计算机科学
COMPUTER SCIENCE

RSA算法在网络数据传输中的研究进展

王鑫淼, 孙婷婷, 马晶军

引用本文

王鑫淼, 孙婷婷, 马晶军.RSA算法在网络数据传输中的研究进展[J]. 计算机科学, 2023, 50(6A): 220300107-7.

WANG Xinmiao, SUN Tingting, MA Jingjun. Research Progress of RSA Algorithm in Network Data Transmission [J]. Computer Science, 2023, 50(6A): 220300107-7.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220300107

RSA 算法在网络数据传输中的研究进展

王鑫淼　孙婷婷　马晶军
河北农业大学理工学院　河北 沧州 061000
(2823429651@qq.com)

摘　要　人们在利用各种各样的电子设备进行“面对面”信息交流的过程中,双方都不希望自己的信息被第三方获取,由此衍生了通信安全问题。数据安全性不够,数据传输过程就容易受到外界干扰,造成信息重复、缺失、丢包或延迟等现象的产生。针对此问题,广大科研工作者积极应对,引入了密码系统,采用密码算法对数据进行加密,减少其在传输过程中受到的干扰,进而起到保护数据的效果。为了进一步了解密码算法在网络数据传输中的工作原理,文中选取了非对称密码系统中的 RSA 算法作为研究对象,详细介绍了该算法的加密解密过程,对比分析了 RSA 算法和 ECC 算法的优缺点,并针对 RSA 算法的缺陷,总结了相应的优化措施和优化效果。最后,总结了 RSA 算法在网络数据传输中的研究进展和实际运用,并对 RSA 算法的未来进行了展望,期望为数据保护工作提供一些参考依据。

关键词:RSA 算法;密码系统;数据加密;身份验证;数字签名
中图法分类号　TP309

Research Progress of RSA Algorithm in Network Data Transmission

WANG Xinmiao,SUN Tingting and MA Jingjun
College of Science and Technology,Hebei Agricultural University,Cangzhou,Hebei 061000,China

Abstract　In the process of people's “face-to-face” information exchange using various electronic devices,both sides do not want their information to be obtained by the third party,which leads to the problem of communication security. Data security is not enough,the data transmission process is vulnerable to external interference,resulting in information duplication,missing,packet loss or delay. These problems are still not completely avoided. One of the important reasons is that the security of data is not enough,and it is disturbed by the outside world in the transmission process. In response to this problem,the majority of scientific researchers have actively responded,invented data encryption technology and introduced cryptography,which uses cryptographic algorithms to encrypt the data to reduce the interference in the transmission process,thereby protecting the data. In essence,among many technologies that guarantee various functional characteristics of information security,data encryption technology is the core and key technology of information security. Data encryption technology encrypts data from plaintext to ciphertext and communicates through encryption algorithm,and then decrypts the plaintext through corresponding decryption algorithm,which can improve the security of data transmission and ensure the integrity of data transmission. In order to further understand the working principle of cryptographic algorithm in network data transmission,this paper selects the RSA algorithm in asymmetric cryptographic system as the research object,introduces the encryption and decryption process of this algorithm in detail,compares and analyzes the advantages and disadvantages of RSA algorithm and ECC algorithm,and summarizes the corresponding optimization measures and optimization results in view of the defects of RSA algorithm. Finally,the research progress and practical application of RSA algorithm in network data transmission are summarized,and the future of RSA algorithm is prospected,hoping to provide some reference for data protection.

Keywords　RSA algorithm,Cryptosystem,Data encryption,Authentication,Digital signature

当今信息时代,智能手机、电脑等各种电子产品早已遍布世界各地,互联网技术又使各种产品紧密联系在一起,成为一个共同体。不同产品之间通过数据传输进行相互间的通信,在整个通信的过程中,数据的安全是最需要关注的问题之一,一旦安全性过低,传递的信息在传输过程中就可能会被其他人员截获,造成信息泄露[1]。一些不法分子还会利用计算机的漏洞生成病毒,影响计算机功能的正常运行与使用,甚至造成设备瘫痪,使用户数据丢失,严重影响到了人们的生活与工作[1-2]。

《中华人民共和国保守国家秘密法》明确规定:涉及国家秘密的计算机信息系统不得直接或间接与国际互联网或者其他公共信息网络相连,必须实行物理隔离[3]。众所周知,政府、军队和银行的网络都是独立的,这就尽可能地保证了数据的安全。物理隔离在一定程度上解决了信息泄露的问题,但

基金项目:河北省重点研发计划(19220119D)
This work was supported by the Key R&D Program of Hebei Province(19220119D).
通信作者:马晶军(mjjwjpmartin@163.com)

只依靠物理隔离是远远不够的，因为数据在传输链路中也有可能被其他非法人员截获，造成信息泄露[1]。为了防止数据被非法人员获取，就必须对其进行加密，目前一般采用数据加密技术和数字签名技术来保证数据的完整性和不可否认性[4-5]。

1 密码系统

密码系统在网络数据传输中是不可或缺的，在不同领域，人们基于不同的目的使用了不同的密码系统，这些密码系统为我们的生活增加了很多安全性。1976 年，Diffie 等提出了在不安全的通道传输密钥，还不影响系统安全性的方法，实现了在发送端和接收端无密钥传输的保密通信，从而开创了公钥密码学的新纪元[6]。

充分考虑可操作性和安全性后，几乎所有允许远程登录的计算机系统，都需要首先使用密码认证协议来认证通信伙伴的身份，然后才能进行下一步的交互。为了避免系统中发生安全缺陷，1981 年，Lamport 提出了一个用户密钥认证方法[7]，这样即使有入侵者能够读取系统的数据，篡改或窃听用户与系统之间的通信，但系统本身还是安全的，因为他们无法解码。1997 年，Yen 等[8]在 Lamport 的研究基础上，开发了一个用于弱密钥保护的一次性密码系统（使用共享防篡改密码令牌的认证方案），增强了大多数远程登录系统的安全性。2005 年，随着手机银行业的发展，为了提高相应系统的安全性，Lee 等[9]有针对性地设计了一个 DAS4M（移动电话用户动态认证系统）密码系统，它可以防止密码在输入过程中暴露给其他人，与传统的密码系统相比，它存在使用性不便的缺点，但由于安全性能高，得到了很多用户的好评。2006 年，Yang 等[10]成功开发了一个基于口令的身份认证和密钥交换系统，该系统能够消除单点漏洞，避免在 PKI 下使用密码，执行效率高，可以直接用来强化现有的标准单服务器密码应用程序，提高单服务器密码系统的安全性，此系统理论上是符合逻辑的，但在实际应用上需要进行二次处理。

密码系统中必不可少的就是密码算法，人们把密码算法都归属于密码技术。密码技术主要是对数据进行加密，将数据信息中的明文转换成只有机器看得懂的密文，在数据链路上传输的一般都是加密后的密文，到达接收方后再利用密码技术对密文进行解密，从而保证数据安全性[11]。数据安全又分为 3 部分：数据加密、数据传输安全和身份认证管理[12]。

密码技术是数据安全的核心技术，也是所有通信安全的基石。一个密码系统由明文空间、密文空间、密钥空间、加密算法和解密算法五大部分组成[13]。通常，密码系统必须要能实现对数据提供秘密性、可靠性、完整性和不可否认性[13-14]。

密码技术主要分为两大类：对称密码技术和非对称密码技术。对称密码技术指发送方在对数据加密时和接收方对加密的数据进行解密时使用同一种密钥，但正由于加、解密使用的是同一种密钥，所以安全性较低；非对称加密技术又被称为公钥加密技术，它使用两种密钥，即公钥和私钥，公钥用于加密，私钥用于解密，其安全性明显高于对称密码技术，是当下的主流密码技术之一[15-16]。目前比较流行的公钥密码体系主要有两类[17]：一类是基于大整数因子分解问题，其中最典型的就是 RSA 算法，这也是本文将要总结分析的算法；另一类是基于离散对数问题，例如椭圆曲线 ECC 算法，本文将在 2.4 节分析对比 RSA 与 ECC 算法的性能。

2 RSA 算法

2.1 算法原理

RSA 算法的首次出现是在 1977 年，由美国麻省理工学院的 Ron Rivest，Adi Shamir 和 Leonard Adleman 三人共同提出，于 1978 年正式发表，“RSA”的名称就是由他们三人的姓氏首字母组成的[18]。

图 1 给出了 RSA 算法对数据和消息的处理过程。由接收方先生成 RSA 密钥对（RSA 公钥和私钥），RSA 公钥通过因特网交给发送方用来加密，私钥用来解密，明文也就是数据或信息，明文在加密之前需要进行数字化处理，即编码处理，然后再利用 RSA 算法进行加密形成密文，在解密后，需要进行解码处理，才能得到明文[15]。

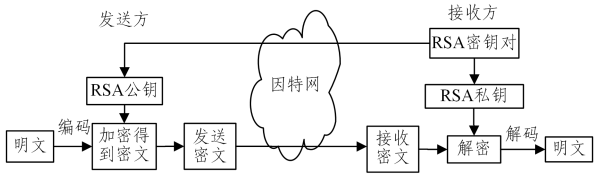

图 1 RSA 算法对数据和消息的处理过程

Fig. 1 RSA algorithm for data and message processing

RSA 算法中涉及数论中的质数、模运算、最大公约数的求解（欧几里得算法）以及欧拉定理和单向函数[19-20]，整个算法的安全性依赖于寻找整数因子分解问题的难易性。到目前为止，密码界还没有找到一个有效的算法来分解两个大素数的积[21]。一般可将 RSA 算法分为密钥对的产生以及对消息的加解密两个部分[22]，其中密钥对的产生中包含大素数的生成。

2.2 密钥的生成

（1）接收方随机选择两个大素数 p 和 q，素数的位数越大，就越不容易被分解，安全性越高；

（2）计算大素数的积 $n=p*q$，n 通常是 1 024 位，计算欧拉函数 $\phi(n)=(p-1)*(q-1)$；

（3）任选一个数 e，使其满足 $gcd(\phi(n),e)=1$，即 $\phi(n)$ 和 e 的最大公约数为 1，即让 e 和 $\phi(n)$ 互质，并且 $1<e<\phi(n)$，这里可以使用欧几里得算法；

（4）计算 d，使 $e*d\equiv 1 \bmod \phi(n)$，即 e 和 d 的积与 1 关于模 $\phi(n)$ 同余，进一步化简为 $e*d\%\phi(n)=1$；

（5）至此，可得到公钥为 (n,e)，私钥为 (n,d)，整个密钥生成流程如图 2 所示[18,23]。

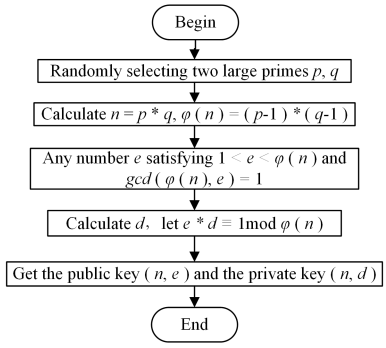

图 2 RSA 密钥的生成过程

Fig. 2 Generation process of RSA key

2.3 加密和解密过程

2.3.1 加密过程

利用公钥(n,e)对数据进行加密,使用公式 $C=m^e \bmod n$,其中 C 为密文,m 为明文经过编码后的内容。在对数据加密时,RSA 对数据的长度是有一定要求的,过长会导致无法加密,为了防止这种情况出现,一般都将数据进行分组,每一组的长度不超过密钥长度[23]。

2.3.2 解密过程

利用私钥(n,d)对密文进行解密,使用公式 $m=C^d \bmod n$,得到 m,之后再对 m 进行解码,就能得到相应的明文[18-19]。

2.4 RSA 算法和 ECC 算法

2.4.1 RSA 算法的优点

RSA 算法是在网络数据传输中使用比较广泛的一个密码算法,由于它在加密过程使用了两个不同的密钥,而不是像对称密码算法那样只使用一个密钥,因此它大大地提高了数据在传输过程中的安全性,实现了数据的不可否认性[24]。相比对称密码算法,RSA 算法将公钥公开,将私钥保密,并且私钥不通过互联网传送,只需要接收方自留,减少了密钥在网络中泄露的风险;而对称算法中,通信双方需要协商加密密钥,并且需要使用一个秘密通道,效率低,且一旦密钥被泄露,通信就会不安全。

2.4.2 RSA 算法的缺陷

鉴于 RSA 算法的生成原理,为了让数据的安全性更强,在密钥的产生过程中,就要使素数的位数尽可能地大。而素数的位数变大将导致密钥的复杂度与计算量增加,算法的加密速度变慢,此方面 RSA 算法与对称密码算法无法相提并论[15,25]。2017 年,Kumar 等[26]通过比较 RSA 算法(非对称密码算法)和 AES 算法(对称密码算法)的编译时间,证明了这一点,他们的结论是对于给定的数据集,AES 算法在加密和解密方面的速度更快。

RSA 算法的安全性是基于两个大素数的积不易分解。2009 年,Aboud 针对此特性提出了一种在已知公钥的情况下攻击 RSA 算法的方法[27]。该方法通过获取 RSA 的私钥,然后根据 RSA 算法的公钥对模数进行分解,通过多次运行该方法得出运行时间,并取其平均值与已经存在的攻击算法进行对比,发现此方法的运行时间更短,速度更快、更有效。

RSA 算法的另一个不足之处就是缺乏容错支持。由于要进行大规模的计算和高速的数据传输,故障是不可避免的,很显然,若没有容错支持,在计算或数据传输中发生的任何错误都将导致整个算法失败[28]。

2.4.3 ECC 算法的优缺点

与 RSA 算法相比,ECC 算法具有更好的潜能,它可以用较小的开销实现较高的安全性,具体如下[29]。

(1)在安全等级相同的情况下,RSA 算法需要的模长为 1 024 位,而 ECC 算法仅需 160 位。ECC 算法的密钥对长度远远短于 RSA 算法,并且当密钥长度增加时,ECC 的安全性会增加地更快。

(2)ECC 算法计算速度快,开销小。ECC 算法密钥的生成没有 RSA 算法那么复杂,它可以在很短的时间内生成对应的密钥。

(3)其安全性是基于椭圆曲线点群上离散对数问题的难解性,但此算法中的椭圆曲线中有两种特殊曲线,即超奇异椭圆曲线和异常曲线,这两种曲线的离散对数问题较简单,因此容易遭到特定算法的攻击。在安全性能相同的情况下这两种算法的性能对比如表 1 所列。

表 1 在安全性能相同的情况下 RSA 算法与 ECC 算法的性能对比

Table 1 Performance comparison between RSA and ECC algorithms under the same security performance

算法	密钥长度	计算速度	计算复杂度	存储需求
RSA	大	慢	高	大
ECC	小	快	低	小

3 RSA 算法的优化和应用

3.1 RSA 算法的优化研究

为了克服 RSA 算法本身的不足,同时加强数据在传输过程中的安全性,人们尝试对 RSA 算法进行优化改进。下面详细介绍了几种改进后的 RSA 算法。

传统的 RSA 算法使用的密钥太大,对设备的内存存储要求较高,导致其不适用于无线通信设备或小型设备。1995 年,Vanstone 等[30]提出了几种构造两个素数乘积的方法,试图在不影响安全性的前提下,降低 RSA 公共模块的存储需求,但研究中发现,若构造方法不当,会使密钥的生成时间变得更长。2020 年,Yu 等[31]利用真素数随机数发生器(TPRNG)生成无法通过生物信号预测的素数,这种方法生成的素数不易被分解,并且该方法使用“一次性”加密密钥来减少停留在内存中的密钥数量,具体来说,当从密钥生成到解密完成的所有步骤完成后,素数、公钥和私钥立即被销毁,然后重新生成,而不是不断地将密钥保存在内存中。使用该方法改进的 RSA 算法由于使用的密钥极小,容易受到攻击,但如果在加密过程中使用一个不可预料的随机数来不断改变密钥,那么就能够以此来补偿加密密钥极小的问题,这种算法适用于多对多通信的物联网设备领域,但还无法满足需要极高级别加密的环境。

2012 年,为了提高计算速度,Bhaskar 等[32]使用吠陀乘法器和改进的恢复除法算法对 RSA 算法进行优化。与优化前相比,优化后省略了移位操作,从而节省了加密时间。2017 年,Qiu 等[33]完全分离了两个大素数的乘法和所得乘积模 N 的减法,也就是本文中密钥的生成部分的步骤 2。对于乘法,通过 Karatsuba 方法[34]将两个 n 字节操作数乘法分成 3 个 $n/2$ 字节数的乘法,然后使用优化的多精度乘法得到 $n/2$ 字节乘法的乘积,最后利用蒙哥马利归约获得结果。在模幂运算中使用 m 元取幂和多精度乘法,有些情况下还利用中国剩余定理来提高模乘法和模幂运算的效率。该方法通过更改数学运算方法,进一步减少了算法的加密时间,进而提高了算法的加密效率。

2016 年,为了进一步增强算法安全性,Pranesh 等通过重新排列原始数据中元素的位置,将重新排列后的数据分为两段,然后将两段合并,从而生成修改后的数据[35]。例如原始数据为 12345,修改后的数据为 13 524,将修改后的数据作为 RSA 算法的输入数据,进行加密。这种方法为传输的数据提供了更好的安全性。

RSA 算法加密速度慢,计算复杂度高,而且由于要选择两个大素数,因此整个因式分解过程相当困难。2017 年,为了降低计算复杂度,Chaudhury 等尝试将两个大素数更改为 4

个小素数，对比测试后结果显示改进后的 RSA 算法在内存消耗和计算速度方面均优于原始的 RSA 算法[36]。2019 年，Thiziers 等[37]在上述研究结果的基础上将 4 个小素数优化为 n 个素数，同时采用了三重加密-解密技术，使优化后的 RSA 算法更安全，但这种安全性的提高是以牺牲加密时间为代价的。

随着数据传输技术的发展，针对图像信息的处理迎来了机遇与挑战。与文本数据相比，图像数据具有许多特殊的特征和特性，如相邻像素间的相关性强、冗余度高和数据量大等。面对变大的数据量，RSA 算法的计算复杂度和算法速度都会受到消极影响。针对此问题，2019 年，Zhu 等[38]将读取到的图像数据传输到数字矩阵 $\boldsymbol{M}$ 中，然后对 $\boldsymbol{M}$ 进行奇异值分解(Singular Value Decomposition)，再对对角矩阵中的对角元素使用 RSA 算法进行加密，将要加密的数据从二维降到一维，减少了加密数据的数量。

2021 年，Zhang 小组根据字符的特征(词性、位置、频率、关联度等)，计算出每个字符的得分，提取出关键字符，然后利用 DES 算法和 RSA 算法组成的一种混合加密算法，对关键字符进行加密[39]。这种方法解决了字符型数据加密传输中的延迟、速率慢、丢包等问题，实现了加密性能和传输性能的共赢。在这种方法中，明文数据使用 DES 算法加密，RSA 算法则用于加密 DES 密钥。表 2 列出了各个优化后的 RSA 算法。

表 2 对 RSA 算法的优化方法

Table 2 Optimization of RSA algorithm

序号	针对问题	改进措施	效果	不足	文献
1	算法使用密钥大，对存储需求要求高	更改构造两个素数乘积的方法	降低了 RSA 公共模块的存储需求	构造方法不当时，会使密钥生成时间更长	[30]
2		使用一次性加密密钥，用真素数随机数发生器(TPRNG)生成素数	密钥极小，适用于使用多对多通信的物联网设备	可能不足以满足需要极高级别加密的环境	[31]
3	算法计算速度较慢，加密效率低	使用吠陀乘法器和改进的恢复除法计算部分乘积	省略了移位操作，节省了时间和硬件，提高了计算速度	—	[32]
4		更改 RSA 算法中的数学运算方法	减少了计算量，提高了计算速度，在嵌入式设备上实现了 RSA 算法	—	[33]
5	算法安全性不够	重新排列原始数据的元素位置	为传输的数据提供了更高级别的安全性	并没有解决 RSA 密钥生成复杂的问题	[35]
6	算法计算复杂度高	将原始算法中使用的两个大素数换成 4 个小素数	降低了计算复杂度，减少了内存需求和消耗	—	[36]
7		使用了 n 个素数和三重加密-解密	素数更难以分解，增加了安全性	密钥生成时间与加解密时间更长，算法复杂性更大	[37]
8	对于加密数据的数据量较大时，不适用于 RSA 算法	提取图像数据，对其进行奇异值分解，再对部分数据加密	需要加密的数据从二维到一维，大大减少了加密数据的数量，提高了加密速度	—	[38]
9		提取关键字符，对关键字符加密	解决了字符型数据加密传输中延迟、速率慢、丢包等问题，实现了加密性能和传输性能的共赢	—	[39]

3.2 加密密钥

为了获取更好的安全性，RSA 算法通常与其他算法混合使用。

隐写术是另一种密码技术，一些科研团队将 RSA 算法和隐写术结合使用[40-42]，以达到提高网络数据传输安全性的目的。2015 年，Sundari 团队[40]同时使用数字水印技术、隐写术和 RSA 算法 3 种技术来进行加密工作，具体做法是：首先将封面图像采用 JPEG 压缩算法进行压缩，同时使用改进的 RSA 算法对发送的消息进行加密，然后将加密后的消息位和水印图像的位嵌入到压缩后的封面图像中。2016 年，Ramaiya 等[41]成功将原始图像的每个像素的强度从二进制值转换为十进制值，然后对每一个像素值使用 RSA 算法进行加密，得到加密图像，再使用隐写术将加密图像隐藏到载体图像中进行数据传输；2017 年，Bangera 等[42]进行了类似的研究工作，他们将加密处理后的音频数据隐藏到载体音频中进行数据传输。

2016 年，Jiang 团队[43]将 RSA 算法与对称密码算法 DES 算法相结合，因为 DES 加密的速度比 RSA 快很多，所以加密过程采用 DES 算法，RSA 算法用于对 DES 算法密钥的加解密。改进后的混合密码算法不仅增大了系统安全系数，而且提高了数据传输速度。

2017 年，Timothy 团队[44]开发了一个由 RSA 算法和对称密码算法 Blowfish 算法组成的混合密码算法。该算法的加密过程为，选择一个 448 位到 1024 位可变长度范围内的密钥 K；在密钥的帮助下应用 Blowfish 算法对所选文件 f 进行加密；使用 RSA 算法加密密钥 K。解密时应用 RSA 解密算法对加密的密钥进行解密；使用解密后的密钥，通过对加密文件应用 blowfish 解密算法，获得原始文件。

3.3 数字签名和身份验证

在网络数据传输的大部分节点上，基本都需要进行身份验证工作，以确保数据的正确性以及完整性[45]。当进行身份验证时，RSA 算法是一个明确的选择[46]。此外，RSA 算法还可应用于数字签名，一般将 RSA 中的私钥用于生成签名，公钥用于验证签名[47]。其生成签名的主要步骤为：输入消息，查找消息摘要并进行函数处理，得到一个整数 $H(msg)$，使用

私钥 d 和公式 $s=[H(msg)]^d \bmod n$ 生成签名，发送数字签名；验证签名，输入发送者的公钥和消息，使用公钥 e 和公式 $v=s^e \bmod n$ 计算信息摘要 v，比较 v 与 $H(msg)$，只有当 v 与 $H(msg)$ 匹配时，签名才有效。

当实体使用其私钥加密消息时，每个知道相应公钥的实体都可以对其进行解密。这样，实体身份验证就发生了，因为使用某个公钥解密的加密数据肯定来自拥有相关私钥的实体[48-49]。

此外，RSA 算法可以在无线传输过程中提供数据包完整性信息，签名算法用于验证信息完整性。可采用 RSA 签名算法，通过填充和加密无线网络中的数据包来完成[50]。每个没有匹配对应签名的控制消息都会被丢弃。

3.4 不同协议下 RSA 算法的应用

为了使 RSA 算法适用于不同网络传输环境，得到更广泛的应用，一些科研工作者提议签订几种基于 RSA 算法的协议。表 3 列出了几种协议的适用环境以及效果。

表 3 不同协议的适用环境和效果

Table 3 Application environment and effect of different agreements

序号	协议名称	适用环境	效果	文献
1	基于 RSA 的密码认证交换(RSA-EKE)协议	非平衡网络(由一组强大的服务器和一组低功耗客户端组成)	足以在大多数低功耗设备上实现，尽可能地降低了客户端的计算复杂度	[51]
2	RSA 握手数据库协议	所有网络网关	提高了 RSA 算法的速度	[52]
3	4G 环境安全系统(Se4GE)	4G 环境下的无线通信	增强了密钥交换的安全性，减少了密钥交换处理时间，提高了数据传输的安全级别，不会造成较长的传输延迟以及恶化数据传输质量	[25]
4	安全密钥传输 RSA(SKT-RSA)协议	用于集中云环境中安全密钥传输	保证了通信的安全可靠，密钥的计算量以及计算时间都大大减少	[53]

2002 年，Zhu 等设计了用于非平衡(非对称)网络的 RSA 的密码认证交换(RSA-EKE)协议[51]，该协议充分考虑了非平衡网络是由一组强大的服务器和一组低功耗客户端组成的。该协议的效率足以在大多数通信目标为低功耗的设备上实现，尽可能地降低了客户端的计算复杂度。

2012 年，Nagar 等为了解决不同通信网络之间数据传输过程中 RSA 算法实现的问题，提出了 RSA 握手数据库协议[52]。此协议负责在所有网络网关中创建相同的 RSA-Key Generations 离线数据库，并在需要时及时进行数据库的更新。其处理思路就是通过离线生成 RSA 密钥对并将其存储在不同的数据库中，来提高 RSA 算法的速度。

2014 年，Huang 等提出了 4G 环境安全系统(Se4GE)，这是一个基于 LTE-A(Long Term Evolution-Advance，属于 4G 系统)的系统，并集成了 RSA 和 Diffie-Hellman 算法来解决一些 LTE-A 的安全缺陷[25]。Se4GE 是一种端到端的密文传输机制，它动态地更改加密密钥以加强 LTE-A 系统中数据传输的安全性。在该系统中，使用 RSA 算法设置了 RSA 三重密钥，密钥安全性更高。它可以有效且高效地提供隐私保护，减少密钥交换处理时间，提高数据传输的安全级别，同时不会造成较长的传输延迟以及恶化数据传输质量。

2020 年，Ambika 等提出了安全密钥传输 RSA(SKT-RSA)协议[53]，它是一种基于树的集群密钥分发方案。为了保证在认证机构和用户之间分配密钥的安全性，他们用 RSA 算法加密了特定用户在特定时间加入的密钥，并将其发送给请求加入组的用户，用户使用密码密钥和私钥解密加密后的密钥，获得密钥值。此协议不仅保证了通信的安全可靠，而且使密钥的计算时间和计算量都大大减少。

3.5 RSA 算法的实际应用

2018 年，Zhu 等将 RSA 算法应用到智能门锁设备中[54]，并提供了一套能使系统完整运行的硬件模型，在此设备中，RSA 算法主要用于在钥匙共享时防止密码泄露。

同年，Lu 等针对现有的 RSA 硬件系统中存在运算量比较大、加解密运算速度较慢和硬件实现的面积较大的问题，发明了一种基于 RSA 密码算法的加解密硬件系统[55]，并申请了专利。此系统包括 RSA 主控模块、密钥产生模块、加密控制模块、解密控制模块、模幂运算模块、模乘运算模块和大数乘法器模块，该硬件系统可以减少 RSA 加解密过程中的运算量，提高 RSA 加解密的速度和降低芯片的面积。

总体来说，RSA 算法在实际生活中的应用很少，更多的是对 RSA 算法的改进方法的专利，期待将来该算法在生活中的应用越来越多。

结束语 RSA 算法属于非对称密码算法中使用比较广泛的一种算法，它既可用于数据加密，也可用作数字签名和身份验证。该算法具有许多对称密码算法所没有的优点，能提供更高的安全性，保证了数据的可靠性、完整性和不可否认性。但同时 RSA 算法也存在计算复杂度高、加密时间长、存储空间大等缺点。科研人员针对该问题进行了研究，现在已开发出了一些基于 RSA 算法的改进算法。在 RSA 算法的实际应用中，大多数都是将 RSA 算法和其他加密算法混合使用，尽量避免 RSA 算法的局限性。在未来的应用中，应尽最大程度地发挥 RSA 算法的优势，使其更安全、更快速、更便捷。

虽然 ECC 算法相比 RSA 算法的优势更多，但 ECC 算法的使用和研究成果都相对较少，ECC 算法值得更进一步的研究，以用来更好地提高系统安全性。

参 考 文 献

[1] GONG L，ZHANG L，ZHANG W，et al. The application of data encryption technology in computer network communication security[C]// AIP Conference Proceedings. New York：American Institute of Physics，2017.

[2] XIE X M. Establishment and Technical Analysis of Computer Network Information Security Protection Mode[J]. Science and Technology Innovation，2019(7)：66-67.

[3] 《Law of the people's Republic of China on Guarding State secrets》[Z]. Beijing, 2010. 10.

[4] LIU S S, WANG P, LUO L, et al. Security Module in Information Unilateral Transmission System among Networks[C]// AASRI Procedia, NETHERLANDS: ELSEVIER SCIENCE BV. 2012: 100-105.

[5] ZHAO Y B, ZHANG X J, JIANG Y L. Application Research of High Strength File Encryption Based on Digital Envelope[J]. Computer Engineering and Design, 2007(18): 4357-4359.

[6] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE transactions on Information Theory, 1976, 22(6): 644-654.

[7] LAMPORT L. Password authentication with insecure communication[J]. Communications of the ACM, 1981, 24(11): 770-772.

[8] YEN S M, LIAO K H. Shared authentication token secure against replay and weak key attacks[J], Information Processing Letters, 1997, 62(2): 77-80.

[9] LEE S, PARK S. Mobile Password System for Enhancing Usability-Guaranteed Security in Mobile Phone Banking[J]. Web and Communication Technologies and Internet-Related Social Issues-HSI 2005, 2005, 3597: 66-74.

[10] YANG Y J, DENG R H, BAO F. A practical password-based two-server authentication and key exchange system[J]. IEEE Transactions on Dependable and Secure Computing, 2006, 3(2): 105-114.

[11] LIU J Z. Internet / INTRANET Security Technology[J]. Software and Integrated Circuit, 1997(1): 16-20.

[12] LIN X F, FUN M F. Data Security in Network Transmission [J]. Software Guide, 2012, 11(1): 139-141.

[13] ZHAO G P. Cryptography Technology in Network Data Transmission Security[J]. Information and Computer(theoretical edition), 2010(20): 19.

[14] HUANG Y, HU W D, CHEN K F. Classification of Network Attack and Security Protection[J]. Computer Engineering, 2001(5): 131-133, 140.

[15] XU C. The Application of AES and RSA Hybrid Encryption Technology in Network Data Transmission[J]. Wireless Interconnection Technology, 2016(13): 142-144.

[16] XU S S, ZHU X M, BAI L F, et al. Application of Attribute-based Cryptosystem in Network Security Level Protection[C]// Papers of the Seventh National Security Level Protection Technology Congress 2018. 2018: 159-164.

[17] HUANG H M. Data Encryption Technology and Its Application in Network Security Transmission[D]. Xiamen: Xiamen University, 2008.

[18] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.

[19] HU J. Research and Implementation of RSA Encryption Algorithm[M]. Maanshan: Anhui University of Technology, 2011: 1-48.

[20] SONG Y. Research and Application of Encryption Communication Based on RSA Algorithm[J]. Electronic Test, 2021(16): 33-36, 138.

[21] ARTO S. Public Key Cryptography[M]. Beijing: National Defense Industry Press, 1998.

[22] LU J Y. Research on Data Transmission Security Technology Based on Web Network[D]. Nanjing: Nanjing University of Technology, 2009: 1-67.

[23] TIAN W Y, LI Z M. Research and Implementation of RSA Encryption Algorithm and Its Improved Algorithm[J]. Shanxi Electronic Technology, 2013(6): 90-92.

[24] LIU W, ZHU M R, LIU Y L. Data Encryption Transmission in Remote Fault Diagnosis System[J]. Network Security Technology & Application, 2008(1): 83-84, 21.

[25] HUANG Y L, LEU F Y, YOU I, et al. A secure wireless communication system integrating RSA, Diffie-Hellman PKDS, intelligent protection-key chains and a Data Connection Core in a 4G environment[J]. Journal of Supercomputing, 2014, 67(3): 635-652.

[26] KUMAR B J S, RAJ V K R, NAIR A. Comparative study on AES and RSA algorithm for medical images[C]// 2017 International Conference on Communication and Signal Processing (ICCSP). New York: IEEE Press, 2017: 501-504.

[27] ABOUD S J. An efficient method for attack RSA scheme[C]// 2009 Second International Conference on the Applications of Digital Information and Web Technologies. New York: IEEE Press, 2009: 587-591.

[28] ZHANG C N. Integrated approach for fault tolerance and digital signature in RSA[J]. IEE Proceedings-Computers and Digital Techniques, 1999, 146(3): 151-159.

[29] ZHANG Y F, QIN Z G, LIU J D. Performance Analysis of Elliptic Curve Encryption System[J]. Journal of University of Electronic Science and Technology of China, 2001(2): 144-147.

[30] VANSTONE S A, ZUCCHERATO R J. Short RSA keys and their generation[J]. Journal of Cryptology, 1995, 8(2): 101-114.

[31] YU H, KIM Y. New RSA Encryption Mechanism Using One-Time Encryption Keys and Unpredictable Bio-Signal for Wireless Communication Devices[J]. Electronics, 2020, 9(2): 246.

[32] BHASKAR R, HEGDE G, VAYA P R. An efficient hardware model for RSA Encryption system using Vedic mathematics [C]// International Conference on Communication Technology and System Design 2011. NETHERLANDS: ELSEVIER SCIENCE BV, 2012: 124-128.

[33] QIU L, LIU Z, PEREIRA G C C F, et al. Implementing RSA for sensor nodes in smart cities[J]. Personal and Ubiquitous Computing, 2017, 21(5): 807-813.

[34] KARATSUBA A, OFMAN Y U. Multiplication of multidigit numbers on automata[J]. Soviet physics doklady, 1963, 7: 595-596.

[35] PRANESH R, HARISH V, VIGNESHWARAN M, et al. A new approach for secure data transmission[C]// Proceedings of IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT 2016). New York: IEEE Press, 2016: 1-4.

[36] CHAUDHURY P, DHANG S, ROY M, et al. ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm[C]// 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON). New York: IEEE Press, 2017: 332-337.

[37] THIZIERS A H, THÉODORE H C, ZOUEU J T, et al. En-

hanced, Modified and Secured RSA Cryptosystem based on n Prime Numbers and Offline Storage for Medical Data Transmission via Mobile Phone[J]. International Journal of Advanced Computer Science and Applications(IJACSA), 2019, 10(10): 353-360.

[38] ZHU K, LIN Z, DING Y. A new RSA image encryption algorithm based on singular value decomposition[J]. International Journal of Pattern Recognition and Artificial Intelligence, 2019, 33(1): 1954002.

[39] ZHANG Y Z. Multi-character Sorting Encryption Transmission Method for Wireless Local Area Network Data[J]. Automation & Instrumentation, 2021(6): 35-38, 42.

[40] SUNDARI M, REVATHI P B, SUMESH S. Secure Communication Using Digital Watermarking with Encrypted Text Hidden in an Image[C]// Security in Computing and Communications (SSCC 2015). Berlin: Springer, 2015: 247-255.

[41] RAMAIYA M K, HEMRAJANI N. Improvisation of Security aspect of Steganographic System by applying RSA Algorithm [J]. International Journal of Advanced Computer Science and Applications, 2016, 7(7): 245-249.

[42] BANGERA K N, REDDY N V S, PADDAMBAIL Y, et al. Multilayer security using RSA cryptography and dual audio steganography[C]// 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology(RTEICT). New York: IEEE Press, 2017: 492-495.

[43] JIANG W B, XU H, DONG H, et al. An improved security framework for Web service-based resources[J]. Turkish Journal of Electrical Engineering & Computer Sciences, 2016, 24(3): 774-792.

[44] TIMOTHY D P, SANTRA A K. A hybrid cryptography algorithm for cloud computing security[C]// 2017 International conference on Microelectronic Devices, Circuits and Systems(ICMDCS). New York: IEEE Press, 2017: 1-5.

[45] FOTOHI R, BARI S F, YUSEFI M. Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol[J]. International Journal of Communication Systems, 2020, 33(4): e4234.

[46] PARMAR N J, VERMA P K, MARTIN V. A Comparative Evaluation of Algorithms in the Implementation of an Ultra-Secure Router-to-Router Key Exchange System[J]. Security and Communication Networks, 2017, 2017: 1467614.

[47] PANKAJ K, SAURABH K S. An Empirical Evaluation of Various Digital Signature Scheme in Wireless Sensor Network[J]. IETE Technical Review, 2022, 39(4): 974-984.

[48] SURACI C, PIZZI S, MOLINARO A, et al. An RSA-based Algorithm for Secure D2D-aided Multicast Delivery of Multimedia Services[C]// 2020 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB). New York: IEEE Press, 2020: 1-6.

[49] MILANOV E. The RSA algorithm[R]. US: RSA laboratories, 2009.

[50] DORUS R, VINOTH P. Mitigation of jamming attacks in wireless networks[C]// 2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology. New York: IEEE Press, 2013: 168-171.

[51] ZHU F, WONG D S, CHAN A H, et al. Password Authenticated Key Exchange Based on RSA for Imbalanced Wireless Networks[J]. Information Security, Proceedings. 2002, 2433: 150-161.

[52] NAGAR S A, ALSHAMMA S. High speed implementation of RSA algorithm with modified keys exchange[C]// 2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications. New York: IEEE Press, 2012: 639-642.

[53] AMBIKA S, RAJAKUMAR S, ANAKATH A S. A novel RSA algorithm for secured key transmission in a centralized cloud environment[J]. International Journal of Communication Systems, 2020, 33(5): e4280.

[54] ZHU M L, LIU J W. An Intelligent Door Lock Device Based on RSA Algorithm: China, 201810181838. 3[P]. 2018-08-03.

[55] LU J C, XIONG X M. A hardware system and method of encryption and decryption based on RSA algorithm: China, CN201810877374. X[P]. 2018-12-18.

WANG Xinmiao, born in 2000, undergraduate. Her main research interest is computer software and theory.

MA Jingjun, born in 1971, professor. His main research interests include data mining and algorithm optimization.