基于前缀保持加密的网络功能外包系统

魏凌波[1,2]，冯晓兵[1]，张驰[1,2]，盛化龙[1]，俞能海[1]

（1. 中国科学技术大学信息科学技术学院中国科学院电磁空间信息重点实验室，安徽 合肥 230026；
2. 中国科学院信息工程研究所信息安全国家重点实验室，北京 100093）

摘 要：基于硬件中间盒实现的网络功能成本高且可扩展性差等问题，越来越多的企业用户将网络功能的实现外包给云服务商。现有的网络功能外包方案要求用户对云服商公开通信流量和网络功能策略，暴露了用户内网的私密信息。基于轻量级的前缀保持加密方案，提出一种保护隐私的网络功能外包系统。与现有同类方案相比，该系统不仅为企业用户同时实现了通信流量与网络功能策略的隐私保护，而且具有更高的吞吐量和更低的时延。

关键词：网络功能外包；云计算；前缀保持加密；隐私保护

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000-436x.2018057

Network function outsourcing system based on prefix-preserving encryption

WEI Lingbo[1,2], FENG Xiaobing[1], ZHANG Chi[1,2], SHENG Hualong[1], YU Nenghai[1]

1. CAS Key Laboratory of Electromagnetic Space Information, School of Information Science and Technology, University of Science and Technology of China, Hefei 230026, China
2. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract: Due to the problem of high cost and limited scalability of dedicated hardware middleboxes, it is popular for enterprises to outsource middleboxes as software processes to the cloud service provider. In the current network function outsourcing schemes, the cloud service provider requires the enterprise's communication traffic and network strategy which poses a serious threat to the enterprise's piracy. Based on prefix-preserving encryption, a privacy preserving network function outsourcing system was proposed. Compared with other similar schemes, the system not only realizes the privacy protection of communication traffic, but also has higher throughput and lower delay.

Key words: network function outsourcing, cloud computing, prefix-preserving encryption, privacy preserving

1 引言

网络功能如防火墙（firewall）、网络地址转换（NAT, network address translation）、深度分组检测[1]（DPI, deep packet inspection）通常是指在源主机和目的主机之间除了交换机和路由器之外的其他中间设备（middleboxes）实现的功能，是现代网络的重要组成部分。图 1 显示了包括防火墙、负载均衡（LB, load balance）在内的几个常用的网络功能。但传统的网络功能由硬件实现，存在着成本高、灵活性低和管理复杂等问题，而网络功能虚拟化可以解决上述问题。

网络功能虚拟化[2]把由硬件实现的网络功能转变为软件实现，可以降低成本并且提高网络功能的灵活性和扩展性，目前，被世界各地越来越多的组织所采用。近些年，随着云计算的发展，人们探索了

收稿日期：2017-10-28；修回日期：2018-01-17
通信作者：张驰，chizhang@ustc.edu.cn
基金项目：国家重点研发计划基金资助项目（No. 2017YFB0802200）；国家自然科学基金资助项目（No. 61702474）
Foundation Items: The National Key Research and Development Program of China (No. 2017YFB0802200), The National Natural Science Foundation of China (No. 61702474)

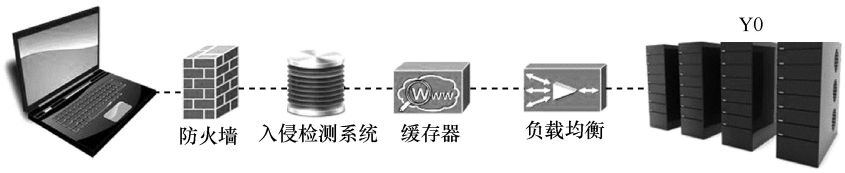


图 1 网络功能示例

网络功能外包部署的新模型，尝试由第三方代理来提供网络功能作为服务。目前，上述网络功能已经可以托管在公共云或嵌入在互联网服务提供商（ISP, Internet service provider）基础设施内的私有云中。将网络功能外包到云，可以获得云计算技术带来的优势，如降低成本和易于管理等。

然而，网络功能外包的同时，也对企业的隐私信息带来了挑战。在外包的过程中，未加密的通信流量和网络功能策略暴露给云服务商。因此，外包框架需要提供保密性、与现有基础设施的兼容性并具有高吞吐量。利用前缀保持的加密（prefix-preserving encryption）方案[3]匿名化 IP 地址，本文提出了一种具有隐私保护的网络功能外包系统（PPNFO, privacy preserving network function outsourcing），它实现了企业向云服务商外包多个网络功能，同时保护了通信流量和网络功能策略的隐私性。相比其他同类解决方案，它具有以下优势。

1) 允许云服务商执行 IP 地址匹配（例如，IP 地址是否在子域 128.0.0.0/24）或端口匹配（例如，端口是否在 500~1 000 范围内）。

2) 不仅保护网络功能策略的隐私，还保护了通信流量的隐私。而目前大多数的解决方案只考虑了网络功能策略的隐私保护，存在流量信息泄露给云服务商的问题。

3) 云服务商处理的是加密的流量，所以很难进行探测攻击。

2 国内外研究现状

现有的网络功能外包的研究工作大体分为以下 3 类：1) 提出网络功能外包的系统架构；2) 实现网络功能外包中策略的隐私保护；3) 实现网络功能外包中通信流量的隐私保护。

网络功能外包系统架构的研究主要有 Sherry 等[4]提出的 APLOMB 系统架构和 Gibb 等[5]的方案。APLOMB 系统将网络功能外包到云服务商，把流入和流出企业的数据流重定向到云端。文献[5]的方案可以使企业将网络功能外包到外部功能提供者，企业只需要转发数据，其他处理全部由外部功能提供者来执行；任何人都可以作为网络服务提供者，没有位置的限制。但这 2 种架构都没有考虑隐私保护问题。

基于上述架构，很多保护网络功能策略隐私的方案被提出来。文献[6]提出了 Ladon，将原始访问策略转换为防火墙决策图，并使用 Bloom filters 算法对防火墙决策图进行匿名化。但 Ladon 不能阻止公共云通过自由探测或仅仅通过传输窃听和分析来推导出原始的防火墙策略。文献[7]提出的 Ladon 混合云增强了 Ladon 的保密性，但用户仍需要在私有云中维护防火墙，且 Ladon 混合云已被证明是不安全的。Shi 等[8]提出了使用加密多线性映射[9]来模糊原始防火墙规则的框架 SOFA，云服务商通过过滤入站和出站通信来执行防火墙功能，但不能恢复原始的防火墙规则。SOFA 还容易受到探测攻击，存在安全漏洞[10]。文献[11]提出的方案考虑了防火墙和其他如负载均衡器、载波级 NAT、入侵检测系统和深度分组检测等网络功能。以上方案的缺点是部分网络功能外包给云，用户仍需要用自己的中间盒来执行剩余的网络功能，系统的通信开销和计算成本较高，没有考虑到通信流量隐私保护。

为了保护通信流量的隐私性，文献[12]提出了 BlindBox 框架，通过使用 HTTPS 协议利用中间盒进行通信，兼顾了网络功能策略隐私和通信流量隐私安全。但 BlindBox 支持的外包中间盒少，而且不适用于短期连接的应用程序。基于 BlindBox，文献[13]提出了一种支持多种网络功能外包方法 Embark，它提出了加密方案 PrefixMatch，可以使服务商快速执行前缀匹配，保证了加密分组的有效性。但该方案只能在明文域处理复杂的操作（除了允许/阻止）。Asghar 等[14]提出了 SplitBox，利用云虚拟机的分布式特性，给出了网络功能的抽象定义，并利用几个云为用户提供网络功能的协同计算。然而，该方案增加了系统的复杂性，且不支持网络功能服务链的外包。

以上 3 类工作的安全性逐步提高，但所采用的

加解密方法的计算复杂度仍有可降低的空间，对用户信息的隐私保护也有待加强。基于前缀保持的加密方法，本文提出了一种隐私保护的网络功能外包系统，同时实现了对用户网络功能策略和通信流量的隐私保护，而且比同类方案具有更高的吞吐量和更低的时延。

3　模型和假设

3.1　系统模型

本文系统使用了 APLOMB[4]架构，将企业通信流量重定向到云服务商。图 2 是 APLOMB 的通信模型：通信流量先被网关发送到云服务商，经过云服务商完成相关的处理之后，再返回到企业网关。特别地，若 2 个企业之间共享了密钥，通信流量信息经过云服务商处理之后便不再需要返回企业网关进行解密操作。

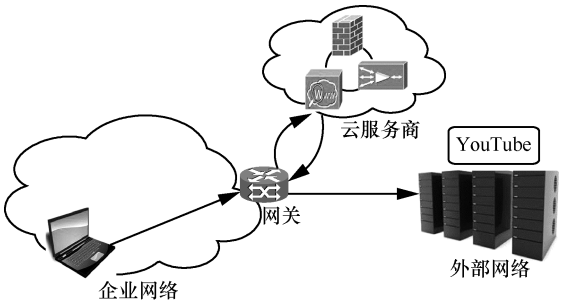


图 2　APLOMB 的通信模型

3.2　威胁模型

这里，假设云服务商是“诚实且好奇”的，或称之为“被动”攻击者[15]。不同于“主动”攻击者会恶意操纵数据、破坏正常运行的协议，“被动”攻击者会按照企业的要求提供很好的服务，并具有所有数据的访问权限，包括从网关接收到的通信流量和网络功能策略信息。另外，由于网关是由企业进行管理和维护的，本文假设网关是可以被信任的，不会泄露任何信息。

3.3　网络功能的形式化建模和分析

本文主要讨论包括防火墙、网络地址转换、负载均衡在内的网络核心功能，用 *Enc* 表示一个通用加密协议，*SIP* 表示源 IP 地址，*DIP* 表示目的 IP 地址，*SP* 表示源端口号，*DP* 表示目的端口号，*P* 表示协议，(*SIP*, *DIP*, *SP*, *DP*, *P*)表示一个连接的五元组，(*SIP*[],*DIP*[],*SP*[],*DP*[],*P*)表示一个规则。

来自不同供应商的防火墙可能具有显著不同的配置和规则，因此，需要提取出防火墙的一般模型。使用文献[16]中的模型，防火墙由多个访问控制列表（ACL, access control list）组成，每个 ACL 由一个规则组成，规则可以用形式（谓词, 动作）解释。其中，谓词定义为源/目标 IP 地址和端口以及协议的范围的组合，可能的动作集合包括“接受”和“拒绝”。一般防火墙具有以下性质。

$$\begin{aligned}&(SIP,\ DIP,\ SP,\ DP,\ P)\in\\&(SIP[],DIP[],SP[],DP[],P)\Leftrightarrow\\&Enc(SIP,\ DIP,\ SP,\ DP,\ P)\in\\&Enc(SIP[],DIP[],SP[],DP[],P)\end{aligned}$$

典型的 NAT 将一对源 IP 和端口转换为一对外部源 IP 和端口。一般来说，NAT 有以下要求。

1)相同的一对源 IP 和端口应映射到相同的外部源 IP 和端口。

2)不同的一对源 IP 和端口不应映射到相同的外部源 IP 和端口。

以下性质可以满足以上 2 个要求。

$$\begin{aligned}&(SIP_1,\ DIP_1)=(SIP_2,\ DIP_2)\Rightarrow\\&Enc(SIP_1,\ DIP_1)=Enc(SIP_2,\ DIP_2)\\&Enc(SIP_1,\ DIP_1)=Enc(SIP_2,\ DIP_2)\Rightarrow\\&(SIP_1,\ DIP_1)=(SIP_2,\ DIP_2)\end{aligned}$$

负载均衡维护一个服务器池，可分为 L3LB 和 L4LB。两者均要满足以下特性：相同的五元组应该转发到相同的服务器，即相同的五元组应具有相同的加密结果，不同的五元组加密结果则不同。

$$\begin{aligned}&(SIP_1,\ DIP_1,\ SP_1,\ DP_1,\ P_1)=(SIP_2,\ DIP_2,\ SP_2,\ DP_2,\ P_2)\Leftrightarrow\\&Enc(SIP_1,\ DIP_1,\ SP_1,\ DP_1,\ P_1)=Enc(SIP_2,\ DIP_2,\ SP_2,\ DP_2,\ P_2)\end{aligned}$$

通过以上分析可以发现，以防火墙、NAT、LB 为代表的网络功能都是对五元组进行操作。以防火墙为例，它查看数据分组的头部，按照数据分组的源地址和目的地址来决定数据分组应该接受还是拒绝。这类网络功能在本地会事先生成一个规则列表，每个规则对应相应的动作。云服务商按照规则对往来的数据分组进行匹配。

4　系统的设计与实现

4.1　PPNFO 总体框架

PPNFO 包含 4 个阶段：第一阶段是策略加密阶段，由企业完成线下操作，不需要实时性；第二阶段是通信流量加密阶段，由企业的管理员在本地完

成；第三阶段是匹配阶段，由云服务商来完成；第四阶段是通信流量解密阶段，在本地完成。PPNFO 应用了基于前缀保持的加密方法，可以使云服务商执行 IP 地址前缀匹配或端口匹配。图 3 是 PPNFO 系统的处理流程。

4.2 前缀保持加密

云服务商按照规则对往来的数据分组进行匹配，匹配方式可以分为 2 种，精确匹配和间隔匹配，例如，检查五元组是否满足（SIP_1, SP_1, DP_1, P_1, SIP_1）=（SIP_2, DIP_2, SP_2, DP_2, P_2），这属于精确匹配；检测端口范围是否在 1 000~2 000 之间或一个 IP 是否属于 56.24.67.0/16，这属于间隔匹配。间隔匹配可以定义成形式为 $f_{[a,b]}(x)$的布尔函数，当且仅当 $x\in[a,b]$时返回真。精确匹配是间隔匹配的一种特殊的情况，更容易实现。本文提出了有效解决前缀表示的间隔匹配的方法，也可用于精确匹配。

对于不是用前缀来表示的规则，首先，要将其转换为前缀表示。举例来说，间隔[32,111]，用 8 位二进制表示为[00100000,01101111]，可以转换成一组前缀的表示形式{001*,010*,0110*}。验证一个数是否在这个间隔中，等价于验证这个数是否和某一个前缀匹配。例如，37（二进制表示为 00100101）与前缀 001*匹配，则属于这个间隔；128（二进制表示为 10000000）不匹配任意一个前缀，则说明 128 不属于这个间隔。算法 1 给出了如何把间隔表示转换成前缀表示的方法。

算法 1 生成前缀

输入 $[p_1p_2\ldots p_n, q_1q_2\ldots q_n]$

步骤 1 for m=1 to n do

步骤 2 if $p_m < q_m$ then

步骤 3 记下 m，break

步骤 4 end if

步骤 5 end for

步骤 6 if 找不到 m

步骤 7 return $p_1p_2\ldots p_n$

步骤 8 else if 所有的 $i\in[m,n], p_i=0, q_i=1$ then

步骤 9 return $p_1p_2\ldots p_{m-1}*$

步骤 10 else

步骤 11 把$[p_1p_2\ldots p_n,\ q_1q_2\ldots q_n]$转变为$[p_1p_2\ldots p_{m-1}0p_{m+1}\ldots p_n,\ q_1q_2\ldots q_{m-1}011\ldots1]$和$[p_1p_2\ldots\ p_{m-1}100\ldots0,\ q_1q_2\ldots q_{m-1}0q_{m+1}\ldots q_n]$

步骤 12 将$[p_{m+1}\ldots p_n, 11\ldots1]$和$[100\ldots0, q_{m+1}\ldots q_n]$作为输入，从步骤 1 开始执行，分别产生前缀

步骤 13 return 所有前缀

步骤 14 end if

接下来，介绍由文献[3]提出的前缀保持加密。对前缀保持加密的定义如下，假设 a 和 b 有 k bit 相同的前缀，则加密后的密文 E(a)和 E(b)也应具有 k bit 相同的前缀。如果明文可以取 n 位数的任何值，则整个明文集合可以由高度为 n 的完整二叉树表示，称为明文树。注意到，整个可能的 IPv4 地址集合可以由高度为 32 的完整二叉树表示，每个地址由叶子节点表示。该树中的每个节点（不包括根节点）对应于一个由节点的高度指示的比特位置和由父节点的分支方向指示的比特值。图 4(a)即一棵明文树。

文献[3]提出的加密方法可以看作对明文树的

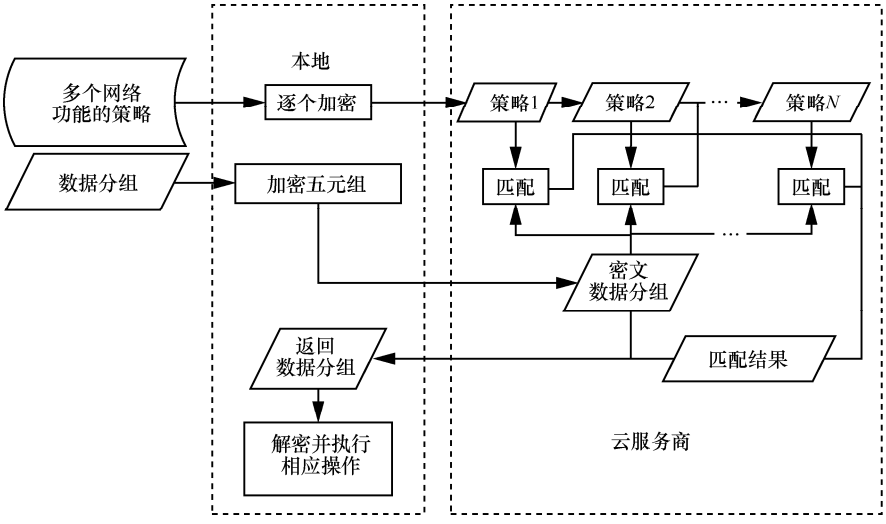


图 3 PPNFO 系统的处理流程

非叶子节点（包括根节点）指定一个二进制变量。此变量决定加密函数是否改变这个点的值。应用了加密函数后，明文树变成了密文树。图 4(b)表示加密树，图 4(c)表示经过图 4(b)处理后的密文树。从图 4 中可以看出，2 个明文串 001 和 010 具有 1 bit 相同的前缀，加密后分别为 111 和 100，同样具有 1 bit 相同的前缀。

用 f_i 来表示加密函数，i=1,2,⋯,n−1，f_0 是一个常数函数。a=$a_1a_2\cdots a_n$ 表示明文，密文用 a'=$a'_1a'_2\cdots a'_n$ 来表示。对于每一个 a'_i，计算 a'_i=$a_i\oplus f_{i-1}(a_1a_2\cdots a_{i-1})$，然后得到密文 a'=$a'_1a'_2\cdots a'_n$。

所使用的 f_i 定义为

$$f_i(a_1a_2\cdots a_i)\coloneqq \mathcal{L}\left(\mathcal{R}\left(\mathcal{P}\left(a_1a_2\cdots a_{i-1}\right),k\right)\right),$$
$$i=0,1,\cdots,n-1 \tag{1}$$

其中，$\mathcal{L}$ 返回“最低有效位”。$\mathcal{R}$ 是伪随机函数或伪随机置换，如文献[17]。$\mathcal{P}$ 是填充函数，扩展 $a_1a_2\cdots a_i$ 为一个与 $\mathcal{R}$ 的块大小匹配的更长的字符串。k 是伪随机函数 $\mathcal{R}$ 中使用的密钥，其长度应该遵循伪随机函数的要求。

4.3　PPNFO 系统

基于前缀保持的加密方法，提出的 PPNFO 系统不仅可以支持防火墙的外包，还可用于 NAT、负载均衡的外包。该系统主要由 4 个阶段组成。

1) 策略加密阶段

此阶段的主要目的是保护网络策略的隐私性，该部分操作是非交动的，在企业本地完成。网络功能策略不发生变化的情况下，该阶段只需在初始化时执行一次。另外该系统支持策略的实时更新。策略更新之前，网关要向云服务商发送信号。然后，网关对新的网络策略进行加密处理并发送给云服务商。在这段时间内，云服务商基于旧的网络策略对通信流量进行处理。一旦网关将所有待更新的策略处理完，便向云服务商发送信号，要求它交换新的数据。收到信号之后的云服务商处理完当前的通信流量后，便更换所有新的网络策略，并通知网关策略已经更新。前缀保持加密算法如算法 2 所示。

算法 2　前缀保持加密

输入　$[p_1p_2\cdots p_i]$

步骤 1　for i=1 to n do

步骤 2　　$p'_i=p_i\oplus g_{i-1}(p_1p_2\cdots p_{i-1})$

步骤 3　return $p'_1p'_2\cdots p'_{i-1}$

2) 通信流量加密阶段

对于往来的通信流量，企业的管理员仍要对其进行加密，然后发送给云服务商。对网络功能策略和通信流量的双重加密，使云服务商无法获取企业的隐私信息，进一步确保了系统的安全性。

以一个数据分组为例，对于到达企业网关的数据分组，首先提取出与网络策略相关的域。本文选择源 IP、目的 IP、源端口和目的端口，然后进行加密处理。加密后的域重新填充到数据分组覆盖掉原来的值，得到新的数据分组，最后将其发送给云服务商。具体如算法 3 所示。

算法 3　通信流量加密

输入　原始通信流量 x

步骤 1　取出 SIP, DIP, SP, DP

步骤 2　　then 转换 SIP, DIP, SP, DP 为二进制形式

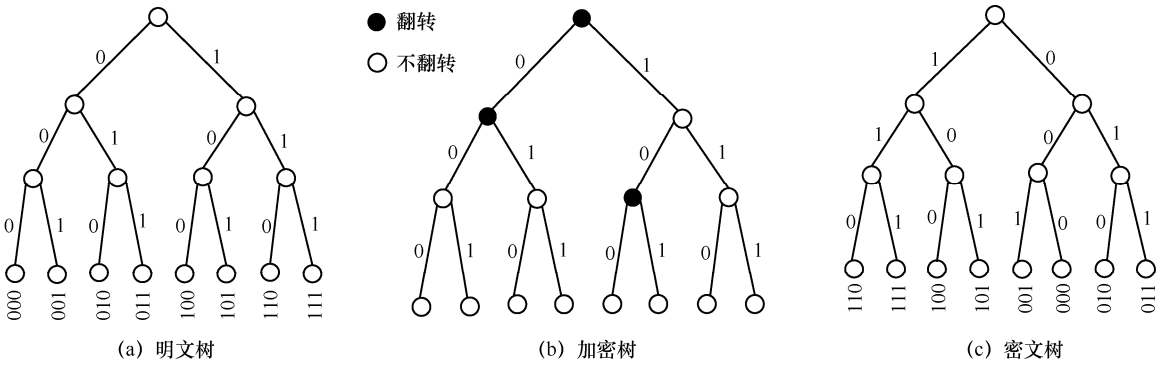
步骤 3　加密 SIP, DIP, SP, DP 得到 SIP', DIP', SP', DP'

步骤 4　　将 SIP, DIP, SP, DP 替换为 SIP', DIP', SP', DP'

步骤 5　return x'

3) 匹配阶段

此阶段由云服务商来完成，由于需要处理大量实时的数据分组，所以对性能的要求很高。对于每



(a) 明文树　　(b) 加密树　　(c) 密文树

图 4　前缀保持加密示例

个到来的数据分组，云服务商对其进行匹配操作。若策略匹配的结果为“拒绝”，则直接丢弃数据分组；若为“接受”，则将数据分组返回企业网关。具体如算法 4 所示。

算法 4 匹配

输入 通信流量 x'、策略 r'

步骤 1 for i =1 to n do

步骤 2 $r_i'=\{SIP_i', DIP_i', SP_i', DP_i'\}$

步骤 3 if $SIP'= SIP_i'$, $DIP' = DIP_i'$, $SP'= SP_i'$, $DP' = DP_i'$

步骤 4 $x'= r_i'$

步骤 5 else

步骤 6 下一条策略

4) 通信流量解密阶段

云服务器在完成通信流量匹配之后，会将符合规则的数据分组返回企业网关。由于网关之前对这个数据分组进行了加密操作，所以仍需要解密还原出原始的数据分组，然后将数据分组发送到对应的目的地址。具体如算法 5 所示。

算法 5 解密

输入 $[p'_1p'_2\cdots p'_n]$

步骤 1 for i =1 to n do

步骤 2 $p_i= p'_i \oplus g_{i-1}(p'_1p'_2\cdots p'_{i-1})$

步骤 3 return $p_1p_2\cdots p_n$

4.4 安全性分析

这里，假设企业网络和外部网络、云服务商之间的连接是在公共网络上，所以攻击者可以窃听并下载加密的消息。本节分析基于前缀保持加密方案的安全性。文献[3]已经证明式(1)实现的功能和一个随机的前缀保持函数是相同的。而且如 4.2 节中所述，当明文可以取任意 n bit 的值时，前缀保持加密函数分组含 2^{n-1} 个二进制变量。所以，密钥有 2^{2^n-1} 种可能性。例如，若 n 为 16，则可能的密钥有 $2^{265\,535}$ 种。因此，式(1)中的 k 有足够多的选择域，攻击者通过暴力攻击的手段破解系统是不切实际的。

对于已知明文攻击，由于加密机制具有前缀保持的特性，攻击者可以从其他密文里推断信息。例如，如果攻击者获取一个明文密文对 $<a_1a_2\cdots a_n, a'_1\ a'_2\ \cdots a'_n>$，然后知道另一个密文 $<a'_1a'_2\cdots a'_{k-1}\overline{a'_k}\ b_{k+1}\cdots b_n>$，那么攻击者将会知道 k 位前缀对应的明文是 $<a_1a_2\cdots\overline{a_k}>$。注意，如果攻击者知道一个明文密文对 $<a_1a_2\cdots a_n, a'_1\ a'_2\ \cdots a'_n>$，也会知道另外一个明文密文对 $<a_1a_2\cdots\overline{a_n}, a'_1a'_2\cdots\overline{a'_n}>$。所以，攻击者总是知道偶数对<明文, 密文>。

假设攻击者知道 2 对<明文, 密文>。给定一个随机的密文，使 $A(n)$表示可以推断出来的前缀的平均长度。明文的 k bit 前缀被推断出的概率是 $\frac{1}{2^k}(1\leqslant k\leqslant n-1)$，若 $k=n$，则概率是 $\frac{2}{2^n}$，因此，有

$$A(n)=\sum_{i=1}^{n-1}\frac{i}{2^i}+\frac{2n}{2^n}=\sum_{i=0}^{n-1}\frac{1}{2^i}=2-\frac{1}{2^{n-1}}<2 \qquad (2)$$

即如果已知 2 对<明文, 密文>，而攻击者从一个随机的密文上推断出的信息平均不超过 2 bit。

若攻击者已知 k 对<明文, 密文>。当 $n\to\infty$时，给定一个密文，攻击者可以推断出的平均长度为 lb$k$+2[3]。因此，攻击者通过比较一个密文和已知的<明文, 密文>获取的前缀信息是有限的。所以，即使攻击者获取到了一些<明文, 密文>，系统也是安全的。当然，这对系统来说是一个潜在的威胁，因为攻击者了解更多的<明文, 密文>对，就会推断出更多的信息。因此在使用过程中，可以定期更新密钥，这时攻击者了解的<明文, 密文>便没有任何用处。

综上，本文采用的前缀加密方法可以有效地抵抗攻击者的暴力攻击和已知明文攻击；在面对“诚实且好奇”的云端服务器时，可以保护企业网络功能策略和通信流量的隐私性。

5 系统实验测评

5.1 实验环境

硬件环境：CPU 是 Intel(R) Core i3-4130，内存是 DDR3 12 GB，硬盘是 1 TB 7 200 转/秒。开发环境：开发操作系统使用了 Ubuntu14.04，开发语言及工具分别为 C/C++、Click 模块路由器。

5.2 实验结果

Embark 和 SplitBox 实现了与 PPNFO 系统相同的隐私保护功能，它们对通信流量和网络功能策略进行了加密，具有很高的安全性。在本节中，将这 2 种方案与本文系统作比较。由于策略加密阶段是在本地完成的，对网络功能外包性能的影响可以忽略不计，3 种方案的此阶段不作比较，而主要比较通信流量加密阶段和匹配阶段的性能。

1) 策略加密阶段的开销

图 5 显示了 PPNFO 随着网络功能策略数量的增加平均时间成本的变化。策略加密阶段只需要一次而且只在网络策略变化时才会进行加密。从图 5 中可以看出，随着网络策略的数量增长，时间开销大致呈线性增加。PPNFO 加密 30 个防火墙策略的时间约为 4.08 ms。这个时间很短，完全不会影响网络功能外包的性能。

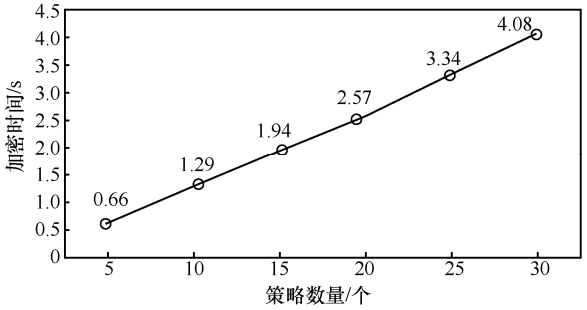


图 5　策略加密阶段开销实验结果

2) 通信流量加密阶段的开销

对于每个传入和传出的数据分组，需要实时地进行通信流量加密。图 6 显示出了 PPNFO 通信流量加密时间随着数据分组增长的时间开销。为了验证 PPNFO 可以实时地进行通信流量加密，实验中分别采用 10^1、10^2、10^3、10^4、10^5 个数据分组计算时间代价，可以看到，在数据分组数量不大的情况下，计算耗时与数据分组数量几乎呈线性关系，在数据量较大时甚至整体性能要优于线性复杂度。这种性能已经符合通信流量处理的实时性要求，且处理相同数量的数据分组，PPNFO 用时最少。

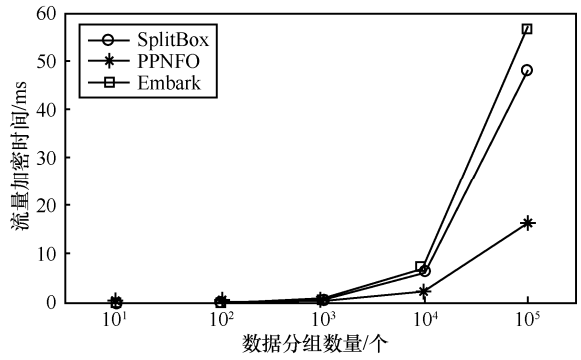


图 6　通信流量加密阶段开销实验结果

3) 匹配阶段的开销

匹配阶段包括执行策略检查以及将分组返回给网关。PPNFO 与其他 2 种方案的匹配时间随着防火墙策略数量的变化曲线如图 7 所示。本实验执行了 1 000 万个数据分组，从图 7 中可以看出，3 种方案的匹配时间都随着防火墙策略数量的增加而增加。但在防火墙策略数量相同的情况下，PPNFO 实验效果最优。

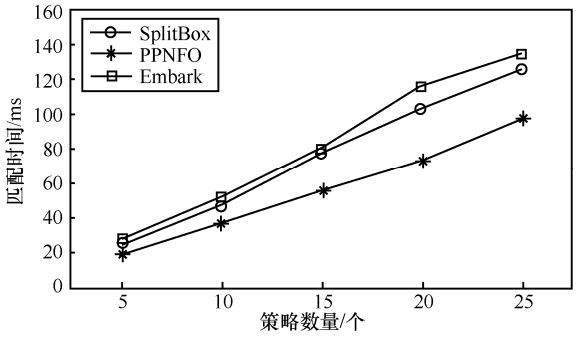


图 7　时间开销随网络功能策略数量变化

3 种方案的网络吞吐量随着防火墙策略数量的变化曲线如图 8 所示。这里，吞吐量的单位是 Gbit/s，代表了系统所能达到的传输速率。从图 8 中可看出，随着防火墙策略数量的增加，3 种方案的吞吐量都在降低。在网络功能策略数目相同的前提下，PPNFO 吞吐量最大，大约是其他 2 种方案的 1.5 倍。

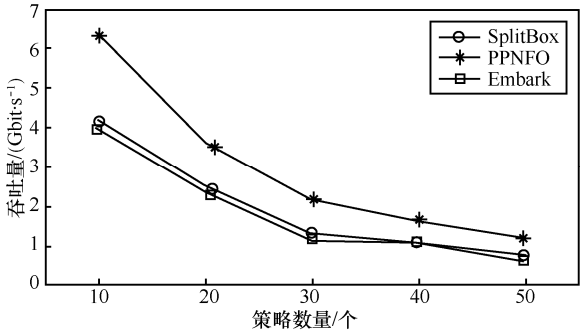


图 8　3 种方案的吞吐量比较

6　结束语

目前，网络功能已经成为人们生活中不可或缺的一部分。随着网络功能虚拟化和云计算技术的发展，越来越多的企业将自己的网络功能外包给云服务商来实现和维护。然而，在网络功能外包的过程中，存在着安全隐患。本文利用前缀保持的加密方案设计和实现了网络功能外包系统，解决了网络功能外包中的隐私保护问题。最后以防火墙为测试用例进行了实验验证，结果表明 PPNFO 比同类方案具有更高的吞吐量和更低的时延，降低了企业和云服务商的成本。

参考文献：

[1] 于强, 霍红卫. 一组提高存储效率的深度包检测算法[J]. 软件学报, 2011, 22(1): 149-163.
YU Q, HUO H W. Algorithms improving the storage efficiency of deep packet inspection[J]. Journal of Software, 2011, 22(1): 149-163.

[2] 袁泉, 汤红波, 黄开枝, 等. 基于 Q-learning 算法的 vEPC 虚拟网络功能部署方法[J]. 通信学报, 2017, 38(8): 172-182.
YUAN Q, TANG H B, HUANG K Z, et al. Deployment method for vEPC virtualized network function via Q-learning[J]. Journal on Communications, 2017, 38(8):172-182.

[3] XU J, FAN J, AMMAR M H, et al. Prefix-preserving IP address anonymization: measurement-based security evaluation and a new cryptography-based scheme[C]//10th IEEE International Conference on Network Protocols. 2002: 280-289.

[4] SHERRY J, HASAN S, SCOTT C, et al. Making middleboxes someone else's problem: network processing as a cloud service[J]. ACM SIGCOMM Computer Communication Review, 2012, 42(4): 13-24.

[5] GIBB G, ZENG H, MCKEOWN N. Outsourcing network functionality[C]//The First Workshop on Hot Topics in Software Defined Networks. 2012: 73-78.

[6] KHAKPOUR A R, LIU A X. First step toward cloud-based fire-walling[C]//2012 IEEE 31st Sym-posium on Reliable Distributed Systems (SRDS). 2012: 41-50.

[7] KUREK T, NIEMIEC M, LASON A. Taking back control of privacy: a novel framework for preserving cloud-based firewall policy confidentiality[J]. International Journal of Information Security, 2016, 15(3): 235-250.

[8] SHI J, ZHANG Y, ZHONG S. Privacy-preserving network functionality outsourcing[J]. arXiv preprint, arXiv:1502.00389, 2015.

[9] CORON J S, LEPOINT T, TIBOUCHI M. Practical multilinear maps over the integers[M]//Advances in Cryptology–CRYPTO. 2013: 476-493.

[10] CHEON J H, HAN K, LEE C, et al. Cryptanalysis of the multilinear map over the integers[M]//Advances in Cryptology–EUROCRYPT 2015: 3-12.

[11] MELIS L, ASGHAR H J, DE CRISTOFARO E, et al. Private processing of outsourced network functions: feasibility and constructions[C]//The 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization. 2016: 39-44.

[12] SHERRY J, LAN C, POPA R A, et al. Blindbox: deep packet inspection over encrypted traffic[J].ACM SIGCOMM Computer Communication Review, 2015, 45(4): 213-226.

[13] LAN C, SHERRY J, POPA R A, et al. Embark: securely outsourcing middle-boxes to the cloud[C]//13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16). 2016: 255-273.

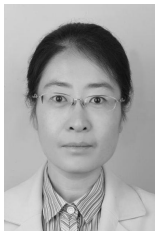
[14] ASGHAR H J, MELIS L, SOLDANI C, et al. SplitBox: toward efficient private network function virtualization[C]//The Workshop on Hot Topics in Middleboxes and Network Function Virtualization. 2016: 7-13.

[15] MATT B. Introduction to computer security[M]. Pearson Education India, 2006.

[16] WANG C, CHOW S S M, WANG Q, et al. Privacy-preserving public auditing for secure cloud storage[J]. IEEE transactions on computers, 2013, 62(2): 362-375.

[17] DAEMEN J, RIJMEN V. The design of Rijndael: AES-the advanced encryption standard[M]. Springer Science & Business Media, 2013.

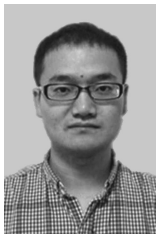
[作者简介]



魏凌波（1979-），女，陕西周至人，博士，中国科学技术大学副研究员，主要研究方向为应用密码学。

冯晓兵（1992-），女，山东聊城人，中国科学技术大学硕士生，主要研究方向为网络安全。

张驰（1977-），男，湖北武汉人，博士，中国科学技术大学副教授，主要研究方向为无线网络与网络安全。



盛化龙（1991-），男，安徽阜阳人，中国科学技术大学硕士生，主要研究方向为网络安全。

俞能海（1964-），男，安徽无为人，中国科学技术大学教授，主要研究方向为多媒体数据处理与分析、数字内容安全。