Advances in Applied Mathematics 应用数学进展, 2022, 11(10), 6984-6989
Published Online October 2022 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2022.1110741

Hans汉斯

基于增强的RSA和ELGamal加密算法的新签名方案

杨倩倩，范自强

安徽理工大学数学与大数据学院，安徽 淮南

收稿日期：2022年9月12日；录用日期：2022年10月2日；发布日期：2022年10月12日

摘　要

密码学解决了安全通信的必要条件，如隐私、机密性、密钥交换、身份验证和不可否认性。邵祖华提出基于因式分解和离散对数的两个数字签名，由于在两个签名协议中引入多个指数密运算，导致计算量大。Malhotra M提出一种基于增强的RSA和ELGamal的新加密方案，相比现有的加密方案效率更高。在他们的基础上本文提出了一种基于增强的RSA和ELGamal密码系统相结合的算法，增强的RSA密码体制基于整数分解问题(IFP)，而ELGamal密码体制依赖于离散对数问题(DLP)。该模型基于IFP与DLP的结合，在解决两个著名难题的困难的基础上，为非对称密码系统提供了很好的计算速度，与ELGamal和现有的RSA-ELGamal混合系统相比，该算法具有更高的吞吐量和更短的加密时间，分析了新加密算法的高安全性。在该模型的基础上引入单向哈希函数，提出了相应的数字签名方案。这个签名方案的安全性不仅基于因数分解和离散对数的困难性，还有求逆函数的困难性，其安全性高于基本的ELGamal数字签名方案。

关键词

密码学，增强的RSA，ElGamal，数字签名方案，IFP，DLP

A New Signature Scheme Based on Enhanced RSA and ELGamal Encryption Algorithms

Qianqian Yang, Ziqiang Fan

School of Mathematics and Big Data, Anhui University of Science and Technology, Huainan Anhui

Received: Sep. 12th, 2022; accepted: Oct. 2nd, 2022; published: Oct. 12th, 2022

Abstract

Cryptography solves the necessary conditions for secure communication, such as privacy, confi-

文章引用: 杨倩倩, 范自强. 基于增强的 RSA 和 ELGamal 加密算法的新签名方案[J]. 应用数学进展, 2022, 11(10): 6984-6989. DOI: 10.12677/aam.2022.1110741

dentiality, key exchange, authentication and non repudiation. Shao Zuhua proposed two digital signatures based on factorization and discrete logarithm. Because of the introduction of multiple exponential secret operations in the two signature protocols, the computation is large. Malhotram proposed a new encryption scheme based on enhanced RSA and ElGamal, which is more efficient than the existing encryption schemes. On their basis, this paper proposed an algorithm based on the combination of enhanced RSA and ElGamal cryptosystems. The enhanced RSA cryptosystem is based on Integer factorization problem (IFP), while ElGamal cryptosystem relies on discrete logarithm problem (DLP). This model is based on the combination of IFP and DLP. On the basis of solving the difficulties of two famous problems, it provides a very good computing speed for asymmetric cryptographic systems. Compared with ElGamal and existing RSA ElGamal hybrid systems, this algorithm has higher throughput and shorter encryption time. The high security of the new encryption algorithm is analyzed. Based on this model, a one-way hash function is introduced and a corresponding digital signature scheme is proposed. The security of this signature scheme is not only based on the difficulty of factorization and discrete logarithm, but also on the difficulty of finding the inverse function. Its security is higher than that of the basic ElGamal digital signature scheme.

Keywords

Cryptography, Enhanced RSA, ELGamal, Digital Signature Scheme, IFP, DLP

1. 引言

密码学是一种将原始信息加密为任何人都不容易破解形式的一门艺术，只有在对加密的消息进行解密后，才能显示原始消息，公钥和私钥都是为此目的生成的[1]。一般来说，密码系统可以分为对称密码学和非对称密码学。在对称密码学中，加密和解密用相同的密钥，如经典、流、DES 密码系统。而在非对称密码学中，不同的密钥用于加密和解密过程[2]，如 RSA、ELGamal 密码系统、DSS 和 Diffie-Hellman 密钥交换系统。Diffie-Hellman 密钥系统于 1976 年由 Whitfield Diffie 和 Martin Hellman [3] [4]首次创造，它被认为是公钥密码学的第一个重要里程碑[5]。从此之后，各种类型的公钥密码算法被相继提出，最著名的公钥密码算法是 RSA 和 ELGamal，这两种算法都可以用来加密解密和数字签名。这些密码体制的一个共同点就是它们的安全性基本上都建立在一个公认难解的数学问题上[6]。

但随着计算机技术的发展，人们发现算法仅仅基于一个难题，容易被攻击者破解，因此又提出基于多个数学难题的密钥算法。Ahmed 和 Ali 提出一种结合 RSA 和 ELGamal 密码系统，利用数学上公认的两大难题——因数分解和离散对数问题，在加密过程中生成两个密文。该算法提高了对消息的加密，防止被破解，由于加大了计算量，导致加密时间长，加解密速度变慢[1]。Malhotra M 针对 Ahmed 提出的算法问题进一步改进，提出了一种基于增强的 RSA 和 ELGamal 加密算法。作者利用三个素数来生成密钥，相比 Ahmed 的算法中随机挑选的整数作为明文加密的指数，该算法是利用 RSA 的加密密钥对明文加密，从而不仅增强算法的安全性，同时也提高了加密解密速度[2]。

本文基于非对称密码体制，介绍了一种基于增强 RSA 和 ELGamal 密码体制的算法。增强的 RSA 算法基于整数分解问题(IFP)，在密钥生成中使用四个素数来生成公钥和私钥，它支持更快的加密和解密过程，并比原始 RSA 更快地生成公钥和私钥，ELGamal 密码系统基于离散对数问题(DLP) [3] [4]。为了提

高这些算法的强度，使用了增强 RSA 和 ELGamal 的组合，这将提供更高级别的安全性，新提出的是一种比现有 ELGamal 和 RSA-ELGamal 系统更高效、更安全的系统。在此加密算法的基础上提出数字签名算法，从而该签名算法也就建立在整数分解和离散对数难题的基础上，相比传统的 RSA 和 ELGamal 的签名方案安全性有了很大的提高。

2. 新的加密算法

该算法使用四个较大的素数来生成公钥和私钥，然后将生成的公钥和私钥传递给 ELGamal 密码系统。在这种方法中，我们整合了 IFP 和 DLP 技术，该方法是一种集成了增强 RSA 和 ELGamal 密码系统的方法，该方法比 RSA、ELGamal 最初算法[1]和合并 RSA-ELGamal 算法更有效。所提方法的工作原理说明如下：

2.1. 密钥生成

以下是生成加密和解密密钥对的过程[7]。

1) 对于该方案的密钥生成是基于下列等式：

$$p = 4p_1q_1 + 1$$
$$p_1 = 2p_2 + 1$$
$$q_1 = 2q_2 + 1$$

其中模数 n 为

$$n = \frac{p-1}{4} = p_1q_1$$

这里的 p, p_1, q_1, p_2, q_2 都是素数，且 p_1, q_1, p_2, q_2 互不相同。

2) 利用欧拉算法计算：$\varphi(n) = (p_1 - 1)(q_1 - 1)$

3) 任取一整数 e 作为公钥，满足 $1 < e < \varphi(n)$，$gcd(e, \varphi(n)) = 1$。计算算法的私钥 d：

$$ed \equiv 1 mod(\varphi(n))$$

4) 从剩余类环 $z_p = z/(p)$ 中选取一个阶为 n 的生成元 g，再挑选一个大素数 q，以及用于加密的密钥

$$x\left(1 < x < \frac{n}{2}\right)$$

5) 算法的公钥为 $\{e, n, p, q\}$，私钥为 $\{d, x\}$。

2.2. 加密方案

发送方将消息 m 使用公钥 e 加密成密文对 (c_1, c_2) [8]，具体的过程如下：

首先计算 $y \equiv g^x (modq)$，再把生成的公钥 y 代入以下公式中可得密文对 (c_1, c_2)。

$$c_1 \equiv g^e (modn), \quad c_2 \equiv my(modq)$$

发送方将密文对 (c_1, c_2) 传送给收件人。

2.3. 解密方案

将密文对 (c_1, c_2) 转换回原来的形式 m，解密的方法如下：

1) 计算 $g \equiv c_1^d (modn)$；2) 计算 $g^{-x} (modq)$ 并把它当做 y^{-1}；3) 最后计算 $m \equiv c_2 y^{-1} (modq)$。接下来用图的形式把新提出的算法具体过程描述，见图 1。

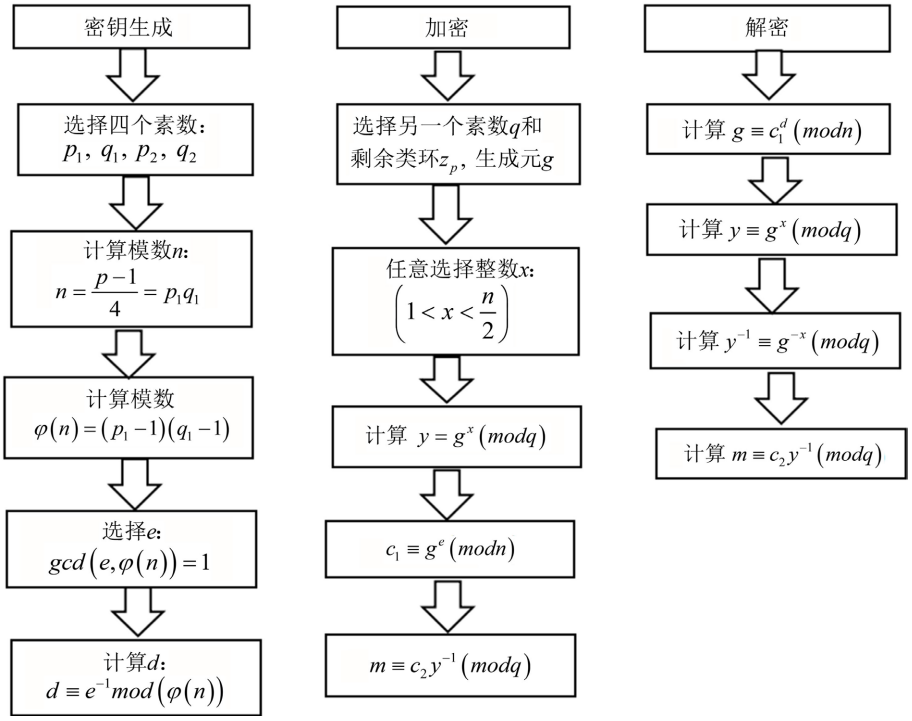

Figure 1. Algorithm flow chart
图 1. 算法流程图

2.4. 所提方法的有效性

2.4.1. 加密方案

消息 m 在密钥 y 和原根元素 g 的帮助下被加密成密文 c。密文 c 的计算公式为：

$$c\equiv my(modq) \tag{1}$$

此时密钥 $y\equiv g^x(modq)$，因此，将 y 的值代入(1)得到，

$$c\equiv mg^x(modq) \tag{2}$$

2.4.2. 解密方案

通过 y^{-1} 和 c 将加密后的文本 c 解密为原始消息 m。

$$m\equiv cy^{-1}(modq) \tag{3}$$

将 y^{-1} 的值等于 g^{-x} 代入(3)中我们得到：

$$m\equiv cg^{-x}(modq) \tag{4}$$

取式(2)中计算的 c 值，在上式(3)中得到：

$$m\equiv mg^xg^{-x}(modq)$$

从而求解得到 $m=m$，这就证明了消息 m 被加密成 c，成功地将加密后的消息解密回原来的形式 m。

3. 数字签名方案

3.1. 签名参数

1) 由前面的加密算法选取的一些参数知，签名者选择多个素数 p, p_1, q_1, p_2, q_2，这些素数满足

$p=4p_1q_1+1$，$p_1=2p_2+1$，$q_1=2q_2+1$和$n=p_1q_1$，则有$n|(p-1)$。从剩余类环z_p选择生成元g，从而g的阶为n，挑选一个大素数q，以及用于加密的密钥

$$x\left(1<x<\frac{n}{2}\right),\ (x,n)=1。$$

2) 设$H(x,y)$为单向安全的杂凑函数，单向函数具有很好地性质，这类函数正向求解很容易，但反过来求逆过程很困难[9]。

3) 签名算法的公钥为$\{p,q,y,g,e,H\}$，私钥为$\{d,x,p_1,q_1\}$。

3.2. 签名过程

签名者对任意的消息m签名，要进行如下计算：

1) 计算$k=g^x(modp)$，$r\equiv g^e(modp)$，再令$h\equiv H(r,m)(modp)$，其中$H(x,y)$是单向函数。

2) 计算$s=(x-eh)^d(modn)$。

将$sign(m)=(r,s)$作为消息m的签名。

3.3. 验证过程

验证者要对签名者的签名(r,s)进行验证，有以下过程：

1) 计算$s'=s^e(modn)$。

2) 验证等式$k=g^{s'}r^h(modp)$是否成立。若该等式成立，则签名(r,s)有效，否则签名无效。

如果签名者用上述签名算法对消息进行签名，则验证者可以接受该签名。因为$s'=s^e(modn)=(x-eh)^{ed}(modn)=x-eh$，$g^{s'}r^h(modp)=g^{x-eh}r^h(modp)=g^{x-eh}g^{eh}(modp)=g^x(modp)=k$，从而$(r,s)$是签名者对消息$m$的签名。

3.4. 安全性分析

新加密算法的安全性是基于IFP和DLP的结合，提出了一种比现有ELGamal和RSA-ELGamal系统更高效、更安全的系统。在此加密算法的基础上提出数字签名算法，从而该签名算法的安全性也就建立在整数分解和离散对数难题的基础上，相比传统的RSA和ELGamal的签名方案安全性有了很大的提高。

攻击者想要从公钥$\{p,q,y,g,e,H\}$中破解秘钥$\{d,x,p_1,q_1\}$，他就要从方程$y\equiv g^x(modq)$中解出x，其难度等价于解离散对数$y\equiv g^u(modq)$。如果离散对数问题可解，攻击者还需从方程$ed\equiv 1(mod\varphi(n))$中恢复出$d$，其难度又相当于对$n=p_1q_1$进行因数分解。

在签名过程中引入单向杂凑函数$H(x,y)$，求$H(x,y)$的逆比对$n=p_1q_1$因数分解和对$y\equiv g^u(modq)$解离散对数要困难。假设攻击者找到一个算法可以解$H(r,m)$的逆函数m，设a是任意整数，$x^d=a(mod\ p_1q_1)$是一个指数方程。我们应用假设算法求单向哈希函数$H(r,m)=a$的逆m。m是该指数方程的根，$m^d=a(mod\ p_1q_1)$。求解指数方程$x^d=a(mod\ p_1q_1)$相当于分解$y\equiv g^u(modq)$和p_1q_1。相反，如果有可行的因子分解算法，我们可以求解指数方程$x^d=a(mod\ p_1q_1)$。给定$H(r,m)=a$，我们构造了一个指数方程$x^d=a(mod\ p_1q_1)$。求其解m就是求单向散列函数$H(r,m)$的逆m。

3.5. 性能分析

在我们设计的数字签名协议中，计算签名(r,s)需要计算两个模指数，签名的验证需要计算三个模指数。在验证中加法和乘法所需的时间可以忽略不计，这种性能类似于基本ELGamal协议。然而，在RSA-ELGamal数字签名协议中，每个签名计算需要两个模指数运算。在我们的数字签名协议中，所有用户都使用公共素数模n和生成元g。这一特性是ELGamal签名相对于RSA的主要优势。与RSA-ELGamal

签名算法一样中，我们方案中的每个用户也都有两个公钥。在我们的数字签名协议中使用了一个简单的单向哈希函数 $H(r,m)$。求其逆函数的难度大于因子分解和离散对数。然而，对于常用的单向哈希函数的单向性并没有严格的证明。在我们的数字签名协议中，h 和 d 都参与验证方程的计算，因此它可以更有效地抵抗生日悖论的攻击。

4. 结论

本文提出的算法是基于增强 RSA 和 ELGamal 密码体制的算法。增强的 RSA 算法基于整数分解问题(IFP)，在密钥生成中使用四个素数来生成公钥和私钥，它支持更快的加密和解密过程，并比原始 RSA 更快地生成公钥和私钥，ELGamal 密码系统基于离散对数问题(DLP)。为了提高这些算法的强度，使用了增强 RSA 和 ELGamal 的组合，这将提供更高级别的安全性，新提出的是一种比现有 ELGamal 和 RSA-ELGamal 系统更高效、更安全的系统。在此加密算法的基础上提出数字签名算法，从而该签名算法也就建立在整数分解和离散对数难题的基础上，相比传统的 RSA 和 ELGamal 的签名方案安全性有了很大的提高，在数据的安全传输、电子银行、电子商务等方面有很大用处。

致　谢

感谢导师范老师对本文在创作过程中提供的帮助与指导。

基金项目

安徽理工大学 2022 年研究生创新基金立项建设项目(2022CX2134)。

参考文献

[1] Ahmed, J.M. and Ali, Z.M. (2011) The Enhancement of Computation Technique by Combining RSA and El-Gamal Cryptosystems. *Proceedings of the* 2011 *International Conference on Electrical Engineering and Informatics*, Bandung, 17-19 July 2011, 1-5.

[2] Malhotra, M. (2014) A New Encryption Scheme Based on Enhanced RSA and ElGamal. IJETCAS 14-336, 138-142.

[3] Stallings, W. (2012) Cryptography and Network Security-Principles and Practice. 5th Edition, Pearson Publication, London, 259-262.

[4] Cormen, T.H., Leiserson, C.E., Rivest, R.L. and Stein, C. (2003) Introduction Algorithms. 2nd Edition, The MIT Press and McGraw-Hill Book Company, Cambridge, USA, 2003.

[5] Diffie, W. and Hellman, M. (1976) New Directions in Cryptography. *IEEE Transactions on Information Theory*, **22**, 644-654. https://doi.org/10.1109/TIT.1976.1055638

[6] Mao, W. (2003) Modern Cryptography: Theory and Practice. Prentice Hall, Hoboken, 294-296.

[7] Hellman, M.E. (2002) An Overview of Public Key Cryptography. *IEEE Communications Magazine*, **40**, 42-49.

[8] 邵祖华. 基于因数分解和离散对数的数字签名协议[J]. 信息安全与通信保密, 1998(4): 36-41.

[9] 朱福全, 杨丽平. 一个基于离散对数和因数分解的数字签名方案[J]. 中国西部科技, 2010, 9(19): 20-21.