TrustZone 架构下基于优化 RSA 的食品追溯可信采集方法

王朝阳 汪颢懿* 左 敏 张青川
(北京工商大学农产品质量安全追溯技术及应用国家工程实验室 北京 100048)

摘 要 针对食品安全追溯数据在上传服务器前易遭到篡改的问题,在 TrustZone 架构基础上,利用时间戳认证等技术搭建可信执行环境,同时引入 Rabin、霍夫曼编码和随机分量,构建 TrustZone 架构下基于优化 RSA 的食品追溯可信采集方法。实验结果表明,该方法可以高效、安全地对食品追溯数据进行加密,防止篡改,并且提高加密速度,降低文件量级。

关键词 食品安全追溯 可信采集方法 TrustZone

中图分类号 TP309 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2022.07.049

RELIABLE COLLECTION METHOD FOR FOOD TRACEABILITY BASED ON OPTIMIZED RSA IN THE TRUSTZONE FRAMEWORK

Wang Zhaoyang Wang Haoyi* Zuo Min Zhang Qingchuan
(*National Engineering Laboratory for Agri-product Quality Traceability, Beijing Technology and Business University, Beijing 100048, China*)

Abstract Aiming at the problem that food safety traceability data is very likely to be tampered before being uploaded to the server, this paper adoptd technologies such as timestamp authentication to build a trusted execution environment based on the TrustZone framework. It introduced Rabin, Huffman coding, and random components to construct a reliable collection method for food traceability based on optimized RSA in the TrustZone framework. Experimental results show that this method can efficiently and securely encrypt food traceability data, prevent tampering, improve encryption speed, and reduce file magnitude.

Keywords Food safety traceability Reliable collection method TrustZone

0 引 言

随着人民生活水平的不断提高,消费者对食品品质以及安全的要求也越来越高,大众对食品的关注点已经转变为食材的源头,食品加工过程、仓储、运输等。同时近年来食品安全问题频发,从最早的三聚氰胺、地沟油到现如今的台湾“塑化剂”风波、湖南大米镉元素超标、天津独流调料造假等事件,当前食品安全隐患愈发严重。另一方面,大多数食品对于加工、运输、仓储等环节中的温度、湿度、光强等环境因素有较高要求,一旦这些因素未达标,食品变质的可能性增大,若这样的食品流向市场,将会严重危害公众的健康。因此,亟需采用安全、可信、透明的食品安全溯源系统来加强对食品产业链的监管与效率,提高食品安全水平,保障国民饮食健康。随着信息科学的飞速发展,在食品安全溯源系统中融入智能技术、物联网技术,极大地促进了我国食品安全溯源体系的发展,使得公众能参与到食品安全监管中。在服务器端,以去中心化的分布式结构应用、不可篡改的时间戳、安全信任机制为核心的区块链技术成为了信息技术的研究热点。区块链具有去中心化、唯一性、自治性、不可篡改性、匿名性等特性[1],是目前搭建食品安全追溯系统的不二之选,在实现追溯透明化的同时可以有效地保证服务器端的数据安全性。

但是,区块链等技术并不能保证追溯信息在上“链”前的数据安全,若追溯信息在上传至服务器端前

收稿日期:2020-02-24。国家重点研发计划项目(2016YFD0401205);北京市自然科学基金项目(4202014);教育部人文社会科学研究青年基金项目(17YJCZH007)。**王朝阳**,硕士生,主研领域:食品安全追溯,区块链,大数据。**汪颢懿**,实验师。**左敏**,教授。**张青川**,副教授。

就遭到篡改,后续的追溯过程将毫无意义。为此,如何杜绝企业上传虚假或被篡改的追溯信息已经是目前亟需解决的问题。针对这一问题,本文设计实现了一种 TrustZone[2-3] 架构下基于优化 RSA 的食品追溯可信采集方法,利用可信执行环境、时间戳、非对称加密算法等技术,并设计加密机制,可部署在养殖场、运输车辆、销售货柜等嵌入式环境,对上传至服务器端前的追溯数据提供安全保障。此外,由于食品安全追溯数据量极大,且嵌入式环境硬件计算能力有限,运算速度较慢,为了防止出现数据堆积的问题,本文对 RSA 算法进行优化,在保证安全性的同时提高运算速度。

1　相关工作

1.1　国内外研究现状

针对攻击者在数据采集端的窃取、篡改、破坏等恶意行为,国内外已有研究者基于国产密码算法、ARMA 的无线传感器网络、数字水印等技术,展开研究并提出了可行的防护方案。冯云等[4]提出了基于国产密码算法的可信计算体系,将基于国产密码算法的可信技术应用于采集终端的安全加固。王海元等[5]提出了基于 ARMA 的无线传感器网络可信数据采集方法,在保证采集数据的高度可信的同时显著提高了网络的整体性能。李红涛等[6]提出了一种全新的数字水印嵌入方法,保障涉密图像在传输过程中的安全性、可靠性和完整性。Zhao 等[7]利用静态随机存取存储器在不添加安全硬件的前提下生成可信根,来得到加密数据的安全密钥,通过将加密后的数据存储在系统硬件上来保证数据安全。Hein 等[8]设计实现了一种基于安全密钥和 Merkle-Tree 认证加密的安全设备,可有效防止攻击者对数据的篡改、窃取、破坏。

1.2　非对称加密算法

非对称加密算法中包含公开密钥(Public Key,PK)和私有密钥(Private Key,SK)。公钥与私钥是一对,如果用公钥对数据进行加密,只有用对应的私钥才能解密,非对称加密算法强度复杂,安全性主要由算法和密钥管理决定。对称密码体制则是单一密钥,并且是非公开的,所以保证其安全性就是保证密钥的安全,但在解密时必须将密钥向对方公开,而非对称密钥体制有两种密钥,其中一个是公开的,这样就可以不需要像对称密码那样将密钥传输给对方,确保了密钥对的安全性,因此非对称加密算法安全性更好。本文列出了 RSA、DSA、ECC、RABIN 这 4 种目前应用最多的非对称加密算法[9-13],并从成熟度、安全性、运算速度、资源消耗等特点进行对比,对比结果如表 1 所示。

表 1　算法对比结果

名称	成熟度	安全性	运算速度	资源消耗
RSA	高	高	慢	高
DSA	中	高	慢	中
ECC	低	高	中	低
RABIN	高	高	慢	高

2　TrustZone 架构下的食品追溯可信采集方法

本文设计的 TrustZone 架构下的食品追溯可信采集方法主要包括数据采集层、加密层、存储三部分。通过设计基于非对称加密算法和时间戳的加密机制,在可信执行环境中对追溯信息进行加密,以确保追溯信息的可信性。

2.1　数据采集类型

追溯数据采集,是指从传感器和其他待测设备等模拟和数字被测单元中自动采集追溯信息(非电量或者电信号),送到上位机中进行分析、处理。由于传统的采集系统存在响应慢、精度低、可靠性差、效率低、操作繁琐等弊端,已经不能完全适应当前追溯领域的需求。如今嵌入式技术已经相对成熟,因此,基于嵌入式的追溯信息采集设备是目前最优的选择方案。经过对现有的食品安全追溯领域的调研,本文对追溯环节以及数据类型进行了总结,并确定了本文方法所采集的数据类型;食品安全追溯可以分为生产环节、仓储环节、运输环节三部分,具体追溯对象以及追溯信息如表 2 所示。

表 2　追溯对象与追溯信息

追溯环节	追溯对象	追溯信息
生产环节	原料,添加剂	名称、生产日期、数量、规格、保质期等
	加工环境	生产地点、责任人员信息、环境信息等
	产品信息	产品名称、规格、生产日期、保质期等
仓储环节	仓储环境	仓储地点、责任人员信息、环境信息
	物流信息	物流公司信息、驾驶员信息、车辆信息
运输环节	运输环境	运输路线、责任人员信息、环境信息

2.2　方法与加密机制设计

本文方法所需的硬件设备主要包括:电源、ARM

核心控制模块、传感器、存储设备等模块,系统框架如图 1 所示。通过调用温度传感器、湿度传感器、位置传感器、光强传感器、气压传感器等传感器对食品追溯环境中的环境信息进行数据采集。采集到的追溯数据在 ARM 核心控制模块中由 CA 端传入 TA 端,在 TrustZone 技术构建的可信执行环境中,通过基于时间戳和优化后的非对称加密算法的加密机制,对数据加密,最后将追溯信息与密文共同存储。在上传至服务器前,可通过公钥对数据进行解密验证,进一步确保数据的可信性。由于全部加密过程均在可信执行环境中进行,不仅可以确保私钥的可信性,由于私钥存放在安全的永久存储器中,还可以防止遭受来自外界攻击者的窃取与篡改。

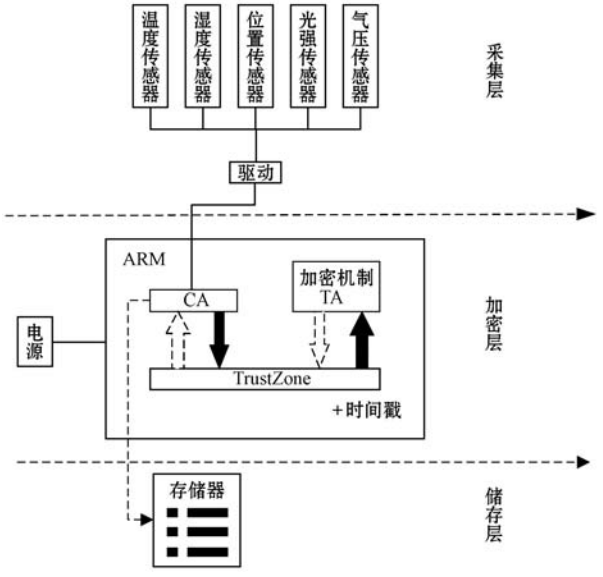

图 1 系统框架

在追溯过程中,追溯信息通常由数据、采集时间两部分构成。对于传统的追溯系统,不法分子可以在数据上传服务器或区块链之前,在本地对追溯数据以及采集时间进行篡改,以此来欺骗公众及监管部门,对此文章将通过加密机制来保证追溯信息的可信性以及时效性(时间的递推)。加密机制如图 2 所示。

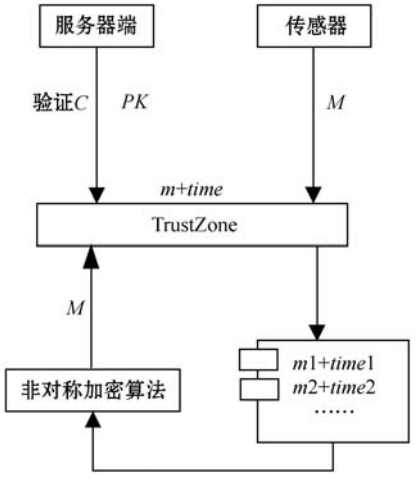

图 2 加密机制设计

(1) 在可信执行环境内生成公钥私钥对(*PK*, *SK*),私钥将永久存储在可信执行环境中。

(2) 将传感器采集到的追溯信息(*m*)传输至可信执行环境。

(3) 在可信执行环境内对追溯信息加盖时间戳(*time*),以确保追溯信息中时间参数的单一性。

(4) 加盖时间戳的若干条追溯信息将在内存中组成数据块,等待处理。

(5) 使用非对称加密算法,通过私钥对追溯信息进行加密。

(6) 将原始追溯信息、时间戳、密文组成新的追溯信息(*M*),并进行存储。

(7) 在上传至区块链或服务器前,需要用公钥(*PK*)对密文(*C*)进行验证,以确保追溯信息上链前的可信性。

2.3 基于 TrustZone 技术的方法实现

TrustZone 是 ARM 提出的一种提供基于硬件的隔离机制,为需要高安全性的代码构建安全可靠的环境[14-15]。它将系统的硬件和软件资源分为两部分,一个是可信执行环境,另一个是普通环境。所有的敏感操作都应该在可信执行环境中被保护,其余安全性要求较低的操作在普通执行环境中执行,例如 Rich OS 和大多数应用程序。核心状态由安全配置寄存器(SCR)中的 NS 位区分,NS 位只能由安全核心修改。通过安全监控呼叫(SMC),无论在何种环境中,它都可以进入监控模式并切换到其他环境。

2.3.1 可信执行环境

可信执行环境(Trusted Execution Environment, TEE)[16-17]首先由 Global Platform(GP)提出,并制定技术规范,它是与设备上的 Rich OS(通常是 Android 等)并存的运行环境,并且给 Rich OS 提供安全服务。可信执行环境可分为硬件层与软件层两部分,其中软件层包括系统层、接口层、应用层,如图 3 所示。TEE 所需的软硬件资源通过 TrustZone 技术与 Rich OS 分离,为了保护 TA 的资源和数据的保密性,完整性和访问权限,安全性需求较高的应用(可信应用,TA)需要在 TEE 中得到授权后才能通过客户端应用(CA)端进行调用,每个 TA 是相互独立的,而且不能在未授权的情况下互相访问。为了保证 TEE 本身的可信根,TEE 在安全启动过程中是要通过验证并且与 Rich OS 隔离[18]。

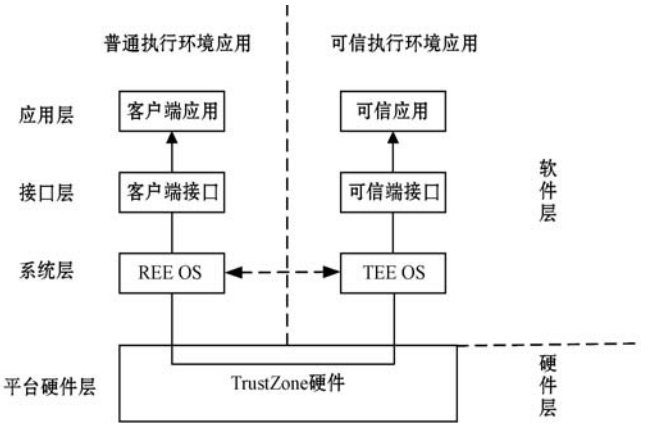

图 3　可信执行环境框架

TEE 内部 API 主要包含了密钥管理、密码算法、安全存储、安全时钟资源和服务,还有扩展的可信 UI 等 API。可信 UI 是指当有关涉密或关键信息需要显示或输入时,显示器和键盘等硬件资源将全部由 TEE 接管,Rich OS 中的应用不能对其进行访问。在进行 TA 程序开发时,TEE 内部 API 是提供给 TA 的编程接口,而 TEE 外部 API 则是让运行在 Rich OS 中的 CA 访问 TA 服务和数据的底层通信接口。

2.3.2　时间戳认证

在传统的食品安全追溯领域中存在这样一种现象,有一些不法分子在篡改食品安全追溯信息时,通过伪造数据中的时间信息等方法,使用篡改后的数据对真实信息进行覆盖,来欺骗数据库以及数据认证。针对这一问题,本文将根据 TrustZone 的内置时钟,对追溯信息加盖无法篡改的时间戳,进一步确保追溯信息的可信性。

时间戳是指一个能表示一份数据在某个特定时间之前已经存在的、完整的、可验证的数据,通常是一个字符序列,唯一地标识某一刻的时间。基于 TrustZone 技术的可信执行环境具有自己独特的时间机制,该时钟具有唯一且连贯性。在可信执行环境中,当可信时钟源产生中断或某些受监控的系统行为发生时都将会触发安全指令,任何对时间信息的篡改、插入或删除都将被系统拒绝,以保证系统内全部数据时间的真实性以及时序单一性,因此即使攻击者侵入可信执行环境或破解了密钥对,也无法对已经加盖时间戳的追溯数据进行篡改。本文将使用绝对时间戳,以便用户以及监管部门在服务器端的食品安全追溯系统中通过时间信息对系统中的数据进行检索。

2.3.3　加密机制的实现

在 OP-TEE 中进行 TA 程序的编写,实现追溯信息加密。

(1) 在 TA 中使用 Privkey Generator 生成密钥对,并将私钥永久存储在 TA 中。

(2) 创建 CA-TA 通话,将追溯信息传入 TA 端,并使用 command ID 调用 TA 端的加密程序。

(3) 应用 TrustZone 技术中可信执行环境时间不可篡改这一特点,为追溯信息加盖时间戳。

(4) 加盖时间戳的追溯信息将在内存中暂时存储,每当数据累计至 256 KB 时将组成一个数据块。

(5) 使用优化后的加密算法对追溯信息进行加密。

(6) 将原始追溯信息、时间戳、密文组成新的追溯信息,并传回 CA 端进行存储。

(7) 将公钥存入数据库或区块链的智能合约中,在数据传入服务器前进行验证。

3　非对称加密算法的选取与优化

3.1　加密算法的选取

在嵌入式环境下,开发难度较高,因此需要选择安全性高且更加成熟的非对称加密算法,便于根据具体的应用需求做进一步优化。另一方面,嵌入式环境下硬件水平较低,而且由于非对称加密算法较为复杂,使得其运算速度较慢,系统负载过大,资源消耗问题比较严重。因此需要针运算效率、密文大小、资源需求等方面对算法进行优化。通过对比表 1 中 RSA、DSA、ECC、RABIN 四种算法,根据成熟度、安全性、运算速度、资源消耗等特点,最终选择 RSA 算法。

3.2　算法优化

针对嵌入式环境下运算能力较差,食品安全追溯信息量较大,追溯平台负载较重等问题,本文中将引入 Rabin 算法、霍夫曼编码和随机分量 s,对 RSA 算法进行优化。

3.2.1　霍夫曼编码

为了提高加密速度,可以使用霍夫曼编码[19]来对数据进行压缩,它是一种用于无损数据压缩的算法,可以从压缩数据中精确恢复原始数据。该算法用于压缩数据(符号或字母)以生成可变长度代码而不是每个符号的固定长度代码。该算法通过对内容中符号或字母的统计分析以构造频率表,并通过频率表来构建霍夫曼树,用于每个符号分配其适当的代码长度。在数据文件上应用霍夫曼编码将生成两个文件:二进制文件(B)和头文件(H)。二进制文件取决于用于检索原

始数据的头文件,因此,如果头文件丢失,则无法检索真实数据。头文件包含原始数据文件的所有符号或其相应的 ASCII 代码。头文件包含为其出现分配的唯一符号,其中没有符号重复两次,二进制文件包含每个符号的代码。例如原文:Beijing Technology and Business University,e 表示为 110,t 表示为 010 等。

头文件为:

\u00bd\u00b4\u00d1\u00e7\u00ef\u00e0\u00e2\u00b2\u00a9\u0082\u00d1\u0088\u0094\u00d3\u0091\u00c4\8

二进制文件为:

000010011011110110110100000000101101000111100011100001011111011111111000001110001010110010101010010000011010000010110100011000100010010100101000111001000111000100010111000001110000

要解压缩消息,通过头文件来构建霍夫曼树,从树的根开始逐位读取二进制文件,找到 0 位时,向左移动到树上;找到 1 位时,在树上向右移动,直到找到叶节点,然后对所有剩余位重复该过程,直到检索到所有消息字符。

3.2.2 随机分量 s

通过引入随机分量 s,每次加密消息时都会获得不同的密文,因此攻击者很难从关于原始消息的密文中进行破解。本文使用字母 s 来表示随机分量,其中 s 是通过使用加密安全伪随机数生成器生成的随机数,并且对于每个消息(随机数)使用一次。本文使用 s 来隐藏头文件的密文并使二进制文件失效。在 s 小于密文的情况下,多 s 进行多次叠加来作为密文的长度,如果 s 大于密文,则把 s 的个位数除去后为密文的相同长度,在使二进制文件失效时应用相同的方法。为了使加密过程在语义上安全,本文选择随机分量 s 并计算新的密文 $C' = C \times s$。同样,为了使二进制文件 B 在语义上安全,使用 s 对 B 进行盲化,例如 $B' = B \times s$。另一方面,随机分量 s 应该受到保护,本次本文将使用 Rabin 加密算法对 s 进行加密。

3.2.3 优化实现

要解压缩消息,通过头文件来构建霍夫曼树,从树的根开始逐位读取二进制文件,找到 0 位时,向左移动到树上;找到 1 位时,在树上向右移动,直到找到叶节点,然后对所有剩余位重复该过程,直到检索到所有消息字符。

优化后的 RSA 算法依靠霍夫曼编码来增强安全性并加速加密和解密过程。为了增强执行速度,加密算法仅加密头文件并使二进制文件保密,而不是加密整个消息。通过 s 参数对二进制文件进行盲化使得加密消息在语义上是安全的,具体优化算法如下:

步骤 1 在接收端生成公钥/私钥对。

1)计算 RSA 算法公钥/私钥对。

2)计算 Rabin 算法公钥/私钥对。

步骤 2 发送端的加密准备。

1)为每一条加密信息生成随机分量 s。

2)使用霍夫曼代码压缩信息。输出:二进制文件(B)和头文件(H)。

步骤 3 发送端加密过程。

1)使用 RSA 算法对 H 进行加密,任取大整数 N 和 e,加密结果为:$C = H^e \bmod N, 0 < H < N-1$。

2)使用 s 对 C 进行盲化,生成 $C' = C \times s$。

3)使用 s 对 B 进行盲化,生成 $B' = B \times s$。

4)使用 Rabin 算法对 s 进行加密,得到 $s' = s^2 \bmod N$。

步骤 4 接收端的解密过程。

1)使用 Rabin 算法对 s 解密。

2)计算 $C = C' \times s$。

3)计算 $B' = B \times s$。

4)使用 RSA 算法对 C 进行解密,任取大整数 d,生成 $H = C^d \bmod N$。

步骤 5 在接收端解压缩信息。

1)将 H、B 传入霍夫曼代码获得解密结果。

4 方法的实现与分析

4.1 原型系统部署

原型系统试点部署在北京市农业农村局与北京市畜牧总站合作建立的智能禽舍中,位于北京市顺义区。禽舍环境监测系统将数据监测节点分为前部节点、中部节点和尾部节点三个区域,每个区域独立采集、传输数据,实现了不同分区不同情况的差异化处理,可以针对性地对禽舍中环境信息进行监控,为后续的追溯提供数据支持。

实验环境主要分为硬件与软件两部分。

(1)硬件部分:系统硬件部分采用基于 ARM 的树莓派 3B 作为主控板,数据采集端使用 XL51 智能温湿度传感器,该设备支持温湿度、TVOC、大气压力,以及二氧化碳、氨气、硫化氢、甲醛等气体浓度的数据采集。

(2)系统部分:树莓派使用 Linux 操作系统,基于此环境搭建 Python 语言、C 语言、OP-TEE 的软件环境,

数据采集中使用 Python 语言操作 GPIO。使用 OP-TEE 作为 trust OS,C 语言作为开发语言,进行 CA-TA 程序的开发,并部署在树莓派 3B 上,安全操作系统以及开发环境均遵循 GP TEE 系统开发架构规范,追溯系统使用基于 Truffle 框架和 Ganache 可视化应用的北京市畜牧总站智能鸡舍监控管理平台。

4.2　数据采集与加密

实验数据通过在四个禽舍部署的各不同分区的传感器设备采集,传感器均安置在鸡舍中的百叶窗中,实验环境如图 4 所示。每个鸡舍安装 6 个传感器,传感器数据采集频率为每 30 s 一次,每个鸡舍单日产生约 1.7 万条数据样本。实验数据通过 CA 端传入 TA 端,加盖时间戳后进行加密操作,随后由实验数据、时间戳(Time)、密文(Ciphertext)组成追溯信息,由 TA 端传回 CA 端并进行存储。嵌入式环境最终输出的追溯信息如表 3 所示。

图 4　实验环境

表 3　数据加密结果

采集位置	属性	属性值
前部节点环境检测数据	时间	2020 - 03 - 26T00:38:11.000 + 08:00
	温度/℃	11.05
	湿度/% RH	66.3
	二氧化碳	409×10^{-6}
	氨气	0.95×10^{-6}
	硫化氢	0.55×10^{-6}
	甲醛	0×10^{-9}
	密文	\x1f\xae\x17B…

4.3　数据追溯

加密后的数据将上传至基于联盟区块链的北京市畜牧总站智能鸡舍监控管理平台,通过智能合约中的公钥对密文进行检验,由于数据量巨大,系统将对一小时内采集到的验证无误的数据取平均值上传至联盟区块链追溯系统供应用查询使用,通过 Ganache 可视化应用观察到追溯数据成功上传到系统后,区块数正常增加且交易记录增长。在该系统中输入追溯目标的追溯 ID,即可对数据进行查询,如图 5 所示。

```
INPUT:935720190712
LOADING.....
LOADING.....
LOADING.....
LOADING.....
OUTPUT:采集位置:前部节点环境检测数据
时间:2020-03-26-20:04:17-21:04:16
温度:11.05℃
湿度:66.3%RH
二氧化碳:409×10^-6
氨气:0.95×10^-6
硫化氢:0.55×10^-6
甲醛:0×10^-9
```

图 5　追溯数据查询结果

4.4　RSA 算法优化性能测试

在测试中,本文将分别使用 RSA 算法以及优化后的 RSA 算法对 10 个不同尺寸的文件进行加密,每个文件加密三次,并对单位时间运算次数取均值,测试文件大小从 1 MB 到 10 MB。图 6 显示了 RSA 算法优化前后对不同尺寸的文件的加密过程。此外,由图 7 可以看出,对于相同的明文,优化后的 RSA 算法所生成的密文大小明显小于优化前。

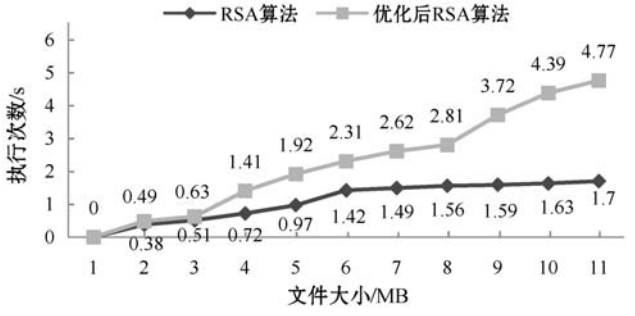

图 6　运算效率对比

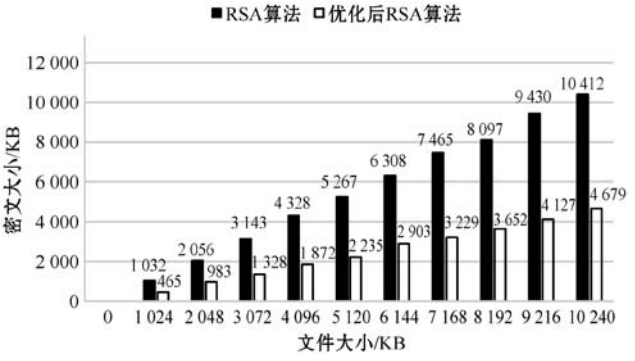

图 7　密文大小对比

4.5 结果分析

由原型系统的试点效果可知,TrustZone 架构下基于优化 RSA 的食品追溯可信采集方法可以有效地确保智能禽舍所采集的追溯信息在上传服务器前的信息安全,实现追溯数据可信采集同时在嵌入式环境下也可以高效工作,并部署在更多的工作环境中。加密后的追溯数据可以通过北京市畜牧总站智能鸡舍监控管理平台进行数据验证,从而确保追溯数据从采集端到存储端的全过程数据安全。在优化后的算法中使用随机分量 s 可以保证加密过程中的语义安全,每次加密消息时都会获得不同的密文,同时二进制文件也通过随机分量 s 进行了盲化,攻击者无法逆向破解密钥对于密文,进一步提了 RSA 算法的安全性。图 6 显示加密速度与两个密码系统加密的文件大小成正比,但优化后的 RSA 算法明显更快,较优化前平均提高了 94.9%,这是由于优化后的 RSA 算法并不加密全部信息,而是通过霍夫曼编码对数据进行压缩后再运行加密算法,这在确保信息安全的同时提高了运算速度。另一方面,在追溯过程中信息量极大,由图 7 可以看出改进后的 RSA 算法生成的密文的大小较优化前平均减少 55.5%,这将有利于减轻本地以及服务器端的存储压力,降低追溯成本。

5 结 语

本文提出并实现一种 TrustZone 架构下基于优化 RSA 的食品追溯可信采集方法,对 TrustZone 技术进行研究并首次将其应用在食品安全追溯领域,有效地解决了追溯数据在上传至服务器端之前的数据安全隐患,填补了当前的行业空白。本文根据嵌入式环境以及应用需求设计了基于优化 RSA 算法的追溯信息加密机制,在可信执行环境中对追溯数据进行加盖时间戳和加密保护,加密后的追溯数据可以在服务器端通过公钥进行验证。通过原型系统试点测试以及分析可以看出,本文方法可以高效、安全地对食品追溯数据进行加密,防止攻击者对数据进行篡改,并适合应用在数据量大且硬件计算能力有限的嵌入式环境中,同时该方法可以与区块链等新兴技术相结合,实现食品生产全流程数据的可信追溯,未来可根据不同种类食品的生产业务逻辑,进一步丰富食品的可信追溯种类。

参 考 文 献

[1] 赵阔,邢永恒. 区块链技术驱动下的物联网安全研究综述[J]. 信息网络安全,2017(5):1-6.

[2] 章张锴,李舟军,夏春和,等. 借助 Hypervisor 强化 TrustZone 对非安全世界的监控能力[J]. 软件学报,2018,29(8):2511-2526.

[3] 张英骏,冯登国,秦宇,等. 基于 TrustZone 的开放环境中敏感应用防护方案[J]. 计算机研究与发展,2017,54(10):2268-2283.

[4] 冯云,翟峰,梁晓兵,等. 基于国产密码的可信用电信息采集终端[J]. 农村电气化,2018(10):55-58.

[5] 王海元,王汝传,黄海平,等. 基于 ARMA 模型的无线传感器网络可信数据采集方法[J]. 南京邮电大学学报(自然科学版),2009,29(4):85-89,96.

[6] 李红涛. 可信的无线数字图像采集与传输系统关键技术研究[D]. 西安:西安科技大学,2013.

[7] Zhao S, Zhang Q, Hu G, et al. Providing root of trust for ARM TrustZone using on-chip SRAM[C]//4th International Workshop on Trustworthy Embedded Devices,2014.

[8] Hein D, Winte R J, Fitzek A. Secure block device-Secure, flexible, and efficient data storage for ARM TrustZone systems[C]//2015 IEEE Trustcom/BigDataSE/ISPA,2015.

[9] 暴金雨. RSA 公钥密码体制的原理及应用[J]. 科技传播,2019,11(6):137-139.

[10] 王芮,周丹红. 计算机网络通信安全中数据加密技术的应用研究[J]. 吉林工程技术师范学院学报,2019,35(5):88-90.

[11] 宋利民,宋晓锐. 一种基于混合加密的数据安全传输方案的设计与实现[J]. 信息网络安全,2017(12):6-10.

[12] 魏文燕,彭维平,李子臣,等. 一种基于 Rabin 和 Paillier 的数字签名方案[J]. 计算机应用与软件,2017,34(12):301-306.

[13] 李雨,张俊. 基于 ECC 算法在数字签名中的分析与研究[J]. 无线互联科技,2019,16(12):110-111.

[14] Dai W, Deng J, Wang Q, et al. SBLWT: A secure blockchain lightweight wallet based on TrustZone[J]. IEEE Access, 2018,6:40638-40648.

[15] 喻潇,田里,刘喆,等. TrustZone 架构下基于 RPMB 的隐私数据保护方法[J]. 计算机应用,2018,38(S2):164-169.

[16] 刘志娟,高隽,丁启枫,等. 移动终端 TEE 技术进展研究[J]. 信息网络安全,2018(2):84-91.

[17] 宁振宇,张锋巍,施巍松. 基于边缘计算的可信执行环境研究[J]. 计算机研究与发展,2019,56(7):1441-1453.

[18] 范冠男,董攀. 基于 TrustZone 的可信执行环境构建技术研究[J]. 信息网络安全,2016(3):21-27.

[19] Salomon D. A concise introduction to data compression[M]. Springer,2008:63-75.