基于数字签名的生鲜水果防伪追溯码设计

王雪，杨慧敏，康静彩，徐晓燕
（东北林业大学 工程技术学院，哈尔滨 150000）

摘要：目的 为了保障消费者对生鲜产品的质量安全诉求，设计生鲜水果的产品追溯标识。**方法** 针对普通二维码易被篡改、伪造等问题，引入数字签名技术，增加算法中素数的数量，同时在签名过程中引入中国剩余定理来提高运算效率，运用中国剩余定理求解包括单基数转换法和混基数转换法，结合费马小定理，分别优化四素数下 RSA 的签名过程，并对比优化前后的签名时间，最后在 python 的运行环境下实现算法。**结果** 优化后的算法签名时间比传统算法平均缩短了 83.8%，并且能够抵抗蛮力攻击、选择密文攻击、出错攻击和连分数攻击等对算法中不同对象的攻击。**结论** 生成了兼顾效率和安全性的防伪追溯码，为消费者购买放心产品提供了保障。

关键词：快速响应码；RSA 数字签名；中国剩余定理；身份认证
中图分类号：F760.3 **文献标识码：**A **文章编号：**1001-3563(2023)05-0149-07
DOI：10.19554/j.cnki.1001-3563.2023.05.019

Design of Anti-counterfeiting Traceability Code for Fresh Fruits Based on Digital Signature

WANG Xue, *YANG Hui-min*, *KANG Jing-cai*, *XU Xiao-yan*

(College of Engineering and Technology, Northeast Forestry University, Harbin 150000, China)

ABSTRACT: The work aims to design a traceability code of fresh fruits to meet consumers' demands for the quality and safety of fresh products. In view of the problems such as ordinary QR codes being tampered and forged, digital signature technology was introduced to increase the number of primes in the algorithm, and the Chinese residual theorem was applied in the signature process to improve the computation efficiency. The Chinese residual theorem was used to solve the existing single radix conversion method and mixed radix conversion method. Combined with Fermat's little theorem, the signature process of RSA under four primes was optimized respectively, and the signature time before and after optimization was compared. Finally, the algorithm was implemented through the Python test algorithm. The signature time under the optimized algorithm was reduced by 83.8% averagely compared with that under the traditional double prime algorithm. The optimized algorithm could resist brute force attacks, choice cipher-text attacks, error attacks and score attacks on different objects in the algorithm. Thus, an anti-counterfeiting traceability code considering efficiency and security is generated, which also provides assurance for consumers in purchasing products.

KEY WORDS: quick response code; RSA digital signature; Chinese residual theorem; authentication

近年来，随着市场经济的快速发展，人们的生活水平和消费能力逐渐提高，食品安全意识不断增强[1]，尤其在新冠疫情持续存在的背景下，追溯生鲜水果种植、包装、运输及销售等各环节的相关信息显得更为紧迫[2]。随着智能手机等高科技的快速发展，以及二维码在使用过程中具有便捷和高效等特点，可

收稿日期：2022−06−06
基金项目：中央高校业务经费（2572016CB11）；校级教育教学研究项目（DGY2020-42）
作者简介：王雪（1998—），女，硕士生，主攻智慧物流。
通信作者：杨慧敏（1980—），女，博士，高级工程师，主要研究方向为智慧物流、冷链物流。

将二维码作为追溯码，成为消费者与生产厂家、运输公司和地方销售等各环节相关联的纽带，能够有效保障产品的质量安全。由于普通二维码的编码算法不具备加密属性，产品在流通过程中会面临信息被篡改造假、商品以假乱真等风险[3]，使消费者在面对问题产品时难以追查根源，最终蒙受损失。

在互联网交易中，RSA 非对称加密算法可以用来加密产品信息，能够防止信息被篡改和伪造，在一定程度上保障产品的安全[4]。在相关研究领域，RSA 算法的安全和运算效率是目前的研究热点[5]。大数分解困难是实现传统 RSA 算法安全、可靠的基础，如果大数被分解，算法的安全将无法得到保障，因此在实际应用中通常会选择增加密钥的长度来提高算法的安全性。由于增加密钥的长度会增加算法的计算难度[6]，因此 RSA 算法容易受到详尽搜索、定时攻击及通用模数攻击等方式的攻击。Jaspin 等[7]采用 AES 和 RSA 双重加密，证明这种方法可增强算法的安全性，可以抵抗一定程度的攻击。Thangavel 等[8]利用四素数方案来提高 RSA 算法的加密程度，方案中将四素数的乘积作为加解密值，但多重素数会增加算法的运算量和空间复杂度。Qjha 等[9]在算法解密过程中运用了中国剩余定理（Chinese Residual Theorem，CRT），实践证明，该方法使多素数 RSA 的签名效率明显提高，但算法中的模数要足够大才能确保安全。Sahu 等[10]提出消除密钥中参数 n 的改进算法，但该方法的安全性和运算效率未得到实践检验，具体结果无法确定。

文中参考国内外学者的研究内容，针对流入市场的生鲜水果，通过数字签名技术设计产品的防伪追溯标识。运用 RSA 数字签名算法结合 SHA512 算法对产品信息进行签名，利用四素数 RSA 算法结合 CRT 来提高签名效率。相较于传统的 CRT 加速 RSA 算法，文中对 CRT 的 2 种不同计算方式分别进行优化，并对比其签名时间，生成可认证的防伪追溯码，以供消费者查验。

1 快速响应码

快速响应码（Quick Response Code，QR Code）能够对汉字进行编码[11]，与传统的一维条码相比，其承载的数据量更大、编码范围更广。由于 QR Code 具有便捷、高效、成本低等特点，自 1994 年 QR Code 被发明以来，已被应用于多种环境，如移动支付、智能交通和农产品溯源等方面。文中认为将其应用于生鲜水果的追溯较为适用。

2 RSA 算法设计优化

2.1 RSA 算法介绍

RSA 算法既可以在信息传播过程中对数据进行加密，又能在身份认证方面实现数字签名[12]。RSA 算法的实现过程：将原文运用单项散列函数（这里采用 SHA–512 函数）生成消息摘要，通过密钥生成、私钥签名和公钥验证过程，可以验证信息的完整性，并确保信息来源，算法实现及认证过程如图 1 所示。

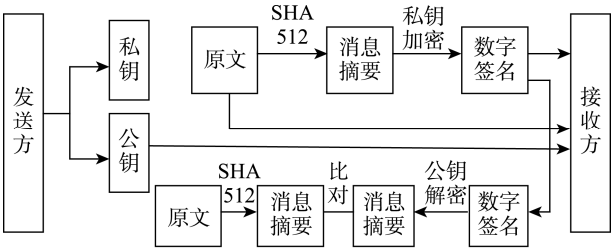


图 1 RSA 数字签名的实现及认证过程
Fig.1 Implementation and authentication process of RSA digital signature

2.2 四素数 RSA 算法

Thangavel 等[13]引入多素数 RSA 来平衡传统算法的安全性和运算效率。文中借鉴这种思想，在四素数的基础上进一步优化 RSA 数字签名算法。在相同条件下，为了降低运算的复杂度，令算法产生的随机素数长度为正常情况下的一半，在增加素数因子数量的同时会增大分解模 n 的难度。算法描述如下。

2.2.1 密钥生成过程

1）随机选出 4 个互不相等的素数 p、q、r、s，计算模 $n(n=p\times q\times r\times s)$，模 n 的欧拉函数 $\varphi(n)=(p-1)(q-1)(r-1)(s-1)$。

2）随机选出正整数 e，令 $1<e<\varphi(n)$、$\gcd(e,\varphi(n))=1$，得到公钥 (e,n)。

3）计算解密密钥 d，令 $ed\equiv 1 \bmod \varphi(n)$，表现为 ed 与 1 关于 $\varphi(n)$ 同余，这里 mod 为求余函数，得到私钥 (d,n)。

2.2.2 签名过程

使用私钥 (d,n) 对明文 M 签名得到密文 C，具体过程如式（1）所示。

$$C = M^d \bmod n \tag{1}$$

2.2.3 验证过程

使用公钥 (e,n) 对密文 C 解密得到新的明文 M_1 计算过程如式（2）所示，比较 M 和 M_1。

$$M_1 = C^e \bmod n \tag{2}$$

式中：M 为明文；C 为密文。

2.3 CRT 加速四素数 RSA 签名

2.3.1 CRT 介绍

CRT 可以将签名过程从指数型模 n 转变为同余方程组的形式[14]，化解大整数的幂乘为小整数的幂乘，显著减少计算时间。利用 CRT 求解包括单基数

转换法（Single-Radex Conversion，SRC）和混基数转换法（Mixed-Radex Conversion，MRC）[15]。文中运用费马小定理结合 SRC 和 MMRC 算法，分别优化四素数下 RSA 的签名过程，并在后文加以验证。

2.3.2　CRT 加速 RSA 签名过程

随机选取 4 个互素的正整数 p、q、r、s，求签名方程 $C=M^d \bmod n$，根据 CRT 的推论[16]，转化为计算模 p、q、r、s 的同余方程组，见式（3）。

$$\begin{cases} C_1 \equiv M^d \bmod p \\ C_2 \equiv M^d \bmod q \\ C_3 \equiv M^d \bmod r \\ C_4 \equiv M^d \bmod s \end{cases} \tag{3}$$

根据费马小定理及推论[17]，转换同余见式（3）。令 $y=d \bmod (p-1)$，则存在正整数 k，满足 $d=k(p-1)+y$，可推导：$C_1 \equiv M^d (\bmod p) \equiv M^{k(p-1)+y} (\bmod p) \equiv (M^{(p-1)} \bmod p)^k M^y (\bmod p)$。由于 $M^{(p-1)}=1 (\bmod p)$，则 $C_1 \equiv 1^k M^y (\bmod p) \equiv (M \bmod p)^{d \bmod (p-1)} (\bmod p)$。同理，可计算 C_2、C_3 和 C_4，求得如下同余方程组，见式（4）。

$$\begin{cases} C_1 \equiv (M \bmod p)^{d_1} \bmod p \\ C_2 \equiv (M \bmod q)^{d_2} \bmod q \\ C_3 \equiv (M \bmod r)^{d_3} \bmod r \\ C_4 \equiv (M \bmod s)^{d_4} \bmod s \end{cases} \tag{4}$$

根据 CRT 和费马小定理的推论[17]，可得式（5）。

$$\begin{aligned} C \equiv & ((M \bmod p)^{d_1} qrs(qrs^{-1} \bmod p) + \\ & (M \bmod q)^{d_2} prs(prs^{-1} \bmod q) + \\ & (M \bmod r)^{d_3} pqs(pqs^{-1} \bmod r) + \\ & (M \bmod s)^{d_4} pqr(pqr^{-1} \bmod s)) \bmod n \equiv \\ & ((M \bmod p)^{d_1} qrs(qrs^{p-2} \bmod p) + \\ & (M \bmod q)^{d_2} prs(prs^{q-2} \bmod q) + \\ & (M \bmod r)^{d_3} pqs(pqs^{q-2} \bmod r) + \\ & (M \bmod s)^{d_4} pqr(pqr^{q-2} \bmod s)) \bmod n \equiv \\ & (a_1 B_1 + a_2 B_2 + a_3 B_3 + a_4 B_4) \bmod n \end{aligned} \tag{5}$$

2.3.3　四素数下优化后的 SRC 签名算法

1）计算 $d_1=d \bmod (p-1)$, $d_2=d \bmod (q-1)$, $d_3=d \bmod (r-1)$, $d_4=d \bmod (s-1)$。

2）计算 $m_1=M \bmod p$, $m_2=M \bmod q$, $m_3=M \bmod r$, $m_4=M \bmod s$。

3）计算 $a_1=m_1^{d_1} \bmod p$, $a_2=m_2^{d_2} \bmod q$, $a_3=m_3^{d_3} \bmod r$, $a_4=m_4^{d_4} \bmod s$。

4）计算 $B_1=qrs^{-1} \bmod n$, $B_2=prs^{-1} \bmod n$, $B_3=pqs^{-1} \bmod n$, $B_4=pqr^{-1} \bmod n$。

5）计算 $C=(a_1 B_1 + a_2 B_2 + a_3 B_3 + a_4 B_4) \bmod n$。

利用 MRC 求解同余方程组，见式（1），得到三角形数值，令 $a_{i1}=a_i$，根据递归公式：$a_{i(j+1)}=(a_{ij}-a_{jj})B_{ji} (\bmod p_i)$，计算得到斜边上的数值 a_{11}、a_{22}、a_{33}、a_{44}，再由 MMRC 得到另一个快速 RSA 签名算法。

2.3.4　四素数下优化后的 MMRC 签名算法

1）计算 $d_1=d \bmod (p-1)$, $d_2=d \bmod (q-1)$, $d_3=d \bmod (r-1)$, $d_4=d \bmod (s-1)$。

2）计算 $m_1=M \bmod p$, $m_2=M \bmod q$, $m_3=M \bmod r$, $m_4=M \bmod s$。

3）计算 $a_1=m_1^{d_1} \bmod p$, $a_2=m_2^{d_2} \bmod q$, $a_3=m_3^{d_3} \bmod r$, $a_4=m_4^{d_4} \bmod s$。

4）计算 $B_{12}=p^{-1} \bmod q$, $B_{13}=p^{-1} \bmod r$, $B_{23}=q^{-1} \bmod r$, $B_{14}=p^{-1} \bmod s$, $B_{24}=q^{-1} \bmod s$, $B_{34}=r^{-1} \bmod s$。

5）计算 $C=a_1+a_2 \times p+a_3 \times pq+a_4 \times pqr$。

3　追溯码生成和认证方案

文中方案的总体思路：采用优化后的 RSA 算法结合二维码技术，实现追溯码的生成和认证过程，追溯码生成和认证流程如图 2 所示。在实际运用中，生产商在确定明文后需通过哈希函数生成摘要，文中使用 SHA–512 单项散列函数，该函数具有单向性、抗碰撞性和雪崩性等特性[18]，可将任意长度的明文压缩成 512 bit 的消息摘要，且比其他哈希函数的安全性更高，因此文中运用 SHA–512 结合 RSA 来实现数字签名。生成和认证实现过程主要从生产商角度和消费者的角度进行描述。

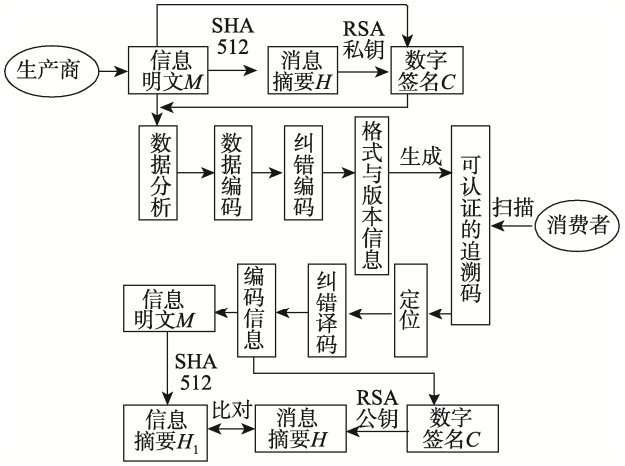


图 2　追溯二维码生成、认证流程
Fig.2 Flowchart for generation and authentication of traceability QR code

3.1　生产商主要操作过程

1）生鲜水果生产商确定各批次商品信息，并作为信息明文 M，使用 SHA512 算法将明文 M 转换成消息摘要 H，对消息摘要 H 用私钥 (d,n) 签名得到 C。

2）将明文 M 与签名 C 结合作为二维码的编码信息，经历二维码的生成过程（如图 2 所示）生成可认证的追溯二维码。

3）生产商将生成的追溯码贴在各批次生鲜水果的追溯单元包装上，此时商品满足可追溯条件，可流入市场中。

3.2　消费者的主要操作过程

1）消费者在购买产品时，可通过手机软件（如微信等）扫描追溯码，得到明文信息 M 和签名 C。

2）接下来消费者可进行在线验证，验证流程如图 3 所示。由于 RSA 算法的优化方式不同，文中算法生成的追溯码只能通过相应的验证函数进行验证，其他方法生成的追溯码无法利用该验证函数进行验证，因此当消费者无法在系统中验证购买产品的追溯码时，该商品为假冒商品。若可以验证，系统的具体操作过程：利用企业对外公布的公钥 (e,n) 对签名 C 解密，获得 H，再使用相同的 SHA512 函数提取信息明文 M，得到 H_1。

3）对比 H 和 H_1，若两者不同，则说明追溯码中的明文信息已被篡改，为假冒商品；若相同，则表明该商品为真品；若出现安全问题，则可进一步向产品负责人追责，此时责任人无法躲避其应承担的相关责任。

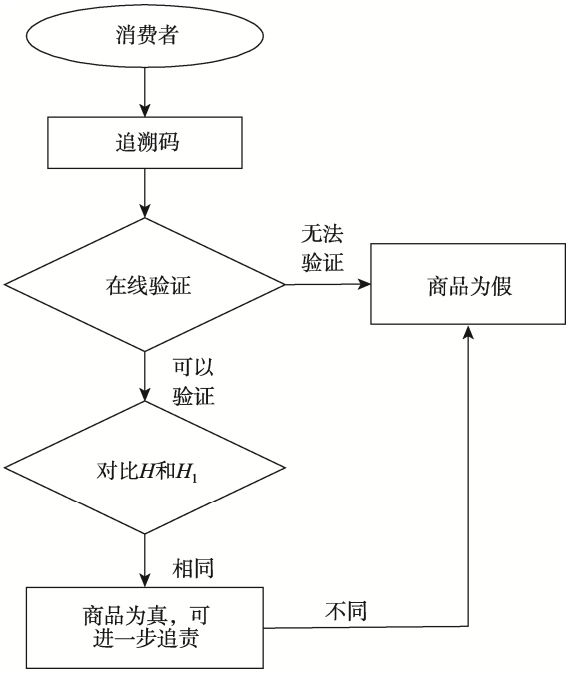


图 3　消费者的验证流程

Fig.3 Flowchart of verification by consumer

4　算法实现

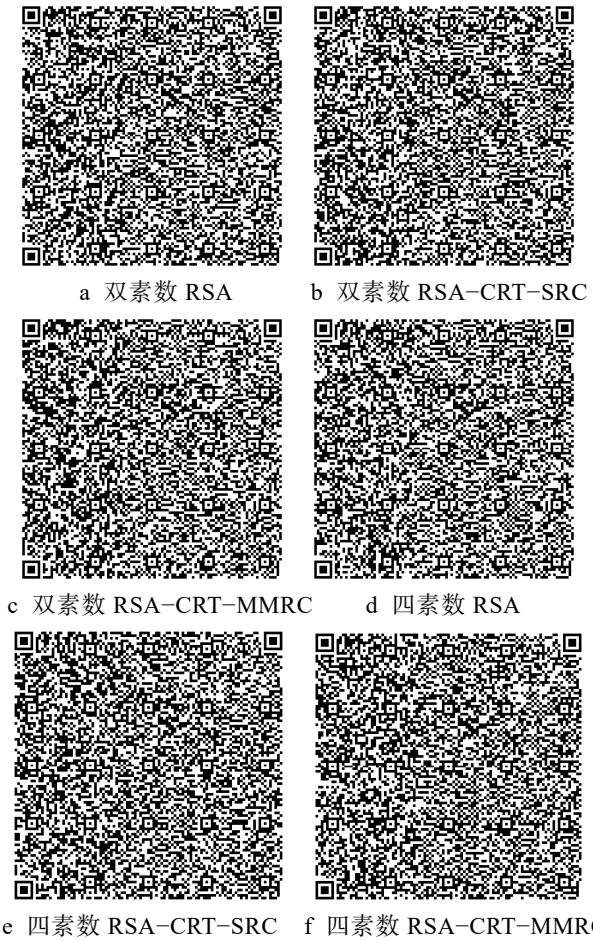
文中的追溯对象为黑龙江省伊春市友好蓝莓基地的蓝莓。蓝莓果实在夏季成熟，采摘后易失水发皱、不耐贮，因此会大大缩短销售时间[19]，对其信息进行追溯，可增加下一环节生产商或消费者的信任程度。文中算法在 python 的运行环境下通过 visual studio code 平台实现，运用 hashlib 库、qrcode 库和 zxing 解析库实现追溯码的生成和识别。蓝莓生产商将蓝莓采摘分装后，会将生成的带有签名的追溯码贴在盒装蓝莓上，下一环节的加工商或消费者可通过智能手机 APP（如微信）进行读取和验证。

密钥长度是制约签名运算效率和安全性的直接影响因素，利用数域晒法（Number Field Sieve，NFS）对 RSA 进行整数分解是当前使用较广泛的方法之一。目前已成功利用 NFS 分解了 RSA−768[20]，因此文中在平衡二者情况的同时考虑了追溯码的实际使用环境，将密钥长度设置为 1 024 bit，在执行如图 4 所示的代码后，可直接生成追溯码。文中分别将优化前后的算法生成了追溯码（如图 5 所示），生成的追溯码版本统一为 20，纠错编码默认为 M。以图 5e 中的追溯码为例，消费者扫描追溯码后，会看到如图 6 所示的“明文丨签名”形式。若要进一步验证真伪并追责，消费者可登录企业官方网站或微信公众号验证，出现问题时凭此签名向责任人追责。签名验证界面如图 7 所示。

```
(base) guoqin@guoqindeMacBook-Air code % python rsa.py
(base) guoqin@guoqindeMacBook-Air code %
```

图 4　追溯码生成执行代码

Fig.4 Execution code generated by traceability code



a 双素数 RSA　　b 双素数 RSA−CRT−SRC

c 双素数 RSA−CRT−MMRC　　d 四素数 RSA

e 四素数 RSA−CRT−SRC　　f 四素数 RSA−CRT−MMRC

图 5　蓝莓追溯码

Fig.5 Blueberry traceability code

图 6　手机微信扫描结果
Fig.6 Scanning results by WeChat on mobile phone

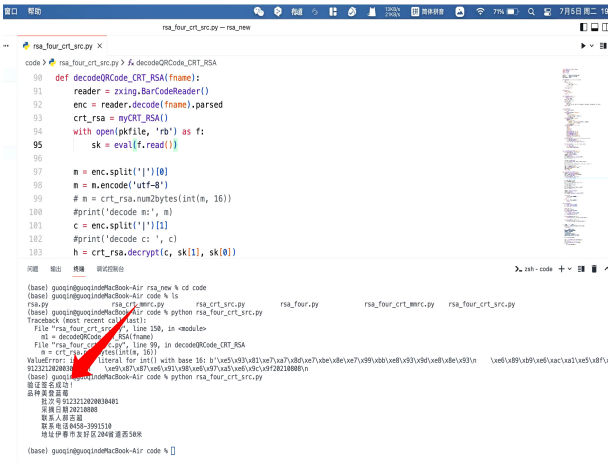


图 7　系统验证
Fig.7 System verification

5　算法验证

算法运行环境：Windows 10，CPU 2.50 GHz，RAM 4G，通过 visual studio code 操作平台测试。在模数 n 一致的情况下，测试几种不同密钥长度下 RSA 算法优化前后的签名时间，并对其安全性进行分析。

5.1　签名时间对比

文中不仅比较了双素数和四素数的签名时间，同时还进一步比较了在中国剩余定理加速情况下，优化后 SRC 和 MMRC 的签名时间（如表 1 所示），并将运用 CRT 优化前后的签名时间及 CRT 中不同计算方式的签名时间进行了对比，用折线图直观地表示出来，如图 8—9 所示。

由图 8 可以明显看出，运用中国剩余定理加速后 RSA 算法的签名时间相较于普通签名时间明显缩短。其中，双素数平均缩短 67.3%，加速后四素数 RSA 签名算法时间的优势更大，平均缩短了 83.8%，中国剩余定理加速后的四素数签名时间相较于双素数，平均缩短了 52.6%。根据图 9 可知，优化后 SRC 和 MMRC 的签名时间实际上无太大差别。综上可知，无论是 CRT 的哪种计算方式，企业选用四素数 RSA 算法相较于双素数在签名时间方面优势更明显。

5.2　安全性分析

传统 RSA 算法的安全性以大整数分解困难为基础，实验表明，当素数较小时，四素数 RSA 算法蛮力分解时间平均是双素数的 2.957 倍；素数长度不断增加，蛮力攻击耗费时间将会更长[3]。随着 RSA 算法的不断优化，在不同情况下出现了不同的攻击方式。由此，文中运用 5 种攻击方式对算法可能受到的攻击进行了安全分析，具体过程如表 2 所示。

表 1　算法签名时间对比
Tab.1 Comparison of algorithm signature time

密钥长度/bit	签名时间/s					
	双素数	双素数 CRT−SRC	双素数 CRT−MMRC	四素数	四素数 CRT−SRC	四素数 CRT−MMRC
1 024	0.001 0	0.000 4	0.000 4	0.001 1	0.000 3	0.000 2
2 048	0.006 2	0.002 0	0.002 0	0.006 1	0.000 9	0.000 9
3 072	0.020 3	0.005 8	0.005 7	0.018 5	0.002 0	0.002 1
4 096	0.041 1	0.012 3	0.012 2	0.042 0	0.0043	0.004 4

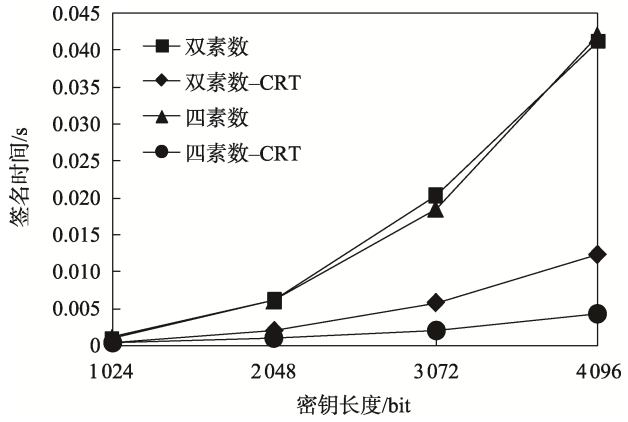


图 8 CRT 影响下签名时间对比
Fig.8 Comparison of signature time under CRT influence

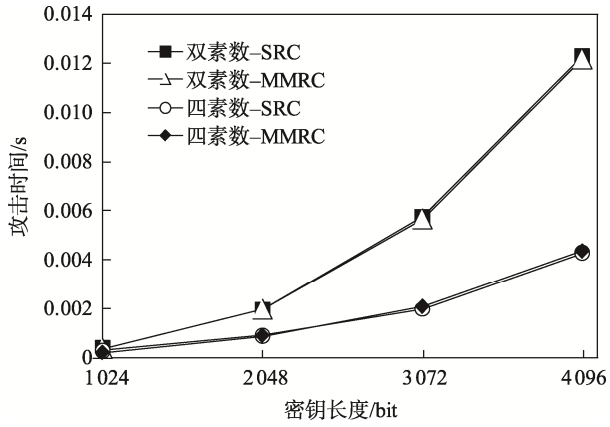


图 9 SRC 和 MMRC 签名时间对比
Fig.9 Comparison of SRC and MMRC signature time

表 2 不同攻击方式下算法安全性分析
Tab.2 Algorithm security analysis under different attack modes

攻击方式	攻击对象	攻击过程	安全性分析
蛮力攻击	模数 n	分解模 n，计算出私钥 d，进而伪造签名	目前已有研究中分解 512 bit 的整数需 8 个月，可知模数达到 1 024 bit 时，综合考虑分解时间和成本可知信息加密是安全的
选择密文攻击	生成的签名 C	通过选择一段密文骗取签名，或伪造合法消息，拼凑出需要的签名	文中并非对消息直接签名，而是对 SHA512 生成的消息摘要进行签名，根据哈希函数的特性，该攻击方式很难实现
对哈希函数攻击	SHA512	利用生日攻击、穷举攻击等方法找到与明文 M 生成摘要相等的信息	文中运用的 SHA512 的安全性较高，攻击者找到合适信息的复杂度过大，目前无法实现
出错攻击	CRT	传统双素数 CRT−RSA 情况下，若求 C_p 时发生错误，则会产生错误的签名 C^*，此时可求出 $q=\gcd(C^*-M \bmod n,n)$	文中运用四素数 CRT−RSA，若签名过程 C_p 出错，求得四素数中除 p 外剩余三素数的乘积：$qrs=\gcd(C^*-M \bmod n,n)$，无法得到其中的素数，因此无法分解模 n
连分数攻击[21]	四素数 CRT−RSA	根据 $ed\equiv 1 \bmod \varphi(n)$ 得到差值百分比 $\delta=1-\frac{p-1}{n}-\frac{1}{kn}$，满足 $\delta<\frac{1}{(3/2)n_m d_m}$ 才能通过连分数算法找到 k 和 d_p。	满足 $kd_p<\frac{2n}{3(n-p+1-1/k)}$，由于 n 和 p 都是大素数，可忽略 $1-1/k$，同时除以 n 得到 $kd_p<\frac{2}{3}\times\frac{1}{1-1/qrs}\approx\frac{2}{3}$，此时 k 必须小于 1，与 k 为正整数矛盾，因此攻击无效

可以看出，优化后的四素数 RSA 算法的安全性较高，在运用不同攻击方式对算法中不同对象进行攻击时都难以实现，可以作为追溯码，在产品追溯过程中的安全性得到保证。

6 结语

设计了一种针对冷链生鲜水果的防伪追溯码。为了解决 RSA 算法的运算效率问题和整数 n 易被分解的安全问题，将算法中的双素数增加到四素数，并分别结合优化后的 SRC 和 MMRC 对签名过程中的模幂运算进行了优化，最后将明文信息与签名拼接生成了可认证的防伪追溯码，消费者或下一环节的生产商可通过扫描追溯码验证信息。通过测试证实优化后的算法可明显提高签名效率，平均缩短了 83.8%，且能够抵抗一些常见的攻击。综上可知，该追溯码相较于传统追溯码，兼顾了效率和安全性，企业可运用此码，并添加自身独有的防伪图层或防伪底纹，来增强企业口碑和消费者的信任，具有一定的推广和实用价值。

参考文献：

[1] 王建强, 陈景华, 郝发义, 等. 冷链物流对鲜肉新鲜度的影响及智能检测[J]. 包装工程, 2022, 43(1): 148-157.
WANG Jian-qiang, CHEN Jing-hua, HAO Fa-yi, et al. Effects of Cold Chain Logistics on Meat Freshness and Intelligent Detection[J]. Packaging Engineering, 2022, 43(1): 148-157.

[2] PANEBIANCO S, MAZZOLENI P, BARONE G, et al. Feasibility Study of Tomato Fruit Characterization by Fast XRF Analysis for Quality Assessment and Food Traceability[J]. Food Chemistry, 2022, 383: 132364.

[3] QIAN Jian-ping, XING Bin, ZHANG Bao-hui, et al. Optimizing QR Code Readability for Curved Agro-Food Packages Using Response Surface Methodology to Improve Mobile Phone-Based Traceability[J]. Food Packaging and Shelf Life, 2021, 28: 100638.

[4] 周金治, 高磊. 基于多素数和参数替换的改进 RSA 算法研究[J]. 计算机应用研究, 2019, 36(2): 495-498.
ZHOU Jin-zhi, GAO Lei. Research on Improved RSA Algorithm Based on Multi-Prime Number and Parameter Substitution[J]. Application Research of Computer, 2019, 36(2): 495-498.

[5] SEO J H. Efficient Digital Signatures from RSA without Random Oracles[J]. Information Sciences, 2020, 512: 471-480.

[6] SWAMI B, SINGH R, CHOUDHARY S. Dual Modulus RSA Based on Jordan-Totient Function[J]. Procedia Technology, 2016, 24: 1581-1586.

[7] JASPIN K, SELVAN S, SAHANA S, et al. Efficient and Secure File Transfer in Cloud through Double Encryption Using AES and RSA Algorithm[C]// 2021 International Conference on Emerging Smart Computing and Informatics (ESCI) Pune, India IEEE, 2021: 791-796.

[8] THANGAVEL M, VARALAKSHMI P, MURRALI M, et al. An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)[J]. Journal of Information Security and Applications, 2015, 20(C): 3-10.

[9] QIHA N, PADHYE S. Cryptanalysis of Multi Prime RSA with Secret Key Greater than Public Key[J]. International Journal of Network Security, 2014, 16(1): 53-57.

[10] SHAU J, SINGH V, SAHU V, et al. An Enhanced Version of RSA to Increase the Security[J]. Journal of Network Communications and Emerging Technologies, 2017, 7(4): 1-4.

[11] ZHAO Xiao-hai, YANG Sheng-du, DENG Jian-guo, et al. Reversibly Stealth QR Code Based on *N*-Methylmaleimide-Vinyl Acetate Copolymers under the Condition of Acid-Base Change[J]. Reactive and Functional Polymers, 2022, 174: 105241.

[12] 蔡群英. 基于数字签名和加密二维码技术的电子投票系统的实现[J]. 现代计算机, 2020(20): 100-103.
CAI Qun-ying. Implementation of Electronic Voting System Using the Techniques of Digital Signature and Encrypted Two-Dimensional Code[J]. Modern Computer, 2020(20): 100-103.

[13] THANGAVEL M, VARALAKSHMI P, MURRALI M, et al. An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)[J]. Journal of Information Security and Applications, 2015, 20(C): 3-10.

[14] 廖彬宇, 陈旭, 赖晓风. RSA 大整数分解算法[J]. 内江师范学院学报, 2019, 34(2): 63-66.
LIAO Bin-yu, CHEN Xu, LAI Xiao-feng. RSA Large Integer Decomposition Algorithm[J]. Journal of Neijiang Normal University, 2019, 34(2): 63-66.

[15] 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.
FANG Wen-he, LI Guo-he, WU Wei-jiang, et al. Optimization of RSA Encryption Algorithm for Android Mobile Phone and Design of QR Code Encryption Security System[J]. Computer Science, 2017, 44(1): 176-182.

[16] XU Ze-shui, LIAO Hu-chang. A Survey of Approaches to Decision Making with Intuitionistic Fuzzy Preference Relations[J]. Knowledge-Based Systems, 2015, 80: 131-142.

[17] LIU Cheng-lian, CHANG Chin-chen, WU Zhi-pan, et al. A Study of Relationship between RSA Public Key Cryptosystem and Goldbach's Conjecture Properties[J]. Int J Netw Secur, 2015, 17: 445-453.

[18] 孙秀丽. 接收方不可抵赖的数字签名方案[J]. 电脑知识与技术, 2008, 4(34): 1721-1722.
SUN Xiu-li. A Specific Function-both of the Transistor and Receiver Non-Repudiation Signature Program[J]. Computer Knowledge and Technology, 2008, 4(34): 1721-1722.

[19] 瞿光凡, 杨玲辉, 巴良杰, 等. 采前喷施复合保鲜液对蓝莓贮藏品质的影响[J]. 包装工程, 2021, 42(15): 65-71.
QU Guang-fan, YANG Ling-hui, BA Liang-jie, et al. Effect of Preharvest Spraying of Composite Preservation Liquid on Postharvest Blueberry Storage Quality[J]. Packaging Engineering, 2021, 42(15): 65-71.

[20] 叶秀芳. RSA 算法的优化策略[J]. 电子设计工程, 2017, 25(20): 83-85.
YE Xiu-fang. An Optimization Strategy of RSA Algorithm[J]. Electronic Design Engineering, 2017, 25(20): 83-85.

[21] 肖振久, 胡驰, 陈虹. 四素数 RSA 数字签名算法的研究与实现[J]. 计算机应用, 2013, 33(5): 1374-1377.
XIAO Zhen-jiu, HU Chi, CHEN Hong. Research and Implementation of Four-Prime RSA Digital Signature Algorithm[J]. Journal of Computer Applications, 2013, 33(5): 1374-1377.

责任编辑：彭颋