

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2024 年 2 月 22 日 (22.02.2024)



(10) 国际公布号
WO 2024/036833 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01) **H04L 9/08** (2006.01)
H04L 9/00 (2022.01)

(21) 国际申请号: PCT/CN2022/137696

(22) 国际申请日: 2022 年 12 月 8 日 (08.12.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202210992927.2 2022年8月18日 (18.08.2022) CN

(71) 申请人: 深圳先进技术研究院 (SHENZHEN INSTITUTE OF ADVANCED TECHNOLOGY) [CN/CN]; 中国广东省深圳市南山区西丽大学城学苑大道1068号, Guangdong 518055 (CN)。

(72) 发明人: 邵翠萍 (SHAO, Cuiping); 中国广东省深圳市南山区西丽大学城学苑大道1068号, Guangdong 518055 (CN)。杨梅 (YANG, Mei); 中国广东省深圳市南山区西丽大学城学苑大道1068号, Guangdong 518055 (CN)。李慧云 (LI, Huiyun); 中国广东省深圳市南山区西丽大学城学苑大道1068号, Guangdong 518055 (CN)。

(74) 代理人: 北京中巡通大知识产权代理有限公司 (BEIJING ZHONG XUN TONG DA INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国北京市西城区西直门外大街1号院2号楼7层7C1, Beijing 100044 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU,

(54) **Title:** METHOD AND APPARATUS FOR ATTACKING ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM, AND DEVICE AND STORAGE MEDIUM

(54) 发明名称: 攻击椭圆曲线签名算法的方法、装置、设备及存储介质

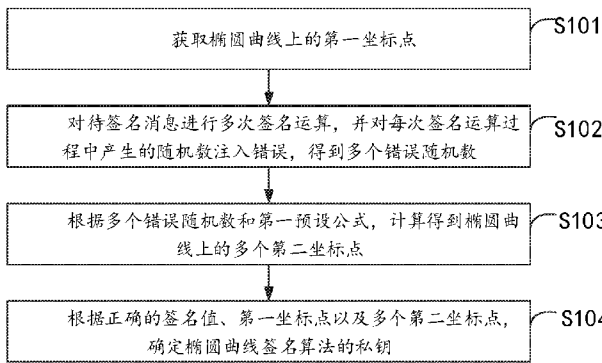


图 1

- S101 Acquire a first coordinate point on an elliptic curve
- S102 Perform a signature operation several times on a message to be signed, and inject an error into a random number generated during each signature operation process, so as to obtain a plurality of erroneous random numbers
- S103 According to the plurality of erroneous random numbers and a first preset formula, perform calculation to obtain a plurality of second coordinate points on the elliptic curve
- S104 Determine a private key of an elliptic curve digital signature algorithm according to a correct signature value, the first coordinate point and the plurality of second coordinate points

(57) **Abstract:** The present application relates to the technical field of information security. Provided are a method and apparatus for attacking an elliptic curve digital signature algorithm, and a device and a storage medium. The method comprises: acquiring a first coordinate point on an elliptic curve; performing a signature operation several times on a message to be signed, and injecting an error into a random number generated during each signature operation process, so as to obtain a plurality of erroneous random numbers; according to the plurality of erroneous random numbers and a first preset formula, performing calculation to obtain a plurality of

CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

- (84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

second coordinate points on the elliptic curve; and determining a private key of an elliptic curve digital signature algorithm according to a correct signature value, the first coordinate point and the plurality of second coordinate points. By means of attacking a random number generated during a signature operation process, coordinate points obtained by means of calculation after the attack are still on an original elliptic curve, are not easily detected, and thus are not easily defended; and the whole attack process is simple, and the degree of difficulty of performing cracking to obtain a private key is reduced, such that a private key of an elliptic curve digital signature algorithm is quickly and accurately acquired.

(57) 摘要: 本申请提供一种攻击椭圆曲线签名算法的方法、装置、终端设备及存储介质, 涉及信息安全技术领域。该方法包括: 获取椭圆曲线上的第一坐标点; 对待签名消息进行多次签名运算, 并对每次签名运算过程中产生的随机数注入错误, 得到多个错误随机数; 根据多个错误随机数和第一预设公式, 计算得到椭圆曲线上的多个第二坐标点; 根据正确的签名值、第一坐标点以及多个第二坐标点, 确定椭圆曲线签名算法的私钥。对签名运算过程中产生的随机数进行攻击, 使得攻击后计算得到的坐标点还在原来的椭圆曲线上, 不容易被检测到, 从而不容易被防御, 整个攻击过程简单, 降低了破解私钥的困难程度, 实现了快速、准确地获取到椭圆曲线签名算法的私钥。

攻击椭圆曲线签名算法的方法、装置、设备及存储介质

5 技术领域

本申请涉及信息安全技术领域，尤其涉及一种攻击椭圆曲线签名算法的方法、装置、终端设备及存储介质。

背景技术

10 椭圆曲线签名算法相比于传统的签名算法，在同样的安全强度下只需更短的密钥长度，更适合于应用到资源受限的芯片中。例如，该椭圆曲线签名算法就非常适用于处理能力、存储空间、带宽及功耗受限的车联网应用环境。

15 针对椭圆曲线签名算法的攻击方法也在不断地出现。然而，现有的攻击方法难度大，还容易被防御，导致无法快速、准确地获取到椭圆曲线签名算法的私钥。

发明内容

有鉴于此，本申请提供一种攻击椭圆曲线签名算法的方法、装置、终端设备及存储介质，以解决现有的攻击方法难度大，还容易被防御，导致无法快速、准确地获取到椭圆曲线签名算法的私钥的问题。

20 第一方面，本申请提供一种攻击椭圆曲线签名算法的方法，包括：获取椭圆曲线上的第一坐标点，第一坐标点是根据待签名消息对应的正确的签名值计算得到的，正确的签名值是根据椭圆曲线签名算法对待签名消息进行正常的签名运算得到的；

25 对待签名消息进行多次签名运算，并对每次签名运算过程中产生的随机数注入错误，得到多个错误随机数；

根据多个错误随机数和第一预设公式，计算得到椭圆曲线上的多个第二坐标点；

根据正确的签名值、第一坐标点以及多个第二坐标点，确定椭圆曲线签名算法的私钥。

5 上述方案中，对签名运算过程中产生的随机数进行攻击，使得攻击后计算得到的坐标点还在原来的椭圆曲线上，不容易被检测到，从而不容易被防御。再基于正确的签名值、正确签名算法情况下计算得到的第一坐标点以及被攻击情况下计算得到的多个第二坐标点，确定椭圆曲线签名算法的私钥。整个攻击过程简单，降低了破解私钥的困难程度，实现了快速、
10 准确地获取到椭圆曲线签名算法的私钥。

在一个可能的实现方式中，随机数包括多个比特位的值，对待签名消息进行多次签名运算，并对每次签名运算过程中产生的随机数注入错误，得到多个错误随机数，包括：针对每次签名运算，改变签名运算过程中产生的随机数中的一个比特位的值，得到错误随机数。

15 在一个可能的实现方式中，根据多个错误随机数和第一预设公式，计算得到椭圆曲线上的多个第二坐标点，包括：

根据多个错误随机数计算得到多个错误的签名值；

根据多个错误的签名值和第一预设公式，计算得到多个第二坐标点。

20 在一个可能的实现方式中，根据正确的签名值、第一坐标点以及多个第二坐标点，确定椭圆曲线签名算法的私钥，包括：

对第一坐标点和多个第二坐标点进行差分运算，得到多个逻辑值；

根据多个逻辑值生成目标随机数；

根据第二预设公式、目标随机数以及正确的签名值，计算得到私钥。

在一个可能的实现方式中，对待签名消息进行签名运算的次数，根据

随机数的比特位的个数和预设取值范围确定。

在一个可能的实现方式中，根据正确的签名值、第一坐标点以及多个第二坐标点，确定椭圆曲线签名算法的私钥之后，该方法还包括：确定椭圆曲线签名算法的防御策略。

5 第二方面，本申请提供一种攻击椭圆曲线签名算法的装置，包括：

获取单元，用于获取椭圆曲线上的第一坐标点，所述第一坐标点是根
据待签名消息对应的正确的签名值计算得到的，所述正确的签名值是根据
椭圆曲线签名算法对所述待签名消息进行正常的签名运算得到的；

运算单元，用于对所述待签名消息进行多次签名运算，并对每次签名
10 运算过程中产生的随机数注入错误，得到多个错误随机数；

计算单元，用于根据所述多个错误随机数和第一预设公式，计算得到
所述椭圆曲线上的多个第二坐标点；

确定单元，用于根据所述正确的签名值、所述第一坐标点以及所述多
个第二坐标点，确定所述椭圆曲线签名算法的私钥。

15 第三方面，本申请提供一种终端设备，包括存储器、处理器以及存储
在该存储器中并可在该处理器上运行的计算机程序，该处理器执行该计算
机程序时实现上述第一方面中任一方式所述的方法。

第四方面，本申请提供一种计算机可读存储介质，该计算机可读存储
介质存储有计算机程序，该计算机程序被处理器执行时实现上述第一方面
20 中任一方式所述的方法。

第五方面，本申请实施例提供一种计算机程序产品，当计算机程序产
品在处理器上运行时，使得处理器执行上述第一方面中任一方式所述的方
法。

第六方面，本申请实施例提供一种芯片，包括处理器，用于从存储器
25 中调用并运行计算机程序，使得安装有所述芯片的终端设备执行上述第一

方面中任一方式所述的方法。

本申请其他方面的有益效果请参考第一方面的有益效果的描述，此处不再赘述。

5 附图说明

图 1 是本申请一示例性实施例提供的一种攻击椭圆曲线签名算法的方法的示意性流程图；

图 2 是本申请另一示例性实施例示出的一种攻击椭圆曲线签名算法的方法的步骤 S103 的具体流程图；

10 图 3 是本申请又一示例性实施例示出的一种攻击椭圆曲线签名算法的方法的步骤 S104 的具体流程图；

图 4 为本申请实施例提供的一种攻击椭圆曲线签名算法的装置的示意图；

图 5 是本申请另一实施例提供的终端设备的示意图。

15

具体实施方式

为使本申请实施例的目的、技术方案和优点更加清楚，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。
20 基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

椭圆曲线签名算法相比于传统的签名算法，在同样的安全强度下只需更短的密钥长度，更适合于应用到资源受限的芯片中。例如，该椭圆曲线签名算法就非常适用于处理能力、存储空间、带宽及功耗受限的车联网应用环境，是我国车联网安全技术中的国产公钥密码方案。
25

安全芯片是有效保障我国车联网安全的核心与基石。其中，安全芯片指可信任平台模块，是一个可独立进行密钥生成、加解密的装置，内部拥

有独立的处理器和存储单元，可存储密钥和特征数据，为电脑提供加密和安全认证服务。用安全芯片进行加密，密钥被存储在硬件中，被窃的数据无法解密，从而保护商业隐私和数据安全。

虽然安全芯片中有复杂的加解密算法和密钥保护机制，但是近年来安全芯片还是很容易受到错误注入攻击，从而导致在加密算法执行的过程中产生瞬态的逻辑错误，攻击者通过分析正确的和错误的加密结果，最终引起密钥的泄露。

安全芯片的错误注入攻击已被列为美国联邦信息处理标准“FIPS 140-3”中重要的一类攻击方式。因此，研究新的错误攻击方法，能够帮助设计者尽早发现算法和硬件中存在的潜在风险，使得在设计阶段就能做出相应的防御措施，规避可能的风险。

例如，在现有的攻击椭圆曲线签名算法的基础上，研究新的攻击椭圆曲线签名算法的方法，并根据该新的攻击椭圆曲线签名算法的方法，查找攻击椭圆曲线签名算法和硬件中存在的潜在风险，制定相应的防御策略，规避可能的风险。能够在椭圆曲线密码产品出厂之前，对椭圆曲线算法的安全性进行评估，减少椭圆曲线密码产品在出厂后存在安全漏洞的情况。

可见，对椭圆曲线签名算法的攻击方法的研究非常有必要。根据攻击位置不同，即故障注入椭圆曲线的位置不同，现有的攻击方法可以分为基点攻击和椭圆曲线参数攻击。前者通过在点乘的运算环节注入故障，然后获取私钥，后者通过结合椭圆曲线上的离散对数问题（ECDLP）来破解私钥。

首先，以上两种攻击方法都很复杂，并且破解时存在一定的随机性。ECDLP方法在基点的阶的最大素因子大到一定位数时，以现在的计算机水平是无法在有限的可计算时间内完成破解的。

其次，以上两种攻击方法的共同点是使得中间点和输出点不在原来安全的椭圆曲线上，即移动到了一条新的弱椭圆曲线上。这种攻击方法恰恰很容易被检测到，即通过检查由国家密码管理部门批准的基于椭圆曲线的

非对称密码算法（SM2）的基点、所有用于计算的中间点以及最终输出点是否在安全的椭圆曲线上，就能判断当前算法是否安全。如果任何一点不在安全椭圆曲线上，则阻止输出。

此外，这两种攻击方法都是围绕点乘操作进行攻击的，然而在实际的运算中，点乘只是签名或者加密过程的中间环节，用于攻击破解的点乘结果数据是运算过程中的中间量，是无法获取的，尤其在安全芯片中。因此，现有的攻击方法难度大，还容易被防御，导致无法快速、准确地获取到椭圆曲线签名算法的私钥。

有鉴于此，本申请提供了一种攻击椭圆曲线签名算法的方法、装置、终端设备及存储介质。通过对签名运算过程中产生的随机数进行攻击，使得攻击后计算得到的坐标点还在原来的椭圆曲线上，不容易被检测到，从而不容易被防御。再基于正确的签名值、正确签名算法情况下计算得到的第一坐标点以及被攻击情况下计算得到的多个第二坐标点，确定椭圆曲线签名算法的私钥。整个攻击过程简单，无需像现有技术中那样逐步缩小范围去推测私钥，降低了破解私钥的困难程度，实现了快速、准确地获取到椭圆曲线签名算法的私钥。且研究这种攻击方法，能够帮助设计者尽早发现算法和硬件中存在的潜在风险，使得在设计阶段就能做出相应的防御措施，规避可能的风险。

下面以具体地实施例对本申请的技术方案进行详细说明。下面这几个具体的实施例可以相互结合，对于相同或相似的概念或过程可能在某些实施例不再赘述。

请参见图 1，图 1 是本申请一示例性实施例提供的一种攻击椭圆曲线签名算法的方法的示意性流程图。本申请提供的攻击椭圆曲线签名算法的方法的执行主体为终端设备，其中，该终端设备包括但不限于车载电脑、平板电脑、计算机、智能手机、可穿戴设备、个人数字助理（Personal Digital Assistant, PDA）等设备。或者，也可以是预先在终端设备上安装应用程序或小程序等，利用安装的应用程序或小程序执行攻击椭圆曲线签名算法

的方法。

本申请提供的攻击椭圆曲线签名算法的方法的执行主体还可以为各种类型的服务器。例如，服务器可以是独立的服务器，也可以是提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、
5 域名服务、安全服务、内容分发网络（Content Delivery Network，CDN）、以及大数据和人工智能平台等基础云计算服务的云服务。

请参见图 1，图 1 是本申请一示例性实施例提供的一种攻击椭圆曲线签名算法的方法的示意性流程图。如图 1 所示的方法可包括：S101~S104，具体如下：

10 S101：获取椭圆曲线上的第一坐标点。

椭圆曲线可以理解为描述了特定点的集合的公式，实质上是一个数学方程，第一坐标点是该椭圆曲线上的一个坐标点。该第一坐标点是根据待签名消息对应的正确的签名值计算得到的，正确的签名值是根据椭圆曲线签名算法对待签名消息进行正常的签名运算得到的。

15 待签名消息指明文，即没有加密的文字或字符串，本示例中用 M 表示明文。基于椭圆曲线签名算法对待签名消息进行正常的签名运算，得到该待签名消息对应的正确的签名值（签名对）。本示例中用 (r,s) 表示正确的签名值（签名对）。其中，正常的签名运算指没有任何攻击情况下进行的签名运算，此时得到的签名值又称为正确的签名值。

20 示例性地，椭圆曲线签名算法可以包括 SM2 签名算法、SM9 签名算法等非对称算法。本示例中以 SM2 签名算法为例进行说明。

例如，预先获取用户的自身消息和椭圆曲线的参数。其中，用户的自身消息可以包括用户的身份信息，椭圆曲线的参数可以包括椭圆曲线的基点，可以理解为椭圆曲线中的第一个点，本示例中用 P 表示基点。

25 对用户的自身消息和椭圆曲线的参数进行杂凑运算，得到杂凑值。杂

凑运算又称哈希函数，就是把任意长度的输入消息串变化成固定长度的输出串的一种函数。杂凑值又称哈希值，本示例中用 Z_A 表示用户 A 的杂凑值。

具体地，输入明文 M 。利用杂凑值 Z_A 计算 $\overline{M}$ 的值，如置 $\overline{M} = Z_A \| M$ ，即令 $\overline{M} = Z_A \| M$ ；

5 根据哈希函数 H 和 $\overline{M}$ 的值计算 e 的值，如计算 $e = H(\overline{M})$ ；

利用随机数生成器生成随机数 k ， $k \in [1, n-1]$ ；

计算 $k * P = (x_1, y_1)$ ，其中， (x_1, y_1) 表示椭圆曲线上的坐标点；

计算 $r = (e + x_1) \bmod n$ ，其中， n 表示椭圆曲线的阶。若 $r = 0$ 或者 $r + k = n$ ，则返回执行利用随机数生成器生成随机数 k 这一步骤；

10 若 $r \neq 0$ 或者 $r + k \neq n$ ，则计算 $s = ((1 + d_A)^{-1} \cdot (k - rd_A)) \bmod n$ ，其中， d_A 表示私钥。若 $s = 0$ ，则返回执行利用随机数生成器生成随机数 k 这一步骤；

若 $s \neq 0$ ，则输出正确的签名值 (r, s) 和明文 M 。

示例性地，根据待签名消息对应的正确的签名值 (r, s) 和第一预设公式计算第一坐标点，本示例中用 $Q(x_1, y_1)$ 表示第一坐标点。

15 由于 $r = (e + x_1) \bmod n$ ，用 i 表示 x_1 的比特位， $i = 0, 1, 2, 3, \dots$ ； i 取使 $0 < x_1 < n$ 的值，再有 Q 满足椭圆曲线 $y^2 + xy = x^3 + 1$ ，推导出第一预设公式为：

$$\begin{aligned} x_1 &= r + i * n - e \\ y_1 &= \sqrt{x_1^3 + \frac{1}{4}x_1 + 1} - \frac{x_1}{2}, \end{aligned}$$

将 r 、 i 、 n 、 e 的值代入第一预设公式中，计算出第一坐标点 $Q(x_1, y_1)$ 的值。

20 S102：对待签名消息进行多次签名运算，并对每次签名运算过程中产生的随机数注入错误，得到多个错误随机数。

S102 步骤中的签名运算与 S101 步骤中的签名运算的区别是，S101 步骤中的签名运算是在没有任何攻击情况下进行的签名运算，而 S102 步骤中的签名运算对签名运算过程中产生的随机数注入了攻击。

示例性地，对待签名消息进行多次签名运算，在每次签名运算过程中都会利用随机数生成器生成随机数，对产生的随机数注入错误，即注入故障，注入错误后的随机数即为错误随机数。本示例中用 k' 表示错误随机数。

可选地，在一种可能的实现方式中，签名运算过程中产生的随机数可以包括多个比特位的值，对待签名消息进行多次签名运算，并对每次签名运算过程中产生的随机数注入错误，得到多个错误随机数，包括：针对每次签名运算，改变签名运算过程中产生的随机数中的一个比特位的值，得到错误随机数。

示例性地，随机数包含的比特位的数量可根据实际情况设定。例如，本实例中随机数可以包括 233 个比特位的值，此处仅为示例性说明，对此不做限定。

针对每次签名运算，改变签名运算过程中产生的随机数中的一个比特位的值，即对签名运算过程中标量乘这一步中的随机数，每次注入一比特位故障，注入故障的随机数即为错误随机数 k' 。

也就是说，对随机数注入错误（注入故障），实际上就是对随机数中的一比特位的值进行改变。例如，某一比特位的值为 1，注入错误就可以是将 1 变为 0；又例如，某一比特位的值为 0，注入错误就可以是将 0 变为 1。

在一种可能的实现方式中，可以按照随机数中各个比特位的值的排列顺序，依次注入错误。例如，对待签名消息进行多次签名运算，第一次签名运算时，改变签名运算过程中产生的随机数中的第一个比特位的值，得到一个错误随机数。第二次签名运算时，改变签名运算过程中产生的随机数中的第二个比特位的值，得到一个错误随机数。以此类推，直至随机数

中每个比特位的值都被注入错误，得到多个错误随机数。

在另一种可能的实现方式中，可以随机对随机数中各个比特位的值注入错误，每次注入错误后，记录本次注入错误的位置，如记录第 N 位比特位，之后注入错误时避开已经注入错误的比特位的值。反复执行，直至随机数中每个比特位的值都被注入错误，得到多个错误随机数。

本实施方式中，在每次签名运算时，改变签名运算过程中产生的随机数中的一个比特位的值，实现了对签名运算过程中产生的随机数的攻击。且每次改变一个比特位的值，便于后续快速计算错误随机数和第二坐标点，从而间接提升了破解私钥的速度。

10 S103：根据多个错误随机数和第一预设公式，计算得到椭圆曲线上的多个第二坐标点。

示例性地，按照 S101 步骤中描述的签名运算的流程，对待签名消息进行签名运算。值得说明的是，此过程中需要将 S101 步骤中签名运算过程中的随机数 k 替换为错误随机数 k' ，其余流程类似，计算得到错误的签名值（签名对），本示例中用 (r', s') 表示错误的签名值（签名对）。

按照 S101 步骤中描述的根据待签名消息对应的正确的签名值 (r, s) 和第一预设公式计算第一坐标点的方式，根据待签名消息对应的错误的签名值 (r', s') 和第一预设公式计算第二坐标点，本示例中用 $Q'(x'_1, y'_1)$ 表示第二坐标点。对每次签名运算过程都进行这样的处理，可计算得到椭圆曲线上的多个第二坐标点。

S104：根据正确的签名值、第一坐标点以及多个第二坐标点，确定椭圆曲线签名算法的私钥。

示例性地，用该第一坐标点与每个第二坐标点都进行差分运算，可得到多个逻辑值。利用多个逻辑值生成目标随机数，目标随机数中包括多个比特位，逻辑值表示目标随机数中任一比特位的值。值得说明的是，目标

随机数中比特位的数量与逻辑值的数量相同。根据第二预设公式、目标随机数以及正确的签名值，计算得到椭圆曲线签名算法的私钥。

本实施方式中，通过对签名运算过程中产生的随机数进行攻击，使得攻击后计算得到的坐标点还在原来的椭圆曲线上，不容易被检测到，从而不容易被防御。再基于正确的签名值、正确签名算法情况下计算得到的第一坐标点以及被攻击情况下计算得到的多个第二坐标点，确定椭圆曲线签名算法的私钥。整个攻击过程简单，无需像现有技术中那样逐步缩小范围去推测私钥，降低了破解私钥的困难程度，实现了快速、准确地获取到椭圆曲线签名算法的私钥。

请参见图 2，图 2 是本申请另一示例性实施例示出的一种攻击椭圆曲线签名算法的方法的步骤 S103 的具体流程图，可选地，在一种可能的实现方式中，上述 S103 可包括 S1031~S1032，具体如下：

S1031：根据多个错误随机数计算得到多个错误的签名值。

示例性地，可重新获取用户的自身消息和椭圆曲线的参数。对用户的自身消息和椭圆曲线的参数进行杂凑运算，得到杂凑值。也可以直接利用步骤 S101 中用到的杂凑值 Z_A ，以实际情况为准，此处不做限定。

具体地，输入明文 M 。利用杂凑值 Z_A 计算 $\overline{M}$ 的值，如置 $\overline{M} = Z_A \| M$ ，即令 $\overline{M} = Z_A \| M$ ；

根据哈希函数 H 和 $\overline{M}$ 的值计算 e 的值，如计算 $e = H(\overline{M})$ ；

利用随机数生成器生成随机数 k ， $k \in [1, n-1]$ ；

改变随机数 k 中的一个比特位的值，得到错误随机数 k' ；

计算 $k' * P = (x_1, y_1)$ ，其中， P 表示椭圆曲线的基点， (x_1, y_1) 表示椭圆曲线上的坐标点；

计算 $r' = (e + x_1) \bmod n$ ，其中， n 表示椭圆曲线的阶。若 $r' = 0$ 或者 $r' + k' = n$ ，

则返回执行利用随机数生成器生成随机数 k 这一步骤；

若 $r' \neq 0$ 或者 $r' + k' \neq n$ ，则计算 $s' = ((1 + d_A)^{-1} \cdot (k' - r d_A)) \bmod n$ ，其中， d_A 表示私钥。若 $s' = 0$ ，则返回执行利用随机数生成器生成随机数 k 这一步骤；

若 $s' \neq 0$ ，则输出错误的签名值 (r', s') 。

5 重复执行上述过程，得到多个错误的签名值。

可以理解的是，步骤 S101 中 $k * P = (x_1, y_1)$ ，本实施方式中 $k' * P = (x_1, y_1)$ ，虽然两个 (x_1, y_1) 都表示椭圆曲线上的坐标点，但是前者是基于随机数 k 确定的，后者是基于错误随机数 k' 确定的，所以两个 (x_1, y_1) 表示的并不是椭圆曲线上的同一个坐标点。

10 S1032：根据多个错误的签名值和第一预设公式，计算得到多个第二坐标点。

示例性地，根据待签名消息对应的一个错误的签名值 (r', s') 和第一预设公式计算一个第二坐标点 $Q'(x'_1, y'_1)$ 。

$$\begin{aligned} & \text{第一预设公式为：} \\ & x_1 = r + i * n - e \\ & y_1 = \sqrt{x_1^3 + \frac{1}{4}x_1 + 1 - \frac{x_1}{2}} \end{aligned}$$

15 将 r' 、 i 、 n 、 e 的值代入第一预设公式中，计算出第二坐标点 $Q'(x'_1, y'_1)$ 的值。重复执行上述过程，得到多个第二坐标点。

本实施方式中，利用错误随机数计算错误的签名值，再利用错误的签名值和第一预设公式，计算得到第二坐标点，这样得到的第二坐标点还在原来的椭圆曲线上，不容易被检测到，从而不容易被防御。

20 请参见图 3，图 3 是本申请又一示例性实施例示出的一种攻击椭圆曲线签名算法的方法的步骤 S104 的具体流程图，可选地，在一种可能的实现方式中，上述 S104 可包括 S1041~S1043，具体如下：

S1041：对第一坐标点和多个第二坐标点进行差分运算，得到多个逻辑

值。

示例性地，用该第一坐标点与每个第二坐标点都进行差分运算，可得到多个逻辑值。例如，假设随机数 k 的第 I 位被注入故障，那么 $k' = k \oplus 2^I$ 。

其中， $0 \leq I < \log_2^k$ ，并且第一坐标点和第二坐标点满足以下关系：

$$Q - Q' \equiv (k - k')P \equiv \begin{cases} -2^I P & \text{if } k_I = 0 \\ +2^I P & \text{if } k_I = 1 \end{cases}$$

由此可以推导出 I 和 k_I 的值，即得到随机数 k 被注入错误的一比特位（二进制位）的逻辑值。通过同样的方法，可以得到多个逻辑值，逻辑值的数量与随机数 k 中比特位的数量相同。

如在签名运算过程中，改变注入错误的位置，遍历所有的 k_I （ $0 \leq I < \log_2^k$ ），直至获取到所有的 k_I 的值。

S1042：根据多个逻辑值生成目标随机数。

对哪个位置的比特位注入错误得到了该逻辑值，该比特位的位置即为该逻辑值对应的比特位的位置。每个比特位在随机数 k 中都有对应的位置，将每个逻辑值按照其对应的比特位的位置进行排列，得到目标随机数。由于目标随机数是由多个逻辑值生成的，目标随机数中比特位的数量与逻辑值的数量相同。

S1043：根据第二预设公式、目标随机数以及正确的签名值，计算得到私钥。

由于 $s = ((1 + d_A)^{-1} \cdot (k - r d_A)) \bmod n$ ，可推导出第二预设公式：

$d_A = (k - s)(s + r)^{-1} \bmod n$ ，值得说明的是 $d_A = (k - s)(s + r)^{-1} \bmod n$ 公式中的 k 表示目标随机数。

示例性地，将正确的签名值 (r, s) 和目标随机数代入第二预设公式，计算得到 d_A 的值，即得到椭圆曲线签名算法的私钥。

本实施方式中，基于正确的签名值、正确签名算法情况下计算得到的第一坐标点以及被攻击情况下计算得到的多个第二坐标点，确定椭圆曲线签名算法的私钥。计算过程简单，降低了破解私钥的困难程度，实现了快速、准确地获取到椭圆曲线签名算法的私钥。

5 可选地，在一种可能的实现方式中，对待签名消息进行签名运算的次数，根据随机数的比特位的个数和预设取值范围确定。

示例性地，预设取值范围为 $0 \leq I < \log_2^k$ ，其中， k 表示随机数， I 表示随机数中的第 I 位比特位， I 取最大值时与随机数的比特位的个数相同。由于要保证遍历所有的 k_I ，因此， I 取的最大值即为进行签名运算的次数。

10 本实施方式中，根据随机数的比特位的个数和预设取值范围确定进行签名运算的次数，从而保证能够遍历所有的 k_I ，进而便于后续基于所有的 k_I 生成目标随机数，为破解私钥提供了保障。

可选地，在一种可能的实现方式中，在步骤 S104 之后，该方法还可包括：确定椭圆曲线签名算法的防御策略。

15 示例性地，S101~S104 描述了椭圆曲线签名算法的攻击方法，即如何对椭圆曲线签名算法进行攻击，从而快速、准确地得到椭圆曲线签名算法的私钥。本实施方式中，根据椭圆曲线签名算法的攻击方法，确定椭圆曲线签名算法的防御策略，即根据 S101~S104 中对椭圆曲线签名算法进行攻击的方法，制定防御这种攻击方法的策略。

20 例如，防御策略可以为监控椭圆曲线签名算法的验签次数，当检测到椭圆曲线签名算法的验签次数比正常次数多时，预测椭圆曲线签名算法受到攻击，从而尽早防御。

又例如，本申请采用的攻击方法是运算过程中的结果量，是可以直接获取的。因此，防御策略可以为对结果量进行监控，实时监测结果量是否
25 异常。此处仅为示例性说明，对此不做限定。

本实施方式中，研究对椭圆曲线签名算法的攻击方法，能够帮助设计者尽早发现算法和硬件中存在的潜在风险，使得在设计阶段就能做出相应的防御措施，规避可能的风险。制定的防御策略，能够规避风险，能够在椭圆曲线密码产品出厂之前，对椭圆曲线算法的安全性进行评估，减少椭圆曲线密码产品在出厂后存在安全漏洞的情况。

可选地，在一种可能的实现方式中，本申请提供了一种验证方法，通过实验、模拟、使用证明上述实施例提供的攻击椭圆曲线签名算法的方法可行。可利用仿真技术（如 verilog 仿真）进行验证。

示例性地，选取美国国家标准与技术研究院 (National Institute of Standards and Technology, NIST) 推荐的 m 取值中的 233，与之对应的三项式： $f(z)=z^{233}+z^{74}+1$ 作为约减多项式。椭圆曲线 $GF(2^m)$ 上的魏尔斯特拉斯函数 (Weierstrass function) 定义为： $y^2+xy=x^3+ax^2+b$ ，其中， $a, b \in GF(2^m)$ ，且 $\Delta=b \neq 0$ ，当 $b=1, a=0$ 时，即为库兹涅茨曲线 (Kuznets curve)，又称倒 U 曲线 (inverted U curve)，是椭圆曲线密码体制实现中速度最快的曲线，

本文简称为 K-233 曲线，曲线参数信息表 1 所示。

表 1

[illegible]

例如, 用户 A 的身份是: ALICE123@YAHOO.COM, 用 ASCII 编码记为: ID_A :
414C494345313233405941484F4F2E434F4D, $ENTL_A=0090$ 。

下面以待签名消息（明文） $M = 6D65737361676520646967657374$ 为例说明攻击椭圆曲线签名算法的过程，具体如下：

（1）输入明文 M ，对明文 M 进行上述 S101 中的签名运算，得到正确的签名值 (r, s) ；

5 $r = 0x67f60a0306056a49579ae48da4579aa38a101280b76a6c856ee4a4760f$ ；

$s = 0x3d2089d9de3b9669af40a52182e50d6d0c3e619025c3936cc13588b6f2$ ；

（2）通过正确的签名值 (r, s) 和第一预设公式计算第一坐标点 $Q(x_1, y_1)$ ；

第一预设公式为：

$$x_1 = r + i * n - e$$

$$y_1 = \sqrt{x_1^3 + \frac{1}{4}x_1 + 1} - \frac{x_1}{2},$$

10 将 r 、 i 、 n 、 e 的值代入第一预设公式中，计算出第一坐标点 $Q(x_1, y_1)$ 的值为：

$x_1 = 0xebee644b9230fe06f800580adc5c276234c2861e947ce115f087c7a7ae$ ；

$y_1 = 0xd487a7fbd71127ae9bc23a64422b9fbff5eeb9a5c4ec85e2a45ee16928$ ；

（3）继续输入同样的明文 M ，对该明文进行签名运算，在签名运算过程中，对标量乘这一步中的随机数 k ，每次注入一比特位故障，注入故障的随机数即为错误随机数 k' 。例如，对标量乘这一步中的随机数 k 的第 233 位注入一比特位故障（ $I = 233$ ），注入故障的随机数即为错误随机数 k' ，最终得到注入故障情况下的签名值，即得到错误的签名值 (r', s') 。

$r' = 0x2d0941109d2dc453ed6b455bd6b5cb4b1f7b4c617f324115668c7a681c$ ；

20 $s' = 0xa247adba046a18f5854422e93d1b413ce12972abb42acfb90da51e844$ ；

（4）由上一步得到的错误的签名值 (r', s') 计算出注入故障情况下的 $Q'(x'_1, y'_1)$ ；

$x'_1 = 01b1019b59295958118dd0b8d90eba6544819feb790522abdb941284f179$;

$y_1' = 001372f062204ba1fe4cca80c2b074e5578350e712fb121652614d80156b$;

(5) 例如, 假设随机数 k 的第 I 位被注入故障, 那么 $k' = k \oplus 2^I$ 。

其中, $0 \leq I < \log_2^k$, 并且第一坐标点和第二坐标点满足以下关系:

$$Q-Q' \equiv (k-k')P \equiv \begin{cases} -2^l P & \text{if } k_l = 0 \\ +2^l P & \text{if } k_l = 1 \end{cases}$$

改变注入错误的位置, 遍历所有的 $k_I (0 \leq I < \log_2^k)$, 直至获取到所有的 k_I 的值, 从而得到目标随机数 k 的值。

[illegible]

(6) 根据第二预设公式: $d_A = (k-s)(s+r)^{-1} \bmod n$, 计算出 d_A 的值, 即得到椭圆曲线签名算法的私钥。

15 $d_A=011101110001111011110011110110111111111010111110001110011011100001$
 $100101011100111000101011100101001001100000100011101100001100100011001100110$
 $001011001010111111011111001011100110000001110101111111010110110011100100100$
 $0000010;$

至此，私钥 d_A 被破解。

图 4 为本申请实施例提供的一种攻击椭圆曲线签名算法的装置的示意
图，如图 4 所示，该装置包括：

获取单元210, 用于获取椭圆曲线上的第一坐标点, 所述第一坐标点是根据待签名消息对应的正确的签名值计算得到的, 所述正确的签名值是根据椭圆曲线签名算法对所述待签名消息进行正常的签名运算得到的;

运算单元 220, 用于对所述待签名消息进行多次签名运算, 并对每次签名运算过程中产生的随机数注入错误, 得到多个错误随机数;

计算单元 230, 用于根据所述多个错误随机数和第一预设公式, 计算得到所述椭圆曲线上的多个第二坐标点;

确定单元 240, 用于根据所述正确的签名值、所述第一坐标点以及所述多个第二坐标点, 确定所述椭圆曲线签名算法的私钥。

5 可选的, 所述随机数包括多个比特位的值, 所述运算单元 220 具体用于: 针对每次签名运算, 改变签名运算过程中产生的所述随机数中的一个比特位的值, 得到所述错误随机数。

可选的, 所述计算单元 230 具体用于:

根据所述多个错误随机数计算得到多个错误的签名值;

10 根据所述多个错误的签名值和所述第一预设公式, 计算得到所述多个第二坐标点。

可选的, 所述确定单元 240 具体用于:

对所述第一坐标点和所述多个第二坐标点进行差分运算, 得到多个逻辑值;

15 根据所述多个逻辑值生成目标随机数;

根据第二预设公式、所述目标随机数以及所述正确的签名值, 计算得到所述私钥。

可选地, 对所述待签名消息进行签名运算的次数, 根据所述随机数的比特位的个数和预设取值范围确定。

20 可选地, 该装置还包括:

策略确定单元, 用于确定所述椭圆曲线签名算法的防御策略。

请参见图 5, 图 5 是本申请另一实施例提供的终端设备的示意图。如图 5 所示, 该实施例的终端设备 3 包括: 处理器 30、存储器 31 以及存储在所述存储器 31 中并可在所述处理器 30 上运行的计算机程序 33。所述处理器 30 执行所述计算机程序 33 时实现上述各个方法实施例中的步骤, 例如图 1 所示的 S101 至 S104。或者, 所述处理器 30 执行所述计算机程序 33 时实现上述各实施例中各单元的功能, 例如图 4 所示单元 210 至 240 功能。

25

示例性地，所述计算机程序 33 可以被分割成一个或多个单元，所述一个或者多个单元被存储在所述存储器 31 中，并由所述处理器 30 执行，以完成本申请。所述一个或多个单元可以是能够完成特定功能的一系列计算机指令段，该指令段用于描述所述计算机程序 33 在所述终端设备 3 中的执行过程。例如，所述计算机程序 33 可以被分割为获取单元、运算单元、计算单元以及确定单元，各单元具体功能如上所述。

所述终端设备可包括，但不仅限于，处理器 30、存储器 31。本领域技术人员可以理解，图 5 仅仅是终端设备 3 的示例，并不构成对设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述终端设备还可以包括输入输出设备、网络接入设备、总线等。

所称处理器 30 可以是中央处理单元（Central Processing Unit，CPU），还可以是其他通用处理器、数字信号处理器（Digital Signal Processor，DSP）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现成可编程门阵列（Field-Programmable Gate Array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

所述存储器 31 可以是所述终端设备的内部存储单元，例如设备的硬盘或内存。所述存储器 31 也可以是所述终端设备的外部存储终端，例如所述终端设备上配备的插接式硬盘，智能存储卡（Smart Media Card，SMC），安全数字（Secure Digital，SD）卡，闪存卡（Flash Card）等。进一步地，所述存储器 31 还可以既包括所述设备的内部存储单元也包括外部存储终端。所述存储器 31 用于存储所述计算机指令以及所述终端所需的其他程序和数据。所述存储器 31 还可以用于暂时地存储已经输出或者将要输出的数据。

本申请实施例还提供了一种计算机存储介质，计算机存储介质可以是非易失性，也可以是易失性，该计算机存储介质存储有计算机程序，该计算机程序被处理器执行时实现上述各个方法实施例中的步骤。

本申请还提供了一种计算机程序产品，当计算机程序产品在终端设备上运行时，使得该终端设备执行上述各个方法实施例中的步骤。

本申请实施例还提供了一种芯片或者集成电路，该芯片或者集成电路包括：处理器，用于从存储器中调用并运行计算机程序，使得安装有该芯片或者集成电路的终端设备执行上述各个方法实施例中的步骤。

所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元、模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元、模块完成，即将装置的内部结构划分成不同的功能单元或模块，以完成以上描述的全部或者部分功能。实施例中的各功能单元、模块可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中，上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。另外，各功能单元、模块的具体名称也只是为了便于相互区分，并不用于限制本申请的保护范围。上述系统中单元、模块的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中沒有详述或记载的部分，可以参见其它实施例的相关描述。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

以上所述实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方

案的本质脱离本申请各实施例技术方案的精神范围，均应包含在本申请的保护范围之内。

权 利 要 求 书

1. 一种攻击椭圆曲线签名算法的方法，其特征在于，包括：

获取椭圆曲线上的第一坐标点，所述第一坐标点是根据待签名消息对应的正确的签名值计算得到的，所述正确的签名值是根据椭圆曲线签名算法对所述待签名消息进行正常的签名运算得到的；

对所述待签名消息进行多次签名运算，并对每次签名运算过程中产生的随机数注入错误，得到多个错误随机数；

根据所述多个错误随机数和第一预设公式，计算得到所述椭圆曲线上的多个第二坐标点；

根据所述正确的签名值、所述第一坐标点以及所述多个第二坐标点，确定所述椭圆曲线签名算法的私钥。

2. 根据权利要求 1 所述的方法，其特征在于，所述随机数包括多个比特位的值，所述对所述待签名消息进行多次签名运算，并对每次签名运算过程中产生的随机数注入错误，得到多个错误随机数，包括：

针对每次签名运算，改变签名运算过程中产生的所述随机数中的一个比特位的值，得到所述错误随机数。

3. 根据权利要求 1 所述的方法，其特征在于，所述根据所述多个错误随机数和第一预设公式，计算得到所述椭圆曲线上的多个第二坐标点，包括：

根据所述多个错误随机数计算得到多个错误的签名值；

根据所述多个错误的签名值和所述第一预设公式，计算得到所述多个第二坐标点。

4. 根据权利要求 1 所述的方法，其特征在于，所述根据所述正确的签名值、所述第一坐标点以及所述多个第二坐标点，确定所述椭圆曲线签名

算法的私钥，包括：

对所述第一坐标点和所述多个第二坐标点进行差分运算，得到多个逻辑值；

根据所述多个逻辑值生成目标随机数；

5 根据第二预设公式、所述目标随机数以及所述正确的签名值，计算得到所述私钥。

5. 根据权利要求 2 至 4 任一项所述的方法，其特征在于，对所述待签名消息进行签名运算的次数，根据所述随机数的比特位的个数和预设取值范围确定。

10 6. 根据权利要求 1 至 4 任一项所述的方法，其特征在于，所述根据所述正确的签名值、所述第一坐标点以及所述多个第二坐标点，确定所述椭圆曲线签名算法的私钥之后，所述方法还包括：

确定所述椭圆曲线签名算法的防御策略。

7. 一种攻击椭圆曲线签名算法的装置，其特征在于，包括：

15 获取单元，用于获取椭圆曲线上的第一坐标点，所述第一坐标点是根
据待签名消息对应的正确的签名值计算得到的，所述正确的签名值是根据
椭圆曲线签名算法对所述待签名消息进行正常的签名运算得到的；

运算单元，用于对所述待签名消息进行多次签名运算，并对每次签名
运算过程中产生的随机数注入错误，得到多个错误随机数；

20 计算单元，用于根据所述多个错误随机数和第一预设公式，计算得到
所述椭圆曲线上的多个第二坐标点；

确定单元，用于根据所述正确的签名值、所述第一坐标点以及所述多
个第二坐标点，确定所述椭圆曲线签名算法的私钥。

8. 一种终端设备，包括存储器、处理器以及存储在所述存储器中并可

在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如权利要求 1 至 6 任一项所述的方法。

9. 一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求 1 至 6
5 任一项所述的方法。

10. 一种芯片，其特征在于，包括：处理器，用于从存储器中调用并运行计算机程序，使得安装有所述芯片的终端设备执行如权利要求 1 至 6 任一项所述的方法。

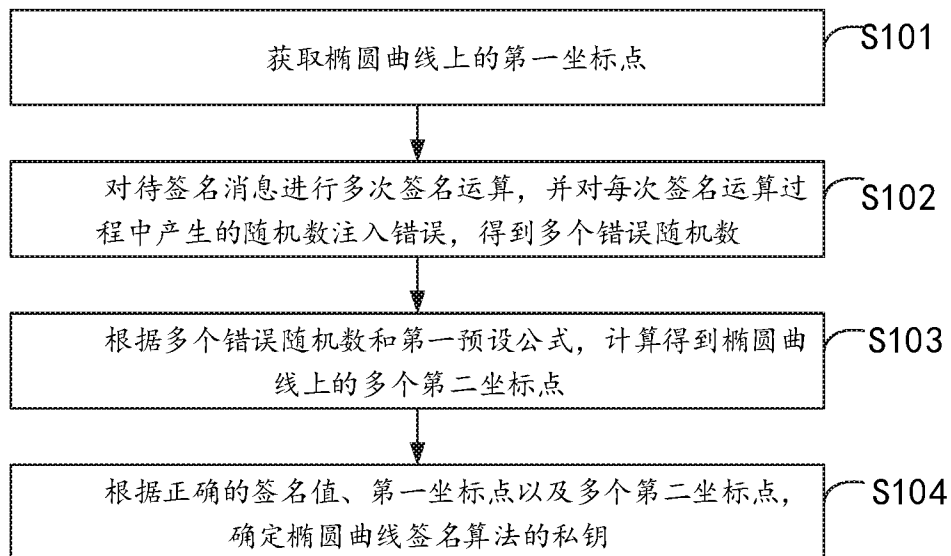


图 1

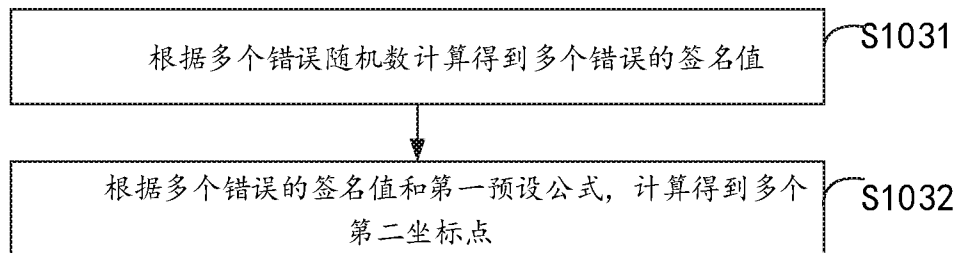


图 2

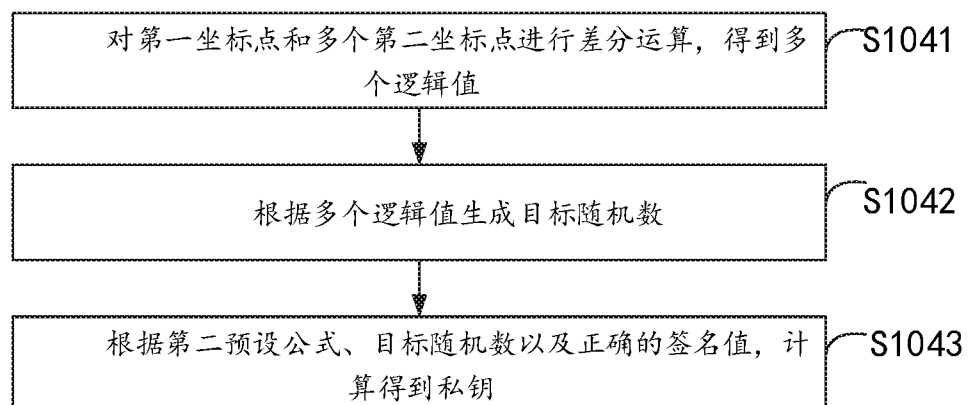


图 3

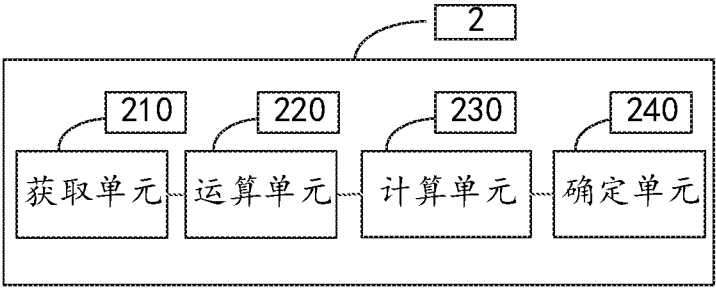


图 4

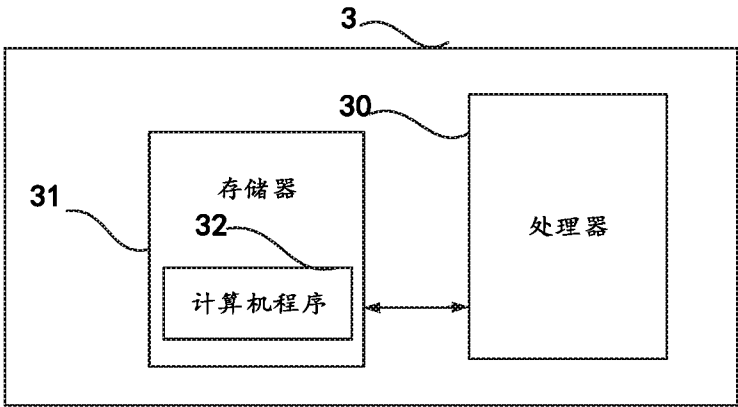


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/137696

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i;H04L 9/00(2022.01)i;H04L 9/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNPAT, CNKI: 椭圆曲线, 攻击, 签名, 坐标, 错误, 注入, 随机数, 私钥, elliptic curve cryptography, attack, signature, coordinate, error, injection, random, private key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 111835518 A (CHINA FINANCIAL CERTIFICATION AUTHORITY CO., LTD.) 27 October 2020 (2020-10-27) description, paragraphs 0002-0110	1-10
A	CN 109067554 A (BEIJING TESTIN INFORMATION TECHNOLOGY CO., LTD.) 21 December 2018 (2018-12-21) entire document	1-10
A	CN 114465728 A (SHANGHAI FUDAN MICROELECTRONICS GROUP CO., LTD.) 10 May 2022 (2022-05-10) entire document	1-10
A	US 2015092941 A1 (GHOSH, S.) 02 April 2015 (2015-04-02) entire document	1-10



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“D” document cited by the applicant in the international application

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

07 February 2023

Date of mailing of the international search report

20 February 2023

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
China No. 6, Xitucheng Road, Jimenqiao, Haidian District,
Beijing 100088

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2022/137696

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	111835518	A	27 October 2020	None	
CN	109067554	A	21 December 2018	None	
CN	114465728	A	10 May 2022	None	
US	2015092941	A1	02 April 2015	None	

国际检索报告

国际申请号

PCT/CN2022/137696

A. 主题的分类

H04L 9/32 (2006.01) i; H04L 9/00 (2022.01) i; H04L 9/08 (2006.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

IPC: H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))

WPI, EPDOC, CNPAT, CNKI: 椭圆曲线, 攻击, 签名, 坐标, 错误, 注入, 随机数, 私钥, elliptic curve cryptography, attack, signature, coordinate, error, injection, random, private key

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 111835518 A (中金金融认证中心有限公司) 2020年10月27日 (2020 - 10 - 27) 说明书第0002-0110段	1-10
A	CN 109067554 A (北京云测信息技术有限公司) 2018年12月21日 (2018 - 12 - 21) 全文	1-10
A	CN 114465728 A (上海复旦微电子集团股份有限公司) 2022年5月10日 (2022 - 05 - 10) 全文	1-10
A	US 2015092941 A1 (GHOSH, Santosh) 2015年4月2日 (2015 - 04 - 02) 全文	1-10

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“D” 申请人在国际申请中引证的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2023年2月7日

国际检索报告邮寄日期

2023年2月20日

ISA/CN的名称和邮寄地址

中国国家知识产权局

中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

授权官员

王国纲

电话号码 (+86) 010-53961755

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2022/137696

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	111835518	A	2020年10月27日	无	
CN	109067554	A	2018年12月21日	无	
CN	114465728	A	2022年5月10日	无	
US	2015092941	A1	2015年4月2日	无	