



文章编号:1001-9081(2018)09-2543-06

DOI:10.11772/j.issn.1001-9081.2018020454

云环境下基于运算电路的同态认证方案

白 平^{1*}, 张 薇^{1,2}, 王绪安^{1,2}

(1. 武警工程大学 密码工程学院 西安 710086; 2. 武警工程大学 信息安全保密重点实验室, 西安 710086)

(*通信作者电子邮箱 bp15771937011@163.com)

摘要:针对云服务器上数据验证效率低的问题,为能够在正确执行用户指令的情况下依然保持对数据的高效验证,构造了一种支持云环境下基于运算电路的同态认证方案。首先,利用标签生成算法对验证标签进行多项式表示;其次,调用转化算法对验证标签进行转化以达到满足同态验证的形式,同时利用同态解密算法对验证标签的大小进行降维处理;最后,运用验证算法对检索结果进行验证。结果表明,所提方案能够支持任意次乘法同态而不会增加验证标签维数,克服了验证标签增长缺陷,提高了验证效率,但其计算复杂度会随着增强电路输入位的增加而增加。

关键词:同态认证;运算电路;同态解密;数据完整性

中图分类号: TP309.7 **文献标志码:**A

Homomorphic MACs for arithmetic circuits on cloud environment

BAI Ping^{1*}, ZHANG Wei^{1,2}, WANG Xu'an^{1,2}

(1. College of cryptographic Engineering, Engineering University of the Chinese Armed Police Force, Xi'an Shaanxi 710086, China;

2. Key Laboratory of Network and Information Security, Engineering University of the Chinese Armed Police Force,
Xi'an Shaanxi 710086, China)

Abstract: Focused on the low efficiency of verifying data on the cloud servers, to ensure correct execution of user's commands and high-efficient validation, a method supporting homomorphic MAC for arithmetic circuits on cloud environment was provided. Precise search was obtained through the following ways. Firstly, a label generation algorithm was used to represent a validation label with a polynomial. Secondly, a transformation algorithm was used to transform the validation label to satisfy homomorphic form, meanwhile, homomorphic decryption was used reduce the dimensionality of the label. Finally, a verification algorithm was used to verify the search result. Moreover, the scheme carries out infinite multiplicative homomorphism without increasing the size of verification labels, and is efficient. The drawback of the scheme is that the computational complexity increases with the increase of the input bits of enhancement circuit.

Key words: homomorphic MAC (Message AuthentiCator); arithmetic circuit; homomorphic decryption; data integrity

0 引言

随着云计算技术^[1]的不断发展,利用“云端”存储数据越来越受到广大用户的青睐;与此同时,外包给“云端”的数据如何确保其安全性和可靠性同样引起了人们的关注。目前,对于外包数据的安全性已经通过各种加密方式^[2]进行了有效的解决。然而,如何对外包数据的计算结果进行有效验证仍是当前比较棘手的问题,见文献[3–5]。本文的研究重点也是侧重于如何进行外包数据的验证。考虑如下一个具体的应用环境:假设用户把数据 m_1, m_2, \dots, m_n 外包给“云端”进行存储,随后用户想要“云端”对这些数据进行某种运算如 $R(m_1, m_2, \dots, m_n) \rightarrow m$ 。存在的问题是用户如何确保云服务器能够正确执行计算指令呢?一个最直观的方法是云服务器把这些数据回传给用户,由用户自己计算,然后与服务器计算的结果进行对比。这种方法虽然简单却极大地削弱了外包的价值,增加了用户的开销花费。此外,由于不同的服务器提供不同的服务功能,用户可能会在服务器之间进行数据传输以保证用户利益最大化,但是服务器是一个不可完全信任的

机构,用户数据可能会因为各种原因被恶意篡改甚至丢失,给用户带来了极大的安全隐患,这就迫切需要去寻找一个安全高效的机制来完成外包计算的验证以及用户数据在不同服务器传输过程中的完整性。

同态消息运算认证(Homomorphic Message AuthentiCator, HomMAC)最初由 Gennaro 等^[6]提出。相比其他验证方法如 PDP(Provable Data Possession)^[7], 同态消息运算认证具有两个独特的优点:1) 允许任何人在不知道私钥的情况下认证待验证的消息;2) 允许拥有私钥用户在不知道原始输入情况下验证计算结果的正确性。

该方案将同态解密思想(homomorphic decryption)运用到 Catalano 等^[8]提出的基于算术电路实用同态消息认证方案中,构造了云环境下基于运算电路的同态认证方案。相比文献[8],方案在复杂度上有所增长。然而,本方案可以进行任意次乘法同态而不会增大验证标签大小,实现了更高效的同态认证。另外,可以提供不同服务器之间数据完整性和有效性的验证,增强了用户外包数据的安全性。同态消息认证允许用户在不知道私钥情况下对数据消息进行验证,从而很大

收稿日期:2018-03-07;修回日期:2018-05-17;录用日期:2018-06-12。 基金项目:国家密码发展基金资助项目(MMJJ20170112)。

作者简介:白平(1990—),男,内蒙古乌兰察布人,硕士研究生,主要研究方向:密码学; 张薇(1976—),女,陕西西安人,教授,博士,主要研究方向:密码学、信息安全; 王绪安(1981—),男,湖北公安人,副教授,博士,主要研究方向:密码学、信息安全。



程度上方便了用户。随着同态认证受到越来越多的关注,涌现出了许多这方面研究成果^[9-11]。

1 预备知识

1.1 标签函数

标签函数(labeled program)由Gennaro等^[6]提出。标签函数定义为 $P = (f, \tau_1, \tau_2, \dots, \tau_n)$, 其中 $f: M^n \rightarrow M$ 是运算函数, $\tau_1, \tau_2, \dots, \tau_n \in \{0, 1\}^*$ 是二进制串。在标签函数 P_1, P_2, \dots, P_t 和函数 $g: M^t \rightarrow M$ 已知情况下, 标签函数也可表示为 $P^* = g(P_1, P_2, \dots, P_t)$ 。文献[6]的方案中限制了标签函数在布尔电路 $f: \{0, 1\}^n \rightarrow \{0, 1\}$ 中, 本文方案中将其扩展到运算电路中, 为 $f: M^n \rightarrow M$ 。

1.2 同态消息运算认证方案

同态消息运算认证(HomMAC)方案主要由4个算法构成, 具体如下。

$\text{KeyGen}(1^\lambda)$ 输入安全参数 λ , 输出私钥 sk 和解密密钥 ek 。

$\text{Auth}(sk, \tau, m)$ 输入私钥 sk , 消息 $m \in M$ 和对应消息标记 τ , 输出验证标签 σ 。

$\text{Ver}(sk, m, P, \sigma)$ 输入私钥 sk 、消息 m 、验证标签 $P = (f, \tau_1, \tau_2, \dots, \tau_n)$ 和标签函数 $P = (f, \tau_1, \tau_2, \dots, \tau_n)$, 则验证结果正确时输出为1; 反之, 输出为0。

$\text{Eval}(ek, f, \sigma)$ 输入解密密钥 ek , 运算电路 $f: M^n \rightarrow M$ 和验证标签向量 $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n)$, 输出新验证标签 σ' 。

1.3 半诚实模型

在半诚实模型中, 如果静态诚实敌手 A 只能从输入方或者输出方通过执行算法协议 η 获得相关信息, 那么协议 η 是安全的。半诚实模型可以通过模拟来形式化表示。协议 η 执行过程中, 规定视图被模拟时只考虑输入与输出, 则参与方 k 的输入 (x, y) 在协议 η 执行过程中可以表示为 $\text{view}_k^\eta(x, y) = (w, r^k, m_1^k, m_2^k, \dots, m_t^k)$, 其中 $w \in (x, y)$ 是 k 的输入, r^k 是 k 内部随机硬币投掷值, m_j^k 表示接收的第 j 份消息。

定义1 半诚实模型: 设 $g = (g_1, g_2)$ 是确定性函数, 如果存在多项式时间的方案 Sim_1 和 Sim_2 , 即:

$$\begin{cases} \{\text{Sim}_1(x, g_1(x, y))\}_{x, y} \equiv \{\text{view}_1^\eta(x, y)\}_{x, y} \\ \{\text{Sim}_2(x, g_2(x, y))\}_{x, y} \equiv \{\text{view}_2^\eta(x, y)\}_{x, y} \end{cases}$$

那么协议 η 在静态半诚实敌手 A 存在情况下是安全的计算函数 g 。

1.4 同态解密

同态解密方法被广泛应用于降低噪声的各种场景中。当进行同态密文乘法运算时, 密文大小会被迅速放大, 从而制约了密文操作次数, 影响了同态效率。在实际云数据传输过程中, 需要对传输数据进行验证。然而, 验证标签的大小会随同态乘法运算被放大, 影响验证的效率。在本方案中, 对同态乘法运算后的密文作同态解密操作, 则可以将验证标签的大小降低到接近初始状态时的大小, 从而达到任意次密文运算的目的。方案中设置了如图1所示的电路, 该电路中包含一个加密电路和一个解密电路, 输入到该电路的多项式验证标签运用某种算法协议进行一系列的加解密操作后可以降低多项式验证标签的次数。为了便于进行下一次运算, 还在电路中

增加一个门电路, 统称为增强验证电路 Ω 。

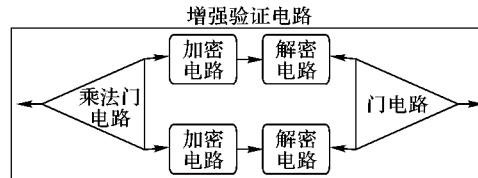


图1 增强验证电路示意图

Fig. 1 Enhanced verification circuit schematic diagram

2 安全模型、结构模型及实例模型分析

2.1 云环境下基于运算电路的同态认证方案安全模型

在同态消息运算认证(HomMAC)中, 敌手 A 和挑战者 B 进行博弈游戏, 具体游戏 $\text{HomUF-CMA}_{A, \text{HomMAC}}(\lambda)$ 过程如下:

Setup 挑战者 B 运行 $\text{KeyGen}(1^\lambda)$ 获得了私钥 sk 和解密密钥 ek , 而后发送解密密钥 ek 给敌手 A , 同时, 初始化列表 $T = \emptyset$ 。

Tag queries 敌手 A 不间断地询问消息标记 τ , 具体分以下三种情况: 1) 假如敌手 A 发送重复询问 $(\tau, m) \in T$ 给挑战者 B , 则挑战者 B 发送相同的答复。2) 假如敌手 A 发送询问 $(\tau', m) \in T$ 给挑战者 B , 即用同一个标记 τ 标记了两个不同消息 m 和 m' , 则挑战者 B 忽略此询问。3) 假如敌手 A 发送询问 $(\tau, m) \notin T$ 给挑战者 B , 则挑战者 B 运算 $\text{TagGen}(sk, \tau, m)$ 生成新的验证标签 $\sigma \leftarrow \text{TagGen}(sk, \tau, m)$, 同时更新 $T = T \cup (\tau, m)$ 。

Verification queries 敌手 A 发送询问 (m, P, σ) 给挑战者 B , 挑战者 B 运用 $\text{Ver}(sk, m, P, \sigma)$ 进行验证, 输出结果为1或者0。

Forgery 敌手 A 发送假验证询问 (m^*, P^*, σ^*) , 其中 $P^* = (f^*, \tau_1^*, \tau_2^*, \dots, \tau_n^*)$ 。当且仅当 $\text{Ver}(sk, m^*, P^*, \sigma^*) = 1$, 并且满足下列条件之一时, 游戏 $\text{HomUF-CMA}_{A, \text{HomMAC}}(\lambda)$ 输出为1。

- 1) 伪造1: P^* 不是定义在 T 上。
- 2) 伪造2: P^* 定义在 T 上, 但是 m^* 不是正确的输出, 即 $m^* \neq f^*(\{m_j\}_{(\tau_j, m_j) \in T})$ 。

若上述游戏概率可表示为 $\Pr[\text{HomUF-CMA}_{C, \text{HomMAC}}(\lambda) = 1] \leq \varepsilon(\lambda)$, 其中 $\varepsilon(\lambda)$ 是一个可忽略的函数, 则可以判定该同态认证方案是安全的。

定义2 标签函数 $P^* = (f^*, \tau_1^*, \tau_2^*, \dots, \tau_n^*)$ 以如下两种方式存在:

1) 对于 $i \in \{1, 2, \dots, n\}$, 存在 $(\tau_i^*, \cdot) \notin T$ 使得所有可能的选择 $m_j \in M$ 输出相同的值。

2) T 包括了所有的消息 m_1, m_2, \dots, m_n 的元组 $\{(\tau_1^*, m_1), (\tau_2^*, m_2), \dots, (\tau_n^*, m_n)\}$ 。

2.2 云环境下基于运算电路的同态认证方案结构模型

当两个多项式验证标签 $\sigma_i (i=1, 2)$ 进行同态乘法运算时, 首先会输入到一个乘法门电路中, 经过乘法门电路的作用后, 验证标签的大小会被迅速放大。为了降低验证标签的大小, 将其结果输入到增强验证电路 Ω 中, 通过增强验证电路中加密电路和解密电路的共同作用, 输出新的密文验证标签大小会接近于一个新鲜密文大小, 从而保持了验证标签的



大小在低水平范围内。反复递归此过程,则可以达到任意次密文运算的目的。

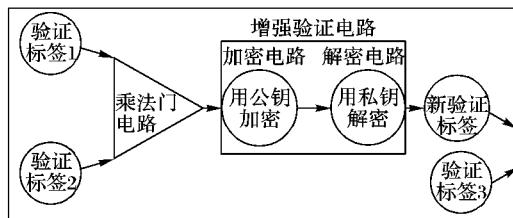


图2 方案运行模拟示意图

Fig. 2 Schematic diagram of program simulation

2.3 云环境下基于运算电路的同态认证方案实例模型

云环境下外包数据的存储主要由三种实体结构组成:普通用户、云服务器、可信第三方。

普通用户 数据存储计算能力相对较弱,倾向于把一些复杂的数据资源交给云服务器来存储或者计算,但希望这些数据不能被云服务器窃取或者篡改。

云服务器 有大量的存储和计算能力,能为用户提供云存储和计算服务,但是云服务器上的数据可能会遭受黑客的恶意攻击,所以必须对存储数据进行验证以确保安全性。

第三方 作为用户与云服务器的中间媒介,第三方(Third Party Administrator, TPA)将得到的最终结果反馈给事先指定用户,确保传输数据的安全性。

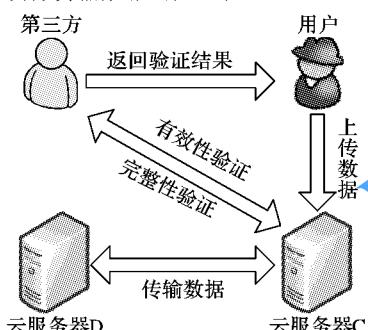


图3 传输数据实例模型

Fig. 3 Example model of transmission data

3 云环境下基于运算电路的同态认证方案

KeyGen(1^λ) 选择一个度长为 λ 位的素数 p ,种子为 K 的伪随机函数 $F_K: \{0,1\}^* \rightarrow Z_p$ 和随机数 $x \xleftarrow{s} Z_p$ 。明文消息空间 $M \in Z_p$,输出公钥 pk ,私钥 $sk = (K, x)$, $ek = p, sk_v$ 。

TagGen(sk, τ, m) 设标记为 $\tau \in \{0,1\}^\lambda$ 的消息 $m \in Z_p$,计算 $\gamma_\tau = F_K(\tau)$ 。定义 y_0, y_1 是深度为1的多项式 $y(z)$ 的系数,同时令 $y_0 = m, y_1 = (\gamma_\tau - m)/x \bmod p$,则可推出当变量取0时,函数值为 m ,即 $y(0) = m$ 。当变量取一个未知随机数 x 时,则函数值 $y(x) = \gamma_\tau$ 。由此类推验证标签 σ 可以由未知变量 z 组成的多项式 $y(z) = \sum_i y_i z^i$ 表示。

Eval(ek, f, σ) 输入解密密钥 $ek = p$ 、运算电路 $f: Z_p^n \rightarrow Z_p$ 以及验证标签向量 $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n)$ 。鉴于验证标签 σ 是多项式 $y^{(i)} \in Z_p[z]$,故需要调用算法 GateEval($ek, g, \sigma_1, \sigma_2$)进行转化。

GateEval($ek, g, \sigma_1, \sigma_2$) 输入两个多项式验证标签

$\sigma_1 = y^{(i)} = (y_0^i, y_1^i, \dots, y_{d_i}^i)$ ($i = 1, 2, \dots$), 运行 $\sigma \leftarrow \text{GateEval}(ek, g, \sigma_1, \sigma_2)$ 生成新的验证标签 σ ,而后输出到下一个门电路,具体算法如下:

1) 同态加法运算。取 $d = \max(d_1, d_2)$,则通过计算 $y(z) = y^{(1)}(z) + y^{(2)}(z)$,得到新多项式验证标签 σ 的系数为 (y_0, y_1, \dots, y_d) :即 $\forall k = 0, 1, \dots, d$,可以定义为 $y_k = \sum_{i=0}^k y_i^{(1)} \cdot y_{k-i}^{(2)}$ 。

2) 同态乘法运算。取 $d = d_1 + d_2$,则通过卷积公式计算 $y(z) = y^{(1)}(z) * y^{(2)}(z)$ 得到新多项式验证标签 σ 的系数为 (y_0, y_1, \dots, y_d) :即 $\forall k = 0, 1, \dots, d$,可以定义为 $y_k = \sum_{i=0}^k y_i^{(1)} \cdot y_{k-i}^{(2)}$ 。而后调用算法 Re-encrypt(σ, pk, sk_v)进行同态解密运算,从而使多项式验证标签系数大小永远保持在最低水平。

3) 带变量的同态乘法运算。取 $d = d_i$ ($i = 1, 2$),另一个标签为变量 c ,则通过计算 $y(z) = c \cdot y^{(1)}(z)$,得到新多项式验证标签 $\sigma = (y_0, y_1, \dots, y_d)$ 。

Homomorphic_decryption(σ, pk, sk_v) 将 GateEval($ek, g, \sigma_1, \sigma_2$)生成的新多项式验证标签 σ 输入到增强验证电路 Ω 中,利用公钥 pk 对新验证标签 σ 进行加密,而后输入解密电路中用私钥 sk_v 进行解密,该解密电路输出的密文相当于一个新鲜密文,它的大小会远远小于之前的密文大小。

Ver(sk, m, P, σ) 定义 $P = (f, \tau_1, \tau_2, \dots, \tau_n)$ 为标签函数,验证标签为 $\sigma = (y_0, y_1, \dots, y_d)$ 以及 $m \in Z_p$ 。具体验证过程如下:

- 1) 如果 $y_0 \neq m$,则返回0;否则进行下一步。
- 2) 令消息标记为 τ ,计算 $\gamma_\tau = F_K(\tau)$ 。
- 3) 对步骤2)中的每一个 γ_{τ_i} ($i = 1, 2, \dots, n$),计算 $f(\gamma_{\tau_1}, \gamma_{\tau_2}, \dots, \gamma_{\tau_n}) \rightarrow \rho$ 。而后运用 x 计算如下等式是否成立:

$$\rho = \sum_{k=0}^d y_k x^k \quad (1)$$

若为真,则输出为1;否则输出为0。

4 方案的分析

4.1 安全性分析

本方案的安全性依赖于同态认证的安全性以及增强验证电路 Ω 的安全性。同态认证的安全性可以利用 Schwartz 等^[12]方案中的命题1进行证明,增强验证电路的安全则可以在半诚实模型下得以证明。

命题1 令 $\lambda, n \in \mathbb{N}, \Pi$ 表示阶为 q 的有限域 M 上的运算电路 $f: M^n \rightarrow M$ 的集合,其中电路 f 的深度最大为 d 且有 $d/q < 1/2$ 。可以得出如下推断:对于 $f \in \Pi$ 存在这样的概率算法: $\forall \mu \in M^n, y \in M$ 使得 $f(\mu) = y$ 的概率至少为 $1 - 2^{-\lambda}$ 。

定理1 如果 F 是一个伪随机函数,则方案的同态消息认证是安全的。

为了证明方案的正确性,定义一个由敌手 A 执行的实验游戏 G_i ($i = 1, 2, \dots, 4$),并最终输出1。

游戏 G_0 输入验证询问 (m, P, σ) ,为了辨别标签函数 P 是否被定义在 T 上,挑战者 B 使用命题1进行概率测试,则任何敌手 A 进行 Q 次验证询问后可得到如下不等式:

$$\| \Pr [\text{HomUF-CMA}_{A, \text{HomMAC}}(\lambda)] - \Pr [G_0(A)] \| \leq$$



$$Q \cdot 2^{-\lambda} \quad (2)$$

游戏 G_1 同游戏 G_0 中的博弈类似,所不同的是游戏 G_1 中所用的是真正随机函数 $R: \{0,1\}^* \rightarrow Z_p$,并随机产生 $\gamma_{\tau} \in Z_p$ 。

游戏 G_2 首先,对于所有验证询问 $(m, P, \sigma = (y_0, y_1, \dots, y_d))$,如果 $y_0 \neq m$ 则输出为 0。其次,对于所有的验证询问 (m, P, σ) ,如果 P 不是被定义在 T 上,则挑战者 B 执行以下步骤:

- 1) 对于每一个 τ_i ,如果 $(\tau_i, \cdot) \notin T$,则计算 $\gamma_{\tau_i} \leftarrow R(\tau_i)$ 。
- 2) 使用算法 $\text{Ver}(sk, m, P, \sigma)$ 计算 ρ 的值。

3) 计算 $Z = \rho - \sum_{k=0}^d y_k x^k$,如果 $Z = 0 \pmod p$,则返回 1;否则返回 0。

游戏 G_3 对于所有验证询问 (m, P, σ) ,其中 $P = (f, \tau_1, \tau_2, \dots, \tau_n)$ 定义在 T 上,挑战者 B 执行以下操作:

假如 $(\tau_i, \cdot) \notin T (i \in \{1, 2, \dots, n\})$,则挑战者 B 选择一个伪造的验证标签 σ_i ,计算 $\hat{\sigma} = (\hat{y}_0, \hat{y}_1, \dots, \hat{y}_d) \leftarrow \text{Eval}(ek, f, (\sigma_1, \sigma_2, \dots, \sigma_n))$ 结果后进行以下判断:

- 1) 如果 $(y_0, y_1, \dots, y_d) = (\hat{y}_0, \hat{y}_1, \dots, \hat{y}_d)$,则输出为 1。
- 2) 如果 $(y_0, y_1, \dots, y_d) \neq (\hat{y}_0, \hat{y}_1, \dots, \hat{y}_d)$,则挑战者 B 继续计算 $Z = \sum_{k=0}^d (y_k - \hat{y}_k) x^k$,当 $Z = 0 \pmod p$,则输出为 1,否则输出为 0。

游戏 G_4 设定 bad 是表示“false”的一个标识符,当挑战者 B 接收到验证询问 (m, P, σ) 后,如果满足以下两个条件:

- 1) 按照验证询问 (m, P, σ) 的要求,挑战者 B 计算出了 Z 的值。
- 2) 计算的输出为 $Z = 0 \pmod p$,则挑战者 B 输出 1,并且设定 $\text{bad} \rightarrow \text{True}$ 。

定义 bad_4 表示游戏 G_4 中 $\text{bad} \rightarrow \text{True}$ 事件,由于所有伪造的验证询问只能是游戏 G_3 中的 1) 或者 2),故任何敌手赢得游戏 G_4 的概率为 0,即 $\Pr[G_4] = 0$ 。

为了证明定理 1,需要证明以下引理:

引理 1 $|\Pr[G_0] - \Pr[G_1]| \leq \text{Adv}_{B,F}^{\text{PRF}}(\lambda)$

引理 1 的证明类似于伪随机函数的安全性证明。

引理 2 $\Pr[G_2] = \Pr[G_3]$

证明 (m, P, σ) 是验证标签,其中 $\sigma = (y_0, y_1, \dots, y_d)$,
 $P = (f, \tau_1, \tau_2, \dots, \tau_n)$ 被定义在 T 上。考虑如下环境:对于
 $\forall i = 1, 2, \dots, n$ 有 $(\tau_i, m_i) \in T$,则挑战者 B 计算 $\hat{\sigma} = (\hat{y}_0, \hat{y}_1, \dots, \hat{y}_d) \leftarrow \text{Eval}(ek, f, (\sigma_1, \sigma_2, \dots, \sigma_n))$ 得出验证标签 σ_i ,从而得出如下结论:

- 1) $\sigma = (y_0, y_1, \dots, y_d) = (\hat{y}_0, \hat{y}_1, \dots, \hat{y}_d) = \hat{\sigma}$;
- 2) $\sigma = (y_0, y_1, \dots, y_d) \neq (\hat{y}_0, \hat{y}_1, \dots, \hat{y}_d) = \hat{\sigma}$;

检查在相同的消息标记 γ_{τ_i} 情况下由 $\text{Ver}(sk, m, P, \sigma)$ 和 $\text{Ver}(sk, m, P, \hat{\sigma})$ 生成的 ρ 是否相等。

引理 3 $\Pr[G_3] - \Pr[G_4] \leq \Pr[\text{Bad}_4]$

如果事件 Bad_4 在游戏 4 中发生,挑战者 B 可能会对某些验证询问提供不同的回应,因此,有 $\Pr[G_3] - \Pr[G_4] \leq \Pr[\text{Bad}_4]$ 。

引理 4 $\Pr[\text{Bad}_4] \leq \frac{2dQ}{q-d(Q-1)}$,其中 q 为素数, Q 为

敌手 A 所能询问次数的最大值。

证明 对于 $j = 1, 2, \dots, Q$,令 B_j 表示这样一个事件:敌手 A 询问了 j 次之后使得 $\text{bad} \rightarrow \text{True}$,则可以得出如下结论:

$$\Pr[\text{Bad}_4] = \Pr\left[\bigvee_{j=1}^Q B_j\right] \leq \sum_{j=1}^Q \Pr[B_j] \quad (3)$$

其中:证明的关键之处在于 $\Pr[B_j]$ 的概率由挑战者 B 随机选择的变量 x 、参数 γ_{τ_j} 和敌手 A 随机选择的参数所评估代替。

定义 (m, P, σ) 表示第 j 次验证询问,根据 P 是否定义在 T 上, B_j 有以下两种可能性:

1) 对于 $Z = \sum_{k=0}^d (y_k - \hat{y}_k) x^k = 0 \pmod p$,至少存在一个参数 $\hat{k} \in \{0, 1, \dots, d\}$ 使得 $y_{\hat{k}} \neq \hat{y}_{\hat{k}}$ 。

2) 对于 $Z = \rho - \sum_{k=0}^d y_k x^k = 0 \pmod p$,其中 P 不被定义在 T 上,则可以使用 γ_{τ_j} 计算得到 ρ 的值,对于 $j = 1, 2, \dots, Q$,定义 Z_j 表示变量 Z 的第 j 询问,通过定义事件 B_j 可知事件 bad 在前 $j-1$ 次询问为假,即:

$$\Pr[B_j] = \Pr[Z_j = 0 \mid Z_1 \neq 0 \wedge Z_2 \neq 0 \wedge \dots \wedge Z_{j-1} \neq 0] \quad (4)$$

在第一次询问之后,如果 $Z_1 \neq 0 \pmod p$,则参数 x 和 $\{\gamma_{\tau_i}\}_{i \in \{1, 2, \dots, n\}}$ 的大小至少为 $q-d$,因为深度为 d 的非零多项式 $\rho(x) = \sum_{k=0}^d c_k x^k$ 的零元最大为 d 。在第 i 次询问之后,如果 $Z_1 \neq 0 \wedge Z_2 \neq 0 \wedge \dots \wedge Z_i \neq 0$,则剩下的 x 和 $\{\gamma_{\tau_i}\}_{i \in T}$ 的数量至少为 $q-di$ 。

令 (m, P, σ) 表示第 j 次询问,定义 E_j^1 表示这样一个事件: P 被定义在 T 上的,存在参数 $\hat{k} \in \{0, 1, \dots, d\}$ 使得 $y_{\hat{k}} \neq \hat{y}_{\hat{k}}$ 。类似地,也可以定义 E_j^2 表示这样一个事件: P 不被定义在 T 上的, ρ 可以通过使用 γ_{τ_j} 计算得到。最后,定义 NotZero_j 表示这样一个事件: $Z_1 \neq 0 \wedge Z_2 \neq 0 \wedge \dots \wedge Z_i \neq 0$ 。

显然,由 $\Pr[B_j] = \Pr[B_j \wedge E_j^1] + \Pr[B_j \wedge E_j^2]$ 则可推出如下不等式:

$$\Pr[B_j] = \Pr[Z_j = 0 \mid \text{NotZero}_j] = \Pr[Z_j = 0 \wedge E_j^1 \mid \text{NotZero}_j] + \Pr[Z_j = 0 \wedge E_j^2 \mid \text{NotZero}_j] \leq \Pr[Z_j = 0 \mid E_j^1 \wedge \text{NotZero}_j] + \Pr[Z_j = 0 \mid E_j^2 \wedge \text{NotZero}_j] \quad (5)$$

因为多项式 $\sum_{k=0}^d (y_k - \hat{y}_k) x^k$ 的零元最多为 d ,参数 x 的值可能有 $q-d(j-1)$ 种,故可推出:

$$\Pr[Z_j = 0 \mid E_j^1 \wedge \text{NotZero}_j] \leq \frac{d}{p - d(j-1)} \quad (6)$$

为了计算概率 $\Pr[Z_j = 0 \mid E_j^2 \wedge \text{NotZero}_j]$,设想这样一种环境:以单变量 γ_{τ_j} 作为深度至多为 d 的多项式 $\rho = \eta(\gamma_{\tau_j})$ 的变量,此外, P 不被定义在 T 上, η 必须为非恒定多项式。情况一:在没有验证询问情况下, γ_{τ_j} 是不能为敌手 A 所获得的,敌手 A 猜对的概率不会超过 $1/q$ 。情况二:敌手 A 不断地进行验证询问,在这种情况下,可以使用类似之前讨论的情况,唯一不同的条件是 $Z = \eta(\gamma_{\tau_j}) \neq 0$,这样可以排除至多 d 种变量 γ_{τ_j} ,因此,当考虑事件 NotZero_j 时,敌手 A 在第 j 次能猜对



$\gamma_{r,*}$ 的概率不会超过 $1/(q-1)(j-1)$ 。因此:

$$\Pr[Z_j = 0 \mid E_j^2 \wedge \text{NotZero}_j] \leq \frac{d}{q-d(j-1)} \quad (7)$$

最后,将式(6)和(7)运用到式(5)中可推导出如下不等式:

$$\Pr[B_j] \leq \frac{2d}{q-d(j-1)} \quad (8)$$

进而可以得到上限值:

$$\Pr[Bad_4] \leq \frac{2d}{q-d(Q-1)} \quad (9)$$

综上所述,可以证明定理1:

$$\begin{aligned} Adv_{A, \text{HomMAC}}^{\text{HomUF-CMA}}(\lambda) &\leq Adv_{B,F}^{\text{PRF}}(\lambda) + \frac{2dQ}{q-d(Q-1)} + \frac{Q}{2^\lambda} \end{aligned} \quad (10)$$

因为 $q \approx 2^\lambda$ 且 d 和 D 是 $\text{poly}(\lambda)$, $\frac{2dQ}{q-d(Q-1)} = negl(\lambda)$, 因此, 如果伪随机函数(Pseudo Random Function, PRF)是安全的,则任何敌手 A 将以可忽略的优势攻破本文同态认证方案。

本方案中增强验证电路的安全性建立在半诚实模型下,参与方(真实方和模拟方)诚实的执行相关算法协议,假设真实方与模拟方分别拥有多项式向量集合 $\mathbf{M}^* = (M_1, M_2, \dots, M_n), S^* = (S_1, S_2, \dots, S_n)$, 模糊匹配的操作对象就是针对 \mathbf{M}^* 和 S^* 中的某两个多项式向量进行作用。

在方案证明过程中为了标识方便,将直接使用 \mathbf{M} 和 S 作为向量,假设真实视图中对向量 \mathbf{M} 输出为 BF_M , 模拟视图中对向量 S 输出为 CF_S , 将 BF_M 和 CF_S 进行作用产生交集 $BCF_{M \cap S}$, 记录交集中匹配成功的个数。如果个数大于或者等于事先设定的门限值 t , 则真实视图和模拟视图具有不可区分性,反之,二者可区分。

定理2 设 \mathbf{M}, \mathbf{S} 分别是预定义的域, g_\cap 是交集函数, $|g_\cap|$ 为交集中匹配成功的个数,那么 \mathbf{M}, \mathbf{S} 匹配的表达式为:

$$\begin{aligned} \text{true} &= |g_\cap(\mathbf{M}, \mathbf{S}) \geq t| = ||g_M(\mathbf{M}, \mathbf{S}), g_S(\mathbf{M}, \mathbf{S})|| \geq t| = \\ &= ||(\mathbf{M} \cap \mathbf{S}, \wedge) \geq t|| \end{aligned}$$

证明 假定方案中所用的不经意传输(Obliviously Transfer, OT)协议是安全的,则真实发送者和模拟发送者的模拟器是存在的,现在利用这两个模拟器作为子程序构建出新的模拟器。

真实视图 构建模拟器 Sim_M , 协议中它可以接收乘法门电路的多项式输出,生成真实的视图。对于 \mathbf{M} 来说, 模拟器 Sim_M 均匀选取随机投掷硬币的结果 r^M , 并且生成 BF_M 。然后 Sim_M 调用 OT 的模拟器,输出模拟视图 $(\mathbf{M}, r^M, Sim_M^{\text{OT}}(BF_M, \wedge))$ 。真实协议执行的视图包括输入 \mathbf{M} , 随机投掷硬币的结果,以及协议中的消息。在模拟视图中,输入向量 \mathbf{M} 与真实执行视图中的对应向量相同,随机投掷硬币结果也是均匀选取,因此其分布与真实执行情况相同。如果 OT 协议是安全的,那么由 $Sim_M^{\text{OT}}(BF_M, \wedge)$ 产生的视图分布与真实 OT 协议执行的视图分布具有不可区分性。因此可以得出结论:模拟视图与真实视图是不可区分的。

模拟视图 构建模拟器 Sim_S , 它同样可以接收乘法门电路的输出,对于 \mathbf{S} 来说,随机均匀选取投掷硬币的结果 r^S , 分

别生成 CF_S 和 $BCF_{M \cap S}$ 。然后 Sim_S 调用不经意传输协议 OT 的模拟器输出模拟视图 $(S, r^S, Sim_S^{\text{OT}}(CF_S, BCF_{M \cap S}))$ 。真实协议执行的视图包括输入 S , 随机投掷硬币的结果 r^S 和 $BCF_{M \cap S}$, 以及协议中的消息。在模拟视图中,输入向量 S 与真实执行视图中的对应向量相同,随机投掷硬币结果 r^S 也是均匀选取, $BCF_{M \cap S}$ 与 $BCF_{M \cap S}^{\text{OT}}$ 具有不可区分性。如果 OT 协议是安全的,那么由 $Sim_M^{\text{OT}}(BF_M, \wedge)$ 产生的模拟视图分布与真实 OT 协议执行的真实视图分布具有不可区分性。因此可以得出结论:模拟视图与真实视图是不可区分的。

4.2 性能分析

在同态认证过程中,当对多项式验证标签进行运算时,验证标签的大小会被迅速放大,影响认证效率,而这种增加主要来自于同态乘法运算。然而,如果对每一次运算后的验证标签作一次同态解密运算,则可以得到一个类似于新鲜密文大小的新验证标签,从而保证了验证标签的大小维持在一个低水平范围内。本方案中较 Catalano 等^[8]提出的基于算术电路可实用的同态消息认证方案最大的不同在于引进了一个 Homomorphic decryption 算法,其作用在于将验证标签的大小降低到类似新鲜密文的大小,从而保证了验证标签大小被保持在一个低水平范围内。Catalano 等提出的方案中存在的最大缺陷是多项式验证标签的大小会随电路的深度增加而递增,在他们的方案中通过限制电路深度克服了这一缺陷。然而他们的解决办法是以牺牲下列条件为代价:事先固定电路所能运算的最大深度值 D 。在本文方案中不需要事先设定电路的深度值,在每次同态乘运算之后自动调动 Homomorphic decryption 算法来降低标签系数,从而可以进行任意次验证计算。本方案中存在的问题是每次调用 Homomorphic decryption 算法势必增加方案的复杂度。下面说明方案的复杂度。

验证标签大小的增长主要来源于同态乘法的运算,本文中增强电路的输入可以表示成多项式函数,故电路的深度可以用输入位的对称多项式来衡量本文假设方案中增强电路中输入的验证标签多项式分别表示为 $y(x_1) = a_1 + a_2(x_1)^2 + a_3(x_1)^3$ 和 $y(x_2) = b_1 + b_2(x_2)^2 + b_3(x_2)^3$, 其中系数 (a_1, a_2, a_3) 和 (b_1, b_2, b_3) 分别表示电路输入,那么如何确定这两个多项式相乘结果的次数呢?运用如下结论:

乘两个 t 位数相当于加 t 位数,输出位是输入位的一个 2 次多项式:

$$\begin{array}{c} a_3 & a_2 & a_1 \\ b_3 & b_2 & b_1 \\ \hline a_3b_1 & a_2b_1 & a_1b_1 \\ a_3b_2 & a_2b_2 & a_1b_2 \\ a_3b_3 & a_2b_3 & a_1b_3 \\ \hline a_3b_3 + (a_3b_2 + a_2b_3) + (a_3b_1 + a_2b_2 + a_1b_3) + (a_2b_1 + a_1b_2) + a_1b_1 \end{array}$$

t 个数相加:3 个数相加得到 2 个数相加,输出位是关于输入位的一个次数最多为 2 次的多项式:

$$\begin{array}{c} a_3 & a_2 & a_1 \\ b_3 & b_2 & b_1 \\ c_3 & c_2 & c_1 \\ \hline a_3 + b_3 + c_3 & a_2 + b_2 + c_2 & a_1 + b_1 + c_1 \\ a_3b_3 + a_3c_3 + b_3c_3 & a_2b_2 + a_2c_2 + b_2c_2 & a_1b_1 + a_1c_1 + b_1c_1 \end{array}$$

那么 t 个数运用这个性质经过 $\log_{3/2}t$ 次相加后得到两个数,输出位的次数为 $2^{\log_{3/2}t} = t^{\log_{3/2}2} = t^{1.71}$ 。



两个 t 位数相加:

进位:

$$\begin{array}{r} a_3 & a_2 & a_1 \\ b_3 & b_2 & b_1 \\ \hline a_2b_2 + a_2a_1b_1 + b_2a_1b_1 & a_1b_1 & b_1 \\ \hline a_3 + b_3 + a_2b_2 + a_2a_1b_1 + b_2a_1b_1 & a_2 + b_2 + a_1b_1 & a_1 + b_1 \end{array}$$

可以类推出:输出位的次数最多为 t 。

综上所述:乘两个 t 位数的次数最多为 $2t^{1.71}t = 2t^{2.71}$ 。

通过以上分析可知,方案中增强验证电路的复杂度为 $2t^{1.71}t = 2t^{2.71}$,另一部分复杂度是计算 $\rho = f(\gamma_{\tau_1}, \gamma_{\tau_2}, \dots, \gamma_{\tau_n})$

的时间 $O(|f|)$ 和计算多项式验证标签 $\sum_{i=0}^d y_i x^i$ 的时间 $O(d)$ 。

本文方案在乘法同态运算进行了改进提高,使得运算电路可以反复递归此过程,从而达到任意次密文运算的目的,实现同态验证的目的,提高了方案的实用性和效率性。

Catalano 等^[13]运用分级编码的思想,构造了一个基于算术电路扩展的同态认证方案,下面将分别在是否支持密文的复合度、验证标签大小、电路深度大小以及是否支持无上界的验证询问方面与文献[6,8,13]进行比较。具体的比较结果如表 1 所示。

表 1 关键词索引结构

Tab. 1 Index of keywords

方案	复合度	验证 标签	电路深度	是否支持无上 界的验证询问
GW13 ^[6]	√	$O(\lambda)$	任意电路深度	✗
CF13-2 ^[8]	✗	$O(d)$	深度为 d 的电路	√
Catalano 方案 ^[13] 深度为 d 的电路		$O(k)$	深度为 $(D+d)$ 的电路	✗
本文方案	✗	$O(d)$	任意电路深度	√

通过表 1 可以得出,本方案相比文献[6,8,13],克服了它们部分缺点,例如相比 GW13 方案,本方案可以支持无上界的验证询问。不足之处是复合度有所减弱。相比 CF13-2 方案,本方案在电路深度进行优化,可以进行深度为任意值的电路,在很大程度上增强了用户数据验证的实用性和可操作性。

5 结语

本文将同态解密方法运用到同态认证方案中,构造了云环境下基于运算电路的同态认证方案。通过引入同态解密方法,方案可以达到对密文作任意功能的运算,进一步提高了云数据认证的效率,增强了用户数据的安全性。由于方案中没有讨论增强验证电路的深度是否在 Permitted Function 集合中,故无法确定方案为全同态认证。进一步的工作是探索方案是否为全同态认证,从而构造效率更高、更为实用的云环境下全同态数据认证方案。

参考文献 (References)

- [1] MEZGHANI K, AYADI F. Factors explaining IS managers attitudes toward cloud computing adoption [J]. International Journal of Technology and Human Interaction, 2016, 12(1): 1–20.
- [2] GENTRY C. Fully homomorphic encryption using ideal lattices [C]// STOC '09: Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM, 2009: 169–178.
- [3] APPLEBAUM B, ISHAI Y, KUSHILEVITZ E. From secrecy to soundness: efficient verification via secure computation [C]// Proceedings of the 2010 International Colloquium on Automata, Languages, and Programming, LNCS 6198. Berlin: Springer, 2010: 152–163.
- [4] CHUNG K M, KALAI Y, VADHAN S. Improved delegation of computation using fully homomorphic encryption [C]// Proceedings of the 2010 Annual Cryptology Conference, LNCS 6223. Berlin: Springer, 2010: 483–501.
- [5] GENNARO R, GENTRY C, PARNO B. Non-interactive verifiable computing: outsourcing computation to untrusted workers [C]// Proceedings of the 2010 Annual Cryptology Conference, LNCS 6223. Berlin: Springer, 2010: 465–482.
- [6] GENNARO R, WICHES D. Fully homomorphic message authenticators [C]// Proceedings of the 2013 International Conference on the Theory and Application of Cryptology and Information Security, LNCS 8270. Berlin: Springer, 2013: 301–320.
- [7] DAN B, LYNN B, SHACHAM H. Short signatures from the Weil pairing [C]// Proceedings of the 2001 International Conference on the Theory and Application of Cryptology and Information Security, LNCS 2248. Berlin: Springer, 2001: 514–532.
- [8] CATALANO D, FIORE D, GENNARO R, et al. Practical homomorphic MACs for arithmetic circuits [C]// Proceedings of the 2013 Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 7881. Berlin: Springer, 2013: 336–352.
- [9] BENABBAS S, GENNARO R, VAHLIS Y. Verifiable delegation of computation over large datasets [C]// CRYPTO '11: Proceedings of the 31st Annual Conference on Advances in Cryptology. Berlin: Springer, 2011: 111–131.
- [10] FIORE D, GENNARO R. Publicly verifiable delegation of large polynomials and matrix computations, with applications [C]// CCS '12: Proceedings of the 2012 ACM Conference on Computer and Communications Security. New York: ACM, 2012: 501–512.
- [11] PARNO B, RAYKOVA M, VAIKUNTANATHAN V. How to delegate and verify in public: verifiable computation from attribute-based encryption [C]// Proceedings of the 2012 Theory of Cryptography Conference, LNCS 7194. Berlin: Springer, 2012: 422–439.
- [12] SCHWARTZ J T. Fast probabilistic algorithms for verification of polynomial identities [J]. Journal of the ACM, 1980, 27(4): 701–717.
- [13] CATALANO D, FIORE D, GENNARO R, et al. Generalizing homomorphic MACs for arithmetic circuit [EB/OL]. [2018-01-09]. <https://www.iacr.org/archive/pkc2014/83830238/83830238.pdf>.

This work is partially supported by the National Cryptography Development Fund of China (MMJJ20170112).

BAI Ping, born in 1990, M. S. candidate. His research interests include cryptology.

ZHANG Wei, born in 1976, Ph. D., professor. Her research interests include cryptology, information security.

WANG Xu'an, born in 1981, Ph. D., associate professor. His research interests include cryptology, information security.