一种彩色二维码混合加密编解码方案

张维纳[1]，陈元枝[2]，姜文英[1]，李志茹[1]

(1. 桂林电子科技大学 电子工程与自动化学院，广西 桂林 541004；
2. 桂林电子科技大学 光电工程学院，广西 桂林 541004)

摘 要：针对彩色二维码在数据传输过程中存在的安全隐患，提出了一种彩色二维码混合加密编解码方案。先将发送方信息数据用 DES 算法密钥加密，再用接收方提供的 RSA 公钥对 DES 密钥进行加密，密文数据通过彩色二维码存储和传输；接收方接收密文数据后，先对彩色二维码进行解码，获得密文信息，再通过 RSA 私钥获得 DES 密钥信息，最后用 DES 密钥解密发送方的原始数据信息。该方案具有无密钥传输、双密钥解密、混合密文无法被单一攻击算法破解等优点，从而保护了彩色二维码的编码信息。不同加密算法下彩色二维码信息的加解密效率测试结果表明，在相同密钥长度和高安全性要求下，该混合算法对数据的加解密效率最高，且在脱离网络连接的情况下，彩色二维码系统也可进行正常的加解密操作，提高了安全性和信息数据传输效率。

关键词：DES；RSA；彩色二维码；信息加密；信息安全

中图分类号：TP391.1　　**文献标志码**：A　　**文章编号**：1673-808X(2023)01-0063-06

A color QR code mixed encryption encoding and decoding scheme

ZHANG Weina[1], CHEN Yuanzhi[2], JIANG Wenying[1], LI Zhiru[1]

(1. School of Electronic Engineering and Automation, Guilin University of Electronic Technology, Guilin 541004, China;
2. School of Optoelectronic Engineering, Guilin University of Electronic Technology, Gulin 541004, China)

Abstract: In order to solve the hidden danger in the process of data transmission by color QR codes, a color QR code mixed encryption encoding and decoding scheme is proposed in this paper. In this scheme, the sender information data is encrypted with the DES algorithm key, and then the DES key is encrypted through the RSA public key provided by the receiver, and the cipher text information data is stored and transmitted through the color QR code. After receiving, the receiver first decodes the color QR code to obtain cipher text information, then obtains DES key information through RSA private key, and finally decrypts the original data information of the sender with DES key. The scheme has the advantages of no key transmission, double key decryption and mixed ciphertext can not be cracked by a single attack algorithm, so as to protect the coded information of color QR codes. The encryption and decryption efficiency of color QR code information under different encryption algorithms is compared through experimental tests. The test results show that the hybrid algorithm has the highest efficiency in encrypting and decrypting data under the condition of the same length and high security requirements. And in the case of out of the network connection, the color QR code system can also be normal encryption and decryption operation, not only improve the security, but also improve the efficiency of information data transmission.

Key words: DES; RSA; color QR code; cryptography; information security

二维码是一种新型的数据储存和传递技术。快速响应(QR)码是二维码的一种，发送者通过二维码图片携带数据信息，将数据传递给接收者。随着移动互联网技术的高速发展和智能设备的普及，二维码技术已经在日常生活中产生了较大影响。

近年来，随着对信息容量的需求增加，彩色二维

收稿日期：2020-12-22

基金项目：广西自动检测技术与仪器重点实验室基金(YQ20106)

通信作者：姜文英(1971—)，女，高级实验师，博士，研究方向为信息处理。E-mail：jiangwy@guet.edu.cn

引文格式：张维纳，陈元枝，姜文英，等. 一种彩色二维码混合加密编解码方案[J]. 桂林电子科技大学学报，2023，43(1)：63-68.

码的研究也初见成果。2012 年，Melgar 等[1]提出了 5 色彩色码(CQR Code-5)，适用于需要大存储容量的密码系统。2014 年，Hiren 等[2]和 Andre 等[3]都提出了一种利用彩色增加容量的多路复用彩色二维码。2015 年，Taveerad 等[4]在 HSV 空间内表示颜色值，将二进制输入数据转换为十六进制读取的新型二维码。2016 年，Melgar 等[5]提出了一种 9 色彩色 QR 码方案。陈元枝等[6]提出了一种在 RGB 空间上的 4 色二维码编码方案，该方案保留了黑白 QR 码的特有结构。Li 等[7]提出了一种高效率编码汉字的彩色二维码。2017 年，庞鹏佳[8]提出分层彩色编码的思路，通过一个彩色二维码实现多种信息的交互。侯亚楠[9]在黑白 QR 码的白色模块上编码彩色，增加了 QR 码的信息容量。2018 年，贾丹等[10]也提出一种彩色二维码扩容理念，生成 16 色(HSV 空间)二维码。王超等[11]通过可拆分彩色二维码设计，将彩色二维码信息拆分成 2 个普通二维码，然后合成彩色二维码。

彩色二维码在信息容量上大大提高，信息提取和存储的安全也更加重要。黑白二维码的信息加密技术对于彩色二维码的信息加密技术具有重要的参考价值。黑白二维码在加密方式上主要分为数据信息加密和二维码图像加密 2 种。2011 年，张定会等[12]采用 DES 加密算法直接对二维码图像进行加解密。2012 年，王印明等[13]提出一种随机加密算法，根据特定规则采用 DES 或 RSA 算法对黑白二维码随机加密。2014 年，安吉旺等[14]结合 RSA 和 key 口令的改进算法对编码数据信息加密。2017 年，杨宏宇等[15]提出一种基于 SHA-256 和 DNA 序列的彩色二维码混沌加密方法，提高了二维码防伪造、抗病毒、抗攻击能力。2018 年，印曦等[16]出于对版权的保护，提出了一种改进的图像混沌加密算法，并设计了一种彩色 QR 码数字水印。杨康等[17]为了满足不同权限用户，针对不同权限信息的获密需求采用属性加密算法对二维码信息分级加密。

以上加密方法存在如下问题：单纯运用 DES、AES 等加密算法，密钥的传递得不到有效保障；分级加密、多重加密等方法计算量大，加解密效率不高；对二维码图像进行水印技术加密的计算量较大，安全性相对较低，且与二维码编码过程结合不紧密，难以嵌入二维码系统中。

鉴于此，针对彩色二维码传输时信息数据的安全问题，提出一种彩色二维码混合加密编解码方案。采用安全性极强的 RSA 和 DES 混合加密算法，对高容量彩色二维码的数据信息进行保护。除了提高彩色二维码信息提取和存储的安全性外，还比较了不同加密算法对彩色二维码信息加解密效率的影响。

1 彩色二维码

黑白二维码码由位置探测图形(大方块)、校正图形(小方块)、2 个定位图形(黑白方块交替的线)、格式信息和版本信息区域、数据存储区域和周围的空白区组成，如图 1 所示。QR 码采用 Reed-Solomon 算法纠错，即使部分 QR 码损坏，数据也能被准确读取。QR 码有 L、M、Q、H 四个纠错级别，可恢复的码字比例分别为 7%、15%、25%、30%，级别越高，容错率越强。

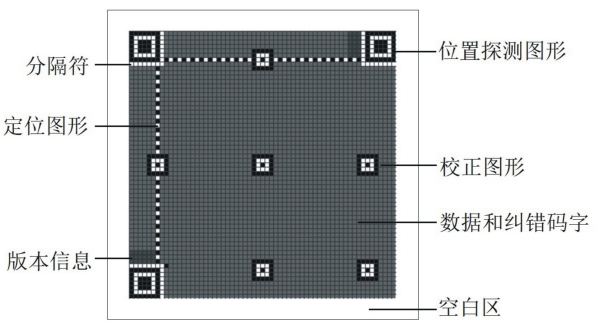

图 1 QR 码结构图

本研究的彩色二维码是在不失去黑白 QR 码原有性质的基础上加入了被编码的彩色信息，从而实现 QR 码信息容量的增加。黑白二维码每个码元仅能放入一个比特数据，彩色二维码每个码元可放入 k ($k\geqslant 2$)位二进制数据，彩色 QR 码的模块可用 2^k 种不同的颜色表征，数据容量扩充为黑白 QR 码的 k 倍。例如，黑白二维码一个模块中只能表示“0”或“1”，但 4 色二维码的单个模块中可表征 2 位二进制数据，即“00”、“01”、“10”或“11”。以“00011011”数据为例，黑白二维码表征此段数据需要 8 个模块，但 4 色二维码只需 4 个模块，单个码元中可表征 2 位二进制，即每个模块可用 2^2 种不同颜色表征，容量扩大为黑白二维码的 2 倍。本研究中，4 色 QR 码主要应用场景为 PC 端，可直接获取彩色二维码图像的像素值，无需进行阈值设定或偏色处理，编码颜色在 RGB 颜色空间中的欧式距离不影响颜色分辨率，可任意选取，4 色彩色 QR 码二进制位流与编码颜色映射关系如表 1 所示。版本为 7 纠错等级为 L 的 4 色 QR 码如图 2 所示。

2 加密算法

2.1 DES 加密算法

DES 算法是密码体制中的对称密码体制，又被

表 1　颜色映射表

单位模块包含的二进制数	颜色种类	二进制值	RGB 值
2	4	00	(255,255,255)
		01	(0,255,255)
		10	(255,0,0)
		11	(0,0,0)

图 2　版本为 7 纠错等级为 L 的 4 色 QR 码

称为美国数据加密标准。DES 是分组密码,以 64 bit 长度为一组对明文数据序列分组,若一组少于 64 bit,就会添加额外的位进行填充,使总数达到 64 bit。DES 密钥长 64 bit,实际上是在 56 bit (8 bit 奇偶校验位)密钥控制下参与 DES 运算。DES 算法采用 Feistel 结构,所以对数据的加密与解密过程几乎相同[18]。DES 算法也是一种迭代算法,它将初始置换进行 16 次迭代,即进行 16 层乘积变换。

DES 算法的加密体系分为数据加密和子密钥生成两部分,结构如图 3 所示。加密过程分为初始置换、乘积变换和逆置换 3 个阶段。首先对 64 bit 明文分组进行初始置换,然后分左(L_0)、右(R_0)两部分分别经过 16 轮迭代,再进行循环移位与变换,最后通过逆置换得出密文。逆置换和初始置换互为逆运算[19]。

在迭代结构中,由 64 bit 初始密钥产生 16 轮 48 bit 子密钥。每轮迭代运算涉及每位数据位,密钥中的比特在每轮都被改变,且每轮的子密钥都进入下一轮进行运算,从而实现数据与密钥结合。迭代式为

$$\begin{cases} L_n = R_{n-1}, \\ R_n = L_{n-1} \oplus f(R_{n-1}, K_n), \end{cases} \tag{1}$$

其中:⊕为异或运算;$n=1,2,\cdots,16$;f 为输出为 32 bit 的函数;K_n 为第 n 个子密钥。

2.2　RSA 加密算法

RSA 是一种典型的非对称密钥加密算法,也是一种将大素数分解的指数函数作为单向陷门函数的公钥体制算法[20]。首先,RSA 算法是“单向”的,即

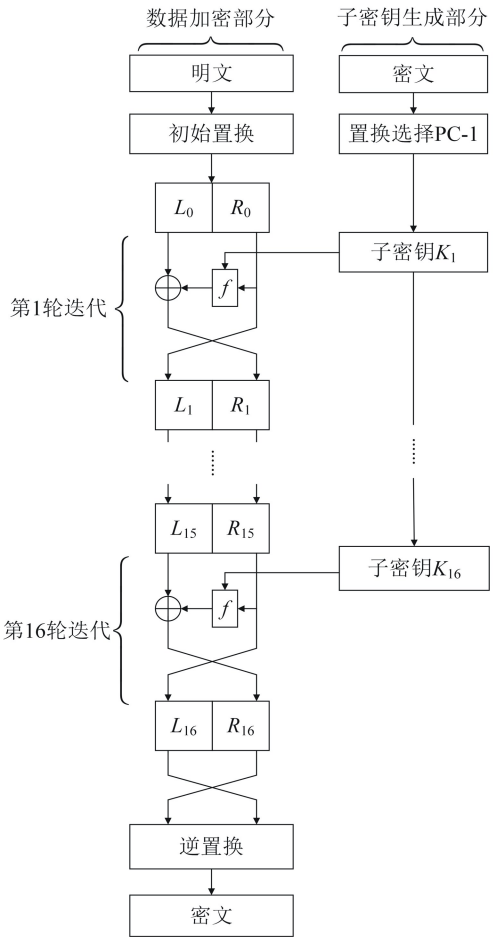

图 3　DES 加密算法结构图

在一个方向上容易计算,但在反方向上很难计算;其次,RSA 算法存在“陷门”,即一旦已知某个陷门信息,其逆函数就很容易计算[18]。RSA 使用公钥、私钥 2 个密钥,公钥用于加密,私钥用于解密。该算法的核心是模幂运算,主要包括密钥的产生和加密解密[21]。

RSA 密钥的生成过程如下:

1)选出 2 个大的素数 p、q,两者不相等,且其差值不能太小;

2)计算模 $n=pq$;

3)计算 $\Phi(n)=(p-1)(q-1)$,$\Phi(n)$ 为欧拉函数;

4)选择一个整数 e,使得 $1<e<\Phi(n)$,$\gcd(e,\Phi(n))=1$;

5)计算解密密钥参数 d,令 $ed=1 \mod \Phi(n)$。

RSA 的加密过程可表示为

$$C=E(M)=M^e \bmod n, \tag{2}$$

RSA 的解密过程可表示为

$$M=D(C)=C^d \bmod n, \tag{3}$$

其中：M 为明文；C 为密文。(e,n)为公钥，(d,n)为私钥。若已知公钥，则可得到密文；若已知私钥，则可得到明文。

3 彩色二维码的混合加密设计

RSA 算法和 DES 算法对数据信息加解密各有优缺点。DES 算法具有易实现、不受数据长度限制和加密速度快等优点。但 DES 算法的密钥太短，只有 56 bit，其密钥量仅为 2^{56}，约为 10^{17}，不足以抵抗穷举式搜索攻击，且在多方发送与多方接收的情况下，使用同一对密钥很容易泄露信息，使用不同密钥对时，密钥对的管理和存储又是一个难题。相比 DES 算法，RSA 算法无需密钥传递，计算复杂度高，不易被破解，密钥分配更为合理，且安全性高[22]。RSA 算法安全性依赖于大素数分解，为了确保因数分解的安全性，RSA 算法通常使用 1 024 bit 以上长度的密钥加密，缺点是加密过程中计算量较大，加密速度慢，一次性加密长度受密钥长度的限制，如 RSA 密钥长度为 1 024 bit 时，一次性加密明文长度不超过 128 byte。综上，单独使用 DES 或 RSA 算法无法满足彩色二维码信息加密需求。因 DES 加密速度快，适合加密彩色二维码高容量数据；RSA 加密速度慢，安全性好，适用于 DES 密钥的加密，可解决 DES 密钥管理与存储的问题，所以将这 2 种算法相结合，用混合加密算法对彩色二维码内存储的信息进行加密保护。混合加解密方案结构如图 4 所示。

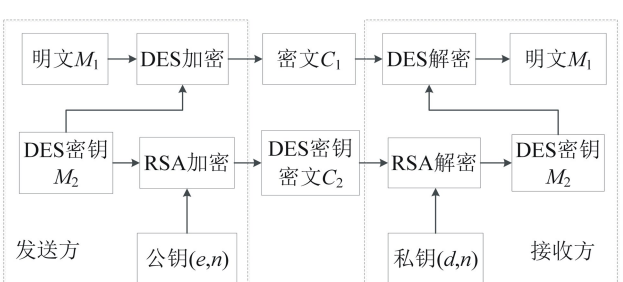

图 4 混合加解密方案结构

3.1 彩色二维码混合加解密步骤

根据混合算法加解密方案，在彩色二维码编解码理论基础上，实现信息加解密功能。彩色二维码信息的混合加密算法设计在明文信息输入之后，信息编码之前；彩色二维码信息的混合解密算法设计在彩色二维码图像解码之后。彩色二维码混合加密步骤如下：

1)接收方将公钥(e,n)发送给发送方，私钥(d,n)留存。

2)发送方通过 DES 加密。信息数据通过 UTF8 编码，输入的 8 个字符作为密钥。数据信息每 64 bit 经初始置换、乘积变换(16 次迭代过程)和逆置换，得到密文 C_1，不足 64 bit 的数据用 PKCS＃7 填充补位。

3)发送方通过 RSA 加密。使用公钥(e,n)加密所输入的 64 bit 密钥，得到密文 C_2。

4)在密文 C_1、C_2 中间添加作为标识的“security”字符串。彩色二维码根据密文 C_1＋security＋C_2 选择相应模式编码成图片储存。混合算法加密原理如图 5 所示。

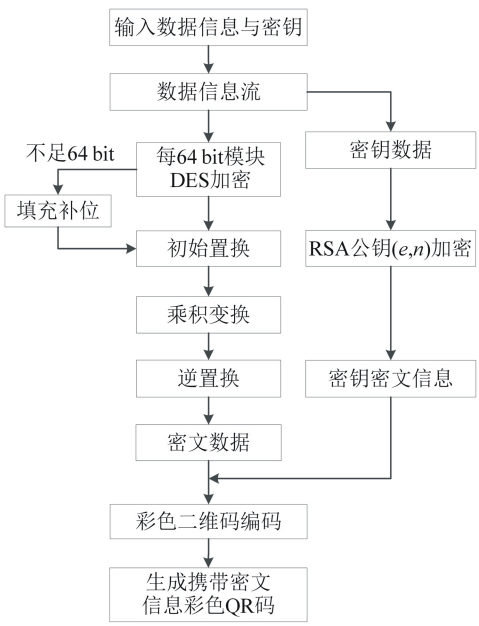

图 5 混合算法加密原理

彩色二维码混合解密步骤如下：

1)接收方解码彩色二维码，得到密文数据，在数据中识别出“security”，并得到密文 C_1、C_2。

2)接收方通过 RSA 解密。使用私钥(d,n)解密 C_2，得到密钥明文 M_2。

3)接收方通过 DES 解密。使用密钥 M_2 解密 C_1，得到明文 M_1。

4 算法测试

4.1 加解密效率比较

以“桂林电子科技大学 ColorQRcode2020 桂林电子科技大学 ColorQRcode2020 桂林电子科技大学 ColorQRcode2020”作为编码信息数据，分别采用 DES、RSA 及 DES & RSA 混合 3 种算法对彩色 QR

码信息加解密性能进行比较。测试环境基于 Microsoft Visual Studio 2019 平台，硬件配置为 Intel i5-7500H CPU @3.40 GHz，RAM 为 8 GiB，编程语言为 C#。根据不同密钥加密结果记录 3 种算法执行 50 次的运行时间，并计算平均值。加解密效率如表 2、3 所示。从表 2 可看出，使用 RSA 算法加密数据所用的时间约是 DES 算法的 2.42 倍，约是混合算法的 1.50 倍。从表 3 可看出，使用 RSA 算法解密数据所用的时间约是 DES 算法的 2.33 倍，约是混合算法的 1.60 倍。测试结果表明，在加解密数据长度相同、安全性要求高的条件下，混合算法加解密数据的效率最高。虽然 DES 算法用时较短，但比混合加密算法安全性低，数据与密钥的安全性都无法得到保证。

表 2　不同算法加密效率

算法	数据长度/byte	密钥长度/bit	平均加密时间/ms	安全性
DES	117	64	2.494	低
RSA	117	1 024	6.036	高
DES & RSA	117	64/1 024	4.012	高

表 3　不同算法解密效率

算法	数据长度/byte	密钥长度/bit	平均解密时间/ms	安全性
DES	117	64	2.637	低
RSA	117	1 024	6.141	高
DES & RSA	117	64/1 024	3.828	高

4.2　安全性分析

在混合算法加密方案中，DES 密钥密文直接与信息密文一同通过彩色二维码编码传输，解决了 DES 的密钥储存与管理问题，且在传输过程中，数据信息安全也受到了有效保护，即使彩色二维码图片被拦截、泄露或是根据颜色判断出表征信息的情况下，解码彩色二维码只能得到包含 2 种算法的混合密文信息，也很难使用某种特定攻击算法破解密文。RSA 算法加密 DES 密钥的密文在无私钥的情况下也大大增加了破解难度。这种双重保障保证了高存储容量的彩色二维码传输信息的安全性。3 种算法加密生成的彩色二维码示例如图 6 所示。

(a) DES算法　(b) RSA算法　(c) DES&RSA算法

图 6　3 种算法加密彩色二维码示例

5　结束语

提出了一种安全性极强的彩色二维码数据加密编解码的方案，提高了彩色 QR 码信息数据传输的安全性。用户可方便地读取彩色二维码的数据信息，且验证过程全自动化。该方案提高了彩色二维码信息提取和存储的安全性，实现了对数据信息传输的加密保护，比单独的 DES 加密算法安全性更高，比单独的 RSA 加密算法更快。另外，彩色二维码系统无需网络连接也可进行正常加解密和编解码操作，这不仅提高了安全性，也提升了信息数据传输的工作效率。下一步将对混合算法的加解密时间进一步优化，以提升系统的运行效率。

参考文献：

[1] MELGAR M，ZAGHETTO A，MACCHIAVELLO B，et al. CQR codes：colored quick-response codes[C]//2012 IEEE Second International Conference on Consumer Electronics. Piscataway，NJ：IEEE Computer Society，2012：321-325.

[2] HIREN J，GALIYAWALA，KINJAL H P. To increase data capacity of QR code using multiplexing with color coding：an example of embedding speech signal in QR code[C]//2014 Annual IEEE India Conference. Piscataway，NJ：IEEE Press，2015：1-6.

[3] ANDRE P S，FERREIR R. Colour multiplexing of quick-response（QR）codes[J]. Electronics Letters，2014，50(24)：1828-1830.

[4] TAVEERAD N，VONGPRADHIP S. Development of color QR code for increasing capacity[C]//2015 11th International Conference on Signal-Image Technology & Internet-Based Systems. Piscataway，NJ：IEEE Press，2015：645-648.

[5] MELGAR M，FARIAS M，ZAGHETTO A，et al. A high density colored 2D-Barcode：CQR Code-9[C]//2016 29th SIBGRAPI Conference on Graphics，Patterns and Images. Piscataway，NJ：IEEE Press，2016：329-334.

[6] 陈元枝，邓艳，史绍亮，等. 基于 Zxing 的彩色 QR 码生成与识别方法[J]. 桂林电子科技大学学报，2016，36(4)：333-337.

[7] LI D，XIE H A. A kind of color two-dimensional QR barcode design[C]//The 2nd Information Technology and Mechatronics Engineering Conference. [S. L.]：Atlantis Press，2016：258-261.

[8] 庞鹏佳. 彩色二维码应用系统的设计与实现[D]. 上海：上海交通大学，2017：24-26.

[9] 侯亚楠. 彩色 QR 码编码解码算法的研究与实现[D].

西安:西安理工大学,2017:19-20.
[10] 贾丹,尤飞,张庆立. QR 码直接扩容技术[J]. 包装工程,2018,39(1):190-195.
[11] 王超,冉鑫泽,刘毅. 可拆分彩色二维码方案设计[J]. 计算机应用与软件,2018,35(7):110-113.
[12] 张定会,单俊涛,江平,等. QR 码 DES 加密与解密[J]. 数据通信,2011(3):40-42.
[13] 王印明,李阳. 一种基于 DES,RSA 的随机加密算法[J]. 计算机技术与发展,2012,22(4):235-237,241.
[14] 安吉旺,徐凯宏. 基于 RSA 和密钥的二维码加密编码的研究[J]. 森林工程,2014,30(2):125-129.
[15] 杨宏宇,王在明. 基于 SHA-256 和 DNA 序列的彩色二维码混沌加密方法[J]. 大连理工大学学报,2017, 57(6):629-636.
[16] 印曦,黄伟庆. 基于混沌理论的彩色 QR 编码水印技术研究[J]. 通信学报,2018,39(7):50-58.
[17] 杨康,袁海东,郭渊博. 基于属性加密的二维码分级加密算法[J]. 计算机工程,2018,44(6):136-140.
[18] 李海泉,李健. 计算机网络安全与加密技术[M]. 北京:科学出版社,2001:15-30.
[19] PATIL P,NARAYANKAR P,NARAYAN D G,et al. A comprehensive evaluation of cryptographic algorithms:DES,3DES,AES,RSA and Blowfish[J]. Procedia Computer Science,2016,78:617-624.
[20] THIRANANT N, LEE Y S, LEE H. Performance comparison between RSA and elliptic curve cryptography-based QR code authentication[C]//2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops. Piscataway, NJ:IEEE Press,2015:278-282.
[21] RIVEST R L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM,1978,21(2):120-126.
[22] 鲍海燕,芦彩林. 基于改进 RSA 算法的隐私数据集同态加密方法[J]. 太赫兹科学与电子信息学报,2020,18(5):177-181.

编辑:张所滨