

(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
2022 年 5 月 5 日 (05.05.2022)



(10) 国际公布号
WO 2022/089014 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01)

圣赞(SHENG, Zan); 中国上海市浦东新区含笑路
36号银联大厦, Shanghai 200135 (CN)。

(21) 国际申请号: PCT/CN2021/117032

(22) 国际申请日: 2021 年 9 月 7 日 (07.09.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202011202674.1 2020年11月2日 (02.11.2020) CN

(71) 申请人: 中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.) [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。

(72) 发明人: 陈林(CHEN, Lin); 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。

(74) 代理人: 北京东方亿思知识产权代理有限公司 (BEIJING EAST IP LTD.); 中国北京市东城区东长安街 1 号东方广场东方经贸城东 2 座 1601 室, Beijing 100738 (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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, 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,

(54) Title: DATA ENCRYPTION METHOD, APPARATUS AND DEVICE, DATA DECRYPTION METHOD, APPARATUS AND DEVICE, AND STORAGE MEDIUM

(54) 发明名称: 数据加、解密方法、装置、设备及存储介质

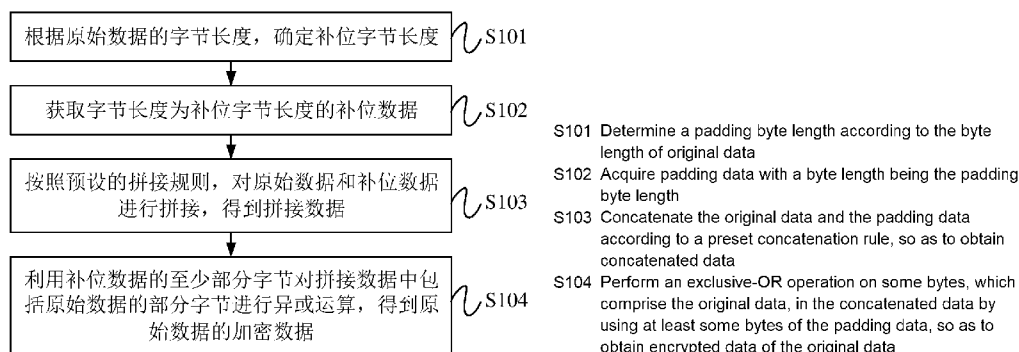


图 1

(57) Abstract: A data encryption method, apparatus and device, a data decryption method, apparatus and device, and a storage medium, which relate to the field of data processing. The encryption method comprises: determining a padding byte length according to the byte length of original data (S101); acquiring padding data with a byte length being the padding byte length (S102); concatenating the original data and the padding data according to a preset concatenation rule, so as to obtain concatenated data (S103); and performing an exclusive-OR operation on some bytes, which comprise the original data, in the concatenated data by using at least some bytes of the padding data, so as to obtain encrypted data of the original data (S104). By means of the method, risks in the security aspect of data information can be reduced.

(57) 摘要: 一种数据加、解密方法、装置、设备及存储介质, 涉及数据处理领域。该加密方法包括: 根据原始数据的字节长度, 确定补位字节长度 (S101); 获取字节长度为补位字节长度的补位数据 (S102); 按照预设的拼接规则, 对原始数据和补位数据进行拼接, 得到拼接数据 (S103); 利用补位数据的至少部分字节对拼接数据中包括原始数据的部分字节进行异或运算, 得到原始数据的加密数据 (S104)。能够降低数据信息安全方面的风险。

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, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, 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, 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))。

数据加、解密方法、装置、设备及存储介质

相关申请的交叉引用

本申请要求享有于 2020 年 11 月 02 日提交的名称为“数据加、解密方法、装置、设备及存储介质”的中国专利申请 202011202674.1 的优先权，该申请的全部内容通过引用并入本文中。

技术领域

本申请属于数据处理领域，尤其涉及一种数据加、解密方法、装置、设备及存储介质。

背景技术

随着信息技术的发展，越来越多的信息以数据的形式存储、传输。在数据中有一部分数据为敏感数据，敏感数据对应的信息可能会涉及到个人信息安全问题或社会信息安全问题。而在存储和传输的过程中，数据可能会发生泄露或被窥探。一旦敏感数据发生泄露或被窥探，会对信息安全带来非常大的风险。

发明内容

本申请实施例提供一种数据加、解密方法、装置、设备及存储介质，能够降低数据信息安全方面的风险。

第一方面，本申请实施例提供一种数据加密方法，包括：根据原始数据的字节长度，确定补位字节长度；获取字节长度为补位字节长度的补位数据；按照预设的拼接规则，对原始数据和补位数据进行拼接，得到拼接数据；利用补位数据的至少部分字节对拼接数据中包括原始数据的部分字节进行异或运算，得到原始数据的加密数据。

第二方面，本申请实施例提供一种数据解密方法，包括：基于预设的

拼接规则和加密数据，确定加密数据中补位数据包括的异或运算对象；利用异或运算对象，对加密数据中除异或运算对象外的其他字节进行异或运算，得到拼接数据；根据拼接规则和补位字节长度，确定拼接数据中加密数据的原始数据，补位字节长度为补位数据的字节长度。

第三方面，本申请实施例提供一种数据加密装置，包括：长度确定模块，用于根据原始数据的字节长度，确定补位字节长度；获取模块，用于获取字节长度为补位字节长度的补位数据；拼接模块，用于按照预设的拼接规则，对原始数据和补位数据进行拼接，得到拼接数据；运算模块，用于利用补位数据的至少部分字节对拼接数据中包括原始数据的部分字节进行异或运算，得到原始数据的加密数据。

第四方面，本申请实施例提供一种数据解密装置，包括：确定模块，用于基于预设的拼接规则和加密数据，确定加密数据中补位数据包括的异或运算对象；运算模块，用于利用异或运算对象，对加密数据中除异或运算对象外的其他字节进行异或运算，得到拼接数据；解密模块，用于根据拼接规则和补位字节长度，确定拼接数据中加密数据的原始数据，补位字节长度为补位数据的字节长度。

第五方面，本申请实施例提供一种数据加密设备，包括：处理器以及存储有计算机程序指令的存储器；处理器执行计算机程序指令时实现第一方面的数据加密方法。

第六方面，本申请实施例提供一种数据解密设备，包括：处理器以及存储有计算机程序指令的存储器；处理器执行计算机程序指令时实现第二方面的数据解密方法。

第七方面，本申请实施例提供一种计算机存储介质，计算机存储介质上存储有计算机程序指令，计算机程序指令被处理器执行时实现第一方面的数据加密方法和/或第二方面的数据解密方法。

本申请实施例提供一种数据加、解密方法、装置、设备及存储介质，可根据原始数据的字节长度，确定补位字节长度，以获取字节长度为补位字节长度的补位数据。按照拼接规则对原始数据和拼接数据进行拼接，形成新的数据即拼接数据。通过利用补位数据的至少部分字节对拼接数据中

包括原始数据的部分字节进行异或运算，得到原始数据中的加密数据。经过拼接，加密数据的字节长度与原始数据的字节长度不同。经过异或运算，加密数据中的字节的值相对于原始数据中的字节的值也发生了改变。在未知补位数据和拼接规则的情况下，很难破解本申请实施例生成的加密数据，即使发生泄露或被窥探，泄露的或被窥探的也是加密数据，能够根据加密数据得到原始数据的可能性非常小，从而降低了数据信息安全方面的风险。在需要将加密数据恢复为原始数据的情况下，也可通过数据解密方法反向解密得到原始数据。

附图说明

为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例中所需要使用的附图作简单的介绍，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为本申请第一方面提供的数据加密方法的一实施例的流程图；

图 2 为本申请第一方面提供的数据加密方法的另一实施例的流程图；

图 3 为本申请实施例提供的数据加密流程的一示例的流程图；

图 4 为本申请第二方面提供的数据解密方法的一实施例的流程图；

图 5 为本申请第二方面提供的数据解密方法的另一实施例的流程图；

图 6 为本申请第三方面提供的数据加密装置的一实施例的结构示意图；

图 7 为本申请第四方面提供的数据解密装置的一实施例的结构示意图；

图 8 为本申请第五方面提供的数据加密设备的一实施例的结构示意图；

图 9 为本申请第六方面提供的数据解密设备的一实施例的结构示意图。

具体实施方式

下面将详细描述本申请的各个方面的特征和示例性实施例，为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及具体实施例，对本申请进行进一步详细描述。应理解，此处所描述的具体实施例仅意在解释本申请，而不是限定本申请。对于本领域技术人员来说，本申请可以在不需要这些具体细节中的一些细节的情况下实施。下面对实施例的描述仅仅是为了通过示出本申请的示例来提供对本申请更好的理解。

随着数据信息技术的发展，越来越多的信息以数据的方式存储、传输。在承载信息的数据中存在着大量的敏感数据，敏感数据指泄漏后可能会给社会或个人带来严重危害的数据。例如，敏感数据可包括但不限于姓名、身份证号码、住址、电话、银行账号、邮箱、密码等数据。但在数据的存储和传输过程中，数据可能会发生泄露或被窥探。一旦敏感数据发生泄露或被窥探，会对个人或社会的信息安全带来非常大的风险。

本申请提供了一种数据加、解密方法、装置、设备及存储介质，能够对数据进行加密，得到加密数据。由于加密数据难以破解，即使加密数据发生泄露或被窥探，能够得到原始数据的可能性也非常小，从而降低了敏感数据信息安全方面的风险。在某些特定需要恢复原始数据的场景中，可根据与本申请中数据加密方法对应的数据解密方法，根据加密数据解密恢复得到原始数据。

本申请第一方面提供了一种数据加密方法。图 1 为本申请第一方面提供的数据加密方法的一实施例的流程图。如图 1 所示，该数据加密方法可包括步骤 S101 至步骤 S104。

在步骤 S101 中，根据原始数据的字节长度，确定补位字节长度。

原始数据可包括但不限于敏感数据。由于不同的原始数据对应的信息的内容不同，不同的原始数据的字节长度也有可能不同。为了能够统一化对原始数据进行加密，需要对原始数据进行补位，使得原始数据补位后的字节长度具有某种规律，便于处理。在一些示例中，原始数据补位后的字节长度为字节划分阈值的整数倍。字节划分阈值具体可与执行数据加密方法的装置如计算机的处理器一次可运行的数据的字节长度一致，在此并不限定。例如，字节划分阈值可为 8。根据原始数据的长度，以原始数据的

补位后的字节长度为字节划分阈值的整数倍为目的，可确定补位字节长度。补位字节长度可视为补位数据的字节长度。

在一些示例中，原始数据的字节长度为字节划分阈值的整数倍，可将字节划分阈值确定为补位字节长度，从而避免冗余的补位数据，能够减少后续过程中的运算量，且节省加密数据的存储空间。

在另一些示例中，原始数据的字节长度不是字节划分阈值的整数倍，可通过预设的字节划分阈值和补位辅助字节阈值，根据原始数据的字节长度，计算得到补位字节长度。可计算原始数据的字节长度与字节划分阈值相除得到的余数。计算补位辅助字节阈值与余数的差值，将该差值作为补位字节长度。其中，补位辅助字节阈值大于字节划分阈值。具体地，补位字节长度可根据算式（1）计算得到：

$$N=P-(L \bmod Q) \quad (1)$$

其中， N 为补位字节长度， P 为补位辅助字节阈值， L 为原始数据的字节长度， Q 为字节划分阈值， $\bmod$ 为取余数计算。补位辅助字节阈值和字节划分阈值可根据工作场景和工作需求设定，在此并不限定。例如， $P=16$ ， $Q=8$ 。

在一些示例中，通过上述补位字节长度的计算得到的补位字节长度最小为 8，最大为 15，能够避免原始数据补位后增加过多的冗余数据，即避免过多的无用数据掺杂在加密过程中，导致原始数据对应的加密数据的字节长度过长，从而能够保证利用本申请实施例中的数据加密方法得到的原始数据的加密数据占用的存储空间更小，且加密计算速度更快。

在步骤 S102 中，获取字节长度为补位字节长度的补位数据。

补位数据即为对原始数据进行补位所用的数据，可视为对数据加密所使用的加密种子。

在一些示例中，补位数据可为预设的补位数据集合中的一个满足补位字节长度的数据。补位数据集合可预先设定，补位数据集合包括至少一个数据。为了能够与不同字节长度的原始数据对应，补位数据集合可包括多个字节长度不同的数据。在根据原始数据的字节长度确定补位字节长度的情况下，可在补位数据集合中选取一个字节长度为补位字节长度的数据作

为该原始数据的补位数据。

在另一些示例中，补位数据中至少部分字节为随机生成的值。即补位数据可包括完全随机生成的数据，也可包括部分随机生成的数据。补位数据中至少部分字节为随机生成的值，可保证每次加密过程中使用的补位数据具有随机性，提高加密数据被破解的难度，从而进一步提高了加密数据的安全性。在补位数据包括部分随机生成的数据的情况下，可对补位数据中的部分字节有所要求，具体要求可根据工作场景和工作需求设定，在此并不限定。例如，补位数据中可包括表征补位字节长度的第一比特位。即补位数据中的第一比特位可表征该补位数据的补位字节长度，在此并不限定第一比特位在补位数据中的具体位置以及补位数据中第一比特位的数目。例如，第一比特位可位于补位数据最右侧数目为字节划分阈值的字节内，即第一比特位可位于补位数据中数目为字节划分阈值的低位字节内。

下面以一具体示例来进行补位数据的说明。假设字节划分阈值为 8，补位辅助字节阈值为 16，原始数据为字符串“1234567”。通过美国信息交换标准代码（American Standard Code for Information Interchange，ASCII）表，可得到该字符串转换得到的十六进制数据“0x31323334353637”。其中，0x 前缀为十六进制的标志。该字符串转换得到的十六进制数据“0x31323334353637”的字节长度为 7，根据上述算式（1）可计算得到补位字节长度为 9。可将补位数据中的位于最右的一个字节的低 4 比特作为第一比特位，即补位数据包括四个第一比特位。可将补位数据中位于最右的一个字节设为“0x09”、“0xA9”、0x39 等，保证该字节中的第一比特位的值能够表征补位字节长度 9。补位数据中的其他字节可随机生成，如生成的补位数据可为“0xA1B2C3D4E5F637A839”。

在步骤 S103 中，按照预设的拼接规则，对原始数据和补位数据进行拼接，得到拼接数据。

预设的拼接规则可预先写入执行该数据加密方法的装置内，在对数据加密的情况下，读取拼接规则，按照拼接规则对原始数据和补位数据进行拼接。原始数据和补位数据的拼接体即为拼接数据。每次对数据进行加密

的过程中所采用的拼接规则可以相同，也可不同，在此并不限定。

拼接规则用于表征原始数据与补位数据进行拼接的具体方法。例如，拼接规则可包括将补位数据拼接至原始数据的最右侧。又例如，拼接规则可包括将补位数据拼接至原始数据的最左侧。再例如，拼接规则可包括将原始数据分为第一部分和第二部分，将补位数据拼接至原始数据的第一部分与第二部分之间。还例如，拼接规则可包括将补位数据分为第一部分和第二部分，将补位数据的第一部分拼接至原始数据的最左侧，将补位数据的第二部分拼接至原始数据的最右侧。拼接规则的具体内容可根据工作场景和工作需求设定，在此并不限定。

在一些示例中，补位数据中可包括用于表征拼接规则的第二比特位。即补位数据中的第二比特位可表征该补位数据与原始数据的拼接规则，在此并不限定第二比特位在补位数据中的具体位置、补位数据中第二比特位的数目以及第二比特位的值与拼接规则的对应关系。例如，可将补位数据中位于最右的一个字节的高 4 比特作为第二比特位，即补位数据包括四个第二比特位。在该 4 比特中最高比特位为 1，表示将补位数据拼接至原始数据的最右侧；在该 4 比特中最高比特位为 0，表示将补位数据进行了切分，切分方式由该 4 比特中的低 3 比特表示，该 4 比特中的低 3 比特为 1**表示补位数据切分为两部分，分别拼接至原始数据的最左侧和最右侧，该 4 比特中的低 3 比特为 01*表示补位数据切分为三部分，将原始数据切分为两部分，将补位数据的三部分分别拼接至原始数据的最左侧、原始数据两部分之间和原始数据的最右侧。*表示 0、1 中的任意一个数字，不同比特位上的*可表示不同的数字。

例如，原始数据为“0x31323334353637”，拼接数据为“0xFA31CBD2ECF32D34A9”，预设的拼接规则为将拼接数据拼接至原始数据的最右侧，则得到的拼接数据为“0x31323334353637FA31CBD2ECF32D34A9”。

在另一些示例中，拼接规则可为指定拼接规则，在每次对数据加密的过程中，按照该指定拼接规则，对原始数据和补位数据进行拼接。

在又一些示例中，拼接规则为根据原始数据和/或补位数据确定的规

则，即拼接规则可根据原始数据和/或补位数据动态确定。例如，在原始数据的字节长度为 L_1 的情况下，拼接规则为将补位数据拼接至原始数据的最右侧；在补位字节长度为 N_1 的情况下，拼接规则为将补位数据切分为两部分，并分别拼接至原始数据的最左侧和最右侧；在原始数据的字节长度为 L_2 且补位字节长度为 N_2 的情况下，拼接规则为将原始数据切分为两部分，将补位数据切分为三部分，将补位数据的三部分分别拼接至原始数据的最左侧、原始数据两部分之间和原始数据的最右侧。

在步骤 S104 中，利用补位数据的至少部分字节对拼接数据中包括原始数据的部分字节进行异或运算，得到原始数据的加密数据。

可利用补位数据中的所有字节对拼接数据中的原始数据的字节进行异或运算，得到原始数据的加密数据。也可以利用补位数据中的部分字节对拼接数据中的原始数据和拼接数据中补位数据中的另一部分字节进行异或运算，得到原始数据的加密数据。具体可根据原始数据和补位数据来确定进行异或运算的双方，在此并不限定。通过异或运算，改变拼接数据中的原始数据，经过异或运算后的拼接数据即为原始数据的加密数据。

在本申请实施例中，根据原始数据的字节长度，确定补位字节长度，以获取字节长度为补位字节长度的补位数据。按照拼接规则对原始数据和拼接数据进行拼接，形成新的数据即拼接数据。通过利用补位数据的至少部分字节对拼接数据中包括原始数据的部分字节进行异或运算，得到原始数据中的加密数据。经过拼接，加密数据的字节长度与原始数据的字节长度不同。经过异或运算，加密数据中的字节的值相对于原始数据中的字节的值也发生了改变。在未知补位数据和拼接规则的情况下，很难破解本申请实施例生成的加密数据，即使发生泄露或被窥探，泄露的或被窥探的也是加密数据，能够根据加密数据得到原始数据的可能性非常小，从而降低了数据信息安全方面的风险。

而且，本申请实施例中补位和异或运算所需要的计算量较小，与 MD5、SM3、DES 与 3DES 等加密算法相比更为简洁且计算量小。在相同的数据量的情况下，通过测试对比，本申请实施例中的数据加密方法的加密效率相对于 MD5、SM3、DES 与 3DES 等加密算法能够提高 50 倍以

上。本申请实施例中动态产生补位数据，并利用补位数据参与异或运算，在数据传输装置、数据存储装置中即可实现数据的加密，不需额外设置硬件加密设备，也不需要进行密钥管理，简化了数据加密所需的硬件设备，降低了数据加密所需的成本。

图 2 为本申请第一方面提供的数据加密方法的另一实施例的流程图。图 2 与图 1 的不同之处在于，图 1 中的步骤 S104 可具体细化为图 2 中的步骤 S1041 至步骤 S1043。

在步骤 S1041 中，选取补位数据中数目为字节划分阈值的字节组成异或运算对象。

为了生成便于执行数据加密方法的装置处理的数据，可对拼接数据中数据为字节划分阈值的字节分别进行异或运算。异或运算需要至少两个对象参与，异或运算对象可为参与异或运算中的对象，参与异或运算的对象也可根据异或运算对象生成，在此并无限定。

具体选取补位数据中哪些字节组成异或运算对象可根据工作场景和工作需求设定，在此并无限定。例如，可选取补位数据中最右侧的数目为字节划分阈值的字节作为异或运算对象，即可选取补位数据中数目为字节划分阈值的低位字节组成异或运算对象。如字节划分阈值为 8，补位数据为“ 0xFA31CBD2ECF32D34A9 ”，异或运算对象可为“0x31CBD2ECF32D34A9”。

在步骤 S1042 中，利用异或运算对象，对第一目标字节进行异或运算，得到异或运算后的第一目标字节。

第一目标字节包括拼接数据中除异或运算对象外的其他字节。

在原始数据的字节长度小于字节划分阈值的情况下，第一目标字节包括拼接数据中的原始数据和补位数据中除异或运算对象外的其他字节。对应地，利用异或运算对象，对原始数据和补位数据中除异或运算对象外的字节进行异或运算，得到异或运算后的第一目标字节。

在原始数据的字节长度等于字节划分阈值的情况下，第一目标字节包括拼接数据中的原始数据。对应地，利用异或运算对象，对原始数据进行异或运算，得到异或运算后的第一目标字节。

在原始数据的字节长度大于字节划分阈值的情况下，第一目标字节包括拼接数据中的原始数据，或者包括拼接数据中的原始数据和补位数据中除异或运算对象外的字节。按照拼接数据中第一目标字节的排列顺序，将第一目标字节划分为至少两组第一目标字节。一组第一目标字节包括数目为字节划分阈值的第一目标字节。利用异或运算对象，对每一组第一目标字节进行异或运算，得到异或运算后的每一组第一目标字节。

例如，字节划分阈值为 8，补位辅助字节阈值为 16，原始数据的十六进制为“0x313233343536374348494E41”，根据算式（1）计算得到补位字节长度为 12，随机生成补位数据“0xAAB1CBD2ECF31D243E455F6C”。拼接规则为将补位数据拼接至原始数据的右侧，对应地，拼接数据为“0x313233343536374348494E41AAB1CBD2ECF31D243E455F6C”。选取补位数据中最右侧的 8 个字节作为异或运算对象，即异或运算对象为“0xECF31D243E455F6C”。第一目标字节包括“0x313233343536374348494E41AAB1CBD2”，将第一目标字节可划分为两组，一组包括“0x3132333435363743”，另一组包括“0x48494E41AAB1CBD2”。

在原始数据的字节长度大于字节划分阈值的情况下，第一目标字节可划分为 M_1 组， M_1 为大于 1 的正整数。

在一些示例中，可分别对异或运算对象与每一组第一目标字节进行异或运算，得到异或运算后的每一组第一目标字节。即对异或运算对象与第一组第一目标字节进行异或运算，得到异或运算后的第一组第一目标字节；对异或运算对象与第二组第一目标字节进行异或运算，得到异或运算后的第二组第一目标字节；以此类推，直至对异或运算对象与第 M_1 组第一目标字节进行异或运算，得到异或运算后的第 M_1 组第一目标字节。

下面以一示例来进行说明，假设 $M_1=2$ ，拼接数据为“0x313233343536374348494E41AAB1CBD2ECF31D243E455F6C”，原始数据为“0x313233343536374348494E41”，补位数据为“0xAAB1CBD2ECF31D243E455F6C”。异或运算对象为

“ 0xECF31D243E455F6C ”，一组第一目标字节包括“ 0x3132333435363743 ”，另一组第一目标字节包括“ 0x48494E41AAB1CBD2 ”。可将一组第一目标字节“ 0x3132333435363743 ”与异或运算对象“ 0xECF31D243E455F6C ”进行异或运算，得到异或运算后的一组第一目标字节；将另一组第一目标字节“ 0x48494E41AAB1CBD2 ”与异或运算对象“ 0xECF31D243E455F6C ”进行异或运算，得到异或运算后的另一组第一目标字节。

在另一些示例中，可对异或运算对象进行 M_1-1 次移位，得到 M_1-1 个移位后的异或运算对象。即每次移位得到一个移位后的异或运算对象。分别对异或运算对象和 M_1-1 个移位后的异或运算对象，与每一组第一目标字节进行异或运算，得到异或运算后的每一组第一目标字节。每次移位的步长可根据工作场景和工作需求设定，在此并不限定。为了进一步提高加密数据被破解的难度，每次移位的步长可为 S 比特，且 S 不能被 8 整除或不能被 4 整除。例如，每次移位的步长为 1 比特。移位的方向和方式也可根据工作场景和工作需求设定，在此并不限定。例如，移位可为顺序左移并在右补 0 或 1，其中，0 或 1 为补充的比特位的值。又例如，移位可为顺序右移并在左补 0 或 1，其中，0 或 1 为补充的比特位的值。再例如，移位可为循环左移或循环右移。

下面以一具体示例来进行说明，假设 $M_1=2$ ，拼接数据为“ 0x313233343536374348494E41AAB1CBD2ECF31D243E455F6C ”，原始数据为“ 0x313233343536374348494E41 ”，补位数据为“ 0xAAB1CBD2ECF31D243E455F6C ”。异或运算对象为“ 0xECF31D243E455F6C ”，一组第一目标字节包括“ 0x3132333435363743 ”，另一组第一目标字节包括“ 0x48494E41AAB1CBD2 ”。移位为循环左移，每次移位的步长为 1 比特。对异或运算对象进行 1 次移位，得到移位后的异或运算对象“ 0xD9E63A487C8ABED9 ”。可将一组第一目标字节“ 0x3132333435363743 ”与异或运算对象“ 0xECF31D243E455F6C ”进行异或运算，得到异或运算后的一组第一目标字节；将另一组第一目标字节

“ 0x48494E41AAB1CBD2 ” 与 移 位 后 的 异 或 运 算 对 象 “0xD9E63A487C8ABED9” 进行异或运算，得到异或运算后的另一组第一目标字节。

通过对异或运算对象进行移位，以及利用移位后的异或运算对象对成组的第一目标字节进行异或运算，能够进一步提高加密数据被破解的难度，从而进一步降低数据信息安全方面的风险。

在步骤 S1043 中，基于拼接数据中字节的排列顺序，根据异或运算后的第一目标字节和异或运算对象，得到加密数据。

即异或运算后的第一目标字节和异或运算对象按照拼接数据中字节的排列顺序排列，得到加密数据。

在上述实施例中，确定补位字节长度、对数据进行拼接以及输出加密数据可通过补位器实现，即补位字节长度算法、拼接规则均可内置于补位器内。获取补位数据可通过种子生成器实现，补位数据生成算法可内置于种子生成器内。异或运算可通过异或器实现。移位可通过移位器实现。补位器、种子生成器、异或器和移位器可设置于执行本申请的数据加密方法的装置中。下面以字节划分阈值为 8，原始数据的字节长度大于字节划分阈值 8 为一示例来进行说明。图 3 为本申请实施例提供的数据加密流程的一示例的流程图。如图 3 所示，该数据加密流程可包括步骤 S201 至步骤 S215。

在步骤 S201 中，补位器根据原始数据的字节长度，确定补位字节长度。

在步骤 S202 中，补位器向种子生成器请求字节长度为补位字节长度的补位数据。

在步骤 S203 中，种子生成器生成补位数据。

在步骤 S204 中，种子生成器向补位器反馈补位数据。

在步骤 S205 中，补位器按照拼接规则，拼接原始数据和补位数据。

在步骤 S206 中，补位器向异或器发送按照拼接数据中排列顺序排列的第一组字节长度为 8 个字节的第一个目标字节和 8 个字节的异或运算对象，请求异或器进行异或运算。

在步骤 S207 中，异或器对第一组第一目标字节和异或运算对象进行异或运算。

在步骤 S208 中，异或器向补位器反馈异或运算后的第一组第一目标字节。

在步骤 S209 中，补位器向移位器发送异或运算对象，请求移位器进行移位。

在步骤 S210 中，移位器对异或运算对象进行第一次移位，得到第一次移位后的异或运算对象。

在步骤 S211 中，移位器向补位器反馈第一次移位后的异或运算对象。

在步骤 S212 中，补位器向异或器发送按照拼接数据中排列顺序排列的第二组字节长度为 8 个字节的第一目标字节和第一次移位后的异或运算对象，请求异或器进行异或运算。

在步骤 S213 中，异或器对第二组第一目标字节和第一次移位后的异或运算对象进行异或运算。

在步骤 S214 中，异或器向补位器反馈异或运算后的第二组第一目标字节。

在拼接数据还包括第三组或更多组的第一目标字节的情况下，可重复上述步骤 S209 至步骤 S214，移位器进行第二次或更多次的移位，异或器进行第二组或更多组第一目标字节与第二次或更多次的移位后的异或运算对象之间的异或运算。

在步骤 S215 中，补位器按照拼接数据中字节的排列顺序，根据得到的异或运算后的第一目标字节和异或运算对象，输出加密数据。

在一些特殊情况下，可能会需要将加密数据还原为原始数据。与数据加密方法对应，本申请还提供一种数据解密方法。执行数据解密方法的装置可与执行数据加密方法的装置为同一装置，也可为不同装置，在此并不限定。图 4 为本申请第二方面提供的数据解密方法的一实施例的流程图。如图 4 所示，该数据解密方法可包括步骤 S301 至步骤 S303。

在步骤 S301 中，基于预设的拼接规则和加密数据，确定加密数据中

补位数据包括的异或运算对象。

这里的加密数据即为利用上述实施例中数据加密方法得到的加密数据。预设的拼接规则与上述实施例中数据加密方法中的拼接规则相同，加密方和解密方可预先约定。

加密数据中的异或运算对象并没有发生改变，根据拼接规则，可从加密数据中的补位数据中获取到异或运算对象。

在步骤 S302 中，利用异或运算对象，对加密数据中除异或运算对象外的其他字节进行异或运算，得到拼接数据。

加密数据中除异或运算对象外的其他字节是在数据加密过程中进行过异或运算的字节，利用与数据加密过程中相同的异或运算对象，对加密数据中除异或运算对象外的其他字节再次进行异或运算，将加密数据中除异或运算对象外的其他字节恢复至数据加密过程中异或运算前的字节。基于恢复至数据加密过程中异或运算前的字节和异或运算对象，即可得到拼接数据。拼接数据即为原始数据与补位数据拼接后的数据。

在步骤 S303 中，根据拼接规则和补位字节长度，确定拼接数据中加密数据的原始数据。

补位字节长度为补位数据的字节长度。根据补位字节长度和拼接规则，可确定补位数据。在一些示例中，在补位字节长度为字节划分阈值的情况下或在补位字节长度不是字节划分阈值的情况下，将拼接数据与补位字节长度的第一差值确定为原始数据的字节长度；根据拼接规则和原始数据的字节长度，确定拼接数据中原始数据，即拼接数据去除补位数据即可得到原始数据。在另一些示例中，在补位字节长度不是字节划分阈值的情况下，可计算补位辅助字节阈值与补位字节长度的第二差值；将第二差值作为原始数据的字节长度与字节划分阈值相除得到的余数，得到原始数据的字节长度；根据拼接规则和原始数据的字节长度，确定拼接数据中原始数据。具体地，可在已知补位字节长度、字节划分阈值和补位辅助字节阈值的情况下，根据上述实施例中的算式（1）以及加密数据长度的限制，计算得到原始数据的字节长度，从而得到原始数据。

在一些示例中，补位数据中可包括用于表征补位字节长度的第一比特

位。第一比特位可位于补位数据最右侧数目为字节划分阈值的字节内。在对数据进行解密过程中，可基于拼接规则，确定补位数据中第一比特位在加密数据中的位置。通过读取第一比特位的值，确定补位字节长度。例如，拼接规则为补位数据拼接至原始数据右侧，补位数据中位于最右的一个字节中的低 4 比特为第一比特位，补位数据中位于最右的一个字节为“0x09”，可确定补位字节长度为 9。

在一些示例中，补位数据中包括用于表征拼接规则的第二比特位。用于执行数据解密方法的装置可预先设定第二比特位在加密数据中的位置，通过在加密数据中读取第二比特位的值，确定拼接规则。

上述字节划分阈值、补位辅助字节、异或运算对象、拼接规则、原始数据、加密数据等的具体内容可参见上述实施例中的相关说明，在此不再赘述。在一些示例中，字节划分阈值可为 8，补位辅助字节阈值可为 16。

在本申请实施例中，可基于采用上述实施例中数据加密方法得到的加密数据和拼接规则，确定异或运算对象。利用确定的异或运算对象，对加密数据中除异或运算对象外的其他字节进行异或运算，可恢复得到包括原始数据和补位数据的拼接数据。根据拼接规则和补位字节长度，可在拼接数据中得到原始数据，即恢复得到原始数据。但在没有预先约定拼接规则以及未知补位字节长度的情况下，是很难破解本申请实施例的加密数据的，数据的信息安全能够得到保障。

而且，采用 MD5、SM3 等算法的加密数据无法反向解密，在需要反向解密恢复出原始数据的情况下，MD5、SM3 等算法并不适用。而本申请实施例的数据解密方法能够对上述实施例中的加密数据进行反向解密，恢复出原始数据。本申请实施例中的数据解密方法与 DES、3DES 等算法相比更为简洁且计算量小。在需要解密恢复原始数据的场景中，在相同的数据量的情况下，通过测试对比，本申请实施例中的数据解密方法的解密效率相对于 DES 与 3DES 等算法能够提高 50 倍以上。且在解密过程中，根据加密数据中可确定得到补位数据，不需要额外进行密钥管理，简化了数据解密所需的硬件设备，降低了数据机密所需的成本。

图 5 为本申请第二方面提供的数据解密方法的另一实施例的流程图。

图 5 与图 4 的不同之处在于，图 4 中的步骤 S302 可具体细化为图 5 中的步骤 S3021 和步骤 S3022。

在步骤 S3021 中，利用异或运算对象，对第二目标字节进行异或运算，得到异或运算后的第二目标字节。

第二目标字节包括加密数据中除异或运算对象外的其他字节。

在加密数据的字节长度与补位字节长度的差值小于字节划分阈值的情况下，第二目标字节包括加密过程中经过异或运算后的原始数据和经过异或运算的补位数据中除异或运算对象外的其他字节。利用异或运算对象，对第二目标字节进行异或运算，得到异或运算后的第二目标字节。

在加密数据的字节长度与补位字节长度的差值等于字节划分阈值的情况下，第二目标字节包括加密过程中经过异或运算后的原始数据。利用异或运算对象，对第二目标字节进行异或运算，得到异或运算后的第二目标字节。

在加密数据的字节长度与补位字节长度的差值大于字节划分阈值的情况下，按照加密数据中第二目标字节的排列顺序，将第二目标字节划分为至少两组第二目标字节。一组第二目标字节包括数目为字节划分阈值的第二目标字节。利用异或运算对象，对每一组第二目标字节进行异或运算，得到异或运算后的每一组第二目标字节。

在加密数据的字节长度与补位字节长度的差值大于字节划分阈值的情况下，第一目标字节可划分为 M_2 组， M_2 为大于 1 的正整数。

在一些示例中，分别对异或运算对象与每一组第二目标字节进行异或运算，得到异或运算后的每一组第二目标字节。即对异或运算对象与第一组第二目标字节进行异或运算，得到异或运算后的第一组第二目标字节；对异或运算对象与第二组第二目标字节进行异或运算，得到异或运算后的第二组第二目标字节；以此类推，直至对异或运算对象与第 M_2 组第二目标字节进行异或运算，得到异或运算后的第 M_2 组第二目标字节。

在另一些示例中，对异或运算对象进行 M_2-1 次移位，得到 M_2-1 个移位后的异或运算对象。即每次移位得到一个移位后的异或运算对象。分别对异或运算对象和 M_2-1 个移位后的异或运算对象，与每一组第二目标字

节进行异或运算，得到异或运算后的每一组第二目标字节。即对异或运算对象与第一组第二目标字节进行异或运算，得到异或运算后的第一组第二目标字节；对第一次移位后的异或运算对象与第二组第二目标字节进行异或运算，得到异或运算后的第二组第二目标字节；以此类推，直至对第 M_2-1 次移位后的异或运算对象与第 M_2 组第二目标字节进行异或运算，得到异或运算后的第 M_2 组第二目标字节。

移位的步长、方式、方向的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在步骤 S3022 中，基于加密数据中第二目标字节的排列顺序，根据异或运算后的第二目标字节和异或运算对象，得到拼接数据。

即异或运算后的第二目标字节和异或运算对象按照加密数据中字节的排列顺序排列，得到拼接数据。

本申请第三方面提供一种数据加密装置。图 6 为本申请第三方面提供的数据加密装置的一实施例的结构示意图。如图 6 所示，该数据加密装置 400 可包括长度确定模块 401、获取模块 402、拼接模块 403 和运算模块 404。

长度确定模块 401 可用于根据原始数据的字节长度，确定补位字节长度。

获取模块 402 用于获取字节长度为补位字节长度的补位数据。

拼接模块 403 用于按照预设的拼接规则，对原始数据和补位数据进行拼接，得到拼接数据。

运算模块 404 用于利用补位数据的至少部分字节对拼接数据中包括原始数据的部分字节进行异或运算，得到原始数据的加密数据。

在本申请实施例中，根据原始数据的字节长度，确定补位字节长度，以获取字节长度为补位字节长度的补位数据。按照拼接规则对原始数据和拼接数据进行拼接，形成新的数据即拼接数据。通过利用补位数据的至少部分字节对拼接数据中包括原始数据的部分字节进行异或运算，得到原始数据中的加密数据。经过拼接，加密数据的字节长度与原始数据的字节长度不同。经过异或运算，加密数据中的字节的值相对于原始数据中的字节

的值也发生了改变。在未知补位数据和拼接规则的情况下，很难破解本申请实施例生成的加密数据，即使发生泄露或被窥探，泄露的或被窥探的也是加密数据，能够根据加密数据得到原始数据的可能性非常小，从而降低了数据信息安全方面的风险。

而且，本申请实施例中补位和异或运算所需要的计算量较小，与 MD5、SM3、DES 与 3DES 等加密算法相比更为简洁且计算量小。在相同的数据量的情况下，通过测试对比，本申请实施例中的数据加密方法的加密效率相对于 MD5、SM3、DES 与 3DES 等加密算法能够提高 50 倍以上。本申请实施例中动态产生补位数据，并利用补位数据参与异或运算，在数据传输装置、数据存储装置中即可实现数据的加密，不需额外设置硬件加密设备，也不需要进行密钥管理，简化了数据加密所需的硬件设备，降低了数据加密所需的成本。

在一些示例中，上述长度确定模块 401 可用于：在原始数据的字节长度为字节划分阈值的整数倍的情况下，将字节划分阈值确定为补位字节长度。

在另一些示例中，上述长度确定模块 401 可用于：在原始数据的字节长度不是字节划分阈值的整数倍的情况下，计算原始数据的字节长度与字节划分阈值相除得到的余数；计算补位辅助字节阈值与余数的差值，将差值作为补位字节长度，补位辅助字节阈值大于字节划分阈值。

在一些示例中，字节划分阈值为 8，补位辅助字节阈值为 16。

在一些示例中，上述运算模块 404 用于：选取补位数据中数目为字节划分阈值的字节组成异或运算对象；利用异或运算对象，对第一目标字节进行异或运算，得到异或运算后的第一目标字节，第一目标字节包括拼接数据中除异或运算对象外的其他字节；基于拼接数据中字节的排列顺序，根据异或运算后的第一目标字节和异或运算对象，得到加密数据。

在一些示例中，上述运算模块 404 用于：选取补位数据最右侧数目为字节划分阈值的字节组成异或运算对象。

在一些示例中，上述运算模块 404 用于：在原始数据的字节长度大于字节划分阈值的情况下，按照拼接数据中第一目标字节的排列顺序，将第

一目标字节划分为至少两组第一目标字节，一组第一目标字节包括数目为字节划分阈值的的第一目标字节；利用异或运算对象，对每一组第一目标字节进行异或运算，得到异或运算后的每一组第一目标字节。

具体地，第一目标字节划分为 M_1 组， M_1 为大于 1 的正整数。上述运算模块 404 用于：分别对异或运算对象与每一组第一目标字节进行异或运算，得到异或运算后的每一组第一目标字节；或者，对异或运算对象进行 M_1-1 次移位，得到 M_1-1 个移位后的异或运算对象；分别对异或运算对象和 M_1-1 个移位后的异或运算对象，与每一组第一目标字节进行异或运算，得到异或运算后的每一组第一目标字节。

在一些示例中，补位数据中至少部分字节为随机生成的值。

在另一些示例中，补位数据为预设的补位数据集合中的一个满足补位字节长度的数据。

在一些示例中，补位数据中包括用于表征补位字节长度的第一比特位，第一比特位可位于补位数据最右侧数目为字节划分阈值的字节内。

在一些示例中，补位数据中包括用于表征拼接规则的第二比特位。

在一些示例中，拼接规则为指定拼接规则，

在另一些示例中，拼接规则为根据原始数据和/或补位数据确定的规则。

本申请第四方面提供一种数据解密装置。图 7 为本申请第四方面提供的数据解密装置的一实施例的结构示意图。如图 7 所示，该数据解密装置 500 可包括确定模块 501、运算模块 502 和解密模块 503。

确定模块 501 可用于基于预设的拼接规则和加密数据，确定加密数据中补位数据包括的异或运算对象。

运算模块 502 可用于利用异或运算对象，对加密数据中除异或运算对象外的其他字节进行异或运算，得到拼接数据。

解密模块 503 可用于根据拼接规则和补位字节长度，确定拼接数据中加密数据的原始数据。

补位字节长度为补位数据的字节长度。

在本申请实施例中，可基于采用上述实施例中数据加密方法得到的加

密数据和拼接规则，确定异或运算对象。利用确定的异或运算对象，对加密数据中除异或运算对象外的其他字节进行异或运算，可恢复得到包括原始数据和补位数据的拼接数据。根据拼接规则和补位字节长度，可在拼接数据中得到原始数据，即恢复得到原始数据。但在没有预先约定拼接规则以及未知补位字节长度的情况下，是很难破解本申请实施例的加密数据的，数据的信息安全能够得到保障。

在一些示例中，上述解密模块 503 可用于：在补位字节长度为字节划分阈值的情况下，将拼接数据与补位字节长度的第一差值确定为原始数据的字节长度；根据拼接规则和原始数据的字节长度，确定拼接数据中原始数据。

在另一些示例中，上述解密模块 503 可用于：在补位字节长度不是字节划分阈值的情况下，计算补位辅助字节阈值与补位字节长度的第二差值；将第二差值作为原始数据的字节长度与字节划分阈值相除得到的余数，得到原始数据的字节长度；根据拼接规则和原始数据的字节长度，确定拼接数据中原始数据。

在一些示例中，字节划分阈值为 8，补位辅助字节阈值为 16。

在一些示例中，上述运算模块 502 可用于：利用异或运算对象，对第二目标字节进行异或运算，得到异或运算后的第二目标字节，第二目标字节包括加密数据中除异或运算对象外的其他字节；基于加密数据中第二目标字节的排列顺序，根据异或运算后的第二目标字节和异或运算对象，得到拼接数据。

在一些示例中，上述运算模块 502 可用于：在加密数据的字节长度与补位字节长度的差值大于字节划分阈值的情况下，按照加密数据中第二目标字节的排列顺序，将第二目标字节划分为至少两组第二目标字节，一组第二目标字节包括数目为字节划分阈值的第二目标字节；利用异或运算对象，对每一组第二目标字节进行异或运算，得到异或运算后的每一组第二目标字节。

具体地，第一目标字节划分为 M_2 组， M_2 为大于 1 的正整数。上述运算模块 502 可用于：分别对异或运算对象与每一组第二目标字节进行异或

运算，得到异或运算后的每一组第二目标字节；或者，对异或运算对象进行 M_2-1 次移位，得到 M_2-1 个移位后的异或运算对象；分别对异或运算对象和 M_2-1 个移位后的异或运算对象，与每一组第二目标字节进行异或运算，得到异或运算后的每一组第二目标字节。

在一些示例中，补位数据中包括用于表征补位字节长度的第一比特位。第一比特位可位于补位数据最右侧数目为字节划分阈值的字节内。

在一些示例中，补位数据中包括用于表征拼接规则的第二比特位。

上述实施例中的数据加密装置和数据解密装置可为同一装置或不同装置，在此并不限定。

本申请第五方面提供了一种数据加密设备。图 8 为本申请第五方面提供的数据加密设备的一实施例的结构示意图。如图 8 所示，数据加密设备 600 包括存储器 601、处理器 602 及存储在存储器 601 上并可在处理器 602 上运行的计算机程序。

在一个示例中，上述处理器 602 可以包括中央处理器（CPU），或者特定集成电路（Application Specific Integrated Circuit，ASIC），或者可以被配置成实施本申请实施例的一个或多个集成电路。

存储器 601 可包括只读存储器（Read-Only Memory，ROM），随机存取存储器（Random Access Memory，RAM），磁盘存储介质设备，光存储介质设备，闪存设备，电气、光学或其他物理/有形的存储器存储设备。因此，通常，存储器包括一个或多个编码有包括计算机可执行指令的软件的有形（非暂态）计算机可读存储介质（例如，存储器设备），并且当该软件被执行（例如，由一个或多个处理器）时，其可操作来执行参考根据本申请实施例中数据加密方法所描述的操作。

处理器 602 通过读取存储器 601 中存储的可执行程序代码来运行与可执行程序代码对应的计算机程序，以用于实现上述实施例中的数据加密方法。

在一个示例中，数据加密设备 600 还可包括通信接口 603 和总线 604。其中，如图 8 所示，存储器 601、处理器 602、通信接口 603 通过总线 604 连接并完成相互间的通信。

通信接口 603，主要用于实现本申请实施例中各模块、装置、单元和/或设备之间的通信。也可通过通信接口 603 接入输入设备和/或输出设备。

总线 604 包括硬件、软件或两者，将数据加密设备 600 的部件彼此耦接在一起。举例来说而非限制，总线 604 可包括加速图形端口（Accelerated Graphics Port, AGP）或其他图形总线、增强工业标准架构（Enhanced Industry Standard Architecture, EISA）总线、前端总线（Front Side Bus, FSB）、超传输（HyperTransport, HT）互连、工业标准架构（Industrial Standard Architecture, ISA）总线、无限带宽互连、低引脚数（Low pin count, LPC）总线、存储器总线、微信道架构（MicroChannel Architecture, MCA）总线、外围组件互连（Peripheral Component Interconnect, PCI）总线、PCI-Express（PCI-X）总线、串行高级技术附件（Serial Advanced Technology Attachment, SATA）总线、视频电子标准协会局部（Video Electronics Standards Association Local Bus, VLB）总线或其他合适的总线或者两个或更多个以上这些的组合。在合适的情况下，总线 604 可包括一个或多个总线。尽管本申请实施例描述和示出了特定的总线，但本申请考虑任何合适的总线或互连。

本申请第六方面提供了一种数据解密设备。图 9 为本申请第六方面提供的数据解密设备的一实施例的结构示意图。如图 9 所示，数据解密设备 700 包括存储器 701、处理器 702 及存储在存储器 701 上并可在处理器 702 上运行的计算机程序。

在一个示例中，上述处理器 702 可以包括中央处理器（CPU），或者特定集成电路（Application Specific Integrated Circuit, ASIC），或者可以被配置成实施本申请实施例的一个或多个集成电路。

存储器 701 可包括只读存储器（Read-Only Memory, ROM），随机存取存储器（Random Access Memory, RAM），磁盘存储介质设备，光存储介质设备，闪存设备，电气、光学或其他物理/有形的存储器存储设备。因此，通常，存储器包括一个或多个编码有包括计算机可执行指令的软件有形（非暂态）计算机可读存储介质（例如，存储器设备），并且当该

软件被执行（例如，由一个或多个处理器）时，其可操作来执行参考根据本申请实施例中数据解密方法所描述的操作。

处理器 702 通过读取存储器 701 中存储的可执行程序代码来运行与可执行程序代码对应的计算机程序，以用于实现上述实施例中的数据解密方法。

在一个示例中，数据解密设备 700 还可包括通信接口 703 和总线 704。其中，如图 9 所示，存储器 701、处理器 702、通信接口 703 通过总线 704 连接并完成相互间的通信。

通信接口 703，主要用于实现本申请实施例中各模块、装置、单元和/或设备之间的通信。也可通过通信接口 703 接入输入设备和/或输出设备。

总线 704 包括硬件、软件或两者，将数据解密设备 700 的部件彼此耦接在一起。举例来说而非限制，总线 704 可包括加速图形端口（Accelerated Graphics Port, AGP）或其他图形总线、增强工业标准架构（Enhanced Industry Standard Architecture, EISA）总线、前端总线（Front Side Bus, FSB）、超传输（HyperTransport, HT）互连、工业标准架构（Industrial Standard Architecture, ISA）总线、无限带宽互连、低引脚数（Low pin count, LPC）总线、存储器总线、微信道架构（MicroChannel Architecture, MCA）总线、外围组件互连（Peripheral Component Interconnect, PCI）总线、PCI-Express（PCI-X）总线、串行高级技术附件（Serial Advanced Technology Attachment, SATA）总线、视频电子标准协会局部（Video Electronics Standards Association Local Bus, VLB）总线或其他合适的总线或者两个或更多个以上这些的组合。在合适的情况下，总线 704 可包括一个或多个总线。尽管本申请实施例描述和示出了特定的总线，但本申请考虑任何合适的总线或互连。

上述实施例中的数据加密设备和数据解密设备可为同一设备或不同设备，在此并不限定。

本申请实施例还提供一种计算机可读存储介质，该计算机可读存储介质上存储有计算机程序，该计算机程序被处理器执行时可实现上述实施例中的数据加密方法和/或数据解密方法，且能达到相同的技术效果，为避免

重复，这里不再赘述。其中，上述计算机可读存储介质可包括非暂态计算机可读存储介质，如只读存储器（Read-Only Memory，简称 ROM）、随机存取存储器（Random Access Memory，简称 RAM）、磁碟或者光盘等，在此并不限定。

需要明确的是，本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同或相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。对于装置实施例、设备实施例、计算机可读存储介质实施例而言，相关之处可以参见方法实施例的说明部分。本申请并不局限于上文所描述并在图中示出的特定步骤和结构。本领域的技术人员可以在领会本申请的精神之后，作出各种改变、修改和添加，或者改变步骤之间的顺序。并且，为了简明起见，这里省略对已知方法技术的详细描述。

上面参考根据本申请的实施例的方法、装置（系统）和计算机程序产品的流程图和/或框图描述了本申请的各方面。应当理解，流程图和/或框图中的每个方框以及流程图和/或框图中各方框的组合可以由计算机程序指令实现。这些计算机程序指令可被提供给通用计算机、专用计算机、或其它可编程数据处理装置的处理器，以产生一种机器，使得经由计算机或其它可编程数据处理装置的处理器执行的这些指令使能对流程图和/或框图的一个或多个方框中指定的功能/动作的实现。这种处理器可以是但不限于是通用处理器、专用处理器、特殊应用处理器或者现场可编程逻辑电路。还可理解，框图和/或流程图中的每个方框以及框图和/或流程图中的方框的组合，也可以由执行指定的功能或动作的专用硬件来实现，或可由专用硬件和计算机指令的组合来实现。

本领域技术人员应能理解，上述实施例均是示例性而非限制性的。在不同实施例中出现的不同技术特征可以进行组合，以取得有益效果。本领域技术人员在研究附图、说明书及权利要求书的基础上，应能理解并实现所揭示的实施例的其他变化的实施例。在权利要求书中，术语“包括”并不排除其他装置或步骤；数量词“一个”不排除多个；术语“第一”、“第二”用于标示名称而非用于表示任何特定的顺序。权利要求中的任何

附图标记均不应被理解为对保护范围的限制。权利要求中出现的多个部分的功能可以由一个单独的硬件或软件模块来实现。某些技术特征出现在不同的从属权利要求中并不意味着不能将这些技术特征进行组合以取得有益效果。

权 利 要 求 书

1. 一种数据加密方法，包括：

根据原始数据的字节长度，确定补位字节长度；

获取字节长度为所述补位字节长度的补位数据；

按照预设的拼接规则，对所述原始数据和所述补位数据进行拼接，得到拼接数据；

利用所述补位数据的至少部分字节对所述拼接数据中包括原始数据的部分字节进行异或运算，得到所述原始数据的加密数据。

2. 根据权利要求 1 所述的方法，其中，所述根据原始数据的字节长度，确定补位字节长度，包括：

在所述原始数据的字节长度为字节划分阈值的整数倍的情况下，将所述字节划分阈值确定为所述补位字节长度；

在所述原始数据的字节长度不是所述字节划分阈值的整数倍的情况下，计算所述原始数据的字节长度与所述字节划分阈值相除得到的余数；计算补位辅助字节阈值与所述余数的差值，将所述差值作为所述补位字节长度，所述补位辅助字节阈值大于所述字节划分阈值。

3. 根据权利要求 2 所述的方法，其中，所述字节划分阈值为 8，所述补位辅助字节阈值为 16。

4. 根据权利要求 2 所述的方法，其中，所述利用所述补位数据的至少部分字节对所述拼接数据中包括原始数据的部分字节进行异或运算，得到所述原始数据的加密数据，包括：

选取所述补位数据中数目为所述字节划分阈值的字节组成异或运算对象；

利用所述异或运算对象，对第一目标字节进行异或运算，得到异或运算后的所述第一目标字节，所述第一目标字节包括所述拼接数据中除所述异或运算对象外的其他字节；

基于所述拼接数据中字节的排列顺序，根据异或运算后的所述第一目标字节和所述异或运算对象，得到所述加密数据。

5. 根据权利要求 4 所述的方法, 其中, 所述选取所述补位数据中数目为所述字节划分阈值的字节组成异或运算对象, 包括:

选取所述补位数据最右侧数目为所述字节划分阈值的字节组成所述异或运算对象。

6. 根据权利要求 4 所述的方法, 其中, 所述利用所述异或运算对象, 对第一目标字节进行异或运算, 得到异或运算后的所述第一目标字节, 包括:

在所述原始数据的字节长度大于所述字节划分阈值的情况下, 按照所述拼接数据中所述第一目标字节的排列顺序, 将所述第一目标字节划分为至少两组所述第一目标字节, 一组所述第一目标字节包括数目为字节划分阈值的所述第一目标字节;

利用所述异或运算对象, 对每一组所述第一目标字节进行异或运算, 得到异或运算后的每一组所述第一目标字节。

7. 根据权利要求 6 所述的方法, 其中, 所述第一目标字节划分为 M_1 组, M_1 为大于 1 的正整数,

所述根据所述异或运算对象与每一组所述第一目标字节, 通过异或运算, 得到异或运算后的每一组所述第一目标字节, 包括:

分别对所述异或运算对象与每一组所述第一目标字节进行异或运算, 得到异或运算后的每一组所述第一目标字节;

或者,

对所述异或运算对象进行 M_1-1 次移位, 得到 M_1-1 个移位后的所述异或运算对象; 分别对所述异或运算对象和 M_1-1 个移位后的所述异或运算对象, 与每一组所述第一目标字节进行异或运算, 得到异或运算后的每一组所述第一目标字节。

8. 根据权利要求 1 所述的方法, 其中,

所述补位数据中至少部分字节为随机生成的值;

或者,

所述补位数据为预设的补位数据集合中的一个满足所述补位字节长度的数据。

9. 根据权利要求 1 所述的方法, 其中,

所述补位数据中包括用于表征所述补位字节长度的第一比特位, 所述第一比特位位于所述补位数据最右侧数目为所述字节划分阈值的字节内;

所述补位数据中包括用于表征所述拼接规则的第二比特位。

10. 根据权利要求 1 所述的方法, 其中,

所述拼接规则为指定拼接规则,

或者,

所述拼接规则为根据所述原始数据和/或补位数据确定的规则。

11. 一种数据解密方法, 包括:

基于预设的拼接规则和加密数据, 确定所述加密数据中补位数据包括的异或运算对象;

利用所述异或运算对象, 对所述加密数据中除所述异或运算对象外的其他字节进行异或运算, 得到拼接数据;

根据所述拼接规则和补位字节长度, 确定所述拼接数据中所述加密数据的原始数据, 所述补位字节长度为所述补位数据的字节长度。

12. 根据权利要求 11 所述的方法, 其中, 所述根据所述拼接规则和补位字节长度, 确定所述拼接数据中所述加密数据的原始数据, 包括:

在所述补位字节长度为所述字节划分阈值的情况下, 将所述拼接数据与所述补位字节长度的第一差值确定为所述原始数据的字节长度; 根据所述拼接规则和所述原始数据的字节长度, 确定所述拼接数据中所述原始数据;

在所述补位字节长度不是所述字节划分阈值的情况下, 计算补位辅助字节阈值与所述补位字节长度的第二差值; 将所述第二差值作为所述原始数据的字节长度与字节划分阈值相除得到的余数, 得到所述原始数据的字节长度; 根据所述拼接规则和所述原始数据的字节长度, 确定所述拼接数据中所述原始数据。

13. 根据权利要求 12 所述的方法, 其中, 所述字节划分阈值为 8, 所述补位辅助字节阈值为 16。

14. 根据权利要求 12 所述的方法, 其中, 所述利用所述异或运算对

象，对所述加密数据中除所述异或运算对象外的其他字节进行异或运算，得到拼接数据，包括：

利用所述异或运算对象，对第二目标字节进行异或运算，得到异或运算后的第二目标字节，所述第二目标字节包括所述加密数据中除所述异或运算对象外的其他字节；

基于所述加密数据中所述第二目标字节的排列顺序，根据异或运算后的所述第二目标字节和所述异或运算对象，得到所述拼接数据。

15. 根据权利要求 14 所述的方法，其中，所述利用所述异或运算对象，对第二目标字节进行异或运算，得到异或运算后的第二目标字节，包括：

在所述加密数据的字节长度与补位字节长度的差值大于所述字节划分阈值的情况下，按照所述加密数据中所述第二目标字节的排列顺序，将所述第二目标字节划分为至少两组所述第二目标字节，一组所述第二目标字节包括数目为字节划分阈值的所述第二目标字节；

利用所述异或运算对象，对每一组所述第二目标字节进行异或运算，得到异或运算后的每一组所述第二目标字节。

16. 根据权利要求 15 所述的方法，其中，所述第一目标字节划分为 M_2 组， M_2 为大于 1 的正整数，

所述利用所述异或运算对象，对每一组所述第二目标字节进行异或运算，得到异或运算后的每一组所述第二目标字节，包括：

分别对所述异或运算对象与每一组所述第二目标字节进行异或运算，得到异或运算后的每一组所述第二目标字节；

或者，

对所述异或运算对象进行 M_2-1 次移位，得到 M_2-1 个移位后的所述异或运算对象；分别对所述异或运算对象和 M_2-1 个移位后的所述异或运算对象，与每一组所述第二目标字节进行异或运算，得到异或运算后的每一组所述第二目标字节。

17. 根据权利要求 11 所述的方法，其中，

所述补位数据中包括用于表征所述补位字节长度的第一比特位，所述

第一比特位位于所述补位数据最右侧数目为所述字节划分阈值的字节内；
所述补位数据中包括用于表征所述拼接规则的第二比特位。

18. 一种数据加密装置，包括：

长度确定模块，用于根据原始数据的字节长度，确定补位字节长度；

获取模块，用于获取字节长度为所述补位字节长度的补位数据；

拼接模块，用于按照预设的拼接规则，对所述原始数据和所述补位数据进行拼接，得到拼接数据；

运算模块，用于利用所述补位数据的至少部分字节对所述拼接数据中包括原始数据的部分字节进行异或运算，得到所述原始数据的加密数据。

19. 一种数据解密装置，包括：

确定模块，用于基于预设的拼接规则和加密数据，确定所述加密数据中补位数据包括的异或运算对象；

运算模块，用于利用所述异或运算对象，对所述加密数据中除所述异或运算对象外的其他字节进行异或运算，得到拼接数据；

解密模块，用于根据所述拼接规则和补位字节长度，确定所述拼接数据中所述加密数据的原始数据，所述补位字节长度为所述补位数据的字节长度。

20. 一种数据加密设备，包括：处理器以及存储有计算机程序指令的存储器；

所述处理器执行所述计算机程序指令时实现如权利要求 1 至 10 中任意一项所述的数据加密方法。

21. 一种数据解密设备，包括：处理器以及存储有计算机程序指令的存储器；

所述处理器执行所述计算机程序指令时实现如权利要求 11 至 17 中任意一项所述的数据解密方法。

22. 一种计算机存储介质，所述计算机存储介质上存储有计算机程序指令，所述计算机程序指令被处理器执行时实现如权利要求 1 至 10 中任意一项所述的数据加密方法和/或如权利要求 11 至 17 中任意一项所述的数据解密方法。

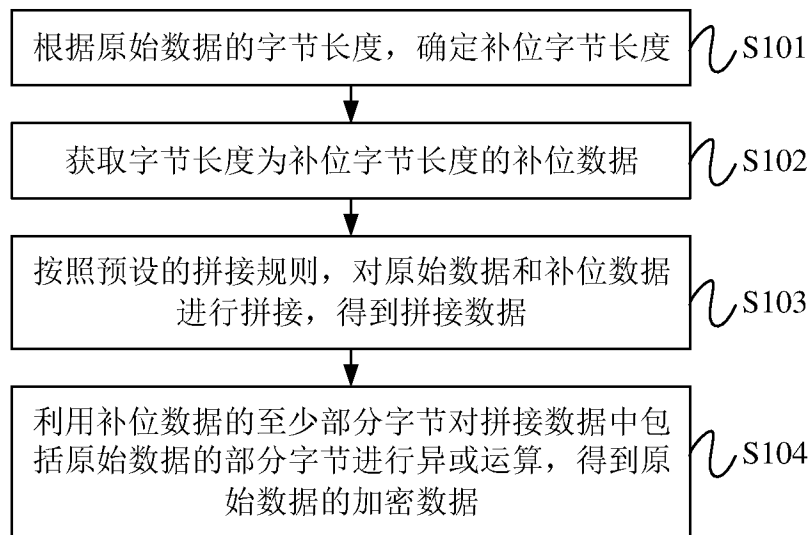


图 1

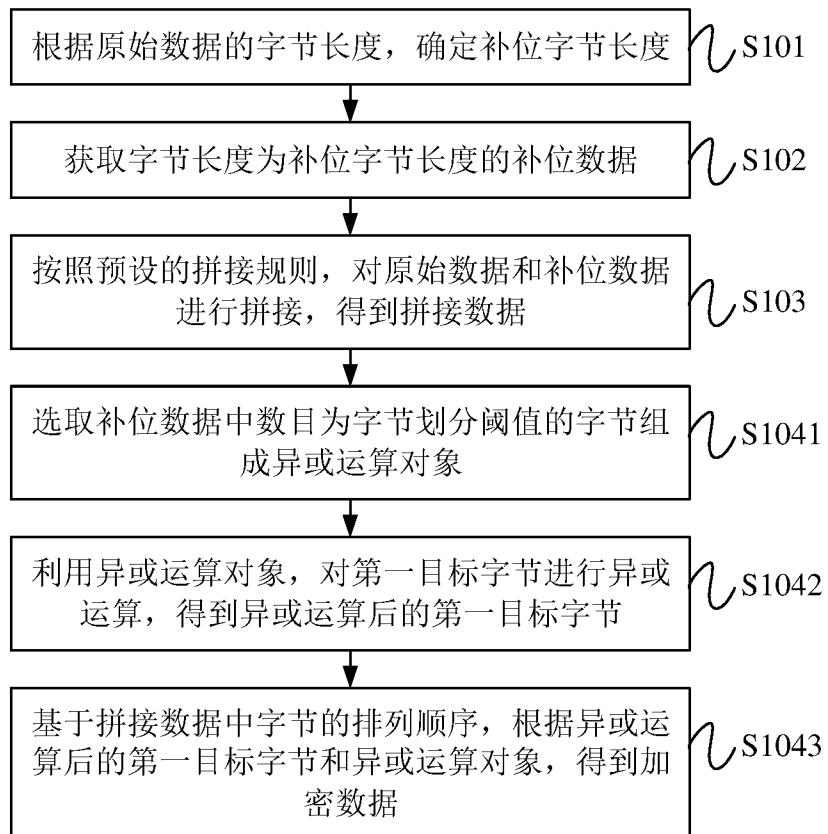


图 2

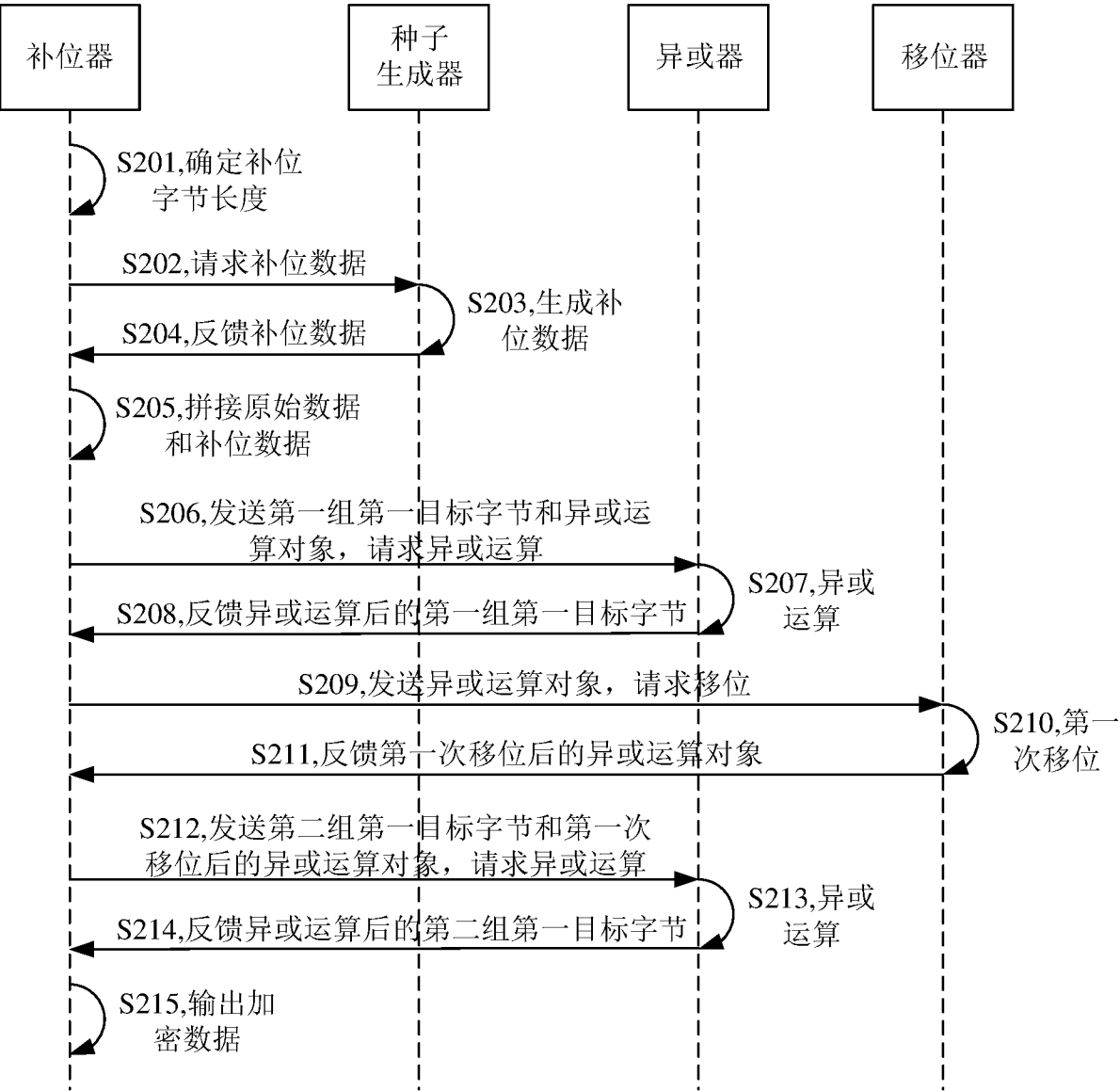


图 3

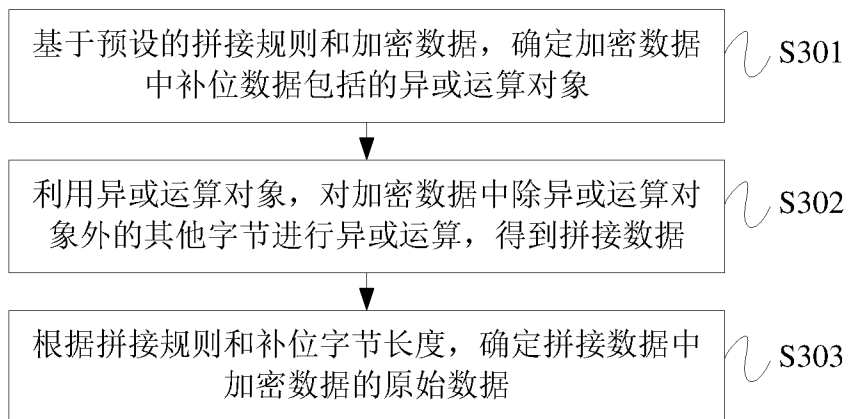


图 4

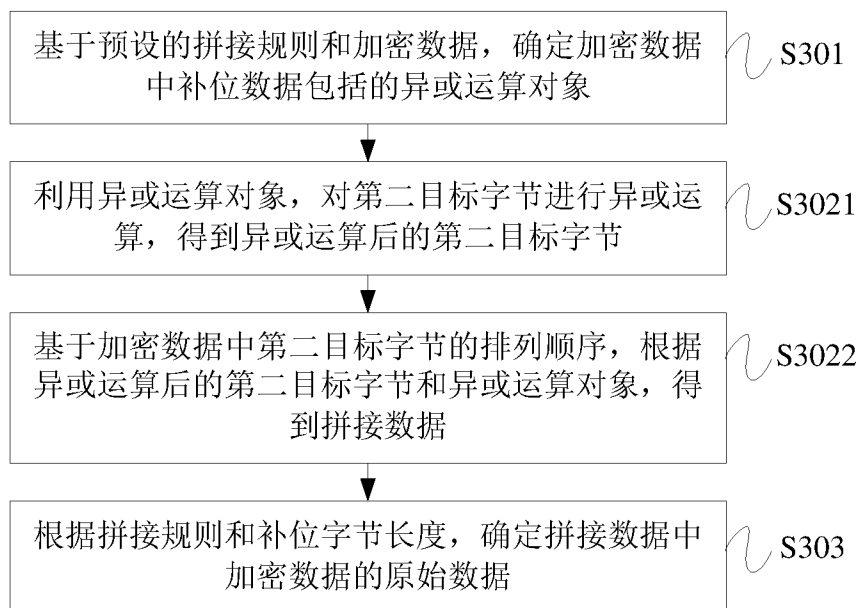


图 5

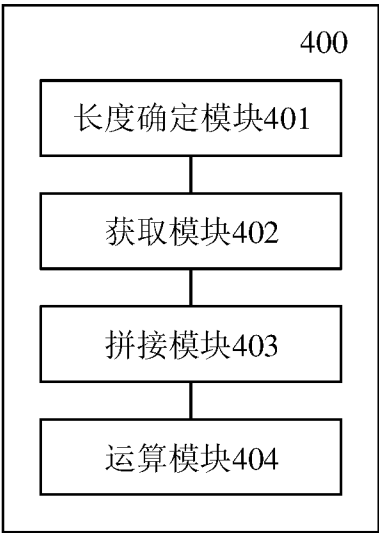


图 6

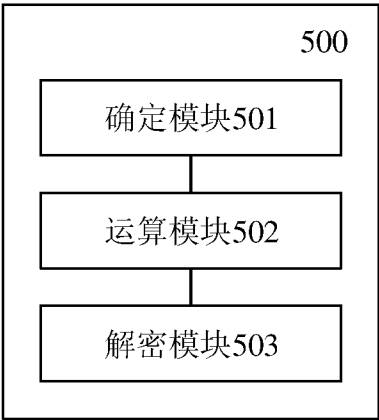


图 7

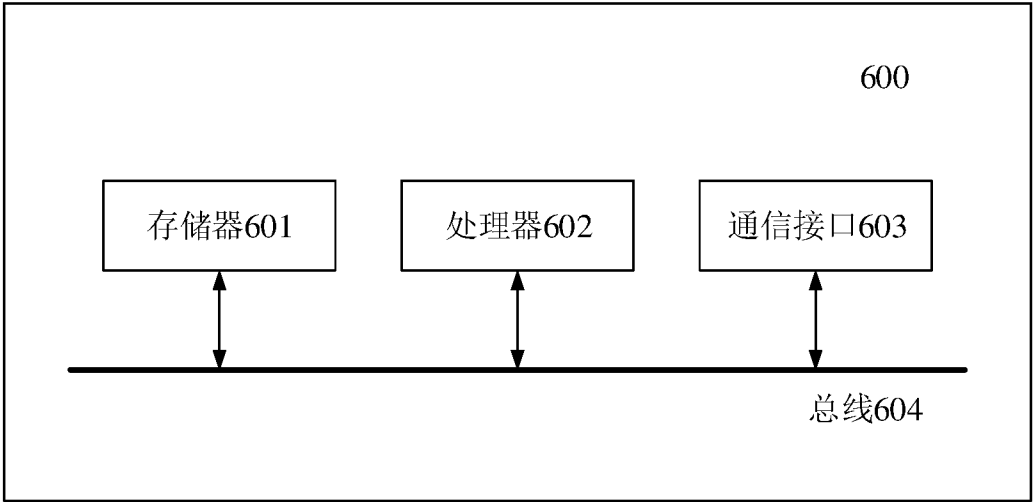


图 8

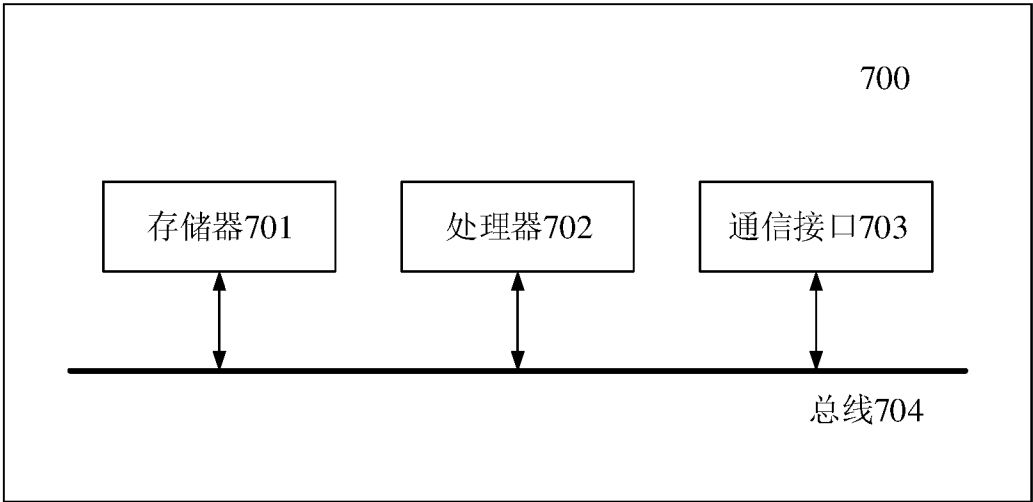


图 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/117032

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(2013.01)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)

G06F

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)

CNPAT, WPI, EPODOC, CNKI, IEEE: 补位, 拼接, 长度, 字节, 异或, 加密, 解密, 部分, 规则, bit, filling, splicing, length, byte, XOR, encryption, decryption, part, rule

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 112464258 A (CHINA UNIONPAY CO., LTD.) 09 March 2021 (2021-03-09) claims 1-22	1-22
A	CN 101895389 A (HEILONGJIANG UNIVERSITY) 24 November 2010 (2010-11-24) abstract, description, paragraphs [0022]-[0061]	1-22
A	CN 102437910 A (NATIONAL SUPERCOMPUTING CENTER IN SHENZHEN (SHENZHEN CLOUD COMPUTING CENTER)) 02 May 2012 (2012-05-02) entire document	1-22
A	CN 105897402 A (LETV HOLDINGS (BEIJING) CO., LTD. et al.) 24 August 2016 (2016-08-24) entire document	1-22
A	US 2017264598 A1 (CORDES, Rene Michael) 14 September 2017 (2017-09-14) entire document	1-22



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

“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

12 October 2021

Date of mailing of the international search report

26 October 2021

Name and mailing address of the ISA/CN

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

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2021/117032

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	112464258	A	09 March 2021	None			
CN	101895389	A	24 November 2010	None			
CN	102437910	A	02 May 2012	None			
CN	105897402	A	24 August 2016	None			
US	2017264598	A1	14 September 2017	EP	2647157	A1	09 October 2013
				WO	2012071597	A1	07 June 2012
				AT	510730	A1	15 June 2012

国际检索报告

国际申请号

PCT/CN2021/117032

A. 主题的分类

G06F 21/60 (2013.01) 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)

G06F

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))

CNPAT, WPI, EPDOC, CNKI, IEEE: 补位, 拼接, 长度, 字节, 异或, 加密, 解密, 部分, 规则, bit, filling, splicing, length, byte, XOR, encryption, decryption, part, rule

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
PX	CN 112464258 A (中国银联股份有限公司) 2021年 3月 9日 (2021 - 03 - 09) 权利要求1-22	1-22
A	CN 101895389 A (黑龙江大学) 2010年 11月 24日 (2010 - 11 - 24) 说明书摘要, 说明书第[0022]-[0061]段	1-22
A	CN 102437910 A (国家超级计算深圳中心深圳云计算中心) 2012年 5月 2日 (2012 - 05 - 02) 全文	1-22
A	CN 105897402 A (乐视控股北京有限公司等) 2016年 8月 24日 (2016 - 08 - 24) 全文	1-22
A	US 2017264598 A1 (CORDES, Rene Michael) 2017年 9月 14日 (2017 - 09 - 14) 全文	1-22

☐ 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

“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

2021年 10月 12日

国际检索报告邮寄日期

2021年 10月 26日

ISA/CN的名称和邮寄地址

中国国家知识产权局(ISA/CN)

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

王思文

电话号码 86-(10)-53961342

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/117032

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	112464258	A	2021年 3月 9日	无			
CN	101895389	A	2010年 11月 24日	无			
CN	102437910	A	2012年 5月 2日	无			
CN	105897402	A	2016年 8月 24日	无			
US	2017264598	A1	2017年 9月 14日	EP	2647157	A1	2013年 10月 9日
				WO	2012071597	A1	2012年 6月 7日
				AT	510730	A1	2012年 6月 15日