(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 109309569 B
(45)授权公告日 2021.10.01

(21)申请号 201811147472.4

(22)申请日 2018.09.29

(65)同一申请的已公布的文献号
申请公布号 CN 109309569 A

(43)申请公布日 2019.02.05

(73)专利权人 北京信安世纪科技股份有限公司
地址 100052 北京市西城区宣武门外大街甲1号环球财讯中心C座4层

(72)发明人 刘婷 汪宗斌

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 黄志华

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/30(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 104618116 A,2015.05.13
CN 107360002 A,2017.11.17
EP 2842070 A1,2015.03.04
US 2012089841 A1,2012.04.12
CN 107196763 A,2017.09.22
尚铭.“SM2椭圆曲线门限密码算法”.《密码学报》.2014,
Reza Tourani.″Security, Privacy, and Access Control in Information-Centric Networking: A Survey″.《IEEE communications surveys & tutorials》.2017,

审查员 高凯

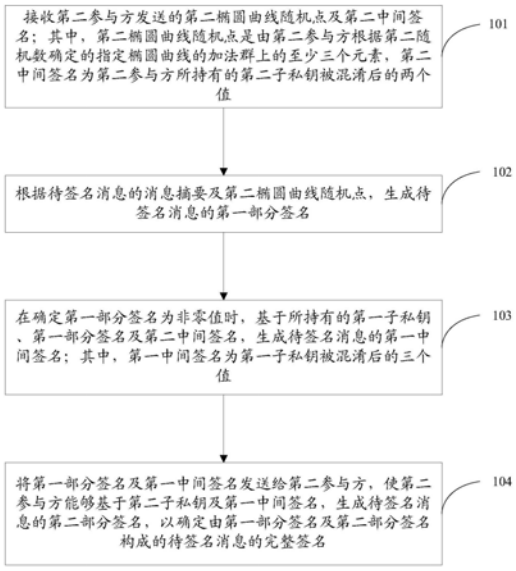
权利要求书7页 说明书19页 附图4页

(54)发明名称

基于SM2算法的协同签名的方法、装置及存储介质

(57)摘要

本发明公开了基于SM2算法的协同签名的方法、装置及存储介质，用以解决现有技术中存在的签名消息易被伪造的技术问题。第一参与方实施的签名方法包括：接收第二参与方发送的由第二随机数确定的第二椭圆曲线随机点及混淆所持有的第二子私钥所产生的第二中间签名；根据待签名消息的消息摘要及第二椭圆曲线随机点，生成待签名消息的第一部分签名；在确定第一部分签名为非零值时，基于所持有的第一子私钥、第一部分签名及第二中间签名生成第一中间签名；将第一部分签名及第一中间签名发送给第二参与方，使第二参与方能够基于第二子私钥及第一中间签名生成待签名消息的第二部分签名，以由第一部分签名及第二部分签名构成待签名消息的完整签名。



CN 109309569 B

1.一种基于SM2算法的协同签名的方法,应用于进行协同签名的第一参与方,其特征在于,包括:

接收第二参与方发送的第二椭圆曲线随机点及第二中间签名;其中,所述第二椭圆曲线随机点是由所述第二参与方根据选取的第二随机数确定的指定椭圆曲线的加法群上的至少三个元素,所述第二中间签名为所述第二参与方所持有的第二子私钥被混淆后的两个值;

根据待签名消息的消息摘要及所述第二椭圆曲线随机点,生成所述待签名消息的第一部分签名;

在确定所述第一部分签名为非零值时,基于所持有的第一子私钥、所述第一部分签名及所述第二中间签名,生成所述待签名消息的第一中间签名;其中,所述第一中间签名为所述第一子私钥被混淆后的三个值,所述第一子私钥、所述第二子私钥均为从[1,n-1]内选取的整数,且所述第一参与方和所述第二参与方均不知对方所持有的子私钥和完整的签名私钥,所述完整的签名私钥为(所述第一子私钥×第二子私钥-1)mod n,mod为模运算,n为所述指定椭圆曲线的基点的阶;

将所述第一部分签名及所述第一中间签名发送给所述第二参与方,使所述第二参与方能够基于所述第二子私钥及所述第一中间签名,生成所述待签名消息的第二部分签名,以确定由所述第一部分签名及所述第二部分签名构成的所述待签名消息的完整签名;

其中:

所述第二中间签名采用下列第五公式确定,所述第五公式为:

$$\begin{cases} s_1 = (k_1 \times d_2^{-1}) \bmod n \\ s_2 = (k_3 \times d_2^{-1}) \bmod n \end{cases}$$

其中,s_1和s_2为所述第二中间签名,k_1和k_3为所述第二随机数中的部分随机数,且k_1和k_3的取值范围均为[1,n-1]内的整数,d_2为所述第二子私钥,d_2^{-1}为d_2在有限素域F_p上的逆元$d_2^{-1} \bmod n$;

所述第一中间签名采用下列公式确定:

$$\begin{cases} s_3 = (k_5 \times d_1^{-1}) \bmod n \\ s_4 = [(r + k_7) \times d_1^{-1}] \bmod n \\ s_5 = (k_4 \times s_1 + k_6 \times d_1^{-1} \times s_2 - r) \bmod n \end{cases}$$

其中,s_3至s_5为所述第一中间签名,k_4至k_7为第一随机数,且k_4至k_7中任一随机数的取值均是[1,n-1]范围内的整数,r为所述第一部分签名,s_1至s_2为第二中间签名,d_1为所述第一子私钥,d_1^{-1}为d_1在有限素域F_p上的逆元$d_1^{-1} \bmod n$。

2.如权利要求1所述的方法,其特征在于,接收所述第二参与方发送的第二椭圆曲线随机点及第二中间签名之前,还包括:

发送所述待签名消息的签名通知给所述第二参与方,使所述第二参与方收到所述签名通知后生成并发送所述第二椭圆曲线随机点及所述第二中间签名给所述第一参与方。

3.如权利要求1所述的方法,其特征在于,根据待签名消息的消息摘要及所述第二椭圆曲线随机点,生成所述待签名消息的第一部分签名之前,还包括:

对所述待签名消息及指定特征数据进行哈希计算，获得所述消息摘要；其中，所述指定特征数据至少包括所述指定椭圆曲线的相关参数及所述第一参与方与所述第二参与方完整的签名公钥被混淆后的值。

4.如权利要求1所述的方法，其特征在于，根据待签名消息的消息摘要及所述第二椭圆曲线随机点，生成所述待签名消息的第一部分签名，包括：

采用指定算法生成第一随机数；其中，所述第一随机数的数量比接收的所述第二椭圆曲线随机点的数量多一个；

采用第一公式对所述第一随机数及所述第二椭圆曲线随机点进行运算，获得指定椭圆曲线上的第一椭圆曲线随机点；所述第一椭圆曲线随机点为指定椭圆曲线的加法群上的一个元素，所述第一公式用于将所述第一椭圆曲线随机点约束在所述指定椭圆曲线的加法群上；

采用第二公式对所述第一椭圆曲线随机点的横坐标与所述消息摘要进行运算，获得所述第一部分签名。

5.如权利要求4所述的方法，其特征在于，

所述第一公式具体为：

$(x_1,y_1)=k_4[*]R_1[+]k_5[*]R_2[+]k_6[*]R_3[+]k_7[*]G$

其中，(x_1,y_1)为所述第一椭圆曲线随机点，x_1和y_1分别为所述第一椭圆曲线随机点的横纵坐标，k_4至k_7为所述第一随机数，且k_4至k_7中任一随机数均为[1,n-1]范围内的整数，R_1至R_3为所述第二椭圆曲线随机点，所述指定椭圆曲线$E(F_q)$定义在有限素域F_q上，G为所述指定椭圆曲线$E(F_q)$的基点，n为所述基点G的阶，[*]表示椭圆曲线点乘运算，[+]表示椭圆曲线点加运算；

所述第二公式具体为：

$r=(x_1+e)\bmod n$；

其中，r为所述待签名消息的第一部分签名，x1为所述第一椭圆曲线随机点的横坐标，e为所述消息摘要转换而成的整数，n为所述指定椭圆曲线的基点G的阶，mod表示求模运算。

6.一种基于SM2算法的协同签名的方法，应用于进行协同签名的第二参与方，其特征在于，包括：

在接收到第一参与方发送的待签名消息的签名通知时，计算第二椭圆曲线随机点及第二中间签名；其中，所述第二椭圆曲线随机点为所述第二参与方基于选取的第二随机数确定的指定椭圆曲线的加法群上的至少三个元素，所述第二中间签名为所述第二参与方所持有的第二子私钥被混淆后的两个值；

将所述第二椭圆曲线随机点及所述第二中间签名发送给所述第一参与方，使所述第一参与方能够生成所述待签名消息的第一部分签名及第一中间签名；其中，所述第一中间签名是所述第一参与方所持有的第一子私钥被混淆后的三个值，所述第一子私钥、所述第二子私钥均为从[1,n-1]内选取的整数，且所述第一参与方和所述第二参与方均不知对方所持有的子私钥和完整的签名私钥，所述完整的签名私钥为(所述第一子私钥×第二子私钥-1)mod n，mod为模运算，n为所述指定椭圆曲线的基点的阶；

接收所述第一参与方发送的所述待签名消息的第一部分签名及所述第一中间签名，根据所述第二子私钥及所述第一中间签名生成所述待签名消息的第二部分签名；

在确定所述第二部分签名为非零值，且不等于n-r时，确定由所述第一部分签名及所述第二部分签名构成的所述待签名消息的完整签名；其中，n为所述指定椭圆曲线的基点的阶，r为所述待签名消息的第一部分签名；

其中：

所述第二中间签名采用下列第五公式确定，所述第五公式为：

$$\begin{cases} s_1 = (k_1 \times d_2^{-1}) \bmod n \\ s_2 = (k_3 \times d_2^{-1}) \bmod n \end{cases}$$

其中，s_1和s_2为所述第二中间签名，k_1和k_3为所述第二随机数中的部分随机数，且k_1和k_3的取值范围均为[1,n-1]内的整数，d_2为所述第二子私钥，d_2^{-1}为d_2在有限素域F_p上的逆元$d_2^{-1} \bmod n$；

所述第一中间签名采用下列公式确定：

$$\begin{cases} s_3 = (k_5 \times d_1^{-1}) \bmod n \\ s_4 = [(r + k_7) \times d_1^{-1}] \bmod n \\ s_5 = (k_4 \times s_1 + k_6 \times d_1^{-1} \times s_2 - r) \bmod n \end{cases}$$

其中，s_3至s_5为所述第一中间签名，k_4至k_7为第一随机数，且k_4至k_7中任一随机数的取值均是[1,n-1]范围内的整数，r为所述第一部分签名，s_1至s_2为第二中间签名，d_1为所述第一子私钥，d_1^{-1}为d_1在有限素域F_p上的逆元$d_1^{-1} \bmod n$。

7.如权利要求6所述的方法，其特征在于，计算第二椭圆曲线随机点及第二中间签名，包括：

采用指定算法生成第二随机数；其中，所述第二随机数为至少三个随机数；

采用第四公式将第二随机数分别作用于所述第一参与方的第一子公钥、所述第二参与方的第二子公钥及所述指定椭圆曲线的基点，获得第二椭圆曲线随机点；其中，所述第二椭圆曲线随机点为指定椭圆曲线的加法群上的至少三个元素；所述第四公式用于将所述第二椭圆曲线随机点约束在所述指定椭圆曲线的加法群上；

采用所述第五公式对第二随机数中的部分随机数及所述第二子私钥进行模运算，获得所述第二中间签名。

8.如权利要求7所述的方法，其特征在于，所述第四公式具体为：

$$\begin{cases} R_1 = k_1[*]P_1 \\ R_2 = (k_2 \times d_2)[*]P_2 \\ R_3 = k_3[*]G \end{cases}$$

其中，R_1至R_3为所述第二椭圆曲线随机点，k_1至k_3为所述第二随机数，且k_1至k_3中任一随机数的取值范围均为[1,n-1]内的整数，G为所述指定椭圆曲线的基点，P_1、P_2分别为所述第一参与方及所述第二参与方的所述第一子公钥及第二子公钥，P_1为所述第一参与方所述第一子私钥与所述基点G计算得到的，P_2为所述第二参与方用所述第二子私钥与所述基点G计算得到的，d_2为所述第二子私钥。

9.如权利要求6-8任一权项所述的方法，其特征在于，接收所述第一参与方发送的所述待签名消息的第一部分签名及所述第一中间签名，根据所述第二子私钥及所述第一中间签

名生成所述待签名消息的第二部分签名，包括：

接收所述第一参与方发送的所述待签名消息的第一部分签名及所述第一中间签名；

采用第六公式，根据所述第二子私钥及所述第一中间签名，生成所述待签名消息的第二部分签名。

10.如权利要求9所述的方法，其特征在于，所述第六公式具体为：

$$s=(s_5+k_2\times d_2\times s_3+d_2^{-1}\times s_4)\bmod n$$

其中，s为所述待签名消息的第二部分签名，s_3至s_5为所述第一中间签名，k_2为所述第二随机数中的部分随机数，且k_2的取值范围均为[1,n-1]内的整数，d_2为所述第二子私钥，d_2^{-1}为所述第二子私钥d_2在有限素域F_p上的逆元d_2^{-1}mod n，mod为求模运算。

11.一种基于SM2算法的协同签名的装置，应用于第一参与方，其特征在于，包括：

接收单元，用于接收第二参与方发送的第二椭圆曲线随机点及第二中间签名；其中，所述第二椭圆曲线随机点是由所述第二参与方根据选取的第二随机数确定的指定椭圆曲线的加法群上的至少三个元素，所述第二中间签名为所述第二参与方所持有的第二子私钥被混淆后的两个值；

生成单元，用于根据待签名消息的消息摘要及所述第二椭圆曲线随机点，生成所述待签名消息的第一部分签名；

所述生成单元，还用于在确定所述第一部分签名为非零值时，基于所持有的第一子私钥、所述第一部分签名及所述第二中间签名，生成所述待签名消息的第一中间签名；其中，所述第一中间签名为所述第一子私钥被混淆后的三个值，所述第一子私钥、所述第二子私钥均为从[1,n-1]内选取的整数，且所述第一参与方和所述第二参与方均不知对方所持有的子私钥和完整的签名私钥，所述完整的签名私钥为(所述第一子私钥×第二子私钥-1) mod n，mod为模运算，n为所述指定椭圆曲线的基点的阶；

发送单元，用于将所述第一部分签名及所述第一中间签名发送给所述第二参与方，使所述第二参与方能够基于所述第二子私钥及所述第一中间签名，生成所述待签名消息的第二部分签名，以确定由所述第一部分签名及所述第二部分签名构成的所述待签名消息的完整签名；

其中：

所述第二中间签名采用下列第五公式确定，所述第五公式为：

$$\begin{cases}s_1=(k_1\times d_2^{-1})\bmod n\\ s_2=(k_3\times d_2^{-1})\bmod n\end{cases}$$

其中，s_1和s_2为所述第二中间签名，k_1和k_3为所述第二随机数中的部分随机数，且k_1和k_3的取值范围均为[1,n-1]内的整数，d_2为所述第二子私钥，d_2^{-1}为d_2在有限素域F_p上的逆元d_2^{-1}mod n；

所述第一中间签名采用下列公式确定：

$$\begin{cases} s_3 = (k_5 \times d_1^{-1}) \bmod n \\ s_4 = [(r + k_7) \times d_1^{-1}] \bmod n \\ s_5 = (k_4 \times s_1 + k_6 \times d_1^{-1} \times s_2 - r) \bmod n \end{cases}$$

其中，s_3至s_5为所述第一中间签名，k_4至k_7为第一随机数，且k_4至k_7中任一随机数的取值均是[1,n-1]范围内的整数，r为所述第一部分签名，s_1至s_2为第二中间签名，d_1为所述第一子私钥，d_1^{-1}为d_1在有限素域F_p上的逆元d_1^{-1}mod n。

12.如权利要求11所述的装置，其特征在于，所述发送单元还用于：

发送待签名消息的签名通知给所述第二参与方，使所述第二参与方收到所述签名通知后生成并发送所述第二椭圆曲线随机点及所述第二中间签名给所述第一参与方。

13.如权利要求11所述的装置，其特征在于，所述生成单元还用于：

对所述待签名消息及指定特征数据进行哈希计算，获得所述消息摘要；其中，所述指定特征数据至少包括所述指定椭圆曲线的相关参数及所述第一参与方与所述第二参与方完整的签名公钥被混淆后的值。

14.如权利要求11所述的装置，其特征在于，所述生成单元具体用于：

采用指定算法生成第一随机数；其中，所述第一随机数的数量比接收的所述第二椭圆曲线随机点的数量多一个；

采用第一公式对所述第一随机数及所述第二椭圆曲线随机点进行运算，获得指定椭圆曲线上的第一椭圆曲线随机点；所述第一椭圆曲线随机点为指定椭圆曲线的加法群上的一个元素，所述第一公式用于将所述第一椭圆曲线随机点约束在所述指定椭圆曲线的加法群上；

采用第二公式对所述第一椭圆曲线随机点的横坐标与所述消息摘要进行运算，获得所述第一部分签名。

15.如权利要求14所述的装置，其特征在于，

所述第一公式具体为：

$(x_1,y_1)=k_4[*]R_1[+]k_5[*]R_2[+]k_6[*]R_3[+]k_7[*]G$

其中，(x_1,y_1)为所述第一椭圆曲线随机点，x_1和y_1分别为所述第一椭圆曲线随机点的横纵坐标，k_4至k_7为所述第一随机数，且k_4至k_7中任一随机数均为[1,n-1]范围内的整数，R_1至R_3为所述第二椭圆曲线随机点，所述指定椭圆曲线$E(F_q)$定义在有限素域F_q上，G为所述指定椭圆曲线$E(F_q)$的基点，n为所述基点G的阶，[*]表示椭圆曲线点乘运算，[+]表示椭圆曲线点加运算；

所述第二公式具体为：

$r=(x_1+e) \bmod n$；

其中，r为所述待签名消息的第一部分签名，x1为所述第一椭圆曲线随机点的横坐标，e为所述消息摘要转换而成的整数，n为所述指定椭圆曲线的基点的阶，mod表示求模运算。

16.一种基于SM2算法的协同签名的装置，应用于进行协同签名的第二参与方，其特征在于，包括：

接收单元，用于在接收到第一参与方发送的待签名消息的签名通知时，计算第二椭圆曲线随机点及第二中间签名；其中，所述第二椭圆曲线随机点为所述第二参与方基于选取

的第二随机数确定的指定椭圆曲线的加法群上的至少三个元素，所述第二中间签名为所述第二参与方所持有的第二子私钥被混淆后的两个值；

发送单元，用于将所述第二椭圆曲线随机点及所述第二中间签名发送给所述第一参与方，使所述第一参与方能够生成所述待签名消息的第一部分签名及第一中间签名；其中，所述第一中间签名是所述第一参与方所持有的第一子私钥被混淆后的三个值，所述第一子私钥、所述第二子私钥均为从[1,n-1]内选取的整数，且所述第一参与方和所述第二参与方均不知对方所持有的子私钥和完整的签名私钥，所述完整的签名私钥为(所述第一子私钥×第二子私钥-1)mod n，mod为模运算，n为所述指定椭圆曲线的基点的阶；

所述接收单元，还用于接收所述第一参与方发送的所述待签名消息的第一部分签名及所述第一中间签名，根据所述第二子私钥及所述第一中间签名生成所述待签名消息的第二部分签名；

生成单元，用于在确定所述第二部分签名为非零值，且不等于n-r时，确定由所述第一部分签名及所述第二部分签名构成的所述待签名消息的完整签名；其中，n为所述指定椭圆曲线的基点的阶，r为所述待签名消息的第一部分签名；

其中：

所述第二中间签名采用下列第五公式确定，所述第五公式为：

$$\begin{cases} s_1 = (k_1 \times d_2^{-1}) \bmod n \\ s_2 = (k_3 \times d_2^{-1}) \bmod n \end{cases}$$

其中，s_1和s_2为所述第二中间签名，k_1和k_3为所述第二随机数中的部分随机数，且k_1和k_3的取值范围均为[1,n-1]内的整数，d_2为所述第二子私钥，d_2^{-1}为d_2在有限素域F_p上的逆元d_2^{-1}mod n；

所述第一中间签名采用下列公式确定：

$$\begin{cases} s_3 = (k_5 \times d_1^{-1}) \bmod n \\ s_4 = [(r + k_7) \times d_1^{-1}] \bmod n \\ s_5 = (k_4 \times s_1 + k_6 \times d_1^{-1} \times s_2 - r) \bmod n \end{cases}$$

其中，s_3至s_5为所述第一中间签名，k_4至k_7为第一随机数，且k_4至k_7中任一随机数的取值均是[1,n-1]范围内的整数，r为所述第一部分签名，s_1至s_2为第二中间签名，d_1为所述第一子私钥，d_1^{-1}为d_1在有限素域F_p上的逆元d_1^{-1}mod n。

17.如权利要求16所述的装置，其特征在于，所述接收单元，具体用于：

采用指定算法生成第二随机数；其中，所述第二随机数为至少三个随机数；

采用第四公式将第二随机数分别作用于所述第一参与方的第一子公钥、所述第二参与方的第二子公钥及所述指定椭圆曲线的基点，获得第二椭圆曲线随机点；其中，所述第二椭圆曲线随机点为指定椭圆曲线的加法群上的至少三个元素；所述第四公式用于将所述第二椭圆曲线随机点约束在所述指定椭圆曲线的加法群上；

采用第五公式对第二随机数中的部分随机数及所述第二子私钥进行模运算，获得第二中间签名。

18.如权利要求17所述的装置，其特征在于，所述第四公式具体为：

$$\begin{cases} R_1 = k_1[*]P_1 \\ R_2 = (k_2 \times d_2)[*]P_2 \\ R_3 = k_3[*]G \end{cases}$$

其中，R_1至R_3为所述第二椭圆曲线随机点，k_1至k_3为所述第二随机数，且k_1至k_3中任一随机数的取值范围均为[1,n-1]内的整数，G为所述指定椭圆曲线的基点，P_1、P_2分别为所述第一参与方及所述第二参与方的所述第一子公钥及第二子公钥，P_1为所述第一参与方所述第一子私钥与所述基点G计算得到的，P_2为所述第二参与方用所述第二子私钥与所述基点G计算得到的，d_2为所述第二子私钥。

19.如权利要求16-18任一权项所述的装置，其特征在于，所述接收单元具体用于：

接收所述第一参与方发送的所述待签名消息的第一部分签名及所述第一中间签名；

采用第六公式，根据所述第二子私钥及所述第一中间签名，生成所述待签名消息的第二部分签名。

20.如权利要求19所述的装置，其特征在于，所述第六公式具体为：

$$s = (s_5 + k_2 \times d_2 \times s_3 + d_2^{-1} \times s_4) \bmod n$$

其中，s为所述待签名消息的第二部分签名，s_3至s_5为所述第一中间签名，k_2为所述第二随机数中的部分随机数，且k_2的取值范围均为[1,n-1]内的整数，d_2为所述第二子私钥，d_2^{-1}为所述第二子私钥d_2在有限素域F_p上的逆元d_2^{-1}mod n，mod为求模运算。

21.一种基于SM2算法的协同签名的装置，其特征在于，包括：

至少一个处理器，以及

与所述至少一个处理器连接的存储器；

其中，所述存储器存储有可被所述至少一个处理器执行的指令，所述至少一个处理器通过执行所述存储器存储的指令，执行如权利要求1-5任一项所述的方法。

22.一种基于SM2算法的协同签名的装置，其特征在于，包括：

至少一个处理器，以及

与所述至少一个处理器连接的存储器；

其中，所述存储器存储有可被所述至少一个处理器执行的指令，所述至少一个处理器通过执行所述存储器存储的指令，执行如权利要求6-10任一项所述的方法。

23.一种计算机可读存储介质，其特征在于：

所述计算机可读存储介质存储有计算机指令，当所述计算机指令在计算机上运行时，使得计算机执行如权利要求1-5中任一项所述的方法。

24.一种计算机可读存储介质，其特征在于：

所述计算机可读存储介质存储有计算机指令，当所述计算机指令在计算机上运行时，使得计算机执行如权利要求6-10中任一项所述的方法。

基于SM2算法的协同签名的方法、装置及存储介质

技术领域

[0001] 本发明涉及信息安全与密码学领域，尤其是涉及基于SM2算法的协同签名的方法、装置及存储介质。

背景技术

[0002] 在信息安全与密码学领域中，PKI(Public Key Infrastructure，公钥基础设施)技术自20世纪80年代出现以来，已经成为越来越广泛使用的通用安全技术。作为一种技术体系，以公钥密码体制为基础的PKI系统，对网络传输层和应用层的数据进行加密、解密、签名、验证，有效保证了用户身份的真实性、信息的机密性、完整性和签名者的不可否认性等。

[0003] 基于PKI的应用，实体的私钥保护问题至关重要。实体所拥有的私钥，只有实体自己才能访问，其他任何实体(包括CA)都不能访问。比如，在桌面应用场景中，通常给用户配备智能密码钥匙、智能卡等安全硬件外设来存储用户私钥，客户端软件通过调用这类安全外设中的私钥，并在其中独立进行加解密或数字签名操作，来保障交易数据的安全。

[0004] 随着最近几年新技术的应用越来越成熟，特别是移动智能终端的普及与云计算的部署，信息安全面临着新的挑战。比如，对于智能手机来说，当用户使用手机支付时，增加额外的安全硬件外设，这会给用户带来很大地不便，也与智能手机的方便易用这一设计目标相违背。另一方面，与大多数智能手机配套的Android操作系统是开源的，针对它的安全攻击层出不穷。在移动端若以软件形式存储完整的私钥，很容易被攻击者窃取，从而导致安全事故。

[0005] 为了在移动智能终端或云环境中不泄露完整的私钥，在身份认证、信息防篡改和服务的不可抵赖性等方面，目前出现了通信双方协同签名的技术方案。即双方各自产生部分私钥，双方都不知道完整的签名私钥，通过交互联合完成整个签名过程。协同签名解决了完整的签名私钥在“瘦终端”环境下容易被窃取的问题。但是，现有的协同签名方案，通信一方在将消息摘要发送给另一方的过程中，消息摘要可能被攻击者替换，导致攻击者可以伪造签名。

[0006] 鉴于此，如何防止伪造签名成为一个亟待解决的技术问题。

发明内容

[0007] 本发明提供一种基于SM2算法的协同签名的方法、装置及存储介质，用以解决现有技术中存在的签名消息易被伪造的技术问题。

[0008] 第一方面，为解决上述技术问题，本发明实施例提供的一种基于SM2算法的协同签名的方法，应用于进行协同签名的第一参与方，该方法的技术方案如下：

[0009] 接收第二参与方发送的第二椭圆曲线随机点及第二中间签名；其中，所述第二椭圆曲线随机点是由所述第二参与方根据选取的第二随机数确定的指定椭圆曲线的加法群上的至少三个元素，所述第二中间签名为所述第二参与方所持有的第二子私钥被混淆后的两个值；

[0010] 根据待签名消息的消息摘要及所述第二椭圆曲线随机点，生成所述待签名消息的第一部分签名；

[0011] 在确定所述第一部分签名为非零值时，基于所持有的第一子私钥、所述第一部分签名及所述第二中间签名，生成所述待签名消息的第一中间签名；其中，所述第一中间签名为所述第一子私钥被混淆后的三个值；

[0012] 将所述第一部分签名及所述第一中间签名发送给所述第二参与方，使所述第二参与方能够基于所述第二子私钥及所述第一中间签名，生成所述待签名消息的第二部分签名，以确定由所述第一部分签名及所述第二部分签名构成的所述待签名消息的完整签名。

[0013] 由于第一参与方与第二参与方分别持有第一子私钥与第二子私钥，为了确定位于第一参与方的待签名消息的完整签名，需要第一参与方在接收到第二参与方发送的第二椭圆曲线随机点及第二中间签名之后，根据待签名消息的消息摘要及第二椭圆曲线随机点，生成待签名消息的第一部分签名；基于所持有的第一子私钥、第一部分签名及第二中间签名，生成第一中间签名；并在确定第一部分签名为非零值时，将第一部分签名及第一中间签名发送给第二参与方，使第二参与方能基于第二子私钥及第一中间签名，生成待签名消息的第二部分签名，以确定待签名消息的完整签名。由上述整个协同签名过程表明，即使是参与了协同签名的第二参与方也不知道第一参与方签署了什么消息，所以本发明的签名方案对于第二参与方来说具有盲签名的效果，在产生数字签名的过程中不会泄露第一参与方的隐私；并且由于通信双方持有各自的签名子私钥，使得攻击者即使获取到任何一方的签名子私钥，都无法伪造待签名消息的完整签名，从而实现了保护完整的签名私钥的技术效果。

[0014] 可选的，接收所述第二参与方发送的第二椭圆曲线随机点及第二中间签名之前，还包括：

[0015] 发送所述待签名消息的签名通知给所述第二参与方，使所述第二参与方收到所述签名通知后生成并发送所述第二椭圆曲线随机点及所述第二中间签名给所述第一参与方。

[0016] 可选的，根据待签名消息的消息摘要及所述第二椭圆曲线随机点，生成所述待签名消息的第一部分签名之前，还包括：

[0017] 对所述待签名消息及指定特征数据进行哈希计算，获得所述消息摘要；其中，所述指定特征数据至少包括所述指定椭圆曲线的相关参数及所述第一参与方与所述第二参与方完整的签名公钥被混淆后的值。

[0018] 可选的，根据待签名消息的消息摘要及所述第二椭圆曲线随机点，生成所述待签名消息的第一部分签名，包括：

[0019] 采用指定算法生成第一随机数；其中，所述第一随机数的数量比接收的所述第二椭圆曲线随机点的数量多一个；

[0020] 采用第一公式对所述第一随机数及所述第二椭圆曲线随机点进行运算，获得指定椭圆曲线上的第一椭圆曲线随机点；所述第一椭圆曲线随机点为指定椭圆曲线的加法群上的一个元素，所述第一公式用于将所述第一椭圆曲线随机点约束在所述指定椭圆曲线的加法群上；

[0021] 采用第二公式对所述第一椭圆曲线随机点的横坐标与所述消息摘要进行运算，获得所述第一部分签名。

[0022] 可选的，所述第一公式具体为：

[0023] $(x_1,y_1)=k_4[*]R_1[+]k_5[*]R_2[+]k_6[*]R_3[+]k_7[*]G$

[0024] 其中，(x_1,y_1)为所述第一椭圆曲线随机点，x_1和y_1分别为所述第一椭圆曲线随机点的横纵坐标，k_4至k_7为所述第一随机数，且k_4至k_7中任一随机数均为[1,n-1]范围内的整数，R_1至R_3为所述第二椭圆曲线随机点，所述指定椭圆曲线$E(F_q)$定义在有限素域F_q上，G为所述指定椭圆曲线$E(F_q)$的基点，n为所述基点G的阶，[*]表示椭圆曲线点乘运算，[+]表示椭圆曲线点加运算；

[0025] 所述第二公式具体为：

[0026] $r=(x_1+e)\ \mathrm{mod}\ n$；

[0027] 其中，r为所述待签名消息的第一部分签名，x1为所述第一椭圆曲线随机点的横坐标，e为所述消息摘要转换而成的整数，n为所述指定椭圆曲线的基点的阶，mod表示求模运算。

[0028] 可选的，基于所持有的第一子私钥、所述第一部分签名及所述第二中间签名，生成第一中间签名，具体包括：

[0029] 采用第三公式对所述第一随机数、所述第一部分签名及所述第一参与方的第一子私钥进行模运算，获得所述第一中间签名；其中，所述第三公式用于约束所述第一中间签名的取值范围；所述第三公式具体为：

[0030] $$\begin{cases} s_3=(k_5\times d_1^{-1})\ \mathrm{mod}\ n \\ s_4=[(r+k_7)\times d_1^{-1}]\ \mathrm{mod}\ n \\ s_5=(k_4\times s_1+k_6\times d_1^{-1}\times s_2-r)\ \mathrm{mod}\ n \end{cases}$$

[0031] 其中，s_3至s_5为所述第一中间签名，k_4至k_7为所述第一随机数，且k_4至k_7中任一随机数的取值均是[1,n-1]范围内的整数，n为所述指定椭圆曲线的基点G的阶，r为所述待签名消息的第一部分签名，s_1至s_2为所述第二中间签名，d_1^{-1}为所述第一子私钥d_1在有限素域F_p上的逆元$d_1^{-1}\ \mathrm{mod}\ n$，mod为求模运算。

[0032] 第二方面，为解决上述技术问题，本发明实施例提供的一种基于SM2算法的协同签名的方法，应用于进行协同签名的第二参与方，该方法的技术方案如下：

[0033] 在接收到第一参与方发送的待签名消息的签名通知时，计算第二椭圆曲线随机点及第二中间签名；其中，所述第二椭圆曲线随机点为所述第二参与方基于选取的第二随机数确定的指定椭圆曲线的加法群上的至少三个元素，所述第二中间签名为所述第二参与方所持有的第二子私钥被混淆后的两个值；

[0034] 将所述第二椭圆曲线随机点及所述第二中间签名发送给所述第一参与方，使所述第一参与方能够生成所述待签名消息的第一部分签名及第一中间签名；其中，所述第一中间签名是所述第一参与方所持有的第一子私钥被混淆后的三个值；

[0035] 接收所述第一参与方发送的所述待签名消息的第一部分签名及所述第一中间签名，根据所述第二子私钥及所述第一中间签名生成所述待签名消息的第二部分签名；

[0036] 在确定所述第二部分签名为非零值，且不等于n-r时，确定由所述第一部分签名及所述第二部分签名构成的所述待签名消息的完整签名；其中，n为所述指定椭圆曲线的基点的阶，r为所述待签名消息的第一部分签名。

[0037] 可选的，计算第二椭圆曲线随机点及第二中间签名，包括：

[0038] 采用指定算法生成第二随机数;其中,所述第二随机数为至少三个随机数;

[0039] 采用第四公式将第二随机数分别作用于所述第一参与方的第一子公钥、所述第二参与方的第二子公钥及所述指定椭圆曲线的基点,获得第二椭圆曲线随机点;其中,所述第二椭圆曲线随机点为指定椭圆曲线的加法群上的至少三个元素;所述第四公式用于将所述第二椭圆曲线随机点约束在所述指定椭圆曲线的加法群上;

[0040] 采用第五公式对第二随机数中的部分随机数及所述第二子私钥进行模运算,获得第二中间签名。

[0041] 可选的,所述第四公式具体为:

[0042] $$\begin{cases} R_1 = k_1[*]P_1 \\ R_2 = (k_2 \times d_2)[*]P_2 \\ R_3 = k_3[*]G \end{cases}$$

[0043] 其中,R_1至R_3为所述第二椭圆曲线随机点,k_1至k_3为所述第二随机数,且k_1至k_3中任一随机数的取值范围均为[1,n-1]内的整数,G为所述指定椭圆曲线的基点,P_1、P_2分别为所述第一参与方及所述第二参与方的所述第一子公钥及第二子公钥,P_1为所述第一参与方所述第一子私钥与所述基点G计算得到的,P_2为所述第二参与方用所述第二子私钥与所述基点G计算得到的,d_2为所述第二子私钥。

[0044] 可选的,所述第五公式具体为:

[0045] $$\begin{cases} s_1 = (k_1 \times d_2^{-1}) \bmod n \\ s_2 = (k_3 \times d_2^{-1}) \bmod n \end{cases}$$

[0046] 其中,s_1和s_2为所述第二中间签名,k_1和k_3为所述第二随机数中的部分随机数,且k_1和k_3的取值范围均为[1,n-1]内的整数,d_2^{-1}为所述第二子私钥d_2在有限素域F_p上的逆元$d_2^{-1} \bmod n$,mod为求模运算。

[0047] 可选的,接收所述第一参与方发送的所述待签名消息的第一部分签名及所述第一中间签名,根据所述第二子私钥及所述第一中间签名生成所述待签名消息的第二部分签名,包括:

[0048] 接收所述第一参与方发送的所述待签名消息的第一部分签名及所述第一中间签名;

[0049] 采用第六公式,根据所述第二子私钥及所述第一中间签名,生成所述待签名消息的第二部分签名。

[0050] 可选的,所述第六公式具体为:

[0051] $$s = (s_5 + k_2 \times d_2 \times s_3 + d_2^{-1} \times s_4) \bmod n$$

[0052] 其中,s为所述待签名消息的第二部分签名,s_3至s_5为所述第一中间签名,k_2为所述第二随机数中的部分随机数,且k_2的取值范围均为[1,n-1]内的整数,d_2为所述第二子私钥,d_2^{-1}为所述第二子私钥d_2在有限素域F_p上的逆元$d_2^{-1} \bmod n$,mod为求模运算。

[0053] 第三方面,本发明实施例提供了一种用于基于SM2算法的协同签名的装置,应用于进行协同签名的第一参与方,该装置包括:

[0054] 接收单元,用于接收第二参与方发送的第二椭圆曲线随机点及第二中间签名;其

中，所述第二椭圆曲线随机点是由所述第二参与方根据选取的第二随机数确定的指定椭圆曲线的加法群上的至少三个元素，所述第二中间签名为所述第二参与方所持有的第二子私钥被混淆后的两个值；

[0055] 生成单元，用于根据待签名消息的消息摘要及所述第二椭圆曲线随机点，生成所述待签名消息的第一部分签名；

[0056] 所述生成单元，还用于在确定所述第一部分签名为非零值时，基于所持有的第一子私钥、所述第一部分签名及所述第二中间签名，生成所述待签名消息的第一中间签名；其中，所述第一中间签名为所述第一子私钥被混淆后的三个值；

[0057] 发送单元，用于将所述第一部分签名及所述第一中间签名发送给所述第二参与方，使所述第二参与方能够基于所述第二子私钥及所述第一中间签名，生成所述待签名消息的第二部分签名，以确定由所述第一部分签名及所述第二部分签名构成的所述待签名消息的完整签名。

[0058] 可选的，在接收所述第二参与方发送的第二椭圆曲线随机点及第二中间签名之前，所述发送单元还用于：

[0059] 发送所述待签名消息的签名通知给所述第二参与方，使所述第二参与方收到所述签名通知后生成并发送所述第二椭圆曲线随机点及所述第二中间签名给所述第一参与方。

[0060] 可选的，所述生成单元还用于：

[0061] 对所述待签名消息及指定特征数据进行哈希计算，获得所述消息摘要；其中，所述指定特征数据至少包括所述指定椭圆曲线的相关参数及所述第一参与方与所述第二参与方完整的签名公钥被混淆后的值。

[0062] 可选的，所述生成单元具体用于：

[0063] 采用指定算法生成第一随机数；其中，所述第一随机数的数量比接收的所述第二椭圆曲线随机点的数量多一个；

[0064] 采用第一公式对所述第一随机数及所述第二椭圆曲线随机点进行运算，获得指定椭圆曲线上的第一椭圆曲线随机点；所述第一椭圆曲线随机点为指定椭圆曲线的加法群上的一个元素，所述第一公式用于将所述第一椭圆曲线随机点约束在所述指定椭圆曲线的加法群上。

[0065] 采用第二公式对所述第一椭圆曲线随机点的横坐标与所述消息摘要进行运算，获得所述第一部分签名。

[0066] 可选的，所述第一公式具体为：

[0067] $(x_1,y_1)=k_4[*]R_1[+]k_5[*]R_2[+]k_6[*]R_3[+]k_7[*]G$

[0068] 其中，(x_1,y_1)为所述第一椭圆曲线随机点，x_1和y_1分别为所述第一椭圆曲线随机点的横纵坐标，k_4至k_7为所述第一随机数，且k_4至k_7中任一随机数均为[1,n-1]范围内的整数，R_1至R_3为所述第二椭圆曲线随机点，所述指定椭圆曲线$E(F_q)$定义在有限素域F_q上，G为所述指定椭圆曲线$E(F_q)$的基点，n为所述基点G的阶，[*]表示椭圆曲线点乘运算，[+]表示椭圆曲线点加运算；

[0069] 所述第二公式具体为：

[0070] $r=(x_1+e)\ \mathrm{mod}\ n$；

[0071] 其中，r为所述待签名消息的第一部分签名，x1为所述第一椭圆曲线随机点的横坐

标，e为所述消息摘要转换而成的整数，n为所述指定椭圆曲线的基点的阶，mod表示求模运算。

[0072] 可选的，基于所持有的第一子私钥、所述第一部分签名及所述第二中间签名，生成第一中间签名，具体包括：

[0073] 采用第三公式对所述第一随机数、所述第一部分签名及所述第一参与方的第一子私钥进行模运算，获得所述第一中间签名；其中，所述第三公式用于约束所述第一中间签名的取值范围；所述第三公式具体为：

[0074] $$\begin{cases} s_3 = (k_5 \times d_1^{-1}) \bmod n \\ s_4 = [(r + k_7) \times d_1^{-1}] \bmod n \\ s_5 = (k_4 \times s_1 + k_6 \times d_1^{-1} \times s_2 - r) \bmod n \end{cases}$$

[0075] 其中，s_3至s_5为所述第一中间签名，k_4至k_7为所述第一随机数，且k_4至k_7中任一随机数的取值均是[1,n-1]范围内的整数，n为所述指定椭圆曲线基点G的阶，r为所述待签名消息的第一部分签名，s_1至s_2为所述第二中间签名，d_1^{-1}为所述第一子私钥d_1在有限素域F_p上的逆元$d_1^{-1} \bmod n$，mod为求模运算。

[0076] 第四方面，本发明实施例提供了一种用于基于SM2算法的协同签名的装置，应用于进行协同签名的第二参与方，该装置包括：

[0077] 接收单元，用于在接收到第一参与方发送的待签名消息的签名通知时，计算第二椭圆曲线随机点及第二中间签名；其中，所述第二椭圆曲线随机点为所述第二参与方基于选取的第二随机数确定的指定椭圆曲线的加法群上的至少三个元素，所述第二中间签名为所述第二参与方所持有的第二子私钥被混淆后的两个值；

[0078] 发送单元，用于将所述第二椭圆曲线随机点及所述第二中间签名发送给所述第一参与方，使所述第一参与方能够生成所述待签名消息的第一部分签名及第一中间签名；其中，所述第一中间签名是所述第一参与方所持有的第一子私钥被混淆后的三个值；

[0079] 接收单元，用于接收所述第一参与方发送的所述待签名消息的第一部分签名及所述第一中间签名，根据所述第二子私钥及所述第一中间签名生成所述待签名消息的第二部分签名；

[0080] 所述生成单元，还用于在确定所述第二部分签名为非零值，且不等于n-r时，确定由所述第一部分签名及所述第二部分签名构成的所述待签名消息的完整签名；其中，n为所述指定椭圆曲线的基点的阶，r为所述待签名消息的第一部分签名。

[0081] 可选的，所述接收单元具体用于：

[0082] 采用指定算法生成第二随机数；其中，所述第二随机数为至少三个随机数；

[0083] 采用第四公式将第二随机数分别作用于所述第一参与方的第一子公钥、所述第二参与方的第二子公钥及所述指定椭圆曲线的基点，获得第二椭圆曲线随机点；其中，所述第二椭圆曲线随机点为指定椭圆曲线的加法群上的至少三个元素；所述第四公式用于将所述第二椭圆曲线随机点约束在所述指定椭圆曲线的加法群上；

[0084] 采用第五公式对第二随机数中的部分随机数及所述第二子私钥进行模运算，获得第二中间签名。

[0085] 可选的，所述第四公式具体为：

[0086] $$\begin{cases} R_1 = k_1[*]P_1 \\ R_2 = (k_2 \times d_2)[*]P_2 \\ R_3 = k_3[*]G \end{cases}$$

[0087] 其中，R_1至R_3为所述第二椭圆曲线随机点，k_1至k_3为所述第二随机数，且k_1至k_3中任一随机数的取值范围均为[1,n-1]内的整数，G为所述指定椭圆曲线的基点，P_1、P_2分别为所述第一参与方及所述第二参与方的所述第一子公钥及第二子公钥，P_1为所述第一参与方所述第一子私钥与所述基点G计算得到的，P_2为所述第二参与方用所述第二子私钥与所述基点G计算得到的，d_2为所述第二子私钥。

[0088] 可选的，所述第五公式具体为：

[0089] $$\begin{cases} s_1 = (k_1 \times d_2^{-1}) \bmod n \\ s_2 = (k_3 \times d_2^{-1}) \bmod n \end{cases}$$

[0090] 其中，s_1和s_2为所述第二中间签名，k_1和k_3为所述第二随机数中的部分随机数，且k_1和k_3的取值范围均为[1,n-1]内的整数，d_2^{-1}为所述第二子私钥d_2在有限素域F_p上的逆元$d_2^{-1} \bmod n$，mod为求模运算。

[0091] 可选的，所述接收单元具体用于：

[0092] 接收所述第一参与方发送的所述待签名消息的第一部分签名及所述第一中间签名；

[0093] 采用第六公式，根据所述第二子私钥及所述第一中间签名，生成所述待签名消息的第二部分签名。

[0094] 可选的，所述第六公式具体为：

[0095] $$s = (s_5 + k_2 \times d_2 \times s_3 + d_2^{-1} \times s_4) \bmod n$$

[0096] 其中，s为所述待签名消息的第二部分签名，s_3至s_5为所述第一中间签名，k_2为所述第二随机数中的部分随机数，且k_2的取值范围均为[1,n-1]内的整数，d_2为所述第二子私钥，d_2^{-1}为所述第二子私钥d_2在有限素域F_p上的逆元$d_2^{-1} \bmod n$，mod为求模运算。

[0097] 第五方面，本发明实施例还提供一种用于基于SM2算法的协同签名的装置，包括：

[0098] 至少一个处理器，以及

[0099] 与所述至少一个处理器连接的存储器；

[0100] 其中，所述存储器存储有可被所述至少一个处理器执行的指令，所述至少一个处理器通过执行所述存储器存储的指令，执行如上述第一方面所述的方法。

[0101] 第六方面，本发明实施例还提供一种用于基于SM2算法的协同签名的装置，包括：

[0102] 至少一个处理器，以及

[0103] 与所述至少一个处理器连接的存储器；

[0104] 其中，所述存储器存储有可被所述至少一个处理器执行的指令，所述至少一个处理器通过执行所述存储器存储的指令，执行如上述第二方面所述的方法。

[0105] 第七方面，本发明实施例还提供一种计算机可读存储介质，包括：

[0106] 所述计算机可读存储介质存储有计算机指令，当所述计算机指令在计算机上运行时，使得计算机执行如上述第一方面所述的方法。

[0107] 第八方面，本发明实施例还提供一种计算机可读存储介质，包括：

[0108] 所述计算机可读存储介质存储有计算机指令，当所述计算机指令在计算机上运行时，使得计算机执行如上述第二方面所述的方法。

[0109] 通过本发明实施例的上述一个或多个实施例中的技术方案，本发明实施例至少具有如下技术效果：

[0110] 在本发明提供的实施例中，由于第一参与方与第二参与方分别持有第一子私钥与第二子私钥，为了确定位于第一参与方的待签名消息的完整签名，需要第一参与方在接收到第二参与方发送的第二椭圆曲线随机点及第二中间签名之后，根据待签名消息的消息摘要及第二椭圆曲线随机点，生成待签名消息的第一部分签名；基于所持有的第一子私钥、第一部分签名及第二中间签名，生成第一中间签名；并在确定第一部分签名为非零值时，将第一部分签名及第一中间签名发送给第二参与方，使第二参与方能基于第二子私钥及第一中间签名，生成待签名消息的第二部分签名，以确定待签名消息的完整签名。由上述整个协同签名过程表明，即使是参与了协同签名的第二参与方也不知道第一参与方签署了什么消息，所以本发明的签名方案对于第二参与方来说具有盲签名的效果，在产生数字签名的过程中不会泄露第一参与方的隐私；并且由于通信双方持有各自的签名子私钥，使得攻击者即使获取到任何一方的签名子私钥，都无法伪造待签名消息的完整签名，从而实现了保护完整的签名私钥的技术效果。

[0111] 进一步的，由于待签名消息的消息摘要不需要在第一参与方和第二参与方进行数据传输的信道中传送，从而使得攻击者不能在双方通信过程中以截取和替换消息摘要的方式达到伪造签名的目的。

[0112] 进一步的，由于通信双方分别选取多个随机数，其中任何一方不能确定对方所使用的随机数，从而不能推导出完整的签名私钥，进而进一步的保护了完整的签名私钥，提高了签名的安全性。

[0113] 进一步的，在本发明提供的实施例中，通过让待签名消息的第一部分签名，含有协同签名双方分别选取的多个随机数及双方各自持有的子私钥因子，不但使第一部分签名具有更好的混淆效果，而且也使第一部分签名具有签名的作用，从而提高了协同签名双方进行签名的安全性。

[0114] 进一步的，由于在协同签名的过程中，第一参与方与第二参与方通过两次通信便完成了对待签名消息的签名，从而减少了签名数据在网络中传输的总时间，进而能够满足无线移动通信或云计算环境中低延迟、少交互的应用需求。

附图说明

[0115] 图1为本发明实施例提供的一种基于SM2算法的协同签名方法，应用于第一参与方的流程图；

[0116] 图2为本发明实施例提供的一种基于SM2算法的协同签名方法，应用于第二参与方的流程图；

[0117] 图3为本发明实施例提供的基于SM2算法的协同签名方法双方交互的流程图；

[0118] 图4为本发明实施例提供的一种基于SM2算法的协同签名装置，应用于第一参与方的结构示意图；

[0119] 图5为本发明实施例提供的一种基于SM2算法的协同签名装置，应用于第二参与方的结构示意图。

具体实施方式

[0120] 本发明实施例提供一种基于SM2算法的协同签名的方法、装置及存储介质，以解决现有技术中存在的签名消息易被伪造的技术问题。

[0121] 本申请实施例中的技术方案为解决上述的技术问题，总体思路如下：

[0122] 提供一种基于SM2算法的协同签名的方法，包括：接收第二参与方发送的第二椭圆曲线随机点及第二中间签名；其中，第二椭圆曲线随机点是由第二参与方根据第二随机数确定的指定椭圆曲线的加法群上的至少三个元素，第二中间签名是第二参与方所持有的第二子私钥被混淆后的两个值；根据待签名消息的消息摘要及第二椭圆曲线随机点，生成待签名消息的第一部分签名；在确定第一部分签名为非零值时，基于所持有的第一子私钥、第一部分签名及第二中间签名，生成第一中间签名；其中，第一中间签名为第一子私钥被混淆后的三个值；将第一部分签名及第一中间签名发送给第二参与方，使第二参与方能基于第一中间签名及第二子私钥，生成待签名消息的第二部分签名，以确定由第一部分签名及第二部分签名构成的待签名消息的完整签名。

[0123] 在上述方案中，由于第一参与方与第二参与方分别持有第一子私钥与第二子私钥，为了确定位于第一参与方的待签名消息的完整签名，需要第一参与方在接收到第二参与方发送的第二椭圆曲线随机点及第二中间签名之后，根据待签名消息的消息摘要及第二椭圆曲线随机点，生成待签名消息的第一部分签名；并在确定第一部分签名为非零值时，基于所持有的第一子私钥、第一部分签名及第二中间签名，生成第一中间签名；将第一部分签名及第一中间签名发送给第二参与方，使第二参与方能基于第二子私钥及第一中间签名，生成待签名消息的第二部分签名，以确定待签名消息的完整签名。这就使得攻击者获取任何一方的签名子私钥，都无法伪造待签名消息的完整签名。

[0124] 为了更好地理解上述技术方案，下面通过附图以及具体实施例对本发明技术方案做详细地说明，应当理解本发明实施例以及实施例中的具体特征是对本发明技术方案的详细说明，而不是对本发明技术方案的限定，在不冲突的情况下，本发明实施例以及实施例中的技术特征可以相互组合。

[0125] 以下，将分别从第一参与方、第二参与方的角度对SM2算法的协同签名方法进行描述。

[0126] 请参考图1，本发明实施例提供一种基于SM2算法的协同签名方法，应用于第一参与方，该方法的处理过程如下。

[0127] 步骤101：接收第二参与方发送的第二椭圆曲线随机点及第二中间签名；其中，第二椭圆曲线随机点是由第二参与方根据选取的第二随机数确定的指定椭圆曲线的加法群上的至少三个元素，第二中间签名为第二参与方所持有的第二子私钥被混淆后的两个值。

[0128] 在接收第二参与方发送的第二椭圆曲线随机点及第二中间签名之前，第一参与方发送待签名消息的签名通知给第二参与方，使第二参与方接收到签名通知后，能够生成并发送第二椭圆曲线随机点及第二中间签名给第一参与方。

[0129] 需要说明的是，在使用SM2算法进行协同签名之前，通信双方即第一参与方和第二

参与方需要满足:共享指定椭圆曲线$E(F_p)$的参数;通信双方生成并持有各自的签名私钥;通信双方生成并持有各自的签名公钥及完整的签名公钥。

[0130] 第一参与方和第二参与方共享指定椭圆曲线$E(F_p)$参数,包括有限域F_p的素数p、指定椭圆曲线方程的系数a,$b\in F_p$、指定椭圆曲线$E(F_p)$上的基点$G=(x_G,y_G)$ ($G\neq O$,$x_G\in F_p$,$y_G\in F_p$)和基点G的阶n。指定椭圆曲线$E(F_p)$参数的具体取值,见中华人民共和国密码行业标准GM/T 0003.5-2012《SM2椭圆曲线公钥密码算法第5部分:参数定义》。

[0131] 在双方共享了指定椭圆曲线$E(F_p)$的上述参数之后,第一参与方和第二参与方分别生成并持有各自的签名私钥。第一参与方的签名私钥称之为第一子私钥(可用d_1表示),第二参与方的签名私钥称之为第二子私钥(可用d_2表示),d_1和d_2均随机取为[1,n-1]内的整数。完整的签名私钥定义为$d_A=(d_1\times d_2-1)\ \mathrm{mod}\ n$,通信双方均不知对方的签名私钥,也不知完整的签名私钥d_A。其中,mod表示求模运算。

[0132] 在双方生成各自的签名私钥(即第一子私钥和第二子私钥)之后,便需要生成它们各自的签名公钥,进而确定完整的签名公钥(可用P_A表示)。第一参与方的签名公钥称之为第一子公钥(可用P_1表示),第二参与方的签名公钥称之为第二子公钥(可用P_2表示)。具体地,第一参与方用第一子私钥d_1计算第一子公钥$P_1=d_1[*]G$,并将第一子公钥P_1发送给第二参与方;第二参与方接收并保存第一子公钥P_1,用第二子私钥d_2计算第二子公钥$P_2=d_2[*]G$和完整的签名公钥$P_A=d_2[*]P_1[-]G=(x_A,y_A)$,并将第二子公钥$P_2$发送给第一参与方;第一参与方根据第二子公钥$P_2$计算完整的签名公钥$P_A=d_1[*]P_2[-]G$。这样就使得第一参与方与第二参与方双方均拥有完整的签名公钥。其中,[*]表示椭圆曲线点乘运算,[-]表示椭圆曲线点减运算。

[0133] 在第一参与方和第二参与方均拥有完整的签名公钥之后,当需要对位于第一参与方的待签名消息进行签名操作时,第一参与方需要发送待签名消息的签名通知给第二参与方,使第二参与方在得到签名通知后,生成并发送第二椭圆曲线随机点及第二中间签名给第一参与方。使第二参与方能够将其生成的第二随机数作用于第一子公钥、第二子公钥和指定椭圆曲线的基点G获得指定椭圆曲线$E(F_p)$的加法群上的第二椭圆曲线随机点,及混淆第二子私钥产生的第二中间签名。

[0134] 第一参与方在接收到第二参与方发送的第二椭圆曲线随机点及第二中间签名之后,才能执行步骤102。

[0135] 步骤102:根据待签名消息的消息摘要及第二椭圆曲线随机点,生成待签名消息的第一部分签名。

[0136] 在生成第一部分签名之前,还需要对待签名消息及指定特征数据进行哈希计算,获得消息摘要;其中,指定特征数据至少包括指定椭圆曲线的相关参数及第一参与方与第二参与方完整的签名公钥被混淆后的值。

[0137] 例如,假设待签名消息为info,指定特征数据为与指定椭圆曲线及签名公钥$P_A=(x_A,y_A)$相关的特征,记为$Z=\mathrm{Hash}(ENTL_a||ID_A||a||b||x_G||y_G||x_A||y_A)$,其中,$ENTL_a$为由$ID_A$的字节长度转化成的两字节长比特串,$ID_A$为第一参与方的可辩别标识,a、b为指定椭圆曲线方程的系数,x_G、y_G分别为指定椭圆曲线的基点G的横纵坐标,x_A、y_A分别为完整的签名公钥的横纵坐标。将待签名消息info与指定特征数据Z进行拼接得到M,即M=info||Z。那么待签名消息info的消息摘要记为e的计算公式为:

[0138] e＝Hash(M) (1)

[0139] 其中,Hash()函数可以是SM3密码杂凑算法。

[0140] 具体地,根据待签名消息的消息摘要及第二椭圆曲线随机点,生成待签名消息的第一部分签名的步骤是:先采用指定算法生成第一随机数;其中,第一随机数的数量比第二椭圆曲线随机点的数量多一个;再采用第一公式对第一随机数及第二椭圆曲线随机点进行计算,获得指定椭圆曲线上的第一椭圆曲线随机点;其中,第一椭圆曲线随机点为指定椭圆曲线的加法群上的一个元素,第一公式用于将第一椭圆曲线随机点约束在指定椭圆曲线的加法群上;最后,采用第二公式对第一椭圆曲线随机点的横坐标与消息摘要之和进行模运算,获得第一部分签名。

[0141] 需要说明的是,第一随机数可以通过随机数生成器(即指定算法)随机生成,其取值范围为[1,n-1]的整数,n为指定椭圆曲线的基点G的阶。其中,第一参与方与第二参与方可以采用相同的随机数生成器,也可以采用不同的随机数生成器。

[0142] 具体的,第一公式为:

[0143] $(x_1,y_1)=k_4[*]R_1[+]k_5[*]R_2[+]k_6[*]R_3[+]k_7[*]G$ (2)

[0144] 其中,(x_1,y_1)为第一椭圆曲线随机点,x_1和y_1分别为第一椭圆曲线随机点的横纵坐标,k_4至k_7的为第一随机数,且k_4至k_7中任一随机数均为[1,n-1]范围内的整数,R_1至R_3为第二椭圆曲线随机点,指定椭圆曲线$E(F_q)$定义在有限素域F_q上,G为指定椭圆曲线$E(F_q)$的基点,n为基点G的阶,[*]为椭圆曲线点乘运算,[+]为椭圆曲线点加运算。

[0145] 第二公式具体为:

[0146] $r=(x_1+e)\bmod n$ (3)

[0147] 其中,r为待签名消息的第一部分签名,x1为第一椭圆曲线随机点的横坐标,e为消息摘要转换而成的整数,n为指定椭圆曲线的基点的阶,mod表示求模运算。

[0148] 在得到第一部分签名之后,便可执行步骤103。

[0149] 步骤103:在确定第一部分签名为非零值时,基于所持有的第一子私钥、第一部分签名及第二中间签名,生成待签名消息的第一中间签名;其中,第一中间签名为第一子私钥被混淆后的三个值。

[0150] 在获得第一部分签名之后,还需要进一步的判断第一部分签名是否为0,若为0则第一参与方重新生成第一随机数,并重新计算第一部分签名,直到第一部分签名不为0为止。

[0151] 在确定第一部分签名不为0之后,才能基于所持有的第一子私钥、第一部分签名及第二中间签名,生成待签名消息的第一中间签名。

[0152] 具体的,采用第三公式对第一随机数、第一部分签名及第一参与方的第一子私钥进行模运算,获得第一中间签名;其中,第三公式用于约束第一中间签名的取值范围;

[0153] 其中,第三公式具体为:

[0154]
$$\begin{cases} s_3=(k_5\times d_1^{-1})\bmod n \\ s_4=[(r+k_7)\times d_1^{-1}]\bmod n \\ s_5=(k_4\times s_1+k_6\times d_1^{-1}\times s_2-r)\bmod n \end{cases} \quad (4)$$

[0155] 其中,s_3至s_5为第一中间签名,k_4至k_7为第一随机数,且k_4至k_7中任一随机数的取值

均是[1,n-1]范围内的整数，n为指定椭圆曲线的基点G的阶，r为待签名消息的第一部分签名，s_1至s_2为第二中间签名，d_1^{-1}为第一子私钥d_1在有限素域F_p上的逆元$d_1^{-1} \bmod n$，mod为求模运算。

[0156] 在第一参与方生成待签名消息的第一中间值之后，便可执行步骤104。

[0157] 步骤104：将第一部分签名及第一中间签名发送给第二参与方，使第二参与方能够基于第二子私钥及第一中间签名，生成待签名消息的第二部分签名，以确定由第一部分签名及第二部分签名构成的待签名消息的完整签名。

[0158] 下面将从第二参与方的角度进行描述上述协同签名方法。

[0159] 请参考图2，本发明实施例提供一种基于SM2算法的协同签名方法，应用于第二参与方，该方法的处理过程如下。

[0160] 步骤201：在接收到第一参与方发送的待签名消息的签名通知时，计算第二椭圆曲线随机点及第二中间签名；其中，第二椭圆曲线随机点为第二参与方基于选取的第二随机数确定的指定椭圆曲线的加法群上的至少三个元素，第二中间签名为第二参与方所持有的第二子私钥被混淆后的两个值。

[0161] 具体地，第二参与方计算第二椭圆曲线随机点及第二中间签名，需要先采用指定算法生成第二随机数；其中，第二随机数为至少三个随机数；然后再采用第四公式将第二随机数分别作用于第一参与方的第一子公钥、第二参与方的第二子公钥及指定椭圆曲线的基点，获得第二椭圆曲线随机点；其中，第二椭圆曲线随机点为指定椭圆曲线的加法群上的至少三个元素；第四公式用于将第二椭圆曲线随机点约束在指定椭圆曲线的加法群上；最后采用第五公式对第二子随机数中的部分随机数及第二子私钥分量进模n运算，获得第二中间签名。

[0162] 具体的，第四公式为：

[0163]
$$\begin{cases} R_1 = k_1[*]P_1 \\ R_2 = (k_2 \times d_2)[*]P_2 \\ R_3 = k_3[*]G \end{cases} \qquad (5)$$

[0164] 其中，R_1至R_3为第二椭圆曲线随机点，k_1至k_3为第二随机数，且k_1至k_3中任一随机数的取值范围均为[1,n-1]内的整数，G为指定椭圆曲线的基点，P_1、P_2分别为第一参与方及第二参与方的第一子公钥及第二子公钥，P_1为第一参与方用第一子私钥与基点计算得到的，P_2为第二参与方用第二子私钥与基点计算得到的，d_2为第二子私钥。

[0165] 进一步的，第五公式具体为：

[0166]
$$\begin{cases} s_1 = (k_1 \times d_2^{-1}) \bmod n \\ s_2 = (k_3 \times d_2^{-1}) \bmod n \end{cases} \qquad (6)$$

[0167] 其中，s_1和s_2为第二中间签名，k_1和k_3为第二随机数中的部分随机数，且k_1和k_3的取值范围均为[1,n-1]内的整数，d_2为第二子私钥d_2在有限素域Fp上的逆元$d_2^{-1} \bmod n$，mod为求模运算。

[0168] 在获得第二椭圆曲线随机点及第二中间签名之后，便可执行步骤202。

[0169] 步骤202：将第二椭圆曲线随机点及第二中间签名发送给第一参与方，使第一参与

方能够生成待签名消息的第一部分签名及第一中间签名;其中,第一中间签名是第一参与方所持有的第一子私钥被混淆后的三个值。

[0170] 在第二参与方将第二椭圆曲线随机点及第二中间签名发送给第一参与方之后,第二参与方将返回待签名消息的第一部分签名及第一中间签名,进而使第二参与方能接着执行步骤203-204。

[0171] 步骤203:接收第一参与方发送的待签名消息的第一部分签名及第一中间签名,根据第二子私钥及第一中间签名,生成待签名消息的第二部分签名。

[0172] 在第二参与方接收到第一部分签名及第一中间签名时,便可根据第六公式计算第二部分签名,具体的第六公式为:

[0173] $$s=(s_5+k_2\times d_2\times s_3+d_2^{-1}\times s_4)\bmod n \qquad (7)$$

[0174] 其中,s为第二部分签名,s_3至s_5为第一中间签名,k_2为第二随机数中的部分随机数,且k_2的取值范围为[1,n-1]内的整数,d_2为第二子私钥,d_2^{-1}为d_2在有限素域F_p上的逆元$d_2^{-1}\bmod n$,mod为求模运算。

[0175] 在获得第二部分签名之后,便可执行步骤204。

[0176] 步骤204:在确定第二部分签名为非零值,且不等于n-r时,确定由第一部分签名及第二部分签名构成的待签名消息的完整签名;其中,n为指定椭圆曲线的基点的阶,r为待签名消息的第一部分签名。

[0177] 在获得第二部分签名之后,还需要先判断第二部分签名是否等于0,若不等于0还需要进一步判断是否等于n-r。若判断结果为第二部分签名为0或n-r中的任一值,将返回到步骤201重新生成第二随机数,让第二参与方重新生成第二部分签名,直到第二部分签名既不等于0也不等于n-r。

[0178] 在确定第二部分签名既不等于0也不等于n-r时,便可根据获得的第一部分签名r和第二部分签名s,获得待签名消息的完整签名(r,s)。

[0179] 为了使本领域的技术人员能更加清楚的理解上述协同签名过程,下面将从第一参与方和第二参与方进行交互的过程进行详细的描述。

[0180] 假设第一参与方需要对待签名消息info进行签名操作,请参见图3,待签名消息info的签名操作过程为:

[0181] 步骤301:第一参与方发送待签名消息的签名通知给第二参与方。

[0182] 步骤302:第二参与方在接收到签名通知后,生成第二椭圆曲线随机点及第二中间签名。

[0183] 具体地,生成第二椭圆曲线随机点的步骤为:第二参与方使用随机数生成器生成第二随机数,然后将第二随机数分别作用于双方的子公钥及指定椭圆曲线的基点生成第二椭圆曲线随机点;生成第二中间签名的公式具体请参见前述的第五公式,在此不再赘述。

[0184] 需要说明的是,第二参与方选取的第二随机数的数量为至少三个。若数量是三个,表示为k_1,k_2,k_3,则基于这三个随机数确定的第二椭圆曲线随机点的数量也是三个,表示为R_1,R_2,R_3。它们的计算公式具体请参见第四公式(即公式(5))。

[0185] 其中,“至少”的意思是指第二参与方可以选取多于三个的随机数,比如除了k_1,k_2,k_3,还选取k_8,k_9,k_{10}。由于第二参与方持有第一子公钥P_1、第二子公钥P_2和指定椭圆曲线的

基点G这三个基础的指定椭圆曲线的加法群元素，因此，若基于六个随机数k_1，k_2，k_3，k_8，k_9，k_{10}生成六个指定椭圆曲线上的随机点R'_1至R'_6，它们的计算公式可为：

[0186] $$\begin{cases} R'_1 = k_1[*]P_1 \\ R'_2 = (k_2 \times d_2)[*]P_2 \\ R'_3 = k_3[*]G \\ R'_4 = k_8[*]P_1 \\ R'_5 = (k_9 \times d_2)[*]P_2 \\ R'_6 = k_{10}[*]G \end{cases} \quad (8)$$

[0187] 则R'_1至R'_6可以分别合并为指定椭圆曲线上的三个随机点R_1-R_3，即：

[0188] $$\begin{cases} R_1 = R'_1 + R'_4 = (k_1 + k_8)[*]P_1 \\ R_2 = R'_2 + R'_5 = (k_2 + k_9) \times d_2[*]P_2 \\ R_3 = R'_3 + R'_6 = (k_3 + k_{10})[*]G \end{cases} \quad (9)$$

[0189] 而k_1+k_8，k_2+k_9和k_3+k_{10}的结果也是随机数，直接由三个随机数表示即可。所以，第二参与方若选取多于三个的随机数，并产生多于三个的指定椭圆曲线上的随机点，第二参与方可以按照前述方法将多于三个的随机点合并为指定椭圆曲线上的三个随机点。

[0190] 步骤303：第二参与方将第二椭圆曲线随机点及第二中间签名发送给第一参与方。

[0191] 步骤304：第一参与方根据接收到的第二椭圆曲线随机点及第二中间签名，生成待签名消息的第一部分签名。

[0192] 在第一参与方接收到第二椭圆曲线随机点及第二中间签名之后，用随机数生成器生成第一随机数，第一随机数的数量要比第二随机数的数量多一个。

[0193] 然后，采用第一公式对第一随机数及第二椭圆曲线随机点进行计算，获得第一椭圆曲线随机点，具体的计算方式请参见之前的公式。

[0194] 并且，第一参与方还根据待签名消息info及指定特征数据Z计算出待签名消息的消息摘要e，并对消息摘要与坐标点的横坐标求和之后的值进行模运算，获得第一部分签名r。具体的计算方式请参见前述第二公式，在此不再赘述。

[0195] 步骤305：第一参与方判断第一部分签名是否为非零值，若为零则重新执行步骤304，若为非零值，则计算第一中间签名(s_3-s_5)。具体的计算方式请参见前述第三公式，在此不再赘述。

[0196] 步骤306：第一参与方将第一部分签名r及第一中间签名(s_3-s_5)发送给第二参与方。

[0197] 步骤307：第二参与方根据第一部分签名r及第一中间签名(s_3-s_5)，计算第二部分签名s。具体的第二部分签名的公式请见前述第六公式，在此不再赘述。

[0198] 步骤308：判断第二部分s是否不为0且不为n-r，若为是则获得待签名消息的完整签名(r,s)，否则重新从步骤302开始执行，直到第二部分s不为0且不为n-r为止。

[0199] 通过使用本发明的上述协同签名方案，让待签名消息的消息摘要由第一参与方计算得到，并基于通信双方选取的多个随机数确定第一椭圆曲线随机点，第一参与方使用第一椭圆曲线随机点的横坐标混淆消息摘要，从而生成待签名消息的第一部分签名。由于第一参与方通过上述方式对消息摘要进行混淆后得到第一部分签名，所以第一参与方只需要将第一部分签名发送给第二参与方而不需要将消息摘要传送给第二参与方。所以，一方面，第二参与方并不知道第一参与方签署了什么消息，使得本发明的协同签名方案对于第二参

与方来说具有盲签名的效果;另一方面,由于消息摘要不需要在通信过程中传送,使得攻击者不能在通信过程中以替换消息摘要的方式达到伪造签名的目的。

[0200] 通过本发明实施例的上述协同签名方案得到的待签名消息的完整签名(r,s),由第一参与方产生的至少四个随机数、第二参与方产生的至少三个随机数以及双方的签名子私钥确定。因此,一方面,通信双方的任何一方不能确定对方选取的随机数和对方的签名子私钥,从而不能推导出完整的签名私钥d_A,这有效保护了完整的签名私钥的安全性;另一方面,待签名消息的第一部分签名r含有私钥因子和多个随机因子,与SM2算法输出的待签名消息的第一部分签名相比,不但使消息摘要具有更好的混淆效果,而且更具有签名的意义。

[0201] 本发明实施例公开的协同签名方案,首先由第二参与方将产生的第二椭圆曲线随机点及第二中间签名发送给第一参与方,供第一参与方生成待签名消息的第一部分签名;然后第一参与方将生成的第一部分签名及第一中间签名发送给第二参与方,供第二参与方生成待签名消息的第二部分签名,从而确定由第一部分签名及第二部分签名构成的待签名消息的完整签名。可见,本发明实施例中的协同签名方案,第一参与方与第二参与方只需要进行两次通信便可获得待签名消息的完整签名,从而可满足无线移动通信或云计算环境中低延迟、少交互的应用需求,减少交互过程中存在的风险。

[0202] 上述协同签名方案的签名验证方法,遵循SM2签名验证的方法,在此不再赘述。验签公钥,就是完整的签名公钥P_A。

[0203] 基于同一发明构思,本发明一实施例中提供一种用于SM2算法的协同签名的装置,应用于第一参与方,该装置的协同签名方法的具体实施方式可参见第一参与方的方法实施例部分的描述,重复之处不再赘述,请参见图4,该装置包括:

[0204] 接收单元401,用于接收第二参与方发送的第二椭圆曲线随机点及第二中间签名;其中,所述第二椭圆曲线随机点是由所述第二参与方根据选取的第二随机数确定的指定椭圆曲线的加法群上的至少三个元素,所述第二中间签名为所述第二参与方所持有的第二子私钥被混淆后的两个值;

[0205] 生成单元402,用于根据待签名消息的消息摘要及所述第二椭圆曲线随机点,生成所述待签名消息的第一部分签名;

[0206] 所述生成单元402,还用于在确定所述第一部分签名为非零值时,基于所持有的第一子私钥、所述第一部分签名及所述第二中间签名,生成所述待签名消息的第一中间签名;其中,所述第一中间签名为所述第一子私钥被混淆后的三个值;

[0207] 发送单元403,用于将所述第一部分签名及所述第一中间签名发送给所述第二参与方,使所述第二参与方能够基于所述第二子私钥及所述第一中间签名,生成所述待签名消息的第二部分签名,以确定由所述第一部分签名及所述第二部分签名构成的所述待签名消息的完整签名。

[0208] 可选的,在接收所述第二参与方发送的第二椭圆曲线随机点及第二中间签名之前,所述发送单元403还用于:

[0209] 发送所述待签名消息的签名通知给所述第二参与方,使所述第二参与方收到所述签名通知后生成并发送所述第二椭圆曲线随机点及所述第二中间签名给所述第一参与方。

[0210] 可选的,所述生成单元402还用于:

[0211] 对所述待签名消息及指定特征数据进行哈希计算,获得所述消息摘要;其中,所述

指定特征数据至少包括所述指定椭圆曲线的相关参数及所述第一参与方与所述第二参与方完整的签名公钥被混淆后的值。

[0212] 可选的，所述生成单元402具体用于：

[0213] 采用指定算法生成第一随机数；其中，所述第一随机数的数量比接收的所述第二椭圆曲线随机点的数量多一个；

[0214] 采用第一公式对所述第一随机数及所述第二椭圆曲线随机点进行运算，获得指定椭圆曲线上的第一椭圆曲线随机点；所述第一椭圆曲线随机点为指定椭圆曲线的加法群上的一个元素，所述第一公式用于将所述第一椭圆曲线随机点约束在所述指定椭圆曲线的加法群上；

[0215] 采用第二公式对所述第一椭圆曲线随机点的横坐标与所述消息摘要进行运算，获得所述第一部分签名。

[0216] 可选的，所述第一公式具体为：

[0217] $(x_1,y_1)=k_4[*]R_1[+]k_5[*]R_2[+]k_6[*]R_3[+]k_7[*]G$

[0218] 其中，(x_1,y_1)为所述第一椭圆曲线随机点，x_1和y_1分别为所述第一椭圆曲线随机点的横纵坐标，k_4至k_7为所述第一随机数，且k_4至k_7中任一随机数均为[1,n-1]范围内的整数，R_1至R_3为所述第二椭圆曲线随机点，所述指定椭圆曲线$E(F_q)$定义在有限素域F_q上，G为所述指定椭圆曲线$E(F_q)$的基点，n为所述基点G的阶，[*]表示椭圆曲线点乘运算，[+]表示椭圆曲线点加运算；

[0219] 所述第二公式具体为：

[0220] $r=(x_1+e)\ \mathrm{mod}n$；

[0221] 其中，r为所述待签名消息的第一部分签名，x1为所述第一椭圆曲线随机点的横坐标，e为所述消息摘要转换而成的整数，n为所述指定椭圆曲线的基点的阶，mod表示求模运算。

[0222] 可选的，基于所持有的第一子私钥、所述第一部分签名及所述第二中间签名，生成第一中间签名，具体包括：

[0223] 采用第三公式对所述第一随机数、所述第一部分签名及所述第一参与方的第一子私钥进行模运算，获得所述第一中间签名；其中，所述第三公式用于约束所述第一中间签名的取值范围；所述第三公式具体为：

[0224] $$\begin{cases} s_3=(k_5\times d_1^{-1})\bmod n \\ s_4=[(r+k_7)\times d_1^{-1}]\bmod n \\ s_5=(k_4\times s_1+k_6\times d_1^{-1}\times s_2-r)\bmod n \end{cases}$$

[0225] 其中，s_3至s_5为所述第一中间签名，k_4至k_7为所述第一随机数，且k_4至k_7中任一随机数的取值均是[1,n-1]范围内的整数，n为所述指定椭圆曲线的基点G的阶，r为所述待签名消息的第一部分签名，s_1至s_2为所述第二中间签名，d_1^{-1}为所述第一子私钥d_1在有限素域F_p上的逆元$d_1^{-1}\bmod n$，mod为求模运算。

[0226] 基于同一发明构思，本发明一实施例中提供一种用于SM2算法的协同签名的装置，应用于第二参与方，该装置的协同签名方法的具体实施方式可参见第二参与方的方法实施例部分的描述，重复之处不再赘述，请参见图5，该装置包括：

[0227] 接收单元501，用于在接收到第一参与方发送的待签名消息的签名通知时，计算第二椭圆曲线随机点及第二中间签名；其中，所述第二椭圆曲线随机点为所述第二参与方基于选取的第二随机数确定的指定椭圆曲线的加法群上的至少三个元素，所述第二中间签名为所述第二参与方所持有的第二子私钥被混淆后的两个值；

[0228] 发送单元502，用于将所述第二椭圆曲线随机点及所述第二中间签名发送给所述第一参与方，使所述第一参与方能够生成所述待签名消息的第一部分签名及第一中间签名；其中，所述第一中间签名是所述第一参与方所持有的第一子私钥被混淆后的三个值；

[0229] 接收单元501，用于接收所述第一参与方发送的所述待签名消息的第一部分签名及所述第一中间签名，根据所述第二子私钥及所述第一中间签名生成所述待签名消息的第二部分签名；

[0230] 生成单元503，还用于在确定所述第二部分签名为非零值，且不等于n-r时，确定由所述第一部分签名及所述第二部分签名构成的所述待签名消息的完整签名；其中，n为所述指定椭圆曲线的基点的阶，r为所述待签名消息的第一部分签名。

[0231] 可选的，所述接收单元501具体用于：

[0232] 采用指定算法生成第二随机数；其中，所述第二随机数为至少三个随机数；

[0233] 采用第四公式将第二随机数分别作用于所述第一参与方的第一子公钥、所述第二参与方的第二子公钥及所述指定椭圆曲线的基点，获得第二椭圆曲线随机点；其中，所述第二椭圆曲线随机点为指定椭圆曲线的加法群上的至少三个元素；所述第四公式用于将所述第二椭圆曲线随机点约束在所述指定椭圆曲线的加法群上；

[0234] 采用第五公式对第二随机数中的部分随机数及所述第二子私钥进行模运算，获得第二中间签名。

[0235] 可选的，所述第四公式具体为：

[0236] $$\begin{cases} R_1 = k_1[*]P_1 \\ R_2 = (k_2 \times d_2)[*]P_2 \\ R_3 = k_3[*]G \end{cases}$$

[0237] 其中，R_1至R_3为所述第二椭圆曲线随机点，k_1至k_3为所述第二随机数，且k_1至k_3中任一随机数的取值范围均为[1,n-1]内的整数，G为所述指定椭圆曲线的基点，P_1、P_2分别为所述第一参与方及所述第二参与方的所述第一子公钥及第二子公钥，P_1为所述第一参与方所述第一子私钥与所述基点G计算得到的，P_2为所述第二参与方用所述第二子私钥与所述基点G计算得到的，d_2为所述第二子私钥。

[0238] 可选的，所述第五公式具体为：

[0239] $$\begin{cases} s_1 = (k_1 \times d_2^{-1}) \bmod n \\ s_2 = (k_3 \times d_2^{-1}) \bmod n \end{cases}$$

[0240] 其中，s_1和s_2为所述第二中间签名，k_1和k_3为所述第二随机数中的部分随机数，且k_1和k_3的取值范围均为[1,n-1]内的整数，d_2^{-1}为所述第二子私钥d_2在有限素域F_p上的逆元$d_2^{-1} \bmod n$，mod为求模运算。

[0241] 可选的，所述接收单元501具体用于：

[0242] 接收所述第一参与方发送的所述待签名消息的第一部分签名及所述第一中间签名；

[0243] 采用第六公式，根据所述第二子私钥及所述第一中间签名，生成所述待签名消息的第二部分签名。

[0244] 可选的，所述第六公式具体为：

[0245] $$s=(s_5+k_2\times d_2\times s_3+d_2^{-1}\times s_4)\bmod n$$

[0246] 其中，s为所述待签名消息的第二部分签名，s_3至s_5为所述第一中间签名，k_2为所述第二随机数中的部分随机数，且k_2的取值范围均为[1,n-1]内的整数，d_2为所述第二子私钥，d_2^{-1}为所述第二子私钥d_2在有限素域F_p上的逆元$d_2^{-1}\bmod n$，mod为求模运算。

[0247] 基于同一发明构思，本发明实施例中提供了一种用于SM2算法的协同签名的装置，包括：至少一个处理器，以及

[0248] 与所述至少一个处理器连接的存储器；

[0249] 其中，所述存储器存储有可被所述至少一个处理器执行的指令，所述至少一个处理器通过执行所述存储器存储的指令，执行如上所述的第一参与方和第二参与方进行协同签名的方法。

[0250] 基于同一发明构思，本发明实施例还提一种计算机可读存储介质，包括：

[0251] 所述计算机可读存储介质存储有计算机指令，当所述计算机指令在计算机上运行时，使得计算机执行如上所述的第一参与方和第二参与方进行协同签名的方法。

[0252] 在本发明提供的实施例中，由于第一参与方与第二参与方分别持有第一子私钥与第二子私钥，为了确定位于第一参与方的待签名消息的完整签名，需要第一参与方在接收到第二参与方发送的第二椭圆曲线随机点及第二中间签名之后，根据待签名消息的消息摘要及第二椭圆曲线随机点，生成待签名消息的第一部分签名；并在确定第一部分签名为非零值时，将第一部分签名及第一中间签名发送给第二参与方，使第二参与方能基于第二子私钥及第一中间签名，生成待签名消息的第二部分签名，以确定待签名消息的完整签名。从而使得既使是参与了协同签名的第二参与方也不知道第一参与方签署了什么消息，进而使本发明的签名方案对于第二参与方来说具有盲签名的效果，在产生数字签名的过程中不会泄露第一参与方的隐私，并且由于通信双方持有各自的签名子私钥，使得攻击者即使获取到任何一方的签名子私钥，都无法伪造待签名消息的完整签名，从而实现了保护完整的签名私钥的技术效果。

[0253] 本领域内的技术人员应明白，本发明实施例可提供为方法、系统、或计算机程序产品。因此，本发明实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0254] 本发明实施例是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理

器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0255] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0256] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0257] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

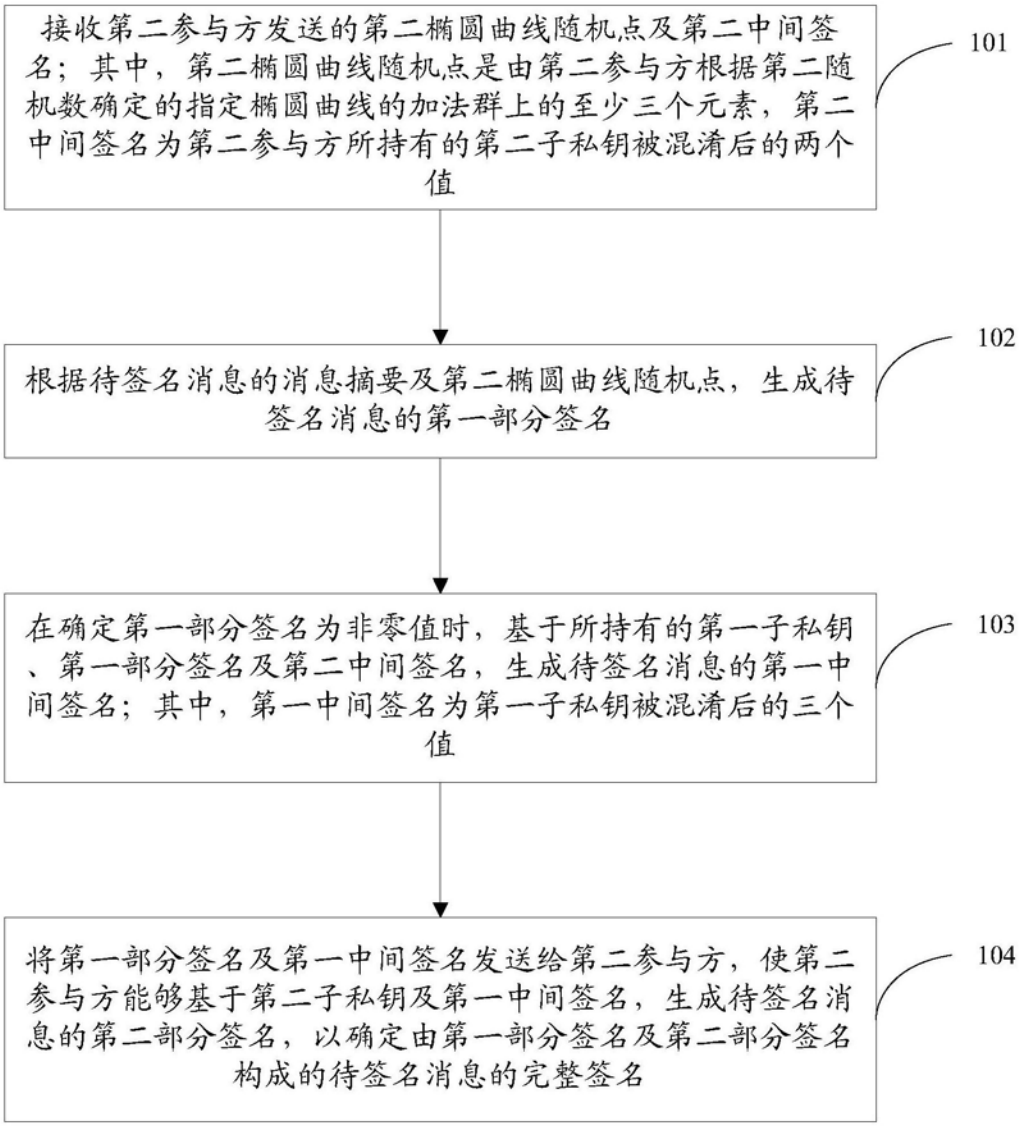

接收第二参与方发送的第二椭圆曲线随机点及第二中间签名；其中，第二椭圆曲线随机点是由第二参与方根据第二随机数确定的指定椭圆曲线的加法群上的至少三个元素，第二中间签名为第二参与方所持有的第二子私钥被混淆后的两个值
101
根据待签名消息的消息摘要及第二椭圆曲线随机点，生成待签名消息的第一部分签名
102
在确定第一部分签名为非零值时，基于所持有的第一子私钥、第一部分签名及第二中间签名，生成待签名消息的第一中间签名；其中，第一中间签名为第一子私钥被混淆后的三个值
103
将第一部分签名及第一中间签名发送给第二参与方，使第二参与方能够基于第二子私钥及第一中间签名，生成待签名消息的第二部分签名，以确定由第一部分签名及第二部分签名构成的待签名消息的完整签名
104

图1

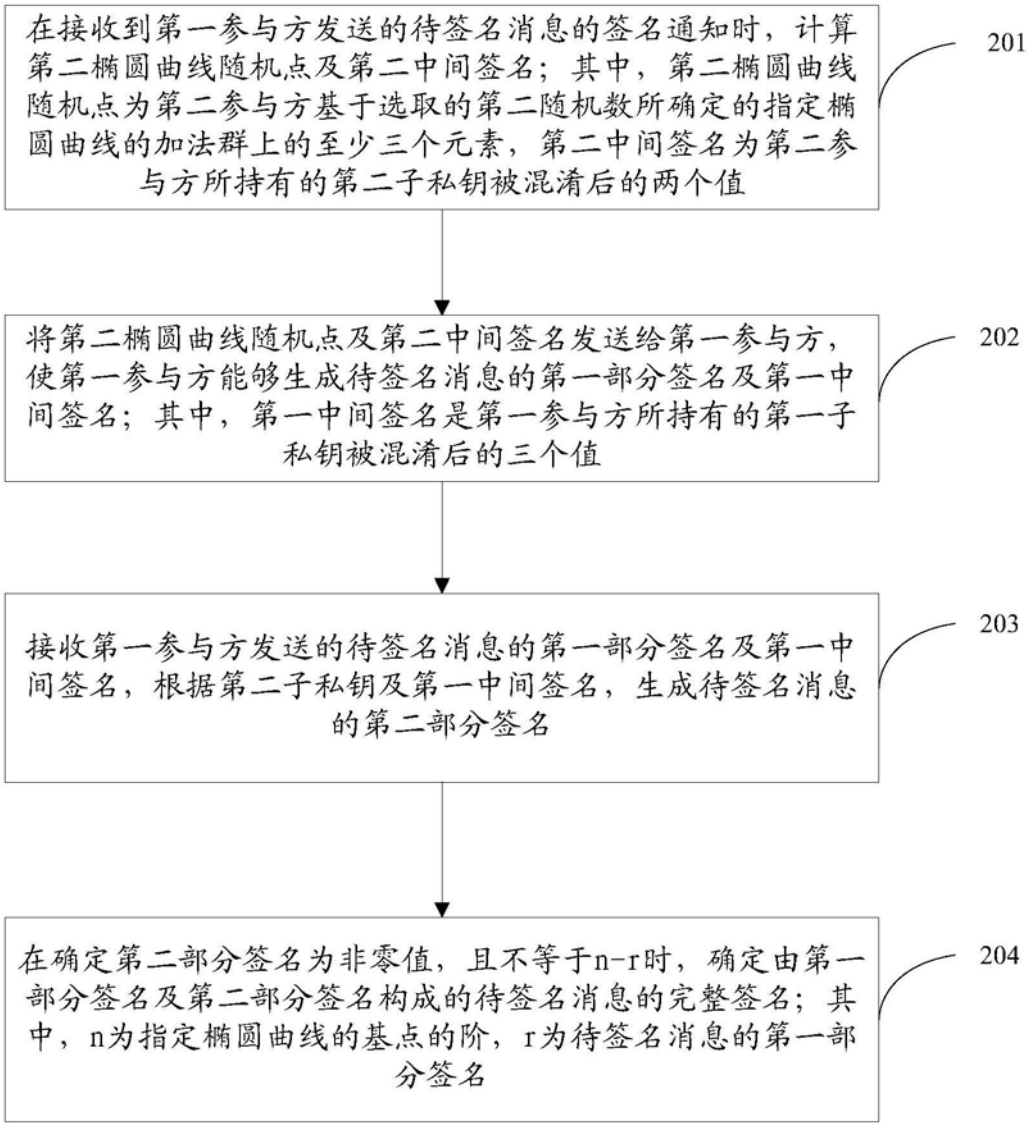

在接收到第一参与方发送的待签名消息的签名通知时，计算第二椭圆曲线随机点及第二中间签名；其中，第二椭圆曲线随机点为第二参与方基于选取的第二随机数所确定的指定椭圆曲线的加法群上的至少三个元素，第二中间签名为第二参与方所持有的第二子私钥被混淆后的两个值
201
将第二椭圆曲线随机点及第二中间签名发送给第一参与方，使第一参与方能够生成待签名消息的第一部分签名及第一中间签名；其中，第一中间签名是第一参与方所持有的第一子私钥被混淆后的三个值
202
接收第一参与方发送的待签名消息的第一部分签名及第一中间签名，根据第二子私钥及第一中间签名，生成待签名消息的第二部分签名
203
在确定第二部分签名为非零值，且不等于n-r时，确定由第一部分签名及第二部分签名构成的待签名消息的完整签名；其中，n为指定椭圆曲线的基点的阶，r为待签名消息的第一部分签名
204

图2

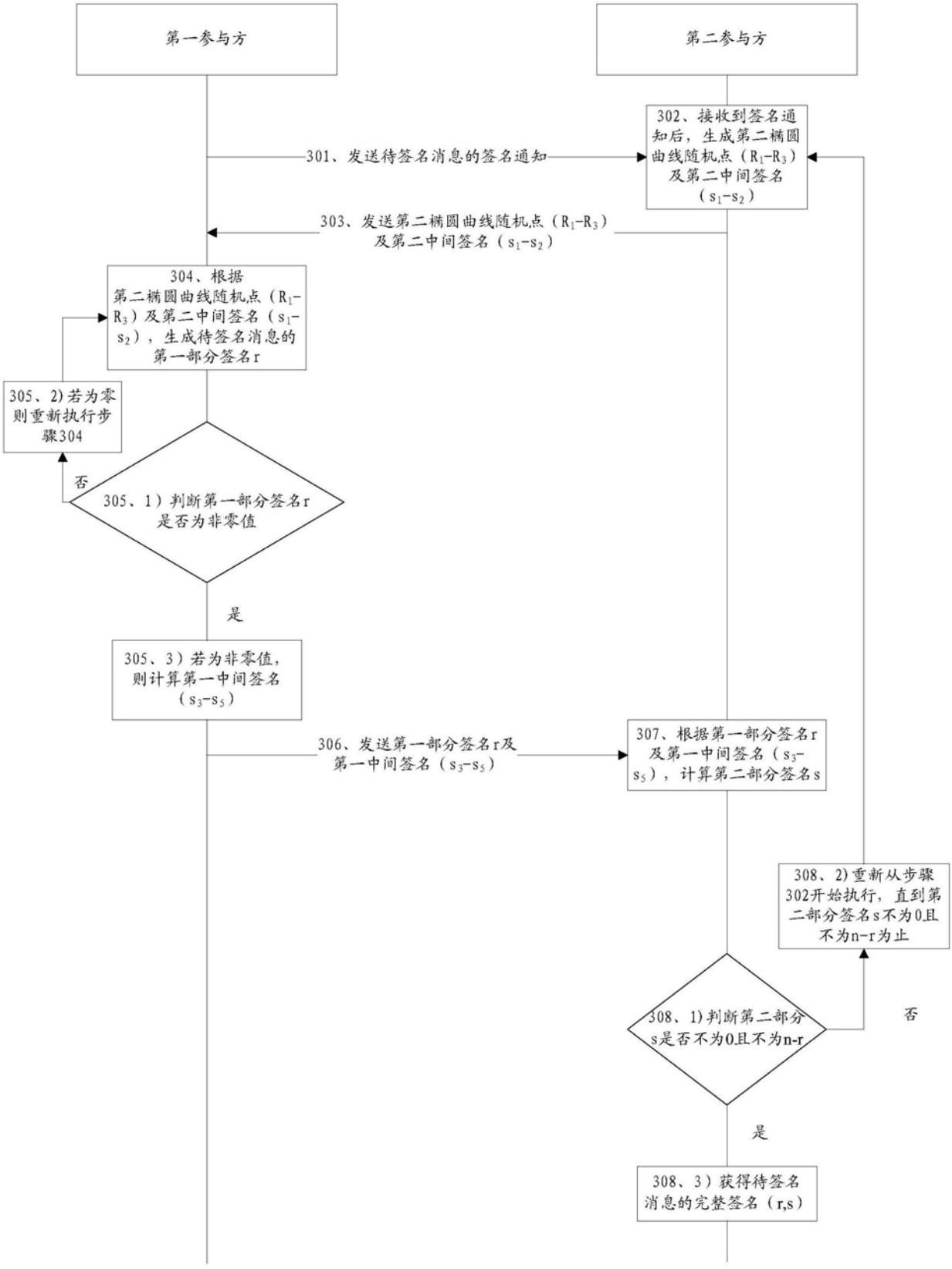

第一参与方
第二参与方
302、接收到签名通知后，生成第二椭圆曲线随机点（R_1-R_3）及第二中间签名（s_1-s_2）
301、发送待签名消息的签名通知
303、发送第二椭圆曲线随机点（R_1-R_3）及第二中间签名（s_1-s_2）
304、根据第二椭圆曲线随机点（R_1-R_3）及第二中间签名（s_1-s_2），生成待签名消息的第一部分签名r
305、2）若为零则重新执行步骤304
否
305、1）判断第一部分签名r是否为非零值
是
305、3）若为非零值，则计算第一中间签名（s_3-s_5）
306、发送第一部分签名r及第一中间签名（s_3-s_5）
307、根据第一部分签名r及第一中间签名（s_3-s_5），计算第二部分签名s
308、2）重新从步骤302开始执行，直到第二部分签名s不为0且不为n-r为止
308、1）判断第二部分s是否不为0且不为n-r
否
是
308、3）获得待签名消息的完整签名（r,s）

图3

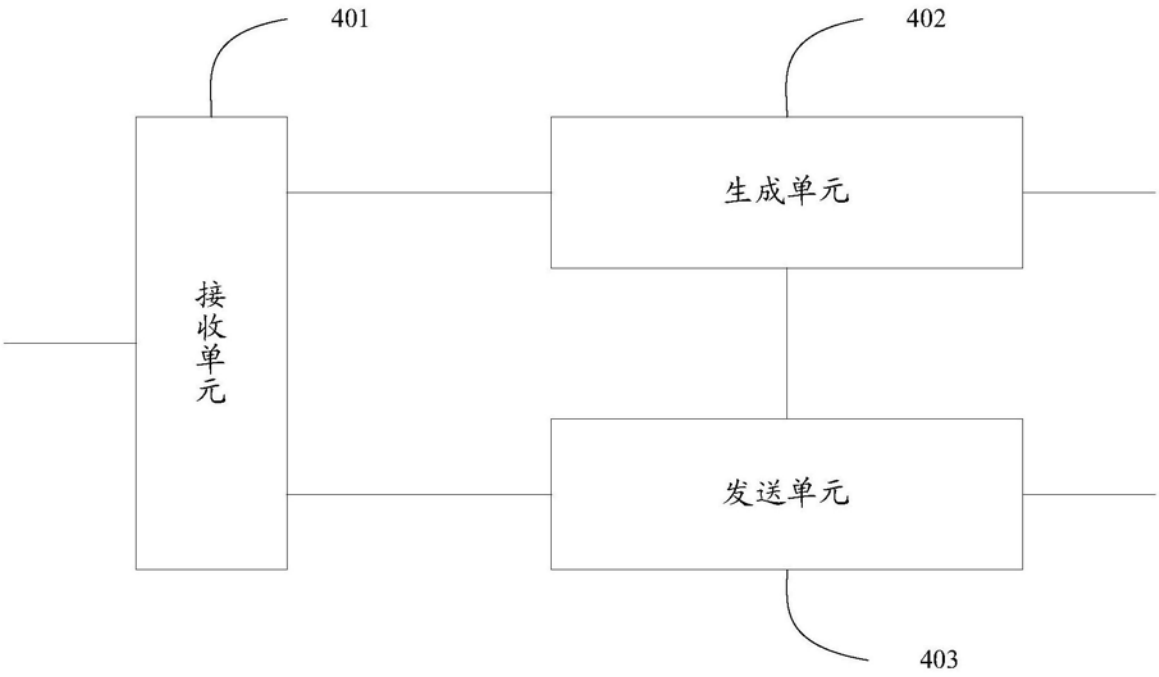


图4

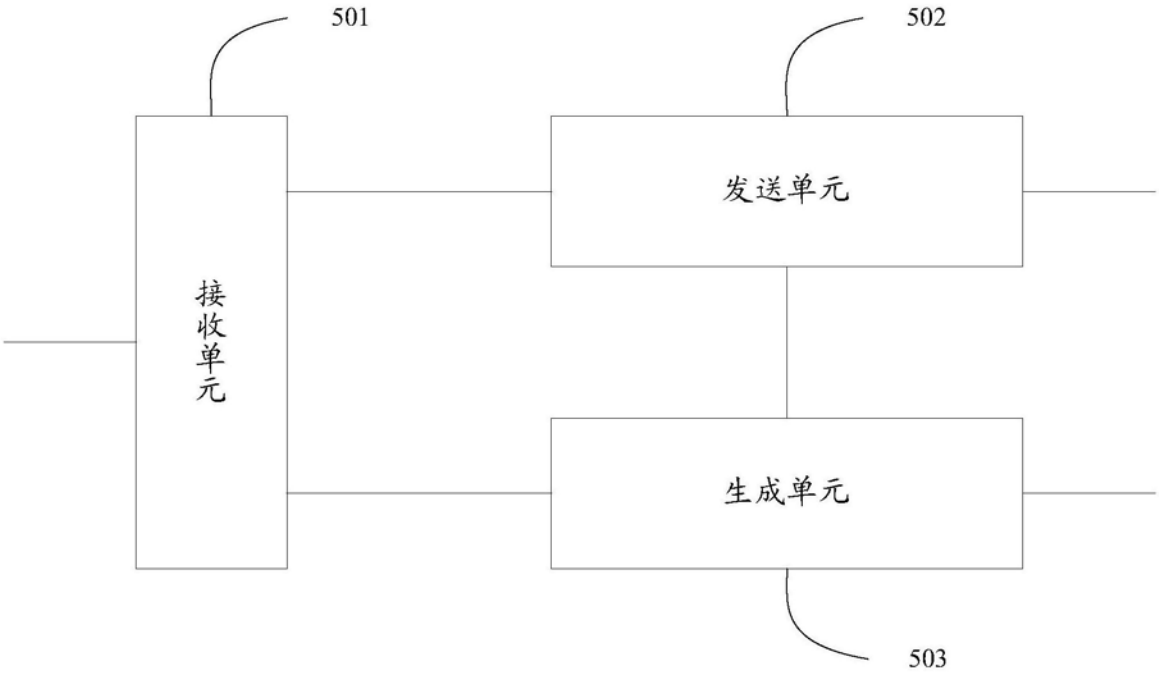


图5