|  |  |  |  |
| --- | --- | --- | --- |
| 第３７卷 第６期  ２０１９年１２月 | | 陕西科技大学学报  ＪｏｕｒｎａｌｏｆＳｈａａｎｘｉＵｎｉｖｅｒｓｉｔｙｏｆＳｃｉｅｎｃｅ ＆ Ｔｅｃｈｎｏｌｏｇｙ | Ｖｏｌ．３７Ｎｏ．６  Ｄｅｃ．２０１９ |
| ＊ | 文章编号：２０９６－３９８Ｘ（２０１９）０６－０１５３－０７ | | |

一种结合优化后 ＡＥＳ与 ＲＳＡ 算法的二维码加密算法



刘海峰１，刘 洋２，梁星亮１

（１．陕西科技大学 文理学院，陕西 西安 ７１００２１；２．陕西科技大学 电子信息与人工智能学院，陕西 西安

７１００２１）

摘 要：针对目前的二维码信息安全发展现状，提出一种结合了改进后的 ＡＥＳ和 ＲＳＡ 算法的二维码加密算法。该算法在 ＱＲ 二维码编码之前实现加密，即对明文信息进行加密，利用改进后的 ＡＥＳ算法先对明文信息进行对称加密，然后使用 ＲＳＡ 非对称加密算法对于改进后的 ＡＥＳ算法中使用到的参数进行加密生成参数密文，最后将信息密文和参数密文拼接后生成二维码并进行网络信道传输．该算法的特点是通过对 ＡＥＳ算法密钥扩展和列混淆变换两方面的改进、又用中国剩余定理进行 ＲＳＡ 解密算法的优化，减少了算法运行所消耗的时间，提高了安全性．该算法高效易行，结合两种算法优点，实现了对密钥的高效管理和对信息的安全保护，具 有一定的推广和实用价值．

关键词：改进 ＡＥＳ；ＲＳＡ 优化；二维码加密算法

中图分类号：ＴＰ３０９．７ 文献标志码：Ａ

DOI:10.19481/j.cnki.issn2096-398x.2019.06.026

Ａ ＱＲｃｏｄｅｅｎｃｒｙｐｔｉｏｎｔｅｃｈｎｉｑｕｅｃｏｍｂｉｎｉｎｇｏｐｔｉｍｉｚｅｄ ＡＥＳａｎｄＲＳＡａｌｇｏｒｉｔｈｍｓ

ＬＩＵ Ｈａｉ－ｆｅｎｇ１，ＬＩＵ Ｙａｎｇ２，ＬＩＡＮＧ Ｘｉｎｇ－ｌｉａｎｇ１

（１．ＳｃｈｏｏｌｏｆＡｒｔｓａｎｄＳｃｉｅｎｃｅｓ，ＳｈａａｎｘｉＵｎｉｖｅｒｓｉｔｙｏｆＳｃｉｅｎｃｅ ＆ Ｔｅｃｈｎｏｌｏｇｙ，Ｘｉ′ａｎ７１００２１，Ｃｈｉｎａ；２．Ｓｃｈｏｏｌ ｏｆＥｌｅｃｔｒｏｎｉｃＩｎｆｏｒｍａｔｉｏｎａｎｄＡｒｔｉｆｉｃｉａｌＩｎｔｅｌｌｉｇｅｎｃｅ，Ｘｉ′ａｎ７１００２１，Ｃｈｉｎａ）

Ａｂｓｔｒａｃｔ：Ａｃｃｏｒｄｉｎｇｔｏｔｈｅｐｒｅｓｅｎｔｓｉｔｕａｔｉｏｎｏｆｔｈｅｔｗｏ－ｄｉｍｅｎｓｉｏｎａｌｃｏｄｅ′ｓｉｎｆｏｒｍａｔｉｏｎｓｅｃｕｒｉ－ ｔｙ，ａｔｗｏ－ｄｉｍｅｎｓｉｏｎａｌｃｏｄｅｅｎｃｒｙｐｔｉｏｎａｌｇｏｒｉｔｈｍ ｂａｓｅｄｏｎｔｈｅｉｍｐｒｏｖｅｄＡＥＳａｎｄＲＳＡａｌｇｏ－ ｒｉｔｈｍｉｓｐｒｏｐｏｓｅｄｉｎｔｈｉｓｐａｐｅｒ．Ｔｈｅａｌｇｏｒｉｔｈｍ ｅｎｃｒｙｐｔｓｂｅｆｏｒｅ ＱＲ ｃｏｄｅｅｎｃｏｄｉｎｇ，ｗｈｉｃｈ ｍｅａｎｓｉｔｅｎｃｒｙｐｔｓｔｈｅｐｌａｉｎｔｅｘｔｉｎｆｏｒｍａｔｉｏｎ，ｕｓｉｎｇｔｈｅｉｍｐｒｏｖｅｄＡＥＳｓｙｍｍｅｔｒｉｃａｌｅｎｃｒｙｐｔｉｏｎ ａｌｇｏｒｉｔｈｍｔｏｅｎｃｒｙｐｔｔｈｅｐｌａｉｎｔｅｘｔｉｎｆｏｒｍａｔｉｏｎ，ｔｈｅｎｕｓｉｎｇｔｈｅＲＳＡ ａｓｙｍｍｅｔｒｉｃｅｎｃｒｙｐｔｉｏｎ ａｌｇｏｒｉｔｈｍｔｏｅｎｃｒｙｐｔｓｔｈｅｉｍｐｒｏｖｅｄ ＡＥＳａｌｇｏｒｉｔｈｍ′ｓｐａｒａｍｅｔｅｒｓｔｏｇｅｎｅｒａｔｅｔｈｅｐａｒａｍｅｔｅｒ

ｃｉｐｈｅｒｔｅｘｔ．Ｆｉｎａｌｌｙ，ｔｈｅｉｎｆｏｒｍａｔｉｏｎｃｉｐｈｅｒｔｅｘｔａｎｄｔｈｅｐａｒａｍｅｔｅｒｃｉｐｈｅｒｔｅｘｔａｒｅｓｐｌｉｃｅｄｔｏｇｅｎ－ ｅｒａｔｅｔｗｏ－ｄｉｍｅｎｓｉｏｎａｌｃｏｄｅａｎｄｔｒａｎｓｍｉｔｉｔｉｎｔｈｅｎｅｔｗｏｒｋｃｈａｎｎｅｌ．Ｔｈｉｓａｌｇｏｒｉｔｈｍｉｓｃｈａｒａｃ－ ｔｅｒｉｚｅｄｂｙｔｈｅｉｍｐｒｏｖｅｍｅｎｔｏｆｔｈｅｋｅｙｅｘｐａｎｓｉｏｎａｎｄｃｏｌｕｍｎｏｂｆｕｓｃａｔｉｏｎｔｒａｎｓｆｏｒｍａｔｉｏｎｏｆ ＡＥＳａｌｇｏｒｉｔｈｍ，ａｎｄｏｐｔｉｍｉｚｅｄｏｆｔｈｅＲＳＡ ｄｅｃｒｙｐｔｉｏｎａｌｇｏｒｉｔｈｍ ｗｉｔｈｔｈｅＣｈｉｎｅｓｅｒｅｍａｉｎｄｅｒ ｔｈｅｏｒｅｍ，ｗｈｉｃｈｒｅｄｕｃｅｓｔｈｅｒｕｎｎｉｎｇｔｉｍｅｏｆｔｈｅａｌｇｏｒｉｔｈｍａｎｄｉｍｐｒｏｖｅｓｔｈｅａｌｇｏｒｉｔｈｍ′ｓｓｅｃｕ－ ｒｉｔｙ．Ｔｈｉｓａｌｇｏｒｉｔｈｍｉｓｅｆｆｉｃｉｅｎｔａｎｄｅａｓｙｔｏｉｍｐｌｅｍｅｎｔ，ｃｏｍｂｉｎｅｄｗｉｔｈｔｈｅａｄｖａｎｔａｇｅｓｏｆｔｈｅ

＊ 收稿日期：２０１９－０７－０９

基金项目：陕西省科技厅自然科学基础研究计划项目（２０１７ＪＱ１０２６）；陕西省教育厅专项科研计划项目（１７ＪＫ０１０２）

作者简介：刘海峰（１９６４－），男，陕西泾阳人，副教授，硕士生导师，研究方向：计算机网络与信息安全、代数编码与密码学

·１５４·

# 陕西科技大学学报 第３７卷

ｔｗｏａｌｇｏｒｉｔｈｍｓ，ｉｔｃａｎｅｆｆｅｃｔｉｖｅｌｙｍａｎａｇｅｔｈｅｋｅｙａｎｄｐｒｏｔｅｃｔｔｈｅｓｅｃｕｒｉｔｙｏｆｔｈｅｉｎｆｏｒｍａｔｉｏｎ． Ｉｔｈａｓｃｅｒｔａｉｎｇｅｎｅｒａｌｉｚａｔｉｏｎａｎｄｐｒａｃｔｉｃａｌｖａｌｕｅ． Ｋｅｙｗｏｒｄｓ：ｉｍｐｒｏｖｉｎｇＡＥＳ；ＲＳＡｏｐｔｉｍｉｚａｔｉｏｎ；ｂｉｖａｒｉａｔｅｃｏｄｅｅｎｃｒｙｐｔｉｏｎａｌｇｏｒｉｔｈｍ

０ 引 言

二维码作为一种存储、传递和识别信息的技术现已在多个领域得到了广泛的使用，例如物流、交通、电子商务等．但随着二维码在市面上的推广，二 维码的信息泄露危险也日益突出．由于二维码的生 成标准是公开的，且未能在编码过程中实现信息加 密，攻击者可以通过二维码截获到存储和传递的信息，存在着一定安全问题［１］．对于未加密的二维码，任何获得二维码的人进行扫描后均可得到二维码中保存的信息，这对涉及个人隐私敏感信息领域造 成使用上的不便．例如在追溯系统中，产品信息生成的未加密的二维码在传输过程中，若被不法分子 获得，便可进行假冒印刷等一系列违法行为，使用加密后的二维码作为保存、传递产品信息的媒介， 可以起到规范市场，打击假冒的目的．对于二维码信息进行加密，既保证了它的隐私性，也为使用者的个人安全提供了保障．因此，有关二维码的加解密的研究成为一个热点问题．

目前，国内对于二维码信息安全的研究取得了

一些初步进展．２０１４ 年，于 英政等［２］提 出结合了 ＤＥＳ和 ＲＣ４ 加密算法，选取 ＤＥＳ 和 ＲＣ４ 两种算法之一，针对不同阶段的二维码信息进行加密，实现了对二维码分阶段加密；安吉旺等［３］提出对编码信息采用 ＲＳＡ 和ｋｅｙ口令的算法进行二维码混合加密，对明文信息分组加密后，通过ｋｅｙ 口令对分

组明文加密，再使用 ＲＳＡ 算法对ｋｅｙ 口令的密钥

进行加密．在专用的识别软件上，如果输入正确的私钥可解密出相应的明文信息．２０１５ 年，肖 本海等［４］基于 ＳＨＡ５１２ 和 ＡＥＳ 两种算法对二维码信息及其密钥进行了加密，提高了对密文的保护；同年，廖镇勋等［５］提出一种针对二维码的不同阶段，探究其差异并采用不同的方法进行二维码的加密，提高了二维码加密的程度．２０１７年，龙强等［６］提出一种基于非对称密码体制的二维码加密算法，该算法将非对称加密算法 ＲＳＡ 与 Ｌｏｇｉｓｔｉｃ混沌模型相结合，对二维码中信息及密钥进行加密编码，保证了二维码中信息可以在不安全的信道中安全地传输．２０１８年，张华［７］探讨了利用非对称 加密算法加密二维码的可行性和安全性；葛娅敬等［８］提出对二维码图片矩阵进行奇异值分解从而加密得到密文，解密得到 明文，使基于图像处理上的二维码信息安全有了一定进展．杨康等［９］针对不同的信息权限和属性集，生成访问控制树，通过不同用户的属性分配对应的不 同私钥，实现了二维码的分级加密．

综上，当前针对二维码加密的方式分为对生成的二维码图像的加密和对未进行生成二维码之前的初始明文信息的加密．在对二维码信息加密的讨 论中，主要是针对二维码加密算法安全性的讨论， 使用 ＲＳＡ 非对称算法为例的加密算法存在着加密或解密算法时间复杂度高的问题，而使用以 ＤＥＳ 对称算法为例的二维码加密算法，又存在着 ＤＥＳ 超期服役和密钥传输是否安全的问题．

本文提出一种结合改进的 ＡＥＳ 算法和 ＲＳＡ 优化算法的二维码加密算法．本算法在生成二维码之前，对明文信息加密，利用 ＡＥＳ对称密码算法加密效率快和 ＲＳＡ 非对称算法便于密钥管理的优势，基于算法安全性的基础之上实现了对密钥的安全管理．同时通过对两种算法的优化减少加解密消耗的时间，实验证明，该算法提高了二维码加密的效率．

１ 算法理论

１．１ 二维码

二维码，又称二维条码或 ＱＲ Ｃｏｄｅ．在固定好的平面区域，二维码通过散落的黑白相间的图形按一定的规律排序，从而记录数据信息．ＱＲ 码与传统一维条码相比：数据承载量更大；属于纠错编码；可以引入加密体系；编码范围更广．ＱＲ 码的这些特性，决定了其作为载体，在信息时代会有更多的发展空间．

１．２ ＡＥＳ算法

ＡＥＳ 算法是一种新型加密方法，具有更加可靠的加密过程和更加适合的密钥长度．ＡＥＳ 算法包含三大部分：密钥扩展，加密和解密．密钥长度有１２８位、１９２位、２５６位３种．密钥扩展算法的输入是一个４字的密钥，输出是一个４４ 字的一维线性数组．每轮的密钥由种子密钥经过扩展得到．１２８ 位的 ＡＥＳ加解密算法由十轮组成（１９２ 位１２ 轮，２５６ 位 １４轮），每一轮有四个基本步骤：ＢｙｔｅＳｕｂ 变换：用一个Ｓ 盒完成分组中的按字节的代换，ＳｈｉｆｔＲｏｗ变换：一个置换过程，ＭｉｘＣｏｌｕｍｎ 变换：一个利用在ＧＦ （２８ ）上的算术特 性的代换，ＡｄｄＲｏｕｎｄＫｅｙ变换：当前分组按位异或扩展密钥的一部分．解密 算法和加密算法不同，仅仅密钥扩展形式一样，但

对于加密解密中转换顺序是不同的． １．３ ＡＥＳ算法改进

１．３．１ 密钥扩展改进

在传统 ＡＥＳ算法密钥扩展部分，使用初始输

第６期 刘海峰等：一种结合优化后 ＡＥＳ与 ＲＳＡ 算法的二维码加密算法

·１５５·

入的４ 字（１６ 字节）的密钥进行密钥扩展后，得到 ４４个字（１５６字节）组成的扩展密钥数组 Ｗ ＝（ｗ０， ｗ１，…，ｗ４３）．由输入的密钥可直接先得到 Ｗ 的前 ４个字：ｗ０，ｗ１，ｗ２，ｗ３，Ｗ 剩余的字由前一字以及前面第四个字进行如下运算操作得到：当下标数字 不为４的倍数时，直接进行异或操作，否则，先与前 一字进行ｇ变换，再和前第四字进行异或操作，如 图１所示．这种密钥扩展算法面临的主要挑战是攻 击者若是截取到其中一轮密钥，便可通过相应变换 得到剩余所有密钥．

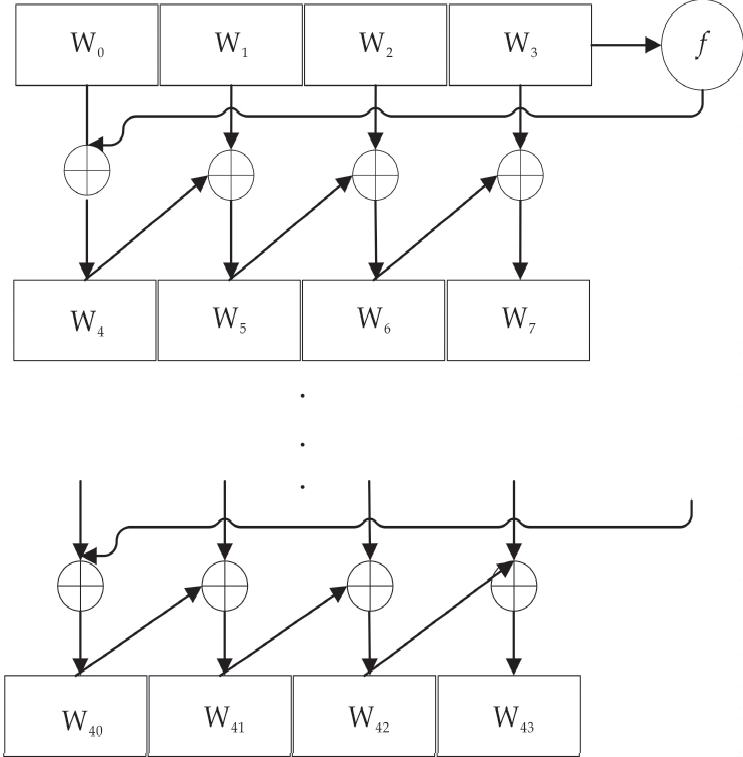


图１ 传统 ＡＥＳ算法密钥扩展过程

文献［１０］提出一种密钥改进算法：在密钥扩展过程中，初始密钥不变，在密钥扩展过程中，使用与初始密钥无关的一套新密钥填充为第一轮扩展密钥，求解剩余密钥则继续使用 ＡＥＳ 密钥扩展算法依据新密钥扩展，最终得到全部密钥．算法原理如图２所示．

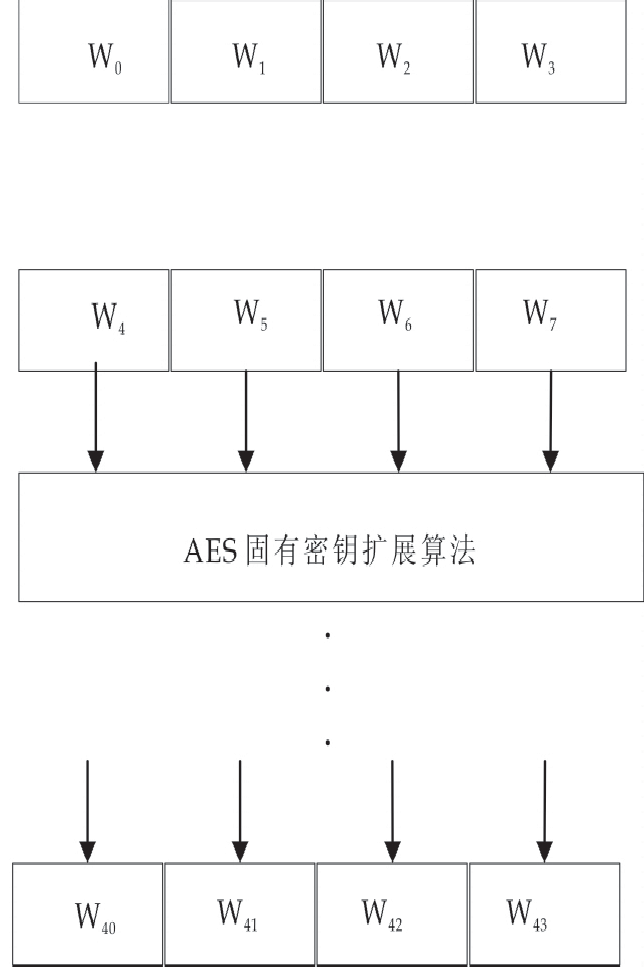


图２ 改进 ＡＥＳ算法密钥扩展过程

由于扩展密钥都是由新密钥通过 ＡＥＳ算法扩展得到的，与初始密钥无关，因此扩展密钥和初始密钥不存在代数关系，对于攻击者来说，截取到任

一轮扩展密钥也无法推出初始密钥，反之，截取到 初始密钥也无法推出扩展密钥．设种子密钥长为ｋ ｂｉｔ，采用穷尽密钥攻击平均复杂度约为２ｋ－１，以１０轮 ＡＥＳ 算法来说，密钥攻击者平均需尝试２１２７ 次可能的密钥，而改进后的密钥扩展算法使平均需尝试２２２５次可能的密钥，以目前的计算能力很难破解．因此该算法在保证与程序效率不变的基础上克服 了程序被截取一轮密钥即可破解全部密钥的漏洞．

在这种密钥扩展改进算法中，若攻击者已知算

法密钥扩展改进过程，又成功截取到初始密钥ｘ０ 和其后由任一轮由新密钥或新密钥扩展得到的密钥，那么攻击者依然可根据密钥扩展过程由任一轮密钥穷尽推出新密钥，进而得到全部密钥．

面对这种挑战，本文提出一种在文献［１０］密钥

扩展算法上的改进算法：初始密钥不变，依照原始密钥扩展算法进行轮密钥扩展，增加随机轮数ｋ（１

＜ｋ≤１０），在随机ｋ 轮时加入新密钥，加入新密钥

后，剩余密钥更改为以新密钥为该轮密钥进行密钥扩展．改进后的算法原理如图３所示．

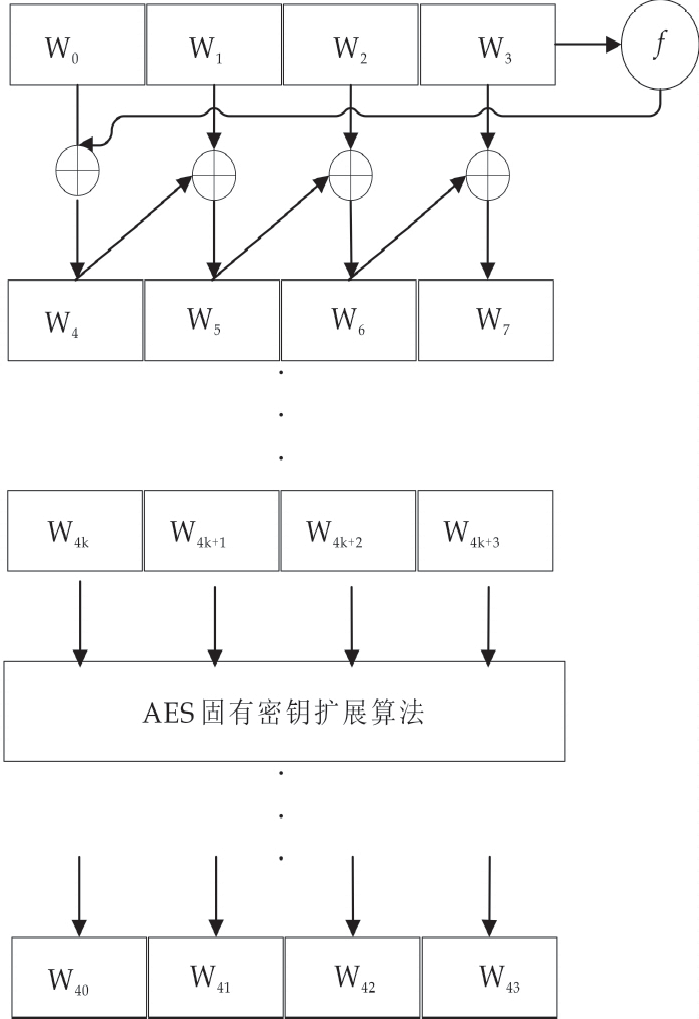


图３ 本文 ＡＥＳ算法密钥扩展过程

对于之前的攻击者，攻击分为以下情况：

（１）攻击者截取到十轮中任两轮密钥，但未知随机轮数ｋ 情况下：① 两轮密钥均由初始密钥或新密钥之一进行密钥扩展而来，由于开始选取的新密钥与初始密钥无关，则攻击者无法推得另一密钥及其扩展密钥，进而无法获得全部密钥；② 两轮密钥分别由初始密钥和新密钥之一密钥扩展而来，则攻击者在未知捕获的两种密钥分别属于新密钥或

初始密钥和未知分别属于两种密钥扩展的哪一轮密钥扩展情况下一共有９０ 种可能的密钥组合，大大增加了破解难度．

（２）若攻击者截取到随机数ｋ 和初始密钥的

·１５６·

# 陕西科技大学学报 第３７卷

情况下，由于不知道新密钥，无法通过计算获得全部密钥．

（３）若攻击者截取到随机数和新密钥，情况和

（２）相似．

１．３．２ 列混淆变换改进

在传统 ＡＥＳ加密算法中，ＭｉｘＣｏｌｕｍｎ 变换即列混淆变换，分为正向列混淆变换和逆向列混淆变 换，提供算法的扩散性．列混淆变换的正向列混淆变化对每列独立地进行操作．每列中每个字节被映射为新值．式（１）表示ＧＦ（２８）上正向列混淆变换，用于数据加密，式（２）表示 ＧＦ （２８ ）上逆向列混淆变换，用于数据解密．

烄Ｓ′ ，烌 烄０２ ０３ ０１ ０１烌烄 烌

０ｊ Ｓ０，ｊ

使用两个密钥的密码算法，具有方便密钥管理和传送的特点．它的基础是大数分解的困难性，它的核心是模幂运算．主要包括两个方面：密钥的产生和加密解密．

ＲＳＡ 密钥的生成过程：

（１）首先选出两个大的素数ｐ 和ｑ，要求ｐ 不能等于ｑ，且ｐ 和ｑ 有一定的差距．

（２）计算出ｎ ＝ｐ＊ｑ．

（３）计算出*Ф*（ｎ）＝ （ｐ －１）＊（ｑ－１）．

（４）选择ｅ，使得 １ ＜ｅ ＜ *Ф*（ｎ），同时ｅ 和

*Ф*（ｎ）要互素．

（５）计算解密密钥参数ｄ 时，要求ｅｄ ＝１ ｍｏｄ

*Ф*（ｎ），可用扩展的欧几里得算法求解．由此得出，

Ｓ１，ｊ

′

Ｓ２，ｊ

′

０１ ０２ ０３ ０１

＝

０１ ０１ ０２ ０３

Ｓ１，ｊ Ｓ２，ｊ

（１）

私钥（ｄ，ｎ），然后公开ｎ 参数，其中ｎ 又被称为模，保密原始素数ｐ 和ｑ．

烆Ｓ３，ｊ烎烄Ｓ０，ｊ烌

′

Ｓ１，

烆０３ ０１ ０１ ０２烎烆Ｓ３，ｊ烎

烄０Ｅ ０Ｂ ０Ｄ ０９烌烄Ｓ０，ｊ烌

′

０９ ０Ｅ ０Ｂ ０Ｄ Ｓ ，

′

其中 （ｅ，ｎ）是公钥，（ｄ，ｎ）是私钥．ｄ 是秘密

的，而ｎ 是公开的．密文的解密者（或系统）将公钥公开，而将密钥和系统参数两个大素数 ｐ、ｑ 藏起

ｊ

Ｓ２，ｊ Ｓ ，

＝

０Ｄ ０９ ０Ｅ ０Ｂ

０Ｂ ０Ｄ ０９ ０Ｅ

１ｊ

Ｓ２，ｊ

′

′

（２）

来．

对于 ＲＳＡ 算法：Ｄ（Ｅ（Ｍ ））＝（Ｍｅ）ｄ ｍｏｄｎ＝

烆 ３ｊ烎 烆 烎烆Ｓ３，ｊ烎

在 ＡＥＳ算法中，加密过程中，列混淆变换需要

（Ｍｄ ）ｅ ｍｏｄｎ ＋Ｅ（Ｄ（Ｍ ）），其中 Ｍ 为明文，加密

公式Ｃ ＝Ｅ（Ｍ ）＝Ｍｅ ｍｏｄｎ，解密公式 Ｍ ＝Ｄ（Ｃ）

执行４次ｘｏｒ加法和２次ｘｔｉｍｅ乘法，而解密过程

中逆列混淆变换需要执行９次ｘｏｒ加法运算和１２次ｘｔｉｍｅ乘法运算［１０］．加密算法和解密算法因列混淆算法不同，导致加解密耗时不对等，解密算法中需要更多的时间来进行运算．

文献［１０］提供了最简单形式的正向列混淆运

算矩阵和逆向列混淆运算矩阵．

烄２ １ ３ １ 烌１ ２ １ ３

＝Ｃｄ ｍｏｄｎ．

１．５ ＲＳＡ 算法优化

由于 ＲＳＡ 算法中模正整数次幂的运算过程复杂，影响算法执行效率，是限制 ＲＳＡ 发展的主要难题．而 ＲＳＡ 算法的解密者拥有保密的系统参数ｐ、ｑ 和私钥，可以在解密过程中利用中国剩余定理进行解密优化，先对中国剩余定理做简单介绍．对于

同余方程组（５）：

Ｍ ＝Ｍ －１ ＝

３ １ ２ １

（３）

烄ｘ ＝ａ１ｍｏｄｍ２

烆１ ３ １ ２ 烎

ｘ ＝ａ２ｍｏｄｍ２

（５）

用 Ｍ 矩阵代替原 ＡＥＳ 算法中正向列混淆和 烅 …

逆向列混淆运算中矩阵，减少了逆向列混淆运算所消耗时间，使正向列混淆运算和逆向列混淆运算消耗相同的运算资源，均为执行４次ｘｏｒ加法和２ 次 ｘｔｉｍｅ乘法，解决了加解密耗时不对等问题．

烆ｘ ＝ａｒｍｏｄｍｒ

若满足：①ｍ１，ｍ２，…，ｍｒ 为两两互素的正整数；②ａ１，ａ２，…，ａｒ 为整数，则同余方程组（５）的模 Ｍ ＝ｍ１，ｍ２，…，ｍｒ 有唯一解（证明过程省略）：

本文对 Ｍ 矩阵进一步改为：

ｒ

ｘ ＝ ａ Ｍ ｙ

ｍｏｄＭ （６）

烄２ ０ ３ ０ 烌

∑ｉ＝１ ｉ ｉ ｉ

其中：Ｍｉ ＝Ｍ／ｍｉ

Ｍ ＝Ｍ －１ ＝ ０ ２ ０ ３

３ ０ ２ ０

烆０ ３ ０ ２ 烎

（４）

ｙｉＭｉ ≡１ ｍｏｄｍｉ，１≤ｉ ≤ｒ

可见，中国剩余定理能够把高位宽大数的模幂

运算转换为低位宽相对较小的模幂运算．下面叙述

这样改进 Ｍ 后，正向列混淆和逆向列混淆均

减少执行２次ｘｏｒ加法运算，加密耗时和解密耗时的共同降低使运算速度得到一定提升，章节４．１ 中的表１ 罗列了对同样数据量加密或解密所用时间的对比．

１．４ ＲＳＡ 算法

ＲＳＡ 是典型的非对称加密算法，它的特点是

运用中国剩余定理改进 ＲＳＡ 解密的方法［１１］．

在ＲＳＡ 算法中，存在两个互素的数ｐ、ｑ，由中国剩余定理，可知求解密方程Ｍ ＝ Ｄ（Ｃ）＝Ｃｄ ｍｏｄｎ的运算，等价于求同余方程组（７），由此，可实现由计算模ｎ 的数量级转化为计算模ｐ 和模ｑ 的数量级．

Ｍ１ ＝Ｃｄ ｍｏｄｐ Ｍ２ ＝Ｃｄ ｍｏｄｑ

｛

（７）

第６期 刘海峰等：一种结合优化后 ＡＥＳ与 ＲＳＡ 算法的二维码加密算法

·１５７·

（费马小定理）ｐ 为素数，ｘ 为满足ｘ（ｍｏｄｐ）

≠０条件的整数，则：ｘｐ－１ ≡１（ｍｏｄｐ）．

由费马小定理，令ｒ＝ｄ（ｍｏｄｐ－１），则存在ｋ满足：ｄ ＝ｋ（ｐ －１）＋ｒ．故：

Ｍ ＝Ｃｄ （ｍｏｄｐ）≡ Ｃｋ（ｐ－１）＋ｒ （ｍｏｄｐ）

１

≡

（Ｃ（ｐ－１） ｍｏｄｐ）ｋＣｒ （ｍｏｄｐ）≡

１ｋＣｒ （ｍｏｄｐ）≡ Ｃｄ ｍｏｄ（ｐ－１）（ｍｏｄｐ）≡

＝（ｄ，ｎ），并反馈给 Ｂｏｂ，将 Ｋ１ 公开，将系统初始化系数传递给接收方Ｂｏｂ．

（２）信息加密

Ａｌｉｃｅ采用改进 ＡＥＳ 加密算法，选定参数 Ｎ

＝（ｘ ，ｙ ，ｚ ）对明文进行加密，即利用改进后的 ＡＥＳ密钥扩展算法，得到 ＡＥＳ 算法全部密钥，再利用全部密钥进行 ＡＥＳ 加密算法得到密文 Ｍ′ ．将

０

０

０

（Ｃ ｍｏｄ

）ｄ ｍｏｄ （ｐ－１）（ｍｏｄ ）

参数信息 Ｎ 用 ＲＳＡ 算法公钥 Ｋ

进行加密生成

ｐ ｐ １

同理，对同余式 Ｍ２ ＝Ｃｄ （ｍｏｄｑ），有：Ｍ２ ＝（Ｃ

Ｎ′ ．

ｍｏｄｑ）ｄ ｍｏｄ （ｑ－１）（ｍｏｄｑ）．令ｄ

１

＝ｄ ｍｏｄ（ｐ －１），

（３）生成二维码

ｄ２ ＝ｄｍｏｄ（ｑ－１）．因此，同余方程组（７）转化为低指数的同余方程组（８）．

Ｍ１ ＝ （Ｃｍｏｄｐ）ｄ１ ｍｏｄｐ

ｄ２｛

（８）

Ｍ２ ＝ （Ｃｍｏｄｑ） ｍｏｄｑ

又由中国剩余定理和费马小定理可知其解：

Ｍ ＝ （（Ｃ ｍｏｄｐ）ｄ１ｑ（ｑ－１ ｍｏｄｐ）＋

（Ｃ ｍｏｄｑ）ｄ２ｐ（ｐ－１ ｍｏｄｑ））ｍｏｄｎ ＝

（（Ｃ ｍｏｄｐ）ｄ１ｑ（ｑｐ－２ｍｏｄｐ）＋

（Ｃ ｍｏｄｑ）ｄ２ｐ（ｐｐ－２ｍｏｄｑ）ｍｏｄｎ ＝

（（Ｃ ｍｏｄｐ）ｄ１ｑ（ｑｐ－２ｍｏｄｎ）＋

（Ｃ ｍｏｄｑ）ｄ２ｐ（ｐｑ－２ ｍｏｄｎ）ｍｏｄｎ ＝

（（Ｃ ｍｏｄｐ）ｄ１ （ｑｐ－１ｍｏｄｎ）＋

（Ｃ ｍｏｄｑ）ｄ２ｐｑ－１ｍｏｄｎ）ｍｏｄｎ

将中国剩余定理应用在 ＲＳＡ 算法解密过程中，远远小于直接进行解密所需指数运算数量级， 而且通过多项式运算代替逆元的求解，进一步减少 运算时间，从而提高运算速度．

根据 ＲＳＡ 的快速 ＭＭＲＣ 解密算法［１２］，步骤 １－５为快速解密算法．运用这种算法共有１ 次逆元， ２次乘法，１次加法，１ 次减法和１ 次ｋ 比特模余， ＲＳＡ 算法解密效率得到进一步提升．计算以下各式：

（１）ｄ１ ←ｄ（ｍｏｄｐ－１）与ｄ２ ←ｄ（ｍｏｄｑ－１）

Ａｌｉｃｅ将明文密文 Ｍ′ 和参数密文Ｎ′ 拼接在一起并进行一系列后续操作即数据分析、数据编码、纠错编码、构造最终信息、生成掩膜和格式与版本 信息等，生成含有加密信息的二维码．

（４）密文解密

接收方Ｂｏｂ 收到二维码信息后，扫描并通过 ＲＳＡ 算法的私钥 Ｋ２ 进行解密得到二维码参数密文 Ｎ ，结合改进后 ＡＥＳ 解密算法进而得到明文信息 Ｍ ．

算法加密流程如图４所示，算法解密流程如图

５所示．

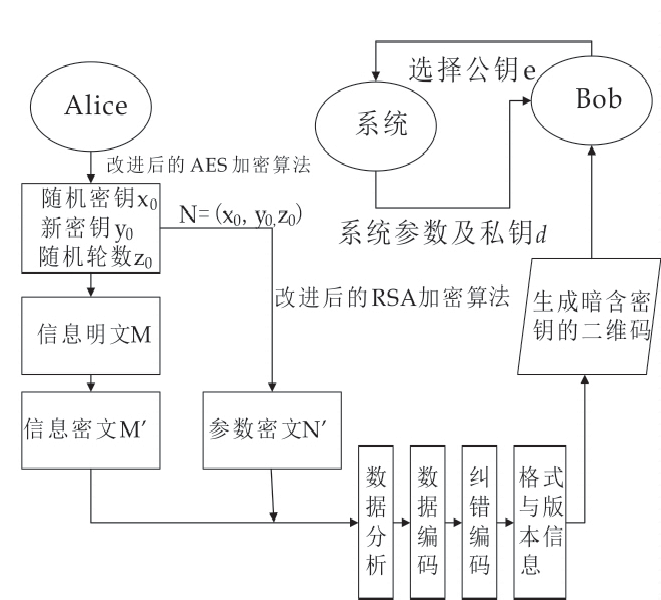
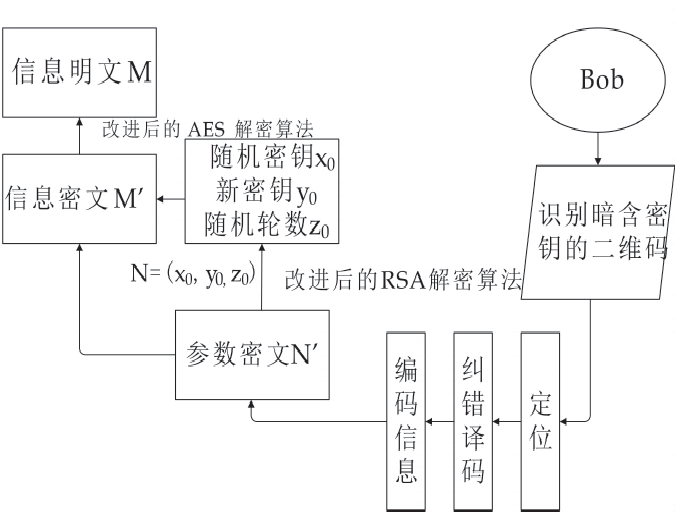


图４ 算法加密流程图

（２）Ｃ１ ← Ｃ（ｍｏｄｐ）与Ｃ２ ← Ｃ（ｍｏｄｑ）

（３）Ｍ１ ←Ｃ ｄ１ （ｍｏｄｐ）与Ｍ２ ←Ｃ ｄ２ （ｍｏｄｑ）

１ １

（４）Ｂ ← ｐ－１（ｍｏｄｐ）

（５）ｍ ← Ｍ１ ＋ ［（Ｍ２ －Ｍ１）＊Ｂ（ｍｏｄｑ）］＊ｐ

\* 结合改进后 ＡＥＳ和改进后ＲＳＡ 的 ＱＲ 加密算法

方案总体思路：采用以改进后的 ＡＥＳ 算法为主、改进后的 ＲＳＡ 算法为辅的加密算法，将改进后ＡＥＳ算法加密结果与改进后 ＲＳＡ 算法加密结果结合作为 ＱＲ 码算法的输入，然后进行二维码编码．不妨设 Ａｌｉｃｅ是二维码的生成方和发送方，Ｂｏｂ是二维码的接收方和验证方，明文为 Ｍ ．算法主要分为以下步骤：

３ 算法实现

图５ 算法解密流程图

（１）系统建立

发送方 Ａｌｉｃｅ选择 ＡＥＳ算法参数随机密钥ｘ０和第一轮密钥ｙ０，系统利用 ＲＳＡ 生成算法及 Ｂｏｂ选择的 ＲＳＡ 公钥 Ｋ１ ＝ （ｅ，ｎ），系统生成私钥 Ｋ２

算法实现基于 ＰｙＣｈａｒｍ 平台，编 程语言为 ｐｙｔｈｏｎ．ＱＲ 二维码的生成识别采用ｚｘｉｎｇ 解析库、 ＰＩＬ，ｐｉｌｌｏｗ 和ｑｒＣｏｄｅ库．

Ａｌｉｃｅ在线传输明文信息给接收方 Ｂｏｂ．Ａｌｉｃｅ

·１５８·

# 陕西科技大学学报 第３７卷

作为二维码生成以及发送方，传输 Ｍ ＝′ｉａｍｇｌａｄ－ ｔｏｓｅｅｙｏｕｓ′作为信息明文，进行测试运行．Ａｌｉｃｅ 选择随机密钥ｘ０ ＝２３４５６７８９１０１１１２１３，新密钥ｙ０ ＝ １５２０２５１２２１５２１１１３，ｚ０ ＝２，加 密之后密文 Ｍ′ ＝ ｃ０５９ｅ８７３ｂ５ａ６０ａ９１０４ｅｆ４９９ｆ９６１ａ３２０Ｂ，Ｂｏｂ选取 ＲＳＡ 算法公钥后，由系统生成１０２４ 位密钥，ＲＳＡ 算法加密ｘ０ 得到ｘ′ ，加密ｙ０ 得到ｙ′ ，加密ｚ０得到ｚ′ ，

０

０

０

表１ 算法加解密时间比较

算法 加密 Ｅｎｃｒｙｐｔ／ｍｓ 解密 Ｄｅｃｒｙｐｔ／ｍｓ ＡＥＳ ０．４０１ ０．４２８

３ＤＥＳ １６．１１５ １６．０６７

ＡＥＳ＋ＲＳＡ ０．９３８ １４．４２５

综合改进 ＡＥＳ

＋ＲＳＡ 优化 ０．８８９ ５．２９７

由表１ 可以看出，由于使 用了 ＲＳＡ 算法对

中间用′／／′分隔．ｘ ′ ＝１２９０６４１６８９８９００５９８３４９６７４ ３５９０４５０２９７３９７０２６０６５４０５９７，ｙ ′ ＝４２５４２０４０４２８６ １７６２７５３８３９８６１３７４９２１３０４７６８２０３０５３８９８９７，ｚ′ ＝ ８，将 Ｍ′ 和 Ｎ′ 用′／／′拼接后进行后续二维码编码．

０

０

０

如图６所示，接收方Ｂｏｂ扫描得到：由 ＡＥＳ算法加密的密文 Ｍ′ ，由 ＲＳＡ 算法加密的 ＡＥＳ 算法初始向量与第一轮密钥密文 Ｎ′ ．首先使用系统建立时的私钥 Ｋ２ 进行 ＲＳＡ 解密，得 到参数明文

（ｘ０，ｙ０，ｚ０）．再利用 ＡＥＳ解密算法和参数 Ｎ 解密由二维码传递的密文Ｍ′ ，最终获得信息明文 Ｍ ＝

′ｉａｍｇｌａｄｔｏｓｅｅｙｏｕｓ′．



图６ 带有密文和参数密文信息的

ＱＲ 二维码图片

４ 算法测试

４．１ 加密速度比较

程序 运 行 环 境 为：Ｗｉｎｄｏｗｓ １０，ＣＰＵ ２．５ ＧＨｚ，ＲＡＭ ４Ｇ．测试软件为 ＰｙＣｈａｒｍ２０１８．１．２．测试采用四种算法对二维码编码前明文加密：

（１）文献［１３］提出的 ＡＥＳ算法．

（２）文献［１４］提出的３ＤＥＳ算法．

（３）数据加密经典传输方案 ＡＥＳ＋ＲＳＡ 算法．

（４）本文提出的结合了改进后的 ＡＥＳ 与 ＲＳＡ优化算法的加密算法．其中３ＤＥＳ 使用３ 个５６ 位的密钥进行加密．ＡＥＳ 密钥长度均采用最广泛的 １２８位，二维码存储明文字符串，四种算法对相同的４８字节的字符串分别进行１０００次加解密，取得加解密的平均时间，算法加密和解密时间测试结果在表１中列出．

ＡＥＳ密钥参数加密，结合 ＡＥＳ 和 ＲＳＡ 的算法比仅使用 ＡＥＳ 算法耗费的时间长，但依然在加密速度上优于３ＤＥＳ 算法，而采用综合改进后的 ＡＥＳ 和 ＲＳＡ 优化算法加、解密消耗时间更少．

４．２ 安全性比较

３ＤＥＳ 算法是 ＤＥＳ 算法的一个安全变形，以ＤＥＳ 为基本模块，通过组合分组方法设计出分组加密算法．目前，针对３ＤＥＳ算法的批评主要有：

（１）３ＤＥＳ易受差分和线性密码分析攻击．

（２）３ＤＥＳ使用６４位的块长度，不能满足大多数数据传输的要求．

（３）用软件实现该算法的速度比较慢．

针对３ＤＥＳ的缺陷［１５］，ＡＥＳ算法得到了解决：

（１）ＡＥＳ 与３ＤＥＳ 相比对差分、截断差分、线性、插值和平方攻击具有很强的抵抗力．

（２）ＡＥＳ 最小密钥长度为１２８ｂｉｔｓ，最大密钥长度为２５６ｂｉｔｓ，目前技术不存在穷举破解的可能．并且 ＡＥＳ算法的密钥长度根据不同加密级别选择不同密钥长度，而分组长度同样可变，设计的灵活 性高．

（３）ＡＥＳ块长度１２８位，是３ＤＥＳ块长度的两倍 ．

（４）ＡＥＳ具有很高的加密效率．

３ＤＥＳ算法和 ＡＥＳ算法两种对称密钥密码体制，密钥的分配均存在严重的缺陷，即若黑客在密钥传输过程中截取到密钥，则密文就不再保密．针对这一缺陷，ＲＳＡ 非对称密码体制使用两个独立的密钥，密钥的分配问题得到了解决．

５ 结 论

本文提出一种结合了改进后的 ＡＥＳ 与 ＲＳＡ 优化算法的 ＱＲ 加密算法．该算法结合两种算法优点，特别是对 ＡＥＳ 密钥扩展和列混淆变换两方面的改进实现了对明文的高效加密、通过 ＲＳＡ 算法仅对参数信息加密，将明文信息加密后的信息密文和参数信息加密后的参数密文拼接生成二维码编码，再传送给接收方．在解密算法中，又对 ＲＳＡ 解密算法使用中国剩余定理进行了优化．该算法相对

第６期 刘海峰等：一种结合优化后 ＡＥＳ与 ＲＳＡ 算法的二维码加密算法

·１５９·

于传统二维码传送信息和密钥而言，其加解密过程兼顾了效率和安全性，安全性能得到提高，加解密时间得到减少．该算法具有一定的推广和实用价值．

参考文献

［１］郑 君，李海霞．基于动态二维码的安全身份认证方案的研究［Ｊ］．湖北理工学院学报，２０１５，３１（２）：３５－３８．

［２］于英政，许宏丽．基于 ＱＲ 二维码的多级融合加密算法的设计与实现［Ｊ］．计算机与数字工程，２０１４，４２（１２）：２３６２－２ ３６４．

［３］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．

［４］肖本 海，郑 莹娜，龙 建明，等．基 于 ＳＨＡ５１２ 哈希函数和 ＡＥＳ加密算法 ＱＲ 二维码信息安全设计［Ｊ］．计算机系统应用，２０１５，２４（７）：１４９－１５４．

［５］廖镇勋，王 珏．基于 ＱＲ 二维码的多重加密算法研究［Ｊ］．电脑知识与技术，２０１５，１１（３０）：６４－６５．

［６］龙 强，刘小华．基于非对称密码体制的二维码加密算法

［Ｊ］．重庆师范大学学报（自然科学版），２０１７，３４（３）：９１－９５．

［７］张 华．基于非对称加密算法的 ＱＲ 二维码［Ｊ］．电子技术与软件工程，２０１８（５）：２９．

［８］葛娅敬，赵礼峰．基于奇异值分解的二维码加密算法［Ｊ］．计算机科学，２０１８，４５（１１Ａ）：３４２－３４３，３６０．

［９］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．

［１０］肖振久，胡 驰，姜正涛．ＡＥＳ与 ＲＳＡ 算法优化及其混合加密体制 ［Ｊ］．计算机应用研 究，２０１４，３１（４）：１ １８９－ １１９４，１１９８．

［１１］叶秀芳．ＲＳＡ 算法的优化策略［Ｊ］．电子设计工程，２０１７，

２５（１０）：８３－８９．

［１２］方文和，李国和，吴卫江，等．面向 Ａｎｄｒｏｉｄ 的 ＲＳＡ 算法优化与二维码加密防伪系统设计［Ｊ］．计算机科学，２０１７， ４４（１）：１７６－１８２．

［１３］周佳华，李福山．基于嵌入式的 ＱＲ 二维码加密系统设计与实现［Ｊ］．信息技术与网络安全，２０１８，３７（２）：３７－３９，５０．

［１４］叶志琼，郑维清，郑 健，等．疫苗 ＱＲ 二维码加密防伪技术［Ｊ］．齐齐哈尔大学学报，２０１５，３１（４）：４１－４４．

［１５］Ｎｏｕｒａ Ａｌｅｉｓａ．Ａ ｃｏｍｐａｒｉｓｏｎｏｆｔｈｅ３ＤＥＳａｎｄ ＡＥＳｅｎ－ ｃｒｙｐｔｉｏｎｓｔａｎｄａｒｄｓ［Ｊ］．ＩｎｔｅｒｎａｔｉｏｎａｌＪｏｕｒｎａｌｏｆＳｅｃｕｒｉｔｙ ａｎｄＩｔｓＡｐｐｌｉｃａｔｉｏｎｓ，２０１５，９（７）：２４０－２４６．

【责任编辑：蒋亚儒】

檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯檯

（上接第１４１页）

（２）通过高温质量流量计及不均匀加热方式模拟出传热设备在实际工程中存在热负荷偏差时，Ｚ型管组支管中流体流量偏差变化机制．通过实验发现，在低质量流速条件下，吸热较强的支管内流体质量流速较高，即吸热管的自补偿特性，通过这一发现，在管组设计时，通过合理的支管布置，可以有效的避免热负荷偏差造成的流量偏差的恶化，提高设备安全运行的能力．

（３）在相同的入口流速、压力及热流密度条件

下，通过采用六头内螺纹管研究管型结构对于 Ｚ 型并联管组支管流体流量偏差的影响规律．通过实验可知六头内螺纹管可以有效的减小支管流量偏差，但无法消除，并且从经济性角度分析，螺纹管结构复杂，造价较高，管内阻力较大，不推荐在支管设计中全部改成内螺纹管．

参考文献

［１］车得福，庄正宁，李 军，等．锅炉［Ｍ］．２ 版．西安：西安交通大学出版社，２００８．

［２］杨 冬，于 辉，高 峰，等．超超临界垂直管圈锅炉水冷壁流量分配及壁温计算［Ｊ］．中国电机工程学报，２００８，２８

（１７）：３２－３８．

［３］朱玉琴，毕勤成，陈听宽．超临界变压运行直流锅炉中间集箱分配特性的试验研究［Ｊ］．热能动力工程，２００９，２４（１）： ８１－８４．

［４］杨 军，朱才广．螺旋管圈直流锅炉水平混合集箱汽水分

配特性的试验研究［Ｊ］．动力工程，１９９３，１３（２）：４３－４７．

［５］Ｊｕｎ Ｋ，Ｙｏｕｎｇ Ｌｅｅ，Ｓａｎｇ Ｙｏｎｇ．Ｄｉｓｔｒｉｂｕｔｉｏｎｏｆｔｗｏ－ｐｈａｓｅ ａｎｎｕｌａｒｆｌｏｗａｔｈｅａｄｅｒ－ｃｈａｎｎｅｌｊｕｎｃｔｉｏｎｓ［Ｊ］．Ｅｘｐｅｒｉｍｅｎｔａｌ ＴｈｅｒｍａｌａｎｄＦｌｕｉｄＳｃｉｅｎｃｅ，２００４，２８（２－３）：２１７－２２２．

［６］ＳｃｈｍｉｄｔＪ，ＧｉｅｓｂｒｅｃｈｔＨ，ＶａｎｄｅｒＧｅｌｄＣ Ｗ．Ｐｈａｓｅａｎｄｖｅ－ ｌｏｃｉｔｙｄｉｓｔｒｉｂｕｔｉｏｎｓｉｎｖｅｒｔｉｃａｌｌｙｕｐｗａｒｄｈｉｇｈｖｉｓｃｏｓｉｔｙｔｗｏ ｐｈａｓｅｆｌｏｗｓ［Ｊ］．ＩｎｔｅｒｎａｔｉｏｎａｌＪｏｕｒｎａｌｏｆＭｕｌｔｉｐｈａｓｅＦｌｏｗ， ２００８，３４（４）：３６３－３７４．

［７］ＩｇｏｒＬＰ，ＲｏｍｎｅｙＢ Ｄ，ＴｙｌｅｒＪＤ．Ｈｙｄｒａｕｌｉｃｒｅｓｉｓｔａｎｃｅｏｆ ｆｌｕｉｄｓｆｌｏｗｉｎｇｉｎｃｈａｎｎｅｌｓａｔｓｕｐｅｒｃｒｉｔｉｃａｌｐｒｅｓｓｕｒｅｓ［Ｊ］．Ｎｕ－ ｃｌｅａｒＥｎｇｉｎｅｅｒｉｎｇａｎｄＤｅｓｉｇｎ，２００４，２３１（２）：１８７－１９７．

［８］ＳａｃｈｉｙｏＨｏｒｉｋｉ，ＴｏｍｏｓｈｉｇｅＮａｋａｍｕｒａ，ＭａｓａｈｉｒｏＯｓａｋａｂｅ． Ｔｈｉｎｆｌｏｗ ｈｅａｄｅｒｔｏｄｉｓｔｒｉｂｕｔｅｆｅｅｄ ｗａｔｅｒｆｏｒｃｏｍａｐａｃｔ ｈｅａｔｅｘｃｈａｎｇｅｒｓ［Ｊ］．ＩｎｔｅｒｎａｔｉｏｎａｌＪｏｕｒｎａｌｏｆ Ｍｕｌｔｉｐｈａｓｅ Ｆｌｏｗ，２００８，３４（２）：１２８－１４４．

【责任编辑：蒋亚儒】