

(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
2016 年 2 月 11 日 (11.02.2016)



(10) 国际公布号
WO 2016/019670 A1

- (51) 国际专利分类号:
H04L 9/00 (2006.01)
- (21) 国际申请号: PCT/CN2014/093472
- (22) 国际申请日: 2014 年 12 月 10 日 (10.12.2014)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410384592.1 2014 年 8 月 6 日 (06.08.2014) CN
- (71) 申请人: 国家电网公司 (STATE GRID CORPORATION OF CHINA (SGCC)) [CN/CN]; 中国北京市西城区西长安街 86 号, Beijing 100031 (CN)。北京南瑞智芯微电子科技有限公司 (BEIJING NARI SMARTCHIP MICROELECTRONICS COMPANY LIMITED) [CN/CN]; 中国北京市海淀区西小口路 66 号东升科技园北领地 A-3 座, Beijing 100192 (CN)。
- (72) 发明人: 赵东艳 (ZHAO, Dongyan); 中国北京市海淀区西小口路 66 号东升科技园北领地 A-3 座, Beijing 100192 (CN)。杜新纲 (DU, Xingang); 中国北京市海淀区西小口路 66 号东升科技园北领地 A-3 座, Beijing 100192 (CN)。于艳艳 (YU, Yanyan); 中国北京市海淀区西小口路 66 号东升科技园北领地 A-3 座, Beijing 100192 (CN)。胡晓波 (HU,

Xiaobo); 中国北京市海淀区西小口路 66 号东升科技园北领地 A-3 座, Beijing 100192 (CN)。李娜 (LI, Na); 中国北京市海淀区西小口路 66 号东升科技园北领地 A-3 座, Beijing 100192 (CN)。甘杰 (GAN, Jie); 中国北京市海淀区西小口路 66 号东升科技园北领地 A-3 座, Beijing 100192 (CN)。

(74) 代理人: 北京中誉威圣知识产权代理有限公司 (GENUINEWAYS INC.); 中国北京市东城区东四块玉南街 32 号金泰银丰大厦 3 层, Beijing 100061 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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,

[见续页]

(54) Title: ANTI-ATTACK ENCRYPTION AND DECRYPTION METHOD AND DEVICE OF BLOCK CIPHER

(54) 发明名称: 一种分组密码防攻击的加解密方法和装置

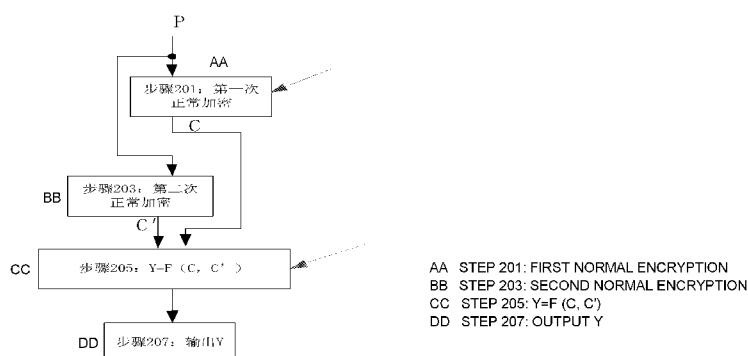


图 2 / FIG. 2

(57) Abstract: Disclosed are an anti-attack encryption and decryption method and device of a block cipher, the encryption method comprising: receiving a plaintext P requiring encryption, conducting normal encryption calculations on the plaintext P twice, and outputting a correct encryption result for input into an F function; when conducting the normal encryption calculations, inserting a fault during the normal encryption calculation process once or twice, and outputting a wrong encryption result; and after inputting the wrong encryption result into the F function, outputting an invalid result unusable by an attacker. An embodiment of the present invention is inserted with the fault during a first and/or second normal encryption calculations, and inputs into the F function two output encryption results, eliminating the step of comparing the two normal encryption calculation results, and the F function outputs the invalid result unusable by the attacker, thus effectively resisting a double-point attack on a block cipher algorithm, and improving the security of the encryption process of the block cipher algorithm.

(57) 摘要:

[见续页]



WO 2016/019670 A1



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))。

本发明公开了一种分组密码防攻击的加解密的方法和装置，其中，该加密方法包括：接收需加密的明文 P，对明文 P 进行两次正常加密运算，输出用于输入 F 函数的正确加密结果；在进行正常加密运算时，正常加密运算过程被一次或两次注入故障，输出错误加密结果；错误加密结果输入 F 函数后，输出攻击者无法利用的无效结果。本发明实施例在进行第一次和/或第二次正常加密运算时被注入故障，并两次输出的加密结果输入到 F 函数中，减少了将两次正常加密运算结果进行比较的步骤，最后由 F 函数输出攻击者无法利用的无效结果，有效的抵抗了对分组密码算法的双点攻击，提高了分组密码算法加密过程的安全性。

一种分组密码防攻击的加解密方法和装置

技术领域

本发明涉及通信领域中信息安全技术领域，具体地，涉及分组密码防攻击的加解密的方法和装置。

5 背景技术

随着计算机和通信技术的发展，用户对信息的安全存储、安全处理和安全传输的需求越来越强烈。特别地，随着 Internet 的广泛应用，信息安全问题显得越来越重要。解决上述问题的有效手段之一是使用现代密码技术，各种密码算法不断出现。分组密码算法是一种最常用的加密手段，
10 分组密码算法具有速度快、易于标准化和便于软硬件实现等特点，通常是信息安全中实现数据加密、消息鉴别和认证的核心密码算法。目前，比较流行的分组密码算法包括 DES 算法、AES 算法等。

随着信息安全问题日益受到人们的关注，对密码算法的各种分析和攻击方法也不断出现。故障攻击是近年来出现的一种强有力的攻击方法。它
15 的基本原理是将密码芯片置于强磁场中，或者改变芯片的电源电压、工作频率、温度等，使密码芯片中的寄存器、存储器在加解密过程中产生随机错误，某些输出比特从原来的 0 变成 1 或 1 变成 0。通过对正确密码输出和错误密码输出的差分比较，经过理论分析，就可得出芯片内部的密码数据信息。

20 分组密码常见的防故障攻击的方法包括：对同一数据进行多次运算，比较多次运算的结果是否一致；对某数据进行正常运算后，对运算结果进行逆运算，比较逆运算结果与原始输入数据是否一致。

如图 1 所示，如果攻击者在对明文 P 进行第一次正常运算时注入故障，那么该第一次正常运算输出的结果 C 即为错误的结果，对明文 P 进行第二
25 次正常运算时输出的结果 C' 为正确的结果，此时 $C \neq C'$ ；然后将结果 C 与结果 C' 进行比较，即判定 C 与 C' 是否相等，并在该结果比较时再次注入故障，由于故障的注入，存在将 " $C \neq C'$ " 攻击成 " $C=C'$ " 的可能。如果注入故障将 " $C \neq C'$ " 攻击成 " $C=C'$ "，则比较结果输出为错误结果 C。攻击者获得该错误结果 C，加上另外之前已获得的正确结果 C'，就
30 能够获得有用的故障信息，从而获得敏感信息。

同理，如果攻击者在对明文 P 进行第一次正常运算时未注入故障，对明文 P 进行第二次正常运算时注入故障，与上述情况类似，攻击者仍就能够获得错误结果 C'，加上另外之前已获得的正确结果 C，就能够获得有用的故障信息，从而获得敏感信息。

5 发明内容

本发明是为了克服现有技术中分组密码在防止攻击时安全性较低的缺陷，根据本发明的一个方面，提出一种分组密码防攻击的加密方法。

根据本发明实施例的分组密码防攻击的加密方法，包括：

接收需加密的明文 P，对明文 P 进行两次正常加密运算，输出用于输入 F 函数的加密结果；

在进行正常加密运算时，当正常加密运算过程被一次或两次注入故障时，输出错误加密结果；

当错误加密结果输入 F 函数后，输出攻击者无法利用的无效结果；当两次正常加密运算过程未被注入故障时，F 函数输出正确的加密运算结果。

15 本发明是为了克服现有技术中分组密码在防止攻击时安全性较低的缺陷，根据本发明的另一个方面，提出一种分组密码防攻击的加密装置。

根据本发明实施例的分组密码防攻击的加密装置，包括：

加密运算模块，用于接收需加密的明文 P，对明文 P 进行两次正常加密运算，输出用于输入 F 函数的加密结果；

20 故障接收模块，用于在进行正常加密运算时，接收正常加密运算过程被一次或两次注入的故障，并指示加密运算模块输出错误加密结果；

结果输出模块，用于错误加密结果输入 F 函数后，输出攻击者无法利用的无效结果；当两次正常加密运算过程未被注入故障时，输出正确的加密运算结果。

25 本发明实施例公开了一种分组密码防攻击的加密方法和装置，在进行第一次和/或第二次正常加密运算时被注入故障，并将第一次正常加密运算输出的加密结果与第二次正常加密运算输出的加密结果输入到 F 函数中，减少了将两次正常加密运算结果进行比较的步骤，最后由 F 函数输出攻击者无法利用的无效结果，有效的抵抗了对分组密码算法的双点攻击，提高了
30 了分组密码算法加密过程的安全性。

本发明是为了克服现有技术中分组密码在防止攻击时安全性较低的缺陷，根据本发明的一个方面，提出一种分组密码防攻击的解密方法。

根据本发明实施例的分组密码防攻击的解密方法，包括：

接收需解密的密文 P，对密文 P 进行两次正常解密运算，输出用于输入 F 函数的解密结果；

在进行正常解密运算时，当正常解密运算过程被一次或两次注入故障时，输出错误解密结果；

当错误解密结果输入 F 函数后，输出攻击者无法利用的无效结果；当两次正常解密运算过程未被注入故障时，F 函数输出正确的解密运算结果。

本发明是为了克服现有技术中分组密码在防止攻击时安全性较低的缺陷，根据本发明的一个方面，提出一种分组密码防攻击的解密装置。

根据本发明实施例的分组密码防攻击的解密装置，包括：

解密运算模块，用于接收需解密的密文 P，对密文 P 进行两次正常解密运算，输出用于输入 F 函数的解密结果；

故障接收模块，用于在进行正常解密运算时，接收正常解密运算过程被一次或两次注入的故障，并指示解密运算模块输出错误解密结果；

结果输出模块，用于在错误解密结果输入 F 函数后，输出攻击者无法利用的无效结果；当两次正常解密运算过程未被注入故障时，输出正确的解密运算结果。

本发明实施例公开了一种分组密码防攻击的解密方法和装置，在进行第一次和/或第二次正常解密运算时被注入故障，并将第一次正常解密运算输出的解密结果与第二次正常解密运算输出的解密结果输入到 F 函数中，减少了将两次正常解密运算结果进行比较的步骤，最后由 F 函数输出攻击者无法利用的无效结果，有效的抵抗了对分组密码算法的双点攻击，提高了分组密码算法解密过程的安全性。

本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

下面通过附图和实施例，对本发明的技术方案做进一步的详细描述。

附图说明

附图用来提供对本发明的进一步理解，并且构成说明书的一部分，与本发明的实施例一起用于解释本发明，并不构成对本发明的限制。在附图中：

5 图 1 为现有技术中对分组密码进行故障攻击的流程故障攻击的流程示意图；

图 2 为本发明分组密码防攻击的加密方法实施例 1 的流程图；

图 3 为本发明分组密码防攻击的加密方法实施例 2 的流程图；

图 4 为本发明分组密码防攻击的加密方法实施例 3 的流程图；

10 图 5 为本发明分组密码防攻击的加密方法实施例 4 的流程图；

图 6 为本发明分组密码防攻击的解密方法实施例 1 的流程图；

图 7 为本发明分组密码防攻击的解密方法实施例 2 的流程图；

图 8 为本发明分组密码防攻击的解密方法实施例 3 的流程图；

图 9 为本发明分组密码防攻击的解密方法实施例 4 的流程图；

15 图 10 为本发明分组密码防攻击的加密装置实施例的结构图；

图 11 为本发明分组密码防攻击的解密装置实施例的结构图。

具体实施方式

下面结合附图，对本发明的具体实施方式进行详细描述，但应当理解本发明的保护范围并不受具体实施方式的限制。

20 本发明的发明人在分析和研究上述现有技术中发现，在运行分组密码算法进行加密或解密运算过程中，如果检测到有故障注入，芯片不宜输出错误的运算结果，否则攻击者就可以利用错误的运算结果进行差分故障攻击。本发明实施例提供了一种分组密码防攻击的方法，当运算过程中有故障注入时不输出错误运算结果，而是输出对于攻击者来说无法利用的无效结果。

25 如果第一次正常运算未被注入故障，第二次正常运算被注入故障，该无效结果是正确的第一次正常运算结果 C 与错误的第二次正常运算结果 C' （即第二错误加密结果）经过某个 F 函数处理后的运算结果。

30 如果第一次正常运算被注入故障，第二次正常运算未被注入故障，该无效结果是错误的第一次正常运算结果 C （即第一错误加密结果）与正确

的第二次正常运算结果 C' 经过某个 F 函数处理后的运算结果。

如果第一次正常运算被注入故障，第二次正常运算也被注入故障，该无效结果是错误的第一次正常运算结果 C （即第一错误加密结果）与错误的第二次正常运算结果 C' （即第二错误加密结果）经过某个 F 函数处理后的运算结果。

如图 2 所示，本发明实施例公开了一种分组密码防攻击的加密方法，包括：

步骤 201：明文 P 输入到加密模块中，进行第一次正常加密运算，同时，本步骤被注入故障，故输出的是错误加密结果 C ；

10 步骤 203：同一明文 P 再次输入到加密模块中，进行第二次正常加密运算，输出的是正确加密结果 C' ；

步骤 205：将步骤 201 中的错误加密结果 C 和步骤 203 中的正确加密结果 C' 输入 F 函数，该函数的输出为 Y ； F 函数的输入中含有错误加密结果 C ，故输出运算结果为攻击者无法利用的无效结果；

15 对于不同的分组算法， F 函数的表达式不同。

以 DES 算法为例，加密结果 C 由 L 和 R 两部分组成，加密结果 C' 由 L' 和 R' 两部分组成，即 $C=L||R$ ， $C' = L' ||R'$ ，则 F 函数可以定义为：

$$F(C,C')=C'\oplus L\oplus L'\oplus R\oplus R'$$

20 在步骤 205 中， F 函数既可以被注入故障，也可以不被注入故障。由于上述 F 函数的存在，故无论是否被注入故障，上述 F 函数输出的运算结果都为攻击者无法利用的无效结果。

步骤 207：对明文 P 进行加密运算，输出攻击者无法利用的无效结果 Y 。

25 图 2 实施例公开了一种分组密码防攻击的加密方法，在进行第一次正常加密运算时被注入故障，并将被注入故障的第一次正常加密运算输出的错误加密结果与第二次正常加密运算输出的正确加密结果输入到 F 函数中，减少了将两次正常加密运算结果进行比较的步骤，最后由 F 函数输出攻击者无法利用的无效结果，有效的抵抗了对分组密码算法的双点攻击，
30 提高了分组密码算法加密过程的安全性。

如图 3 所示,本发明实施例公开了另一种分组密码防攻击的加密方法,包括:

步骤 301: 明文 P 输入到加密模块中, 进行第一次正常加密运算, 输出的是正确加密结果 C;

5 步骤 303: 同一明文 P 再次输入到加密模块中, 进行第二次正常加密运算, 同时, 本步骤被注入故障, 故输出的是错误加密结果 C' ;

步骤 305: 将步骤 301 中的正确加密结果 C 和步骤 303 中的错误加密结果 C' 输入 F 函数, 该函数的输出为 Y; F 函数的输入中含有错误加密结果 C' , 故输出运算结果为攻击者无法利用的无效结果;

10 对于不同的分组算法, F 函数的表达式不同。

以 DES 算法为例, 加密结果 C 由 L 和 R 两部分组成, 加密结果 C' 由 L' 和 R' 两部分组成, 即 $C=L||R$, $C' = L' ||R'$, 则 F 函数可以定义为:

$$F(C,C')=C'\oplus L\oplus L'\oplus R\oplus R'$$

15 在步骤 305 中, F 函数既可以被注入故障, 也可以不被注入故障。由于上述 F 函数的存在, 故无论是否被注入故障, 上述 F 函数输出的运算结果都为攻击者无法利用的无效结果。

步骤 307: 对明文 P 进行加密运算, 输出攻击者无法利用的无效结果 Y。

20 图 3 实施例公开了一种分组密码防攻击的加密方法, 在进行第二次正常加密运算时被注入故障, 并将被注入故障的第二次正常加密运算输出的错误加密结果与第一次正常加密运算输出的正确加密结果输入到 F 函数中, 减少了将两次正常加密运算结果进行比较的步骤, 最后由 F 函数输出攻击者无法利用的无效结果, 有效的抵抗了对分组密码算法的双点攻击, 25 提高了分组密码算法加密过程的安全性。

如图 4 所示,本发明实施例公开了第三种分组密码防攻击的加密方法,包括:

步骤 401: 明文 P 输入到加密模块中, 进行第一次正常加密运算, 同时, 本步骤被注入故障, 故输出的是错误加密结果 C;

30 步骤 403: 同一明文 P 再次输入到加密模块中, 进行第二次正常加密

运算，同时，本步骤被注入故障，故输出的也是错误加密结果 C' ；

步骤 405：将步骤 401 中的错误加密结果 C 和步骤 403 中的错误加密结果 C' 输入 F 函数，该函数的输出为 Y ； F 函数的输入中含有错误加密结果 C 和 C' ，故输出运算结果为攻击者无法利用的无效结果；

5 对于不同的分组算法， F 函数的表达式不同。

以 DES 算法为例，加密结果 C 由 L 和 R 两部分组成，加密结果 C' 由 L' 和 R' 两部分组成，即 $C=L||R$ ， $C' = L' ||R'$ ，则 F 函数可以定义为：

$$F(C,C')=C' \oplus L \oplus L' \oplus R \oplus R'$$

10 在步骤 405 中， F 函数既可以被注入故障，也可以不被注入故障。由于上述 F 函数的存在，故无论是否被注入故障，上述 F 函数输出的运算结果都为攻击者无法利用的无效结果。

步骤 407：对明文 P 进行加密运算，输出攻击者无法利用的无效结果 Y 。

15 图 4 实施例公开了第三种分组密码防攻击的加密方法，在进行第一次和第二次正常加密运算时都被注入故障，并将被注入故障的第一次正常加密运算输出的错误加密结果与同样被注入故障的第二次正常加密运算输出的错误加密结果输入到 F 函数中，减少了将两次正常加密运算结果进行比较的步骤，最后由 F 函数输出攻击者无法利用的无效结果，有效的抵抗
20 了对分组密码算法的双点攻击，提高了分组密码算法加密过程的安全性。

如图 5 所示，本发明实施例公开了第四种分组密码防攻击的加密方法，包括：

步骤 501：明文 P 输入到加密模块中，进行第一次正常加密运算，输出的是正确加密结果 C ；

25 步骤 503：同一明文 P 再次输入到加密模块中，进行第二次正常加密运算，输出的也是正确加密结果 C' ；

步骤 505：将步骤 501 中的正确加密结果 C 和步骤 503 中的正确加密结果 C' 输入 F 函数，该函数的输出为 Y ； F 函数的输入均为正确的加密结果，故输出运算结果为正确的加密运算结果；

30 在步骤 505 中， F 函数既可以被注入故障，也可以不被注入故障。如

果 F 函数未被注入故障，F 函数输出的运算结果为正确的加密运算结果，如果 F 函数被注入故障，如上述实施例一样，F 函数同样将输出攻击者无法利用的无效结果。

步骤 507：对明文 P 进行加密运算，输出正确的加密运算结果。

- 5 图 5 实施例公开了一种分组密码防攻击的加密方法，在进行两次正常加密运算时都未被注入故障，并将两次正常加密运算的正确加密结果输入到 F 函数中，由 F 函数输出正确的加密运算结果，有效的抵抗了对分组密码算法的双点攻击，提高了分组密码算法加密过程的安全性。

- 10 如图 6 所示，本发明实施例公开了一种分组密码防攻击的解密方法，包括：

步骤 601：密文 P 输入到解密模块中，进行第一次正常解密运算，同时，本步骤被注入故障，故输出的是错误解密结果 C；

步骤 603：同一密文 P 再次输入到解密模块中，进行第二次正常解密运算，输出的是正确解密结果 C'；

- 15 步骤 605：将步骤 601 中的错误解密结果 C 和步骤 603 中的正确解密结果 C' 输入 F 函数，该函数的输出为 Y；F 函数的输入中含有错误解密结果 C，故输出运算结果为攻击者无法利用的无效结果；

对于不同的分组算法，F 函数的表达式不同。

- 20 以 DES 算法为例，解密结果 C 由 L 和 R 两部分组成，解密结果 C' 由 L' 和 R' 两部分组成，即 $C=L||R$ ， $C' = L' ||R'$ ，则 F 函数可以定义为：

$$F(C,C')=C'\oplus L\oplus L'\oplus R\oplus R'$$

- 25 在步骤 605 中，F 函数既可以被注入故障，也可以不被注入故障。由于上述 F 函数的存在，故无论是否被注入故障，上述 F 函数输出的运算结果都为攻击者无法利用的无效结果。

步骤 607：对密文 P 进行解密运算，输出攻击者无法利用的无效结果 Y。

- 30 图 6 实施例公开了一种分组密码防攻击的解密方法，在进行第一次正常解密运算时被注入故障，并将被注入故障的第一次正常解密运算输出的错误解密结果与第二次正常解密运算输出的正确解密结果输入到 F 函数

中，减少了将两次正常解密运算结果进行比较的步骤，最后由 F 函数输出攻击者无法利用的无效结果，有效的抵抗了对分组密码算法的双点攻击，提高了分组密码算法解密过程的安全性。

如图 7 所示，本发明实施例公开了另一种分组密码防攻击的解密方法，
5 包括：

步骤 701：密文 P 输入到解密模块中，进行第一次正常解密运算，输出的是正确解密结果 C；

步骤 703：同一密文 P 再次输入到解密模块中，进行第二次正常解密运算，同时，本步骤被注入故障，故输出的是错误解密结果 C' ；

10 步骤 705：将步骤 701 中的正确解密结果 C 和步骤 703 中的错误解密结果 C' 输入 F 函数，该函数的输出为 Y；F 函数的输入中含有错误解密结果 C' ，故输出运算结果为攻击者无法利用的无效结果；

对于不同的分组算法，F 函数的表达式不同。

以 DES 算法为例，解密结果 C 由 L 和 R 两部分组成，解密结果 C' 由 L' 和 R' 两部分组成，即 $C=L||R$ ， $C' = L' ||R'$ ，则 F 函数可以定义为：

$$F(C,C')=C' \oplus L \oplus L' \oplus R \oplus R'$$

在步骤 705 中，F 函数既可以被注入故障，也可以不被注入故障。由于上述 F 函数的存在，故无论是否被注入故障，上述 F 函数输出的运算结果都为攻击者无法利用的无效结果。
20

步骤 707：对密文 P 进行解密运算，输出攻击者无法利用的无效结果 Y。

图 7 实施例公开了一种分组密码防攻击的解密方法，在进行第二次正常解密运算时被注入故障，并将被注入故障的第二次正常解密运算输出的错误解密结果与第一次正常解密运算输出的正确解密结果输入到 F 函数中，减少了将两次正常解密运算结果进行比较的步骤，最后由 F 函数输出攻击者无法利用的无效结果，有效的抵抗了对分组密码算法的双点攻击，提高了分组密码算法解密过程的安全性。
25

如图 8 所示，本发明实施例公开了第三种分组密码防攻击的解密方法，
30 包括：

步骤 801: 密文 P 输入到解密模块中, 进行第一次正常解密运算, 同时, 本步骤被注入故障, 故输出的是错误解密结果 C;

步骤 803: 同一密文 P 再次输入到解密模块中, 进行第二次正常解密运算, 同时, 本步骤被注入故障, 故输出的是错误解密结果 C' ;

- 5 步骤 805: 将步骤 801 中的错误解密结果 C 和步骤 803 中的错误解密结果 C' 输入 F 函数, 该函数的输出为 Y; F 函数的输入中含有错误解密结果 C 和 C' , 故输出运算结果为攻击者无法利用的无效结果;

对于不同的分组算法, F 函数的表达式不同。

- 以 DES 算法为例, 解密结果 C 由 L 和 R 两部分组成, 解密结果 C' 由 L' 和 R' 两部分组成, 即 $C=L||R$, $C' = L' ||R'$, 则 F 函数可以定义为:

$$F(C,C')=C' \oplus L \oplus L' \oplus R \oplus R'$$

- 在步骤 805 中, F 函数既可以被注入故障, 也可以不被注入故障。由于上述 F 函数的存在, 故无论是否被注入故障, 上述 F 函数输出的运算结果都为攻击者无法利用的无效结果。

步骤 807: 对明文 P 进行解密运算, 输出攻击者无法利用的无效结果 Y。

- 图 8 实施例公开了第三种分组密码防攻击的解密方法, 在进行第一次和第二次正常解密运算时都被注入故障, 并将被注入故障的第一次正常解密运算输出的错误解密结果与同样被注入故障的第二次正常解密运算输出的错误解密结果输入到 F 函数中, 减少了将两次正常解密运算结果进行比较的步骤, 最后由 F 函数输出攻击者无法利用的无效结果, 有效的抵抗了对分组密码算法的双点攻击, 提高了分组密码算法解密过程的安全性。

- 如图 9 所示, 本发明实施例公开了第四种分组密码防攻击的解密方法, 包括:

步骤 901: 密文 P 输入到解密模块中, 进行第一次正常解密运算, 输出的是正确解密结果 C;

步骤 903: 同一密文 P 再次输入到解密模块中, 进行第二次正常解密运算, 输出的也是正确解密结果 C' ;

- 30 步骤 905: 将步骤 901 中的正确解密结果 C 和步骤 903 中的正确解密

结果 C' 输入 F 函数，该函数的输出为 Y；F 函数的输入均为正确解密结果，故输出运算结果为正确的解密运算结果；

对于不同的分组算法，F 函数的表达式不同。

以 DES 算法为例，解密结果 C 由 L 和 R 两部分组成，解密结果 C'

5 由 L' 和 R' 两部分组成，即 $C=L\|R$ ， $C' = L' \|R'$ ，则 F 函数可以定义为：

$$F(C,C')=C'\oplus L\oplus L'\oplus R\oplus R'$$

在步骤 905 中，F 函数既可以被注入故障，也可以不被注入故障。如果 F 函数未被注入故障，F 函数输出的运算结果为正确的解密运算结果，

10 如果 F 函数被注入故障，如上述实施例一样，F 函数同样将输出攻击者无法利用的无效结果。

步骤 907：对密文 P 进行解密运算，输出正确的解密运算结果。

图 9 实施例公开了一种分组密码防攻击的解密方法，在进行两次正常解密运算时都未被注入故障，并将两次正常解密运算的正确解密结果输入

15 到 F 函数中，由 F 函数输出正确的解密运算结果，有效的抵抗了对分组密码算法的双点攻击，提高了分组密码算法解密过程的安全性。

如图 10 所示，公开了一种分组密码防攻击的加密装置，包括：

加密运算模块 10，用于接收需加密的明文 P，对明文 P 进行两次正常加密运算，输出正确加密结果；

20 故障接收模块 20，用于在进行正常加密运算时，接收正常加密运算过程被一次或两次注入的故障，并指示加密运算模块 10 输出错误加密结果；

结果输出模块 30，用于当错误加密结果输入 F 函数后，输出攻击者无法利用的无效结果；当两次正常加密运算过程未被注入故障时，输出正确的加密运算结果。

25 其中：在加密运算模块 10 的两次正常加密运算中，第一次正常加密运算的加密结果为 C，第二次正常加密运算的加密结果为 C' ，C 由 L 和 R 两部分组成， C' 由 L' 和 R' 两部分组成，即 $C=L\|R$ ， $C' = L' \|R'$ ，结果输出模块 30 中的 F 函数定义为： $F(C,C')=C'\oplus L\oplus L'\oplus R\oplus R'$ 。

其中：故障接收模块 20 具体用于，在对明文 P 进行第一次正常加密

30 运算时，接收本次正常加密运算被注入的故障，输出错误加密结果；

在对明文 P 进行第二次正常加密运算时，输出正确加密结果。

其中：故障接收模块 20 具体还用于，在对明文 P 进行第一次正常加密运算时，输出正确加密结果；

在对明文 P 进行第二次正常加密运算时，接收本次正常加密运算被注入的故障，输出错误加密结果。

其中：故障接收模块 20 具体还用于，

在对明文 P 进行第一次正常加密运算时，接收本次正常加密运算被注入的故障，输出错误加密结果；

在对明文 P 进行第二次正常加密运算时，接收本次正常加密运算被注入的故障，输出错误加密结果。

图 10 实施例公开了一种分组密码防攻击的加密装置，在进行第一次和/或第二次正常加密运算时被注入故障，并将第一次正常加密运算输出的加密结果与第二次正常加密运算输出的加密结果输入到 F 函数中，减少了将两次正常加密运算结果进行比较的步骤，最后由 F 函数输出攻击者无法利用的无效结果，有效的抵抗了对分组密码算法的双点攻击，提高了分组密码算法加密过程的安全性。

如图 11 所示，公开了一种分组密码防攻击的解密装置，包括：

解密运算模块 40，用于接收需解密的密文 P，对密文 P 进行两次正常解密运算，输出正确解密结果；

故障接收模块 50，用于在进行正常解密运算时，接收正常解密运算过程被一次或两次注入的故障，并指示解密运算模块 40 输出错误解密结果；

结果输出模块 60，用于当错误解密结果输入 F 函数后，输出攻击者无法利用的无效结果；当两次正常解密运算过程未被注入故障时，输出正确的解密运算结果。

其中：在解密运算模块 40 的两次正常解密运算中，第一次正常解密运算的解密结果为 C，第二次正常解密运算的解密结果为 C'，C 由 L 和 R 两部分组成，C' 由 L' 和 R' 两部分组成，即 $C=L\|R$ ， $C'=L'\|R'$ ，结果输出模块 60 中的 F 函数定义为： $F(C,C')=C'\oplus L\oplus L'\oplus R\oplus R'$ 。

其中：故障接收模块 50 具体用于，在对密文 P 进行第一次正常解密运算时，接收本次正常解密运算被注入的故障，输出错误解密结果；

在对密文 P 进行第二次正常解密运算时，输出正确解密结果。

其中：故障接收模块 50 具体还用于，在对密文 P 进行第一次正常解密运算时，输出正确解密结果；

5 在对密文 P 进行第二次正常解密运算时，接收本次正常解密运算被注入的故障，输出错误解密结果。

其中：故障接收模块 50 具体还用于，在对密文 P 进行第一次正常解密运算时，接收本次正常解密运算被注入的故障，输出错误解密结果；

在对密文 P 进行第二次正常解密运算时，接收本次正常解密运算被注入的故障，输出错误解密结果。

10 图 11 实施例公开了一种分组密码防攻击的解密装置，在进行第一次和/或第二次正常解密运算时被注入故障，并将第一次正常解密运算输出的解密结果与第二次正常解密运算输出的解密结果输入到 F 函数中，减少了将两次正常解密运算结果进行比较的步骤，最后由 F 函数输出攻击者无法利用的无效结果，有效的抵抗了对分组密码算法的双点攻击，提高了分组
15 密码算法解密过程的安全性。

本发明能有多种不同形式的具体实施方式，上面以图 2-图 11 为例结合附图对本发明的技术方案作举例说明，这并不意味着本发明所应用的具体实例只能局限在特定的流程或实施例结构中，本领域的普通技术人员应当了解，上文所提供的具体实施方案只是多种优选用法中的一些示例，任
20 何体现本发明权利要求的实施方式均应在本发明技术方案所要求保护的范围之内。

最后应说明的是：以上所述仅为本发明的优选实施例而已，并不用于限制本发明，尽管参照前述实施例对本发明进行了详细的说明，对于本领域的技术人员来说，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。凡在本发明的精神和原则之
25 内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权利要求书

5 1. 一种分组密码防攻击的加密方法，其特征在于，包括：

接收需加密的明文 P，对所述明文 P 进行两次正常加密运算，输出用于输入 F 函数的加密结果；

在进行所述正常加密运算时，当所述正常加密运算过程被一次或两次注入故障时，输出错误加密结果；

10 当所述错误加密结果输入 F 函数后，输出攻击者无法利用的无效结果；
当两次所述正常加密运算过程未被注入故障时，F 函数输出正确的加密运算结果。

15 2. 根据权利要求 1 所述的方法，其特征在于，在所述两次正常加密运算中，第一次正常加密运算的加密结果为 C，第二次正常加密运算的加密结果为 C'，所述 C 由 L 和 R 两部分组成，所述 C' 由 L' 和 R' 两部分组成，即 $C=L\|R$ ， $C'=L'\|R'$ ，所述 F 函数定义为：
 $F(C,C')=C'\oplus L\oplus L'\oplus R\oplus R'$ 。

20 3. 根据权利要求 1 或 2 所述的方法，其特征在于，所述在进行正常加密运算时，所述正常加密运算过程被一次或两次注入故障，输出错误加密结果的步骤具体包括：

在对所述明文 P 进行第一次正常加密运算时，本次正常加密运算被注入故障，输出第一错误加密结果；

25 在对所述明文 P 进行第二次正常加密运算时，输出正确加密结果。

4. 根据权利要求 1 或 2 所述的方法，其特征在于，所述在进行正常加密运算时，所述正常加密运算过程被一次或两次注入故障，输出错误加密结果的步骤具体还包括：

30 在对所述明文 P 进行第一次正常加密运算时，输出正确加密结果；

在对所述明文 P 进行第二次正常加密运算时，本次正常加密运算被注入故障，输出第二错误加密结果。

5. 根据权利要求 1 或 2 所述的方法, 其特征在于, 所述在进行正常加密运算时, 所述正常加密运算过程被一次或两次注入故障, 输出错误加密结果的步骤具体还包括:

在对所述明文 P 进行第一次正常加密运算时, 本次正常加密运算被注入故障, 输出第一错误加密结果;

在对所述明文 P 进行第二次正常加密运算时, 本次正常加密运算被注入故障, 输出第二错误加密结果。

6. 一种分组密码防攻击的解密方法, 其特征在于, 包括:

10 接收需解密的密文 P, 对所述密文 P 进行两次正常解密运算, 输出用于输入 F 函数的解密结果;

在进行所述正常解密运算时, 当所述正常解密运算过程被一次或两次注入故障时, 输出错误解密结果;

15 当所述错误解密结果输入 F 函数后, 输出攻击者无法利用的无效结果; 当两次所述正常解密运算过程未被注入故障时, F 函数输出正确的解密运算结果。

7. 根据权利要求 6 所述的方法, 其特征在于, 在所述两次正常解密运算中, 第一次正常解密运算的解密结果为 C, 第二次正常解密运算的解密结果为 C', 所述 C 由 L 和 R 两部分组成, 所述 C' 由 L' 和 R' 两部分组成, 即 $C=L\|R$, $C'=L'\|R'$, 所述 F 函数定义为:

$F(C,C')=C'\oplus L\oplus L'\oplus R\oplus R'$ 。

8. 根据权利要求 6 或 7 所述的方法, 其特征在于, 所述在进行正常解密运算时, 所述正常解密运算过程被一次或两次注入故障, 输出错误解密结果的步骤具体包括:

在对所述密文 P 进行第一次正常解密运算时, 本次正常解密运算被注入故障, 输出第一错误解密结果;

在对所述密文 P 进行第二次正常解密运算时, 输出正确解密结果。

9. 根据权利要求 6 或 7 所述的方法, 其特征在于, 所述在进行正常解密运算时, 所述正常解密运算过程被一次或两次注入故障, 输出错误解密结果的步骤具体还包括:

在对所述密文 P 进行第一次正常解密运算时, 输出正确解密结果;

5 在对所述密文 P 进行第二次正常解密运算时, 本次正常解密运算被注入故障, 输出第二错误解密结果。

10. 根据权利要求 6 或 7 所述的方法, 其特征在于, 所述在进行正常解密运算时, 所述正常解密运算过程被一次或两次注入故障, 输出错误解密结果的步骤具体还包括:

在对所述密文 P 进行第一次正常解密运算时, 本次正常解密运算被注入故障, 输出第一错误解密结果;

在对所述密文 P 进行第二次正常解密运算时, 本次正常解密运算被注入故障, 输出第二错误解密结果。

11. 一种分组密码防攻击的加密装置, 其特征在于, 包括:

加密运算模块, 用于接收需加密的明文 P, 对所述明文 P 进行两次正常加密运算, 输出用于输入 F 函数的加密结果;

故障接收模块, 用于在进行所述正常加密运算时, 接收所述正常加密运算过程被一次或两次注入的故障, 并指示所述加密运算模块输出错误加密结果;

结果输出模块, 用于当错误加密结果输入 F 函数后, 输出攻击者无法利用的无效结果; 当两次所述正常加密运算过程未被注入故障时, 输出正确的加密运算结果。

12. 根据权利要求 11 所述的装置, 其特征在于, 在所述加密运算模块的两次正常加密运算中, 第一次正常加密运算的加密结果为 C, 第二次正常加密运算的加密结果为 C', 所述 C 由 L 和 R 两部分组成, 所述 C' 由 L' 和 R' 两部分组成, 即 $C=L\|R$, $C'=L'\|R'$, 所述结果输出模块中的 F 函数定义为:

$$F(C,C')=C'\oplus L\oplus L'\oplus R\oplus R'.$$

13. 根据权利要求 11 或 12 所述的装置，其特征在于，所述故障接收模块具体用于，在对所述明文 P 进行第一次正常加密运算时，接收本次正
5 常加密运算被注入的故障，输出第一错误加密结果；

在对所述明文 P 进行第二次正常加密运算时，输出正确加密结果。

14. 根据权利要求 11 或 12 所述的装置，其特征在于，所述故障接收模块具体还用于，在对所述明文 P 进行第一次正常加密运算时，输出正确
加密结果；

10 在对所述明文 P 进行第二次正常加密运算时，接收本次正常加密运算被注入的故障，输出第二错误加密结果。

15. 根据权利要求 11 或 12 所述的装置，其特征在于，所述故障接收模块具体还用于，

15 在对所述明文 P 进行第一次正常加密运算时，接收本次正常加密运算被注入的故障，输出第一错误加密结果；

在对所述明文 P 进行第二次正常加密运算时，接收本次正常加密运算被注入的故障，输出第二错误加密结果。

20 16. 一种分组密码防攻击的解密装置，其特征在于，包括：

解密运算模块，用于接收需解密的密文 P，对所述密文 P 进行两次正常解密运算，输出用于输入 F 函数的解密结果；

故障接收模块，用于在进行所述正常解密运算时，接收所述正常解密运算过程被一次或两次注入的故障，并指示所述解密运算模块输出错误解
25 密结果；

结果输出模块，用于在错误解密结果输入 F 函数后，输出攻击者无法利用的无效结果；当两次所述正常解密运算过程未被注入故障时，输出正确的解密运算结果。

30 17. 根据权利要求 16 所述的装置，其特征在于，在所述解密运算模块

的两次正常解密运算中，第一次正常解密运算的解密结果为 C ，第二次正常解密运算的解密结果为 C' ，所述 C 由 L 和 R 两部分组成，所述 C' 由 L' 和 R' 两部分组成，即 $C=L\|R$ ， $C'=L'\|R'$ ，所述结果输出模块中的 F 函数定义为： $F(C,C')=C'\oplus L\oplus L'\oplus R\oplus R'$ 。

5

18. 根据权利要求 16 或 17 所述的装置，其特征在于，所述故障接收模块具体用于，在对所述密文 P 进行第一次正常解密运算时，接收本次正常解密运算被注入的故障，输出第一错误解密结果；

在对所述密文 P 进行第二次正常解密运算时，输出正确解密结果。

10

19. 根据权利要求 16 或 17 所述的装置，其特征在于，所述故障接收模块具体还用于，在对所述密文 P 进行第一次正常解密运算时，输出正确解密结果；

在对所述密文 P 进行第二次正常解密运算时，接收本次正常解密运算被注入的故障，输出第二错误解密结果。

15

20. 根据权利要求 16 或 17 所述的装置，其特征在于，所述故障接收模块具体还用于，在对所述密文 P 进行第一次正常解密运算时，接收本次正常解密运算被注入的故障，输出第一错误解密结果；

在对所述密文 P 进行第二次正常解密运算时，接收本次正常解密运算被注入的故障，输出第二错误解密结果。

20

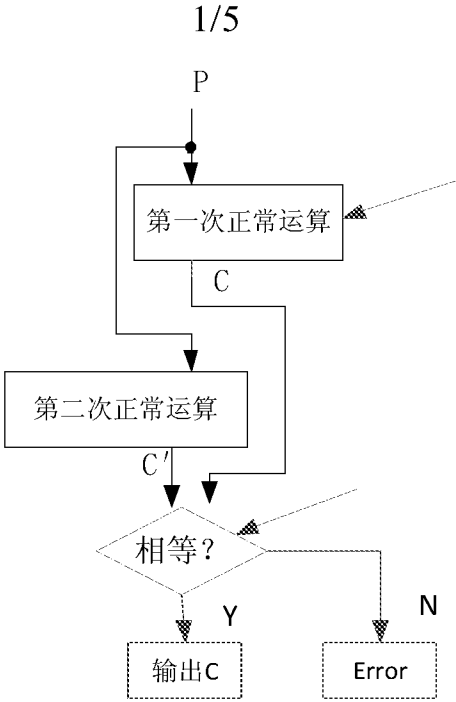


图 1

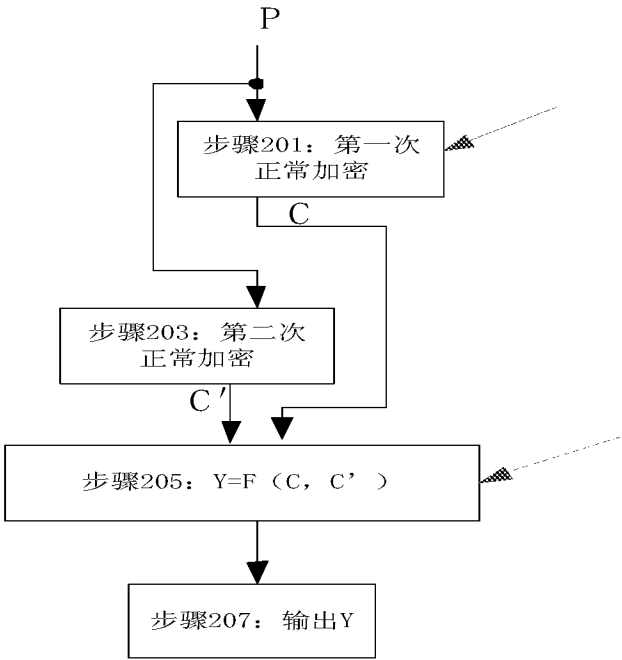


图 2

2/5

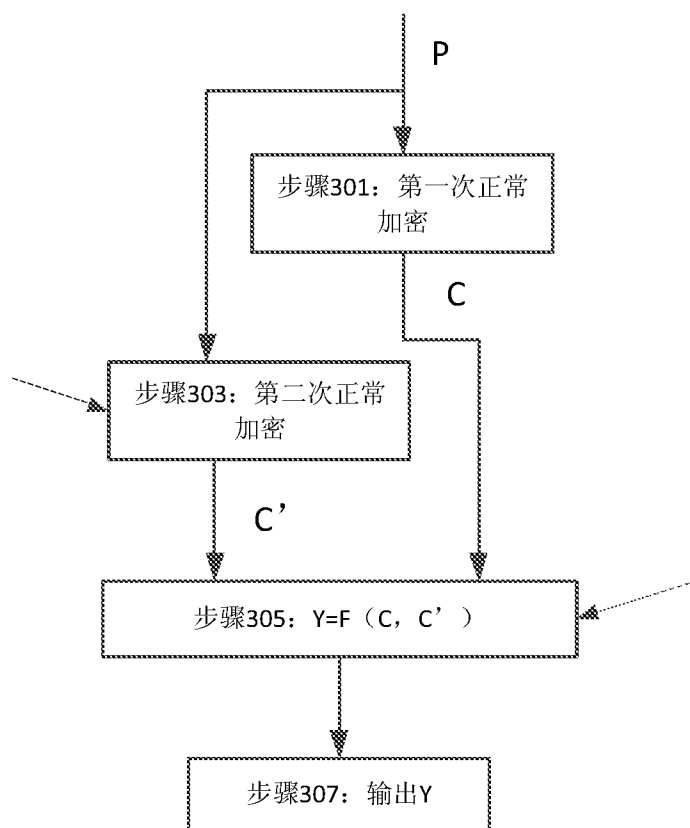


图 3

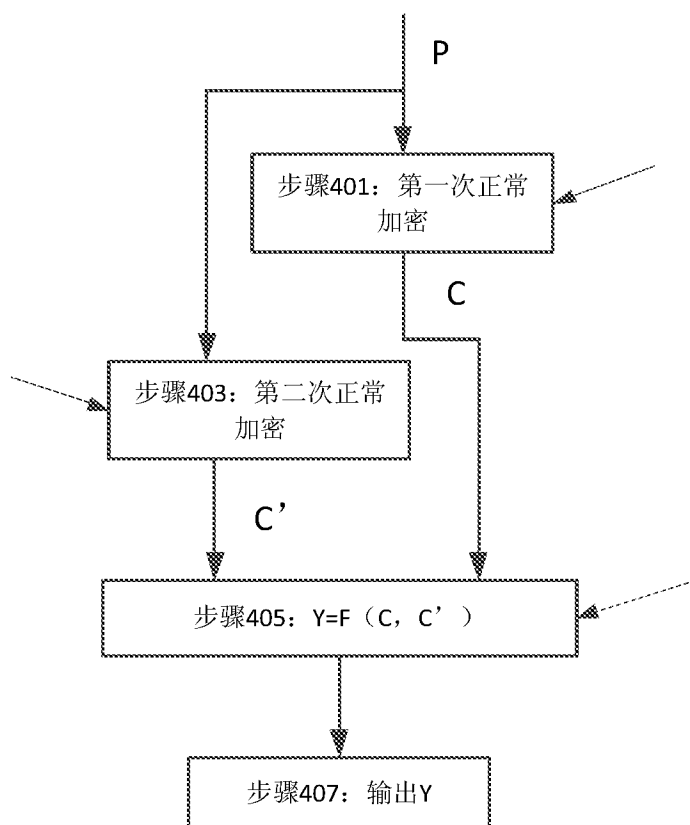


图 4

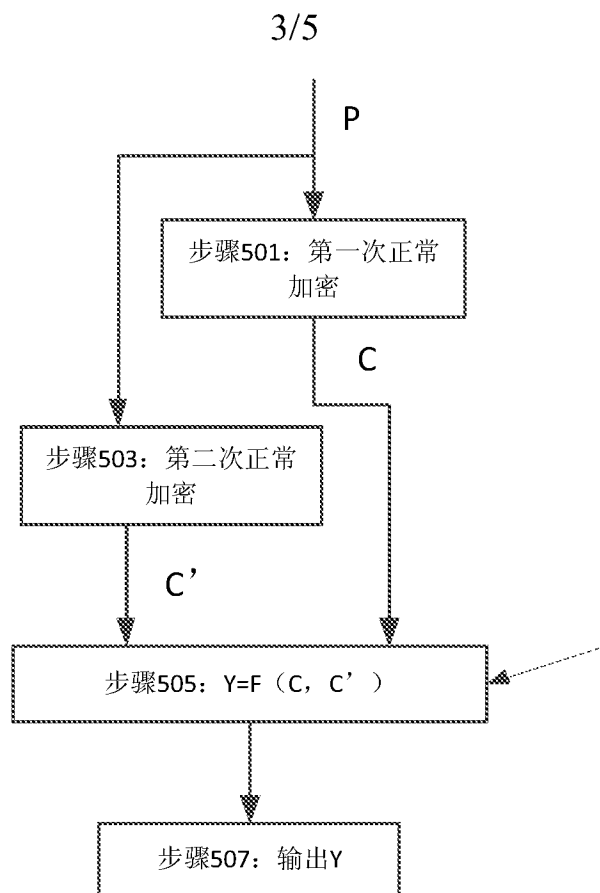


图 5

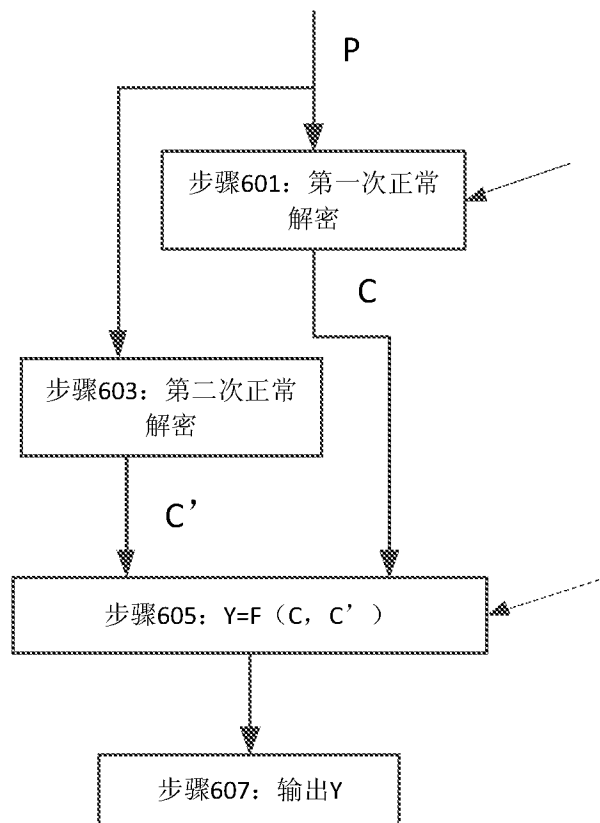


图 6

4/5

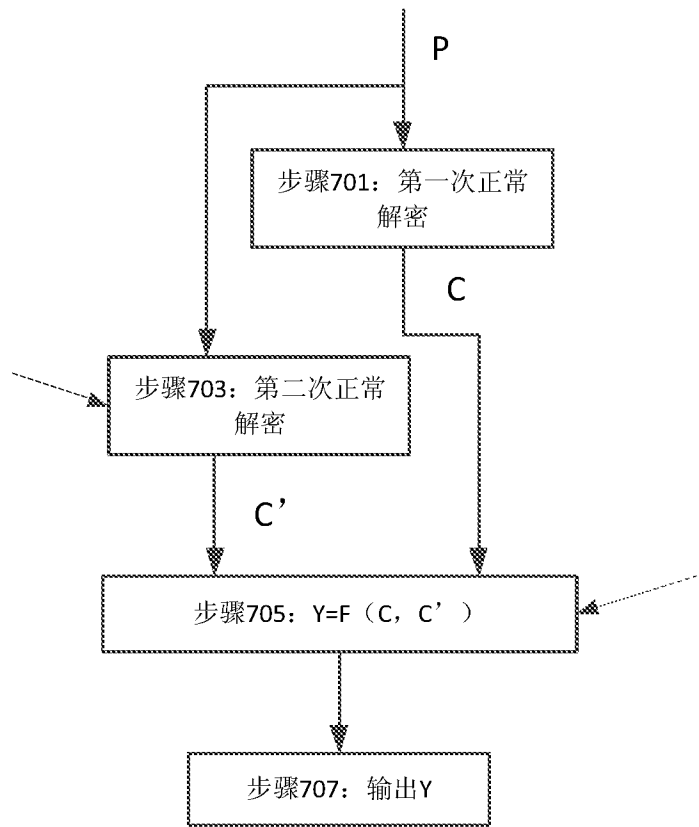


图 7

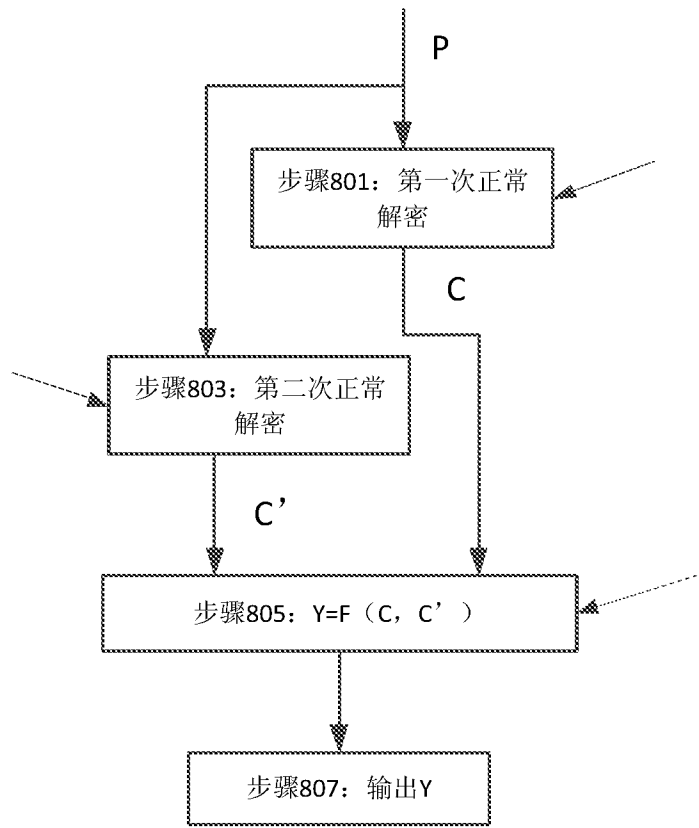


图 8

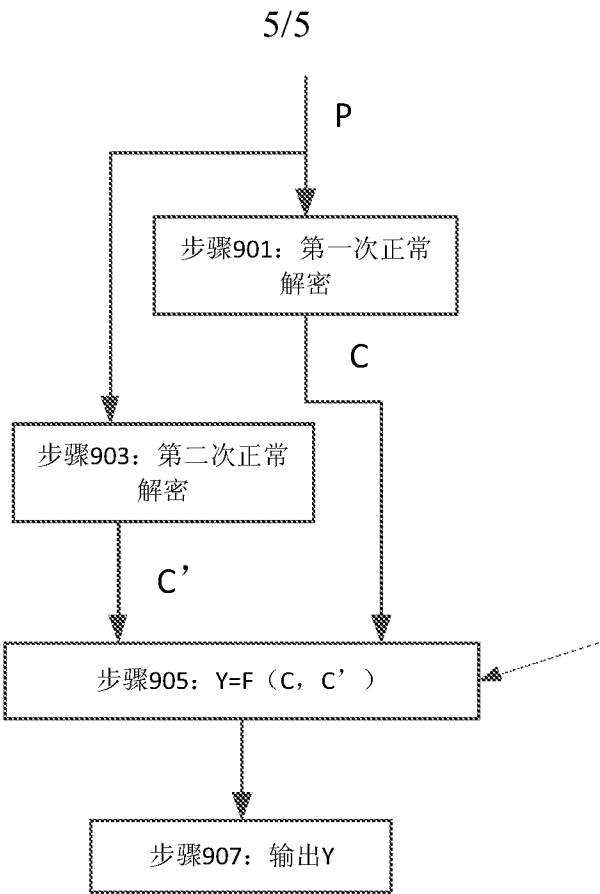


图 9

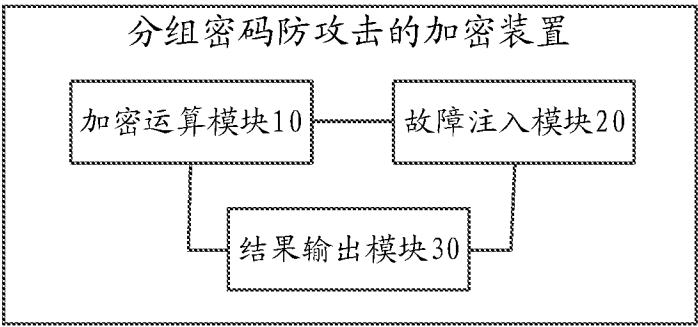


图 10

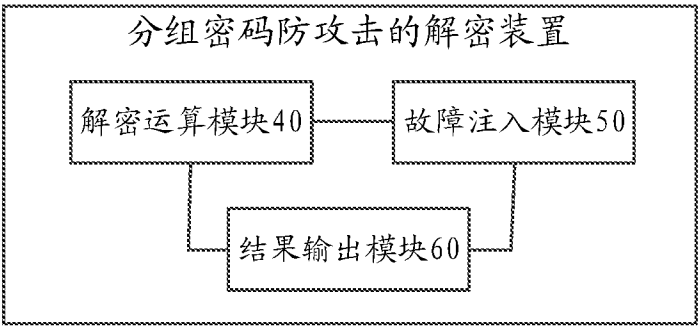


图 11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/093472

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00 (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)

H04L; H04W

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)

CPRSABS, CNTXT, CNKI, VEN: DES, AES, block cipher, attack, fault, encryption, operation, invalid

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101729241 A (NATIONZ TECHNOLOGIES INC.), 09 June 2010 (09.06.2010), the whole document	1-20
A	CN 103634102 A (STATE GRID CORPORATION OF CHINA et al.), 12 March 2014 (12.03.2014), the whole document	1-20
A	CN 102404108 A (NINGBO UNIVERSITY), 04 April 2012 (04.04.2012), the whole document	1-20
A	US 6108419 A (MOTOROLA INC.), 22 August 2000 (22.08.2000), the whole document	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 28 April 2015 (28.04.2015)	Date of mailing of the international search report 12 May 2015 (12.05.2015)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer LI, Yanxin Telephone No.: (86-10) 62089375

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2014/093472

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101729241 A	09 June 2010	WO 2010045843 A1	29 April 2010
		CN 101729241 B	25 January 2012
CN 103634102 A	12 March 2014	None	
CN 102404108 A	04 April 2012	CN 10240410 B	09 July 2014
US 6108419 A	22 August 2000	None	

国际检索报告

国际申请号

PCT/CN2014/093472

A. 主题的分类

H04L 9/00(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)

H04L; H04W

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))

CPRSABS, CNTXT, CNKI, VEN: 分组密码, 攻击, 故障, 错误, 加密, 运算, 无效, DES, AES, block cipher, attack, fault, encryption, operation, invalid

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
A	CN 101729241 A (国民技术股份有限公司) 2010年 6月 9日 (2010 - 06 - 09) 全文	1-20
A	CN 103634102 A (国家电网公司等) 2014年 3月 12日 (2014 - 03 - 12) 全文	1-20
A	CN 102404108 A (宁波大学) 2012年 4月 4日 (2012 - 04 - 04) 全文	1-20
A	US 6108419 A (MOTOROLA INC) 2000年 8月 22日 (2000 - 08 - 22) 全文	1-20

☐ 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

2015年 4月 28日

国际检索报告邮寄日期

2015年 5月 12日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
北京市海淀区蓟门桥西土城路6号
100088 中国

传真号 (86-10)62019451

授权官员

李彦欣

电话号码 (86-10)62089375

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/093472

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	101729241	A	2010年 6月 9日	WO	2010045843	A1	2010年 4月 29日
				CN	101729241	B	2012年 1月 25日
CN	103634102	A	2014年 3月 12日	无			
CN	102404108	A	2012年 4月 4日	CN	102404108	B	2014年 7月 9日
US	6108419	A	2000年 8月 22日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)