验证模块 203 可以用于，将 d_B 与 B 进行标量乘运算，获得形式为 (k_1, k_2) 的数组；利用 k_1 对 c 进行解密，得到 m 和 p；将 k_1 和签密信息发送到仲裁模块；

[0150] 则仲裁模块可以用于，根据 k_1 对 c 进行解密，得到 m 和 p；利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；根据 B 生成 m 的仲裁方填充信息 p”；判断 p 与 p” 是否相等；

[0151] 当然，签密模块 202 也可以用于，随机从小于 G 的阶的正整数中选定 k；将 k 与 Q_B 进行标量乘运算，得到形式为 (k_1, k_2) 的数组；利用 k_2 将 m||p 加密为密文 c；

[0152] 解密与验证模块 203 用于，将 d_B 与 B 进行标量乘运算，获得形式为 (k_1, k_2) 的数组；利用 k_2 对 c 进行解密，得到 m 和 p；将 k_2 和签密信息发送到仲裁模块；

[0153] 则仲裁模块用于，根据 k_2 对 c 进行解密，得到 m 和 p；利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B；根据 B 生成 m 的仲裁方填充信息 p”；判断 p 与 p” 是否相等。

[0154] 利用仲裁模块可以用于防范和解决信息发送的纠纷。由于解密与验证模块 203 将自身所得到的密钥以及签密信息发送给了仲裁模块，因此，仲裁模块可以根据该密钥对密文 c 独立进行解密，得到 m 和 p，并独立生成仲裁方填充信息 p”，以与自身独立获得的 p 进行比较，从而验证发送方是否发送了针对明文 m 的签密信息，这样，在存在信息传输方面的纠纷的情况下，中立的仲裁模块就可以利用自身独立得到的数据来对该纠纷进行仲裁。

[0155] 该系统中，签密模块 202 用于，将 k 与椭圆曲线的基点 G 进行标量乘运算，得到填充点 M；根据 M 生成明文 m 的填充信息 p。

[0156] 该系统中，曲线与密钥生成模块 201 用于，随机从小于 G 的阶的正整数中选取 d_A 作为发送方私钥；将 d_A 与 G 进行标量乘运算，生成发送方公钥 Q_A；随机从小于 G 的阶的正整数中选取 d_B 作为接收方私钥；将 d_B 与 G 进行标量乘运算，生成接收方公钥 Q_B。

[0157] 该系统中，有限域为大素数域或二元域。

[0158] 该系统中，G 的阶为素数，且其二进制比特位数大于 160。

[0159] 该系统中，$f_1(s)$ 的函数式可以为 $f_1(s)=s$，$f_2(s)$ 的函数式也可以为 $f_2(s)=s$。

[0160] 由此可见，本发明具有以下优点：

[0161] (1)本发明中，发送方公私密钥对中的发送方公钥 Q_A 和发送方私钥 d_A，以及接收方公私密钥对中的接收方公钥 Q_B 和接收方私钥 d_B 分别相互对应，且 Q_A 和 Q_B 均为椭圆曲线上的点，发送方可利用椭圆曲线的基点 G 生成明文 m 的填充信息 p，提供给接收方来验证发送方确实发送了针对 m 的签密信息，发送方在将 m 和 p 连接为填充明文 m||p 后，即可根据 Q_B 将 m||p 加密为密文 c，这样，发送方用椭圆曲线签密的方法实现了明文数据的保密和认证工作；发送方利用 c 的哈希值 e 和 d_A 确定出满足 $f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$ 的签密特征值 s，并将 c 和 s 作为签密信息发送给接收方之后，接收方即可利用 c 的哈希值 e 以及 G、s 和 Q_A，根据 $B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$ 得到中间点 B，然后根据 d_B 和 B 对 c 进行解密，从而得到明文信息 m 和填充信息 p，接着，接收方可根据 B 生成 m 的接收方填充信息 p'，通过判断 p 与 p' 是否相等，即可实现认证过程，因此，本发明中，发送方可以利用椭圆曲线签密方法一次性实现对明文 m 进行加密得到密文 c 和验证用的填充信息 p，从而实现保密和认证功能，相对于现有技术先后执行两套算法来实现保密和认证功能，本发明大大提高了保密和认证的运算效率。

[0162] (2)本发明利用有限域中的椭圆曲线签密技术对明文进行签密，任何第三方都极难破解发送方所发送的密文，因而本发明的信息安全性非常高。

[0163] (3)本发明中，由于发送方公钥和接收方公钥均为有限域下椭圆曲线上的点，任何第三方想根据公钥来获得私钥是不可能的，因此，即使发生密文在传输中被第三方截获的情况，该密文也不能被解密，这保证了本发明中密钥和信息的安全性。

[0164] (4)$f_1(s)$ 和 $f_2(s)$ 的函数式分别设置为 $f_1(s)=s$ 和 $f_2(s)=s$，这是符合要求的 $f_1(s)$ 和 $f_2(s)$ 的函数式的最简洁表达式，本发明采用这种设置，可以进一步提高运算效率。

[0165] (5)本发明中，由于发送方所发送的数据的长度远远小于现有技术，因此，本发明能够提高发送方与接收方之间的通信效率，在发送方与接收方之间的通信带宽比较窄的情况下，本发明有利于提高通信的速度，在发送方所发送的数据长度相同的情况下，本发明可比现有技术用更少的通信带宽完成传输，并节省存储数据所占用的存储空间。

[0166] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

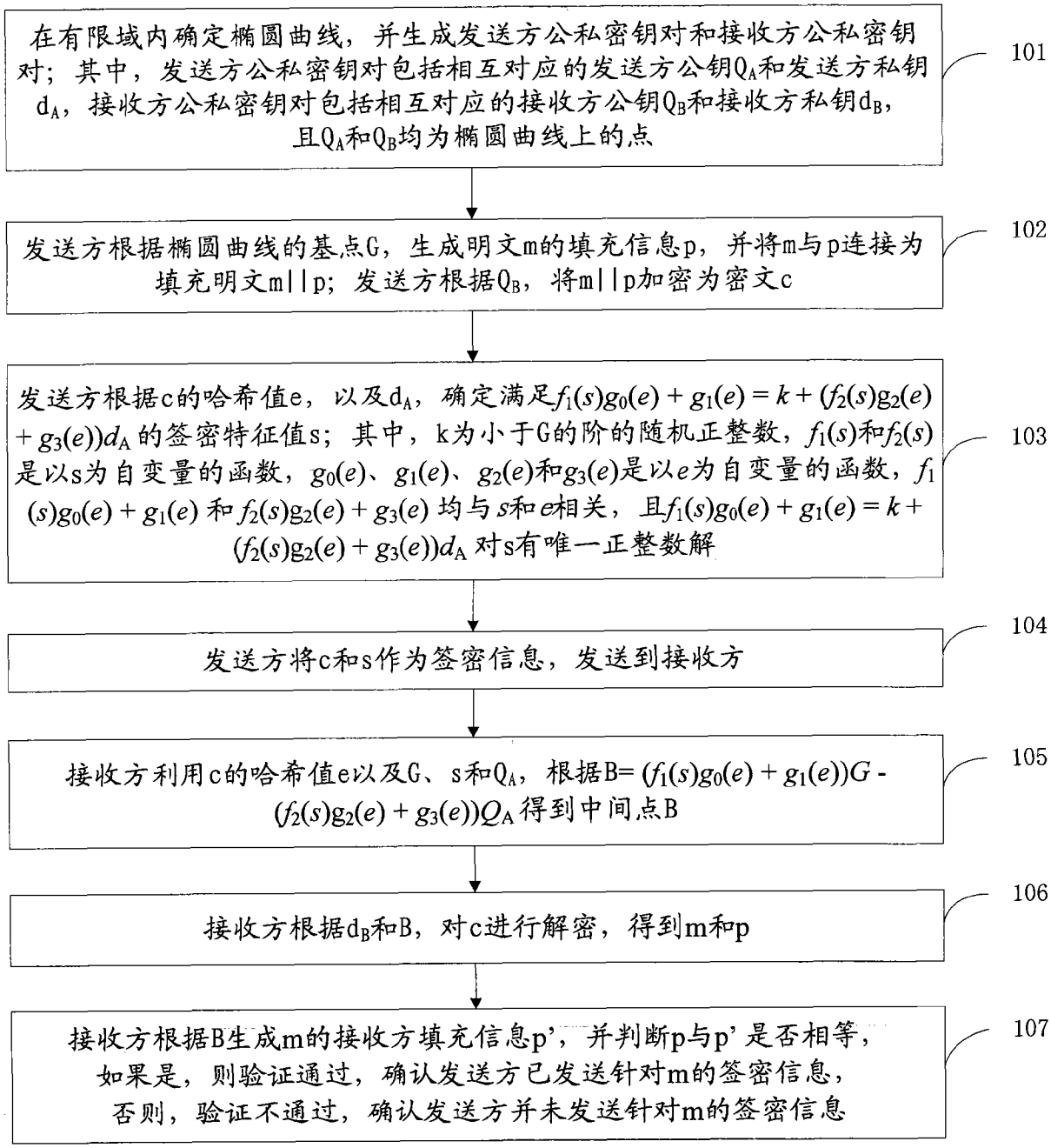

在有限域内确定椭圆曲线，并生成发送方公私密钥对和接收方公私密钥对；其中，发送方公私密钥对包括相互对应的发送方公钥Q_A和发送方私钥d_A，接收方公私密钥对包括相互对应的接收方公钥Q_B和接收方私钥d_B，且Q_A和Q_B均为椭圆曲线上的点
101
发送方根据椭圆曲线的基点G，生成明文m的填充信息p，并将m与p连接为填充明文m||p；发送方根据Q_B，将m||p加密为密文c
102
发送方根据c的哈希值e，以及d_A，确定满足$f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$的签密特征值s；其中，k为小于G的阶的随机正整数，$f_1(s)$和$f_2(s)$是以s为自变量的函数，$g_0(e)$、$g_1(e)$、$g_2(e)$和$g_3(e)$是以e为自变量的函数，$f_1(s)g_0(e)+g_1(e)$和$f_2(s)g_2(e)+g_3(e)$均与s和e相关，且$f_1(s)g_0(e)+g_1(e)=k+(f_2(s)g_2(e)+g_3(e))d_A$对s有唯一正整数解
103
发送方将c和s作为签密信息，发送到接收方
104
接收方利用c的哈希值e以及G、s和Q_A，根据$B=(f_1(s)g_0(e)+g_1(e))G-(f_2(s)g_2(e)+g_3(e))Q_A$得到中间点B
105
接收方根据d_B和B，对c进行解密，得到m和p
106
接收方根据B生成m的接收方填充信息p'，并判断p与p'是否相等，如果是，则验证通过，确认发送方已发送针对m的签密信息，否则，验证不通过，确认发送方并未发送针对m的签密信息
107

图 1

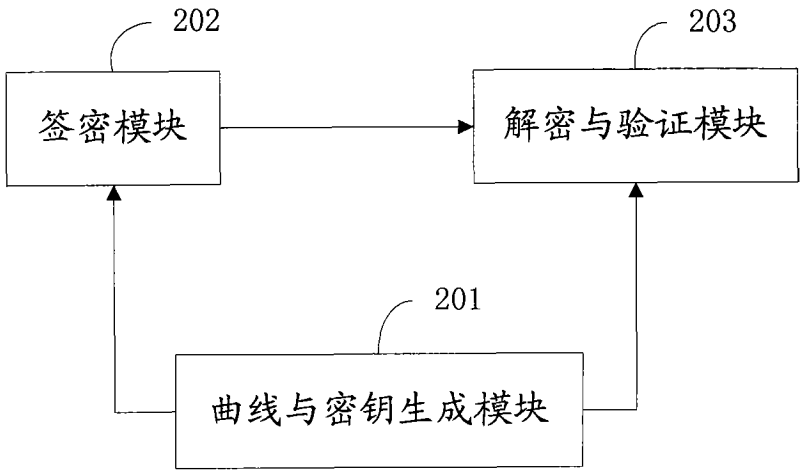


图 2