Computer Science and Application 计算机科学与应用, 2021, 11(11), 2619-2626
Published Online November 2021 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2021.1111265

Hans汉斯

基于RSA属性集工作量证明算法的研究

罗　锐，李子臣

北京印刷学院数字版权保护技术研究中心，北京

收稿日期：2021年10月2日；录用日期：2021年11月1日；发布日期：2021年11月8日

摘　要

工作量证明(Proof Of Work，简称POW)，简单理解就是一份证明，用来确认你做过一定量的工作。监测工作的整个过程通常是极为低效的，而通过对工作的结果进行认证来证明完成了相应的工作量，则是一种非常高效的方式。本文提出了一个基于RSA属性集工作量证明算法，将陷门函数和RSA公钥密码体制中的加解密应用于工作量证明函数中，根据用户的属性是否满足属性集而决定是否分发陷门用于工作量的证明。本文提出的算法同时满足6个性质：有陷门计算容易、无陷门计算困难、易于验证、正确性、可靠性和顺序性。进一步设计了基于RSA属性集工作量证明函数的电子邮件系统，该系统实现了满足属性的用户群发邮件容易、反垃圾邮件、保证邮件内容的机密性和完整性等功能。

关键词

工作量证明，RSA，陷门，邮件系统

Research Based on the RSA Attribute Set Proof of Work Algorithm

Rui Luo, Zichen Li

The Center of Digital Copyright Protection Technology, Beijing Institute of Graphic Communication, Beijing

Received: Oct. 2nd, 2021; accepted: Nov. 1st, 2021; published: Nov. 8th, 2021

Abstract

Proof of work, simply understood, is a certificate that confirms that you have done a certain amount of work. The whole process of monitoring work is usually extremely inefficient, while proving the completion of the corresponding amount of work by certifying the results of the work is a very efficient way. In this article, an RSA attribute set based proof of work algorithm is proposed, which applies the trapdoor function and the encryption and decryption in RSA public key cryptosystem to the proof of work function, and decides whether to distribute the trapdoor for the proof of workload according to whether the user's attributes satisfy the attribute set or not. The algorithm proposed in this paper satisfies six properties simultaneously: easy computation with

文章引用: 罗锐, 李子臣. 基于 RSA 属性集工作量证明算法的研究[J]. 计算机科学与应用, 2021, 11(11): 2619-2626.
DOI: 10.12677/csa.2021.1111265

trapdoors, difficult computation without trapdoors, easy verification, correctness, reliability and sequentiality. Further, an email system based on the RSA attribute set proof of work function is designed, which achieves the functions of easy mass emailing of users satisfying the attributes, anti-spam, and ensuring the confidentiality and integrity of email contents.

Keywords

Proof of Work, RSA, Trap Door, Email System

1. 引言

工作量证明[1]是确认一个用户做过一定量工作的证明，一般要求用户计算一个难于计算但易于验证的函数。简单来说，倘若要求 A 监督 B 工作的完整过程，这将极为费时费力且十分低效，而通过对工作的结果进行认证来证明完成了相应的工作量，则是一种非常高效的方式。因此利用 POW 函数，将重点放在工作的结果上，可以使得验证工作变得高效。

陷门工作量证明函数由 Dwork 和 Naor 提出[2]，是一种应对拒绝服务攻击和其他服务滥用的经济对策。它要求发起者进行一定量的运算，也就意味着需要消耗计算机一定的时间。即是一种有陷门时工作量证明计算容易，无陷门时计算困难的函数，陷门使得 POW 具有更广泛的应用，如在邮件系统中应用陷门 POW 函数，可以使陷门拥有者更容易发送大量邮件。POW 函数时固定的且由系统管理员分配给受信任者，为避免陷门泄露带来安全问题，需要定期更新陷门，给管理员带来不便。

工作量证明函数可以成功地应用于邮件系统中起到反垃圾邮件的作用。其基本思想是：如果用户 A 想给用户 B 发送邮件，那么他必须向服务器提供一个仅与用户 B 和此邮件有关的证明，假设生成证明需要占用用户 A 电脑 CPU10 秒的时间，并且该证明不可被重复使用。这样如果用户 A 要发送一万份垃圾邮件，则占用电脑 CPU 为 10 万秒，时间代价非常大，因此会放弃大量发送邮件，从而实现反垃圾邮件的目的。此外，在邮件系统的实际使用中，有时候需要群发邮件，则可以给某些满足属性的人特权，也就是让满足属性的用户获得陷门，使其群发邮件容易。我们将基于属性的陷门工作量证明函数应用于邮件系统，可以实现满足属性的用户群发邮件容易、反垃圾邮件、保证邮件内容的机密性和完整性等功能。

现有的工作量证明函数存在部分问题，如功能简单、实现复杂、不太完善、安全性能低。近年来，加密货币越来越火爆，其实质是建立在区块链系统之上[3]，区块链是一个分布式的共享账本和数据库，具有去中心化、不可篡改、全程留痕、可以追溯、集体维护、公开透明等特点。这些特点保证了区块链的“诚实”与“透明”，为区块链创造信任奠定基础[4]。工作量证明是目前最流行区块链里不可或缺的重要部分，它被应用于各种加密货币如比特币和以太坊，在工作量证明中，为了选出一位参与者成为领导者并选择下一个加入区块链的区块，参与者必须解决一个特定的难度可动态调整的数学问题。对于给定问题很难找到解决方法，一旦找到问题的答案，很容易就能证实它是对的，每挖出一个新的区块，矿工就会得到一些代币奖励，以此激励他们继续挖矿。并将当前时间段的所有交易打包记入一个新的区块、按照时间顺序链接到比区块主链上，其它节点通过检验该区块数据的哈希值是否小于预设值来验证该区块的有效性。因此结合所学公钥密码体制，将 RSA 加解密体制应用在工作量证明函数中是十分必要的，使得工作量证明函数更加丰富，加密货币交易更加安全可靠。

本文将陷门函数和 RSA 公钥密码体制中的加解密应用于工作量证明函数中，提出了一个基于 RSA 属性集工作量证明算法。根据用户的属性是否满足属性集而决定是否分发陷门，满足属性的用户可以获得陷门，计算函数值容易，不满足属性的用户计算困难。本文提出的算法具有 6 个性质：有陷门计算容易、无陷门计算困难、易于验证、正确性、可靠性和顺序性。基于本文所提出的算法，进一步设计了基于 RSA 属性集工作量证明函数的电子邮件系统，实现了反垃圾邮件的功能。此外，还考虑了管理员群发邮件的实际场景，由于本系统的陷门根据用户的属性分发，使得满足属性的群管理员能更容易的群发邮件，经分析可得本系统实现了满足属性群发邮件容易、反垃圾邮件、保证邮件的机密性和完整性等功能。

2. 相关基础知识

2.1. 工作量证明

工作量证明函数用于协议的证明者向验证者证明其已在某特定时间段内执行了一定量的计算工作，该函数难于计算但易于验证。例如小明上课不认真，老师罚他把《桃花源记》抄写十遍，小明用了两个小时的劳动，最后给老师的就是抄满课文的纸，而老师要确认小明的确付出了大量劳动，只需要看看抄写的纸即可。又比如小美的任务是从城市 A 到城市 B，我们首先确认她确实从城市 A 出发，然后经过一段时间后到达 B 城市，我们可以用他到达 B 城市的结果表示他已经完成了整个任务工作量。

2.2. 陷门

如果一个登陆处理系统允许一个特定的用户识别码，通过该识别码可以绕过通常的口令检查，直观的理解就是可以通过一个特殊的用户名和密码登陆进行修改等操作，这种方式称为陷门，又称为非授权访问。在公钥密码体制中，陷门相当于私有密钥，而利用陷门求解明文相当于解密。例如假设从 A 城市到 B 城市有三种方法，分别是轮船，汽车和飞机，普通人均是选择乘坐汽车或轮船到达 B 城市，速度缓慢，耗时极长。而拥有特权陷门的人，则可以乘坐飞机快速到达 B 城市，从而高效、快捷完成整个任务工作量。

基于属性的陷门工作量证明函数将陷门与用户的属性绑定[5]，由密钥生成算法生成，每个满足属性的用户获得的陷门信息不同，并由用户单独保存，使得陷门的管理与分发更安全，此外顺序性使其不能通过并行来加速其计算，更加节约电能，并且满足 6 个性质：有陷门计算容意、无陷门计算困难、易于验证、正确性、可靠性和顺序性。

2.3. RSA 简介

RSA 算法是 1978 年由 R. Rivest、A. Shamir 和 L. Adleman 提出的一种用数论构造的、也是迄今为止理论上最为成熟完善的公钥密码体制，该体制已得到广泛的应用[6]。它既可用于加密、又可用于数字签字，RSA 算法的安全性基于数论中大整数分解的困难性[7]。

算法描述：① 选两个保密的大素数 p 和 q。② 计算 $n=p\cdot q$，$\varphi(n)=(p-1)(q-1)$，其中 $\varphi(n)$是 n 的欧拉函数值。③ 选一整数 e，满足 $1<e<\varphi(n)$，且 $\gcd(\varphi(n),e)=1$。④ 计算 d，满足 $d\cdot e\equiv 1 \bmod \varphi(n)$，即 d 是 e 在模 $\varphi(n)$下的乘法逆元，因 e 与 $\varphi(n)$互素，由模运算可知，它的乘法逆元一定存在。⑤ 以$\{e,n\}$为公钥，$\{d\}$为私钥。

加密运算：$c\equiv m^e \bmod n$；解密运算为：$m\equiv c^d \bmod n$

基于因子分解困难原理[8]，保证了加解密足够安全。模数生成算法 Gen Modulus (λ)的输入为 λ，输出为(n,p,q)，其中 p 和 q 均是 λ 比特的素数，且满足 $n=p\cdot q$，n 的因子分解为陷门。

2.4. 访问树

在工作量证明函数的构造中，陷门将使用一组描述行的属性进行标识，并根据用户属性是否满足访

问树结构决定是否向用户分发陷门[9]。令 T 表示根为 R 的访问树，T_v 表示以节点 v 为根的子树，所以有 $T = T_R$。令 $T_v(\gamma)$的值表示属性集 γ 与访问树的关系，若 $T_v(\gamma) = 1$，则称属性集 γ 满足访问树 T_v；反之 $T_v(\gamma) = 0$，则称属性集 γ 不满足访问树 T_v。如图 1 构造的一棵访问树：即这些人的属性必须满足职业是老师，并且名字是 Alice 或者 Bob，则系统允许 Alice 或 Bob 拥有陷门，从而可以获得特权。例如，对于属性集 γ_1 = {Job = teacher, Name = Alice}，有 $T(\gamma_1) = 1$，即满足访问树，获得特权；而对于属性集 γ_2 = {Job=teacher，Name = Mary}，有 $T(\gamma_2) = 0$，不会获得特权。

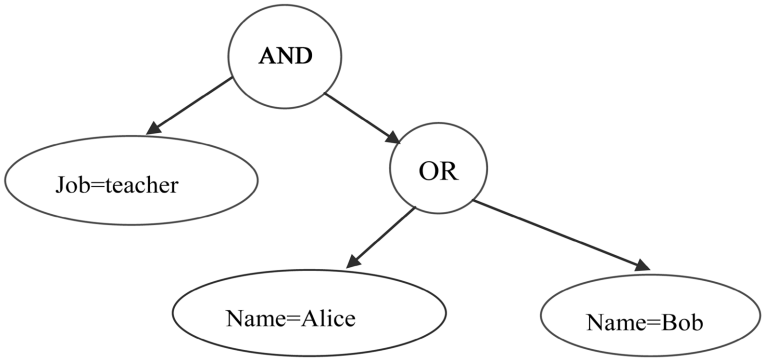
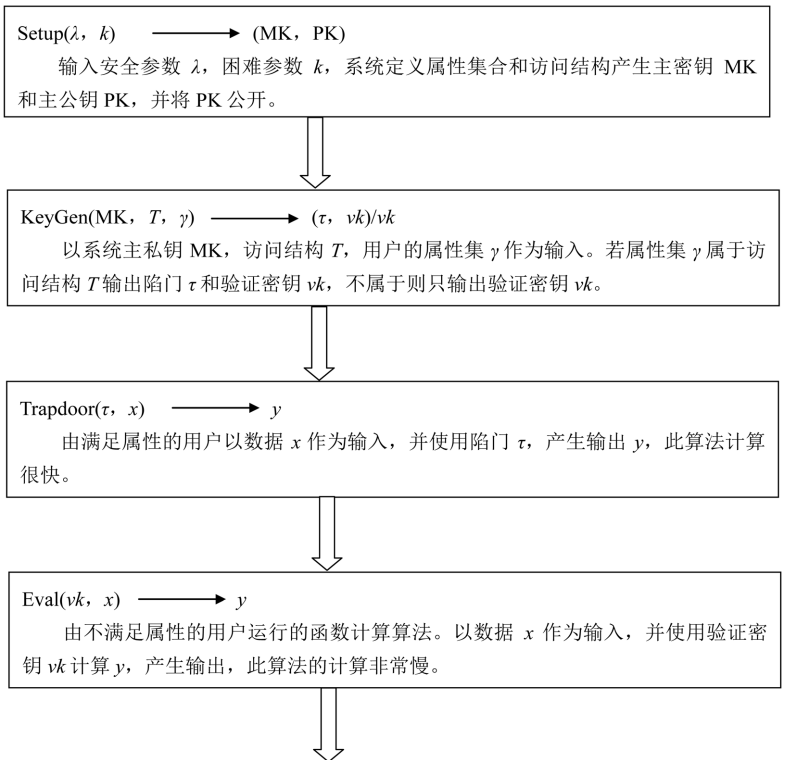


Figure 1. Visits the tree structure
图 1. 访问树结构

3. 基于 RSA 属性集工作量证明函数的构造

3.1. 整体模型

函数的整体模型如图 2：



Verify(vk，x，y) ⟶ {*Ture*,*False*}

给出计算者的验证密钥 vk，数据 x 和输出 y。然后通过验证密钥 vk 计算 $y^e \bmod n$。若满足则输出 *Ture*，否则输出 *False*。

Figure 2. The overall flowchart
图 2. 整体流程图

3.2. 详细构造

Setup(λ) → (MK，PK)

- 输入参数 λ，并且由 Gen Modulus (λ)算法产生 λ 比特的 p 和 q。
- 计算 $n = p \cdot q$， $\varphi(n) = (p-1)(q-1)$，其中 $\varphi(n)$是 n 的欧拉函数值。
- 选一整数 e，满足 $1 < e < \varphi(n)$，且 $\gcd(\varphi(n), e) = 1$。
- 计算 d，满足 $d \cdot e \equiv 1 \bmod \varphi(n)$，即 d 是 e 在模 $\varphi(n)$下的乘法逆元，因 e 与 $\varphi(n)$互素，由模运算可知，它的乘法逆元一定存在。
- 输出主密钥 MK 和主公钥 PK 为：$\{ \mathrm{MK} = \langle d \rangle,\ \mathrm{PK} = \langle e, n \rangle \}$

KeyGen(MK, T, γ) → (τ, vk)/vk

判断用户属性集 γ 是否满足访问树 T，若满足，则 $T_R(\gamma) = 1$，用户得到陷门和验证密钥对(τ, vk)；否则，用户只得到验证密钥 vk。其中陷门 τ 为 $\mathrm{MK} = \langle d \rangle$，验证密钥 $vk = \mathrm{PK} = \langle e, n \rangle$。

Trapdoor(τ, x) → y

使用陷门 τ 对数据 x 计算，输出 y，其中 x 相当于密文，输出的 y 相当于明文。运行 Trapdoor(τ, x)函数，计算过程为： $y = x^d \bmod n$，此计算是容易的。

Eval(vk, x) → y

使用验证密钥 vk 对数据 x 计算，等同于密文 x 通过 RSA 中公钥 e 和 n 计算明文 y，这是极其困难的。

Verify(vk, x, y) → {*True*，*False*}

给出计算者的验证密钥 vk，数据 x 和输出 y。然后通过验证密钥 vk 计算 $y^e \bmod n$，并检查 x 与 $y^e \bmod n$ 是否相等。若相等则输出 *Ture*，否则输出 *False*。

4. 安全性证明

从这个设计流程可以看出，整个系统的安全性能与 RSA 的安全性能完全相同，而 RSA 公钥密码体制的安全性是基于大整数的素分解问题。分析 RSA 公钥密码体制可知：若 n 能分解成 $n = p \cdot q$，就很容易计算 $\varphi(n) = (p-1)(q-1)$，并且 $e \cdot d \equiv 1 \bmod \varphi(n)$，很容易计算出解密密钥 d，也就是此系统中的陷门。因此，破译 RSA 的难度 $\leq n$ 素因子分解难度。若密码分析者直接计算 $\varphi(n)$，因为： $p + q = n - \Phi(n) + 1$，$p - q = \sqrt{(p+q)^2 - 4n}$，可以计算出 p, q，可以对 n 素因子分解，因此：n 素因子分解难度 $\leq$ 直接计算 $\varphi(n)$ 的难度。若密码分析者直接计算 d，那么 ed-1 是 $\varphi(n)$的倍数，利用 $\varphi(n)$的倍数，可以很容易的分解 n，因此：n 素因子分解难度 $\leq$ 直接计算 d 的难度[10]。综合可以得出：破译 RSA 明显方法的难度 $= n$ 素因子分解难度，所以可以得到此系统是足够安全的，并且满足六大性质：有陷门计算容易、无陷门计算困难、已于验证、正确性、顺序性和可靠性。

5. 效率分析

此算法涉及以下三种用户：

1) 具有陷门的用户：此类用户计算输出值 y 是通过 Trapdoor 算法，由构造原理可知，具有陷门的用户并行计算速度极快为 $O(1)$。

2) 没有陷门的用户：此类用户通过 Eval 算法计算 y，且可得，没有陷门计算 y 是极其困难的，只能靠猜测 n 的分解，所以其计算复杂度为 $O(n^2)$。

3) 验证者：验证者通过 Verify 算法验证输出值 y 是否是输入值 x 的正确计算结果，分析可得，验证者的并行计算复杂度为 $O(1)$。

6. 在电子邮件中的应用

6.1. 电子邮件系统中存在的问题

电子邮件是一种通过网络传递信息的现代通信方式，是当今互联网中应用最广泛、技术最成熟、用户数量最庞大的一种服务。但是在邮件系统中，仍然存在窃听、篡改和垃圾邮件等安全问题。根据卡巴斯基实验室发布的 2019 年垃圾邮件和钓鱼邮件分析报告显示垃圾邮件占一半以上。因此加强群发邮件的管理控制是非常有必要的[11]。

工作量证明函数应用于邮件系统可以起到反垃圾邮件的作用。他的原理是要求发件人为每条消息解决一个小小的密码难题，从而增加邮件的发送成本，对于普通用户来送，单个邮件成本可以忽略不计，但面对非常大量的邮件，发送时间成本极高，因此可以起到避免垃圾邮件的作用。但在实际使用邮件过程中，有时企业的管理人员需要群发邮件，若限制所有用户都计算同等难度的密码难题，会影响管理人员的群发体验。因此，本节将基于 RSA 属性集工作量证明算法应用于邮件系统，可以解决邮件中的窃听、篡改和垃圾邮件等问题。

6.2. 系统模型

在本系统中，邮件发送者必须首先计算基于 RSA 基工作量证明函数，并将结果和邮件内容一起发送给服务器，由服务器验证，这一过程可以达到反垃圾邮件的作用。同时函数具有陷门，并且是根据用户属性分发的，则可以赋予满足属性的用户特权，使其群发邮件容易。整个系统主要包括发送者、接收者、邮件服务器和密钥管理中心(KMC)。

系统运行流程如下：首先邮件服务器通过 ServeSetup 算法进行初始化，设置系统参数。然后用户向 KMC 提出申请，KMC 通过 ServerKeyGen 算法根据用户属性分配陷门。之后发送者 S 想要向接收者 R 发送邮件，需要通过 SendEmail 算法完成相关计算工作，并将计算结果发送给服务器。服务器收到计算结果，通过 VerifyEmail 算法验证结果的正确性，若验证通过，将加密邮件发送给接收者 R；否则直接丢弃该邮件。最后接收者 R 对接受的加密邮件进行解密得到原始邮件内容。

6.3. 函数详细构造

Serve Setup (λ)：由邮件服务器执行，邮件服务器运行 RSA 基工作量证明函数中的 Setup (λ)算法，输入为安全参数 λ，定义总的属性集和访问树，输出为主密钥 MK 和主公钥 PK。

Serve KeyGen (MK，T，γ)：由可信第三方 KMC 执行。邮件服务器运行基于 RSA 属性集工作量证明函数中的 KeyGen (MK，T，γ)算法。输入为服务器主密钥 MK，访问树和用户的属性集 γ。如果属性集 γ 满足访问树 T，则输出陷门 τ，验证密钥 vk 以及用户的公私钥(pk，sk)；否则输出验证密钥 vk_s，以及用户的公私钥(pk，sk)。

Send Email (m，pk，$addr$)：由发送者 S 执行。

计算 m 的摘要：$h_m = h(m \| addr)$，其中 m 为邮件内容，h 为密码哈希函数，$addr$ 为接收者 R 的邮件地址；

加密运算：$m' = \mathrm{Enc}(pk, m \| h_m)$，其中 pk 为接收者 R 的公钥，m 为邮件内容，h_m 为 m 的摘要；

邮件服务器运行基于 RSA 属性集工作量证明函数：发送者根据是否具有陷门，分情况计算 Trapdoor (τ_s，m')和 Eval(vk_s，m')输出 y；

发送：将 $Y=\langle y,m',addr\rangle$ 发送给服务器。

VerifyEmail(vk_s，Y)：由服务器执行，计算 Verify(vk_s，m'，y)，若输出结果为 $Ture$，则验证通过，否则直接丢弃该邮件。

ReceiveEmail(m')：由接收者 R 执行。

解密运算：$m\|h_m=\mathrm{Dec}(sk,m')$，即接收者 R 用私钥 sk 对 m 解密，得邮件内容 m 和其摘要 h_m。

完整性验证：计算 m 的摘要的 $h'_m=h(m\|addr)$，检查 h'_m 与 h_m 是否相等，若相等，表面该邮件内容是完整的，否则表明该邮件被破坏。同时邮件系统满足如下四个性质：

满足属性群发邮件容易：即满足属性的用户群发邮件容易。

反垃圾邮件：即不满足属性的用户群发邮件是困难的。

邮件内容的机密性：即邮件内容不会被恶意敌手获取到。邮件的传输过程中是以密文形式发送，即使敌方获取到密文，没有对应解密密钥，也无法进行解密，从而确保了邮件内容的机密性。

邮件内容的完整性：即邮件内容不会被恶意敌手篡改。接受者在接受邮件时会计算哈希摘要是否相等，如果邮件内容被敌首恶意篡改，验证一定不会通过，从而确保了邮件内容的完整性。

7. 总结与展望

本文对属性访问策略、陷门工作量证明函数和 RSA 公钥密码体制进行了研究，首先定义并构造了基于 RSA 属性集工作量证明函数，该构造满足正确性、可靠性等安全性问题，同时引入属性访问树，满足属性的用户很容易计算出函数值，不满足属性的用户计算十分困难。然后将所构造的基于 RSA 属性集工作量证明函数结合公钥密码算法应用于电子邮件系统，并要求发送者在发送邮件时计算函数值，增加邮件发送时间成本，可以实现反垃圾邮件；此外还考虑了部分用户需要群发邮件的实际场景，由于本系统的陷门根据用户的属性分发，使得满足属性的用户可以更容易的群发邮件，因此实现了满足属性的用户群发邮件容易、反垃圾邮件、保证邮件的机密性和完整性等功能。

区块链是以比特币为代表的数字加密货币体系核心支撑技术，区块链技术的核心优势是去中心化，能够通过运用数据加密、时间戳、分布式共识和经济激励等手段，在节点无需互相信任的分布式系统中实现基于去中心化信用的点对点交易、协调与协作，从而为解决中心化机构普遍存在的高成本、低效率和数据存储不安全等问题提供了解决方案[12]。工作量证明是区块链中非常重要的机制，下一步会继续研究 ElGamal、ECC、SM2 等公钥密码体制在工作量证明函数中的应用，同时会广泛阅读区块链文献，掌握区块链的基本原理，把区块链应用于实践中，发挥出更多功能。

参考文献

[1] 程瑶, 高丽芬, 胡全贵. 区块链共识机制之 POW 算法[J]. 数字通信世界, 2019(3): 81.

[2] Dwork, C. and Naor, M. (1993) Pricing via Processing or Combatting Junk Mail. In: Brickell, E.F., Eds, *Advances in Cryptology—CRYPTO*' 92. *CRYPTO* 1992. *Lecture Notes in Computer Science*, Vol. 740, Springer, Berlin, Heidelberg, 139-147. https://doi.org/10.1007/3-540-48071-4_10

[3] Li, J., Chen, Y.S. and Song, H.T. (2021) Research on Digital Currency Supervision Model Based on Blockchain Technology. *Journal of Physics*: *Conference Series*, **1744**, Article ID: 032112. https://doi.org/10.1088/1742-6596/1744/3/032112

[4] Han, S.J., Lee, S., Lee, D. and Park, S. (2020) BACS: An Experimental Study for Access Control System in Public Blockchain. *The Journal of the Institute of Internet*, *Broadcasting and Communication*, **20**, 3-8.

[5] 周超. 结合属性与角色的访问控制关键技术研究[D]: [硕士学位论文]. 郑州: 战略支援部队信息工程大学, 2018.

[6] 张永建. RSA 算法和 SM2 算法的研究[D]: [硕士学位论文]. 赣州: 江西理工大学, 2015.

[7] Somsuk, K. (2020) The New Integer Factorization Algorithm Based on Fermat's Factorization Algorithm and Euler's Theorem. *International Journal of Electrical and Computer Engineering* (*IJECE*), **10**, 1469-1476. https://doi.org/10.11591/ijece.v10i2.pp1469-1476

[8] 孙克泉. RSA 密码分析中分解大整数的判定算法[J]. 计算机工程, 2010, 36(15): 142-144.

[9] 宋衍, 韩臻, 刘凤梅, 刘磊. 基于访问树的策略隐藏属性加密方案[J]. 通信学报, 2015, 36(9): 119-126.

[10] Hoobi, M.M., Sulaiman, S.S. and AbdulMunem, I.A. (2020) Enhanced Multistage RSA Encryption Model. *IOP Conference Series*: *Materials Science and Engineering*, Thi-Qar, 15-16 July 2020, Vol. 928. https://doi.org/10.1088/1757-899X/928/3/032068

[11] Rastenis, J., Ramanauskaitė, S., Janulevičius, J., Čenys, A., Slotkienė, A. and Pakrijauskas, K. (2020) E-Mail-Based Phishing Attack Taxonomy. *Applied Sciences*, **10**, 2363. https://doi.org/10.3390/app10072363

[12] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.