FutureGenerationComputerSystems71（2017）177-191



ScienceDirect提供的内容列表

未来一代计算机系统

期刊主页：www.elsevier.com/locate/fgcs





PICADOR：使用代理重新加密的端到端加密发布-订阅信息分发

✩

CristianBorcea和Arnab''Bobby''DebGupta和YuriyPolyakova，b，KurtRohloff和GerardRyanand

美国新泽西州网络安全研究中心和新泽西理工学院计算机科学系，纽瓦克，新泽西州07102，美国

bCSAIL，麻省理工学院，剑桥，MA02139，USA

强调

•本文介绍PICADOR，一种使用代理重新加密的端到端加密发布-订阅信息分发系统。•PICADOR提供具有端到端加密的信息分发服务，其中发布者和订阅者不需要共享加密和解密密钥。PICADOR确保端到端的信息机密性。

•我们设计并实现了一种新颖的代理重新加密（PRE）方案，该方案利用通用的网格加密软件库，并使用可扩展的基于Java的信息基板对我们的系统进行原型设计。

•我们通过实验评估企业和移动应用程序环境中的性能和可伸缩性权衡。

articleofo

文章记录：2016年5月1日收到修订后的2016年10月5日收到2016年10月8日接受2016年10月17日在线提供

关键词：安全加密信息代理

abstract

本文介绍PICADOR，一种使用代理重新加密的端到端加密发布-订阅信息分发系统。PICADOR专为基于主题的发布/订阅系统而设计，并提供端到端的有效负载机密性。PICADOR的主要新颖之处在于它提供了一种具有端到端加密的信息分发服务，其中发布者和订阅者不需要建立共享加密和解密密钥。多个发布者将加密信息发布到Pub/Sub代理，该代理使用代理重新加密（PRE）将此信息转换为只能由经过批准的订阅者解密的表示。经纪人无法解密信息。为了支持PICADOR，我们设计并实现了一种利用通用网格加密软件库的新颖PRE方案。我们使用可扩展的基于Java的信息基板对系统进行原型设计，该基板支持基于主题的发布/订阅操作。我们通过实验评估企业和移动应用程序环境中的性能和可伸缩性权衡。我们讨论设计权衡和特定于应用程序的自定义。©2016ElsevierB.V.保留所有权利。

1.简介

发布-订阅（Pub/Sub）信息分发提供

一种灵活的异步方法来分发信息

✩本研究得到国家安全局（NSA）的资助H98230-15-1-0274和国家科学基金会（NSF）的资助，编号为CNS1409523和DGE1565478.任何意见，发现，结论或建议均表示在这些材料中是作者的材料，并不一定反映NSA和NSF的观点。尽管有任何版权声明，美国政府仍有权复制和分发重印。\*通讯作者。

电子邮件地址：borcea@njit.edu（C。Borcea），ad479@njit.edu（ABDGupta），polyakov@njit.edu（Y。Polyakov），rohloff@njit.edu（K。Rohloff），gwryan@njit.edu（G。Ryan）。

信息产生者（即出版商）和信息消费者（即订阅者）之间的关系[1]。此分布模型在需要从可能的多个源聚合信息并分发给与信息生产者没有直接联系的消费者的环境中非常有用。发布者和订阅者不需要直接相互交互或共享身份信息。Pub/Sub系统有两种主要类型：基于主题和基于内容。本文重点介绍基于主题的发布/订阅系统：发布者将具有元数据主题标签的信息发布到发布/订阅代理，此代理将发布的信息分发给为特定主题注册的订阅者。

受益于Pub/Sub系统的示例用例在

企业医疗领域，患者过去的医疗记录需要与急救医疗服务提供者共享。在这种情况下

http://dx.doi.org/10.1016/j.future.2016.10.0130167-739X/©2016ElsevierB.V.保留所有权利。

178C.Borcea等。/FutureGenerationComputerSystems71（2017）177-191

保险提供者可以操作Pub/Sub系统来支持过去医疗记录的分发[2,3]。另一个例子，在战术/移动军事领域，当通过地理区域的多个军事单位产生图像或其他信息时。这些单位可能无法直接互动[4,5]，但共享信息会带来明显的好处。在这个军事示例中，当地的前方作战基地或飞行的无人驾驶飞行器可以维持一个发布/订阅经纪人以支持单位之间的信息共享。

Pub/Sub系统面临的主要挑战，如图所示

这两个例子的应用领域是由Pub/Sub代理分发的信息的机密性。现有的发布/订阅系统通过加密保护信息有效载荷，加密要求：（1）发布者和订阅者协调以建立加密和解密密钥或（2）发布者/子代理解密来自发布者的信息有效载荷，然后加密该信息有效载荷再次传输给用户。第一种解决方案与Pub/Sub系统的目标之一相矛盾，即发布者和订阅者的分离。第二个解决方案解决了这个问题，但让代理可以访问未受保护的信息。因此，它使经纪人成为对手妥协和窃取敏感信息的成熟目标[6]。

运行这些可以减轻这些安全限制

Pub/Sub代理仅在可信计算环境中，但这些环境的设置和维护成本很高，因为它们需要专门的管理和专用设施的安装[7]。此外，限制在可信环境中部署限制了Pub/Sub系统的实际适用性。

本文介绍了PICADOR，一个端到端的系统

使用代理重新加密的加密发布-订阅信息分发。PICADOR使用代理重新加密（PRE）[8,9]来维护基于主题的发布/订阅系统中从发布者到订阅者的有效负载的端到端加密。我们的系统不要求发布者或订阅者直接先验地进行交互。PICADOR的PRE功能可以在代理处对发布者加密的有效负载进行安全的重新加密，以便授权订户可以解密有效负载。PICADOR保证代理无法解密有效负载信息。通过这种方式，PICADOR可确保端到端的机密性，同时改善发布者和订阅者的分离。

除了PICADOR系统架构，第二个

本文的主要贡献是一种新颖的PRE方案，基于可证明安全的基于格的密码系统[10]。该PRE方案是单向的。我们的加密设计还具有“后量子”的好处，这意味着它可以抵抗量子计算攻击[11-13]。除了信息有效载荷的机密性之外，PICADOR中的PRE技术还可以与订阅隐私技术[14]组合以保护订阅的隐私（即，主题元数据，其保持未加密以实现代理）。

我们使用可扩展的基于Java的信息对PICADOR进行原型设计

支持Pub/Sub操作的基板。实验结果表明，PICADOR的性能在医疗保健和军事等应用领域非常实用。PICADOR为基于文本的应用程序提供低延迟，适用于没有严格延迟限制的多媒体应用程序。我们通过实验观察到PICADOR操作是计算限制的，这意味着可以通过相对简单且经济高效的多线程和多核增强来提高性能，而不是更昂贵且通常不可行的增加带宽配置。

本文的其余部分组织如下。第2节介绍

PICADOR的概述。第3节描述了我们的新颖PRE方案并分析了它的安全性。第4节介绍了体系结构和

执行PICADOR。第5节评估我们的系统并提供从我们的实验结果中得出的见解。第6节介绍相关工作。第7节讨论了结论和未来的工作。

2.PICADOR概述

PICADOR有两个主要贡献：（1）一个新颖的系统ar-

用于在基于主题的Pub/Sub系统中提供有效载荷机密性的架构;（2）新的PRE方案，使我们的加密协议能够实现安全的发布者/订阅者交互。系统架构解决了设计安全的Pub/Sub交互机制的挑战，这些机制可以在保持有效负载机密性的同时更好地为关键管理直接发布/订阅者交互。新的PRE方案解决了公钥PRE方法遇到的实用性/性能挑战，并增加了发布者/订阅者交互的解耦。

PICADOR的系统架构使用代理重新加密（PRE）

允许订阅者接收和解密他们打算接收的加密数据的功能，而无需直接与数据发布者协调他们的密钥。PRE[15]能够在不解密的情况下将密文从一个密钥安全地重新加密到另一个密钥。从高级别的角度来看，发布者使用主题元数据标记其内容并加密内容数据。发布者/子代理接收由发布者加密的数据并对其重新加密，使得只有预期的订阅者可以解密它。拥有重新加密密钥不会为代理提供对数据的访问权限。以这种方式，在订户和发布者之间保证加密的有效载荷数据的端到端机密性。此外，启用PRE的代理允许与基于主题的代理进行灵活通信，因为可以随时向系统添加新的发布者，订阅者和主题。即使发布者或经纪人不是先验地知道这些新主题和订阅者，代理也可以重新加密这些新主题和订阅者的数据。

我们的新颖PRE方案解决了两个主要的实际挑战

关于密文扩展和操作延迟。密文扩展的挑战是密文可能比明文大得多。延迟问题是加密，解密和重新加密操作对于需要低延迟的应用程序可能需要太长时间。我们的PRE方案提供低密文扩展，这意味着PICADOR具有空间效率，使用更少的磁盘空间来加密信息，减少带宽使用要求，并且总体上导致实际吞吐量。该方案还具有时间效率，与其他PRE方案原型相比，在PICADOR中实现了低延迟通信。

PICADOR承认的限制是它需要更多的

注册订阅的推定和组织开销，这意味着它可能不适合在部署后快速添加许多发布者和订阅者的情况。如第1部分所述，PICADOR也不保护注册订阅的隐私，主题匹配明确，但这个问题可以通过利用现有的解决方案来解决[14]。PICADOR的当前设计也是集中的，具有单个代理实例。我们讨论了一种缩放PICADOR的方法，其中多个代理并行运行。

2.1。威胁模型

从机密性-完整性保证（CIA）安全性

分析视角，PICADOR解决了诚实但好奇的对手的机密性问题，这些对手彻底破坏了Pub/Sub经纪人。我们不关注完整性和身份验证问题，因为我们的PRE支持并未直接解决这些问题，而是关注我们的保密性贡献。我们

C.Borcea等。/FutureGenerationComputerSystems71（2017）177-191179

可以从设计角度解决可用性（通过复制），但我们主要将此留待将来工作。我们在第7节中提供了有关完整性，身份验证和可用性方面的更详细讨论。

2.2。基本操作

PICADOR的基本用法如图1所示。爱丽丝想要

将信息发布到启用PRE的代理（即，发布/订阅代理1），并且Bob是对该信息感兴趣的订户。该图还显示了执行发布者和订阅者软件的客户端。策略管理机构帮助进行密钥管理，并保持对谁从代理接收哪些信息的控制。我们假设政策机构是受信任的（例如，它不与可能诚实但古玩的经纪人勾结）。策略授权（PA）旨在设置重新加密策略，而不涉及资源密集型操作，如数据加密或代理重新加密。

图2详细说明了图1中所示的基本操作

下面，我们解释这个工作流程：

1.政策机构为其生成一对公钥/私钥

爱丽丝，pkA/skA。它将公钥pkA发送给Alice。这可能是离线操作。

2.Bob生成一对公钥/私钥pkB/skB。他寄出

他的公钥pkB给政策局。策略授权基于Alice的私钥skA和Bob的公钥pkB生成重新加密密钥rkAB。它将rkAB发送到启用PRE的代理。这可能是离线操作。

3.Alice用主题元数据标记消息m，用m加密

她的公钥pkA并将此密文cA与元数据一起发送给经纪人。

4.根据Bob批准的主题订阅，经纪人重新

用重加密密钥rkAB加密密文cA，使得Bob能够解密cB并获得由Alice加密的原始信息。

5.Bob从代理检索重新加密的密文cB

并用他的秘密密钥skB解密它。发布者的公钥/私钥对（由...生成）

策略权限）和订阅者（​​自生成）通常在部署之前创建。但是，它们也可以按需创建。

2.3。设计注意事项

在PICADOR中，多个订户可能会收到信息

来自多个发布者，发布者的信息可以流向多个订阅者，从而支持一对一，多对一，一对多和多对多的信息流。启用PRE的代理根据内容的主题和授权的发布者/订阅者对路由内容。发布者将消息发送到主题（而不是特定订户），并且订阅者向代理注册感兴趣的主题。如果获得授权，订阅者可以解密发布者发布的关于他们感兴趣的主题的消息。

基于主题的寻址信息以元数据编码

未加密的，例如地理时间坐标，关键字或其他相关信息。编码是使用特定于域的策略语言完成的[16-18]。

经纪人使用他们的公钥识别订户，

它们还与其重新加密密钥相关联。为此，代理维护从主题到订阅者的映射，

1我们使用术语''broker'来表示托管在''服务器''上的Pub/Sub和PRE软件，我们使用''server''来表示Pub的计算设备/Sub和PRE''broker''托管在。

在将新订户添加到系统时更新。订阅者添加或删除感兴趣的主题时，地图也会更新。代理还维护从批准的发布者/订阅者对到重新加密密钥的映射。当发布者发布有关特定主题的信息时，代理会识别可能感兴趣的订阅者。然后，它查找发布者/订阅者对以找到他们的重新加密密钥。如果存在映射中的条目，则代理使用相关的重新加密密钥来执行重新加密操作，以便批准的订户可以解密信息。还必须更新地图，因为需要为新发布者添加新的重新加密密钥。

在PICADOR，经纪人必须有一个独特的

每个发布者/订阅者对的加密密钥。这为政策制定机构提供了肯定的批准权限，使各个出版商能够与个人订户进行通信。但是，这也意味着PICADOR的扩展程度与先前的Pub/Sub设计不同，后者不需要外部批准和重新加密密钥生成。由于与政策机构的必要互动，随后需要更长时间才能注册订阅。因此，PICADOR更适合用户流失率不高的应用。例如，PI-CADOR预计可以很好地用于在部署之前使代理加载了初始重新加密密钥的应用程序，并且以相对较低的频率添加其他发布者，订阅者和重新加密密钥。

一个重要的设计决策是生成重新加密

政策机构的关键，而不是出版商。我们这样做是为了改善发布者和订阅者的脱钩。通过这种设计，发布者和订阅者不需要知道彼此的信息，这提高了Pub/Sub系统的可伸缩性和安全性。

我们的设计将信任从出版商推向政策制定者-

ity，以及从发布者到代理的计算工作量和带宽要求。策略机构根据重新加密密钥的生成来确定谁可以共享信息。代理使用从策略颁发机构接收的信息访问策略，结合生成的重新加密密钥，确定应将发布者的哪些信息子集发送给订阅者。通常具有最低计算/网络能力（例如，移动设备）的发布者和订阅者需要最低的计算工作量并且仅需要维护单个密钥，因此简化了部署。

政策机构无需经营和支持

端口重新加密在线操作。此外，它可能不经常与经纪人交往。因此，它可以在较低带宽的通信链路（例如卫星）上运行，而发布者，代理和订户之间的通信可能需要通过更高带宽的通信链路，例如地面无线电或有线以太网。

可以扩充PICADOR以支持消息完整性。每

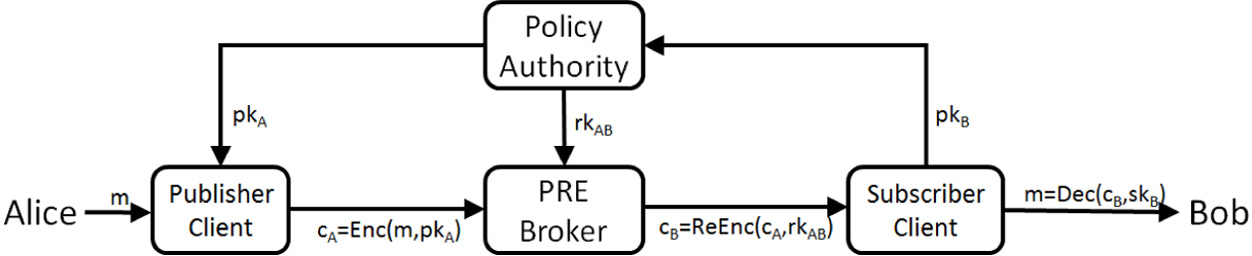
发布者可以使用RSA或EllipticCurve数字签名算法为数字签名生成传统的公钥/私钥对，这些算法目前包含在NSASuiteB[19]中，作为公认的标准安全数字签名技术。每封邮件都使用发布者的私钥进行签名，并由代理使用发布者的公钥进行验证。最后，PRE方案保证了订户接收的消息的完整性。

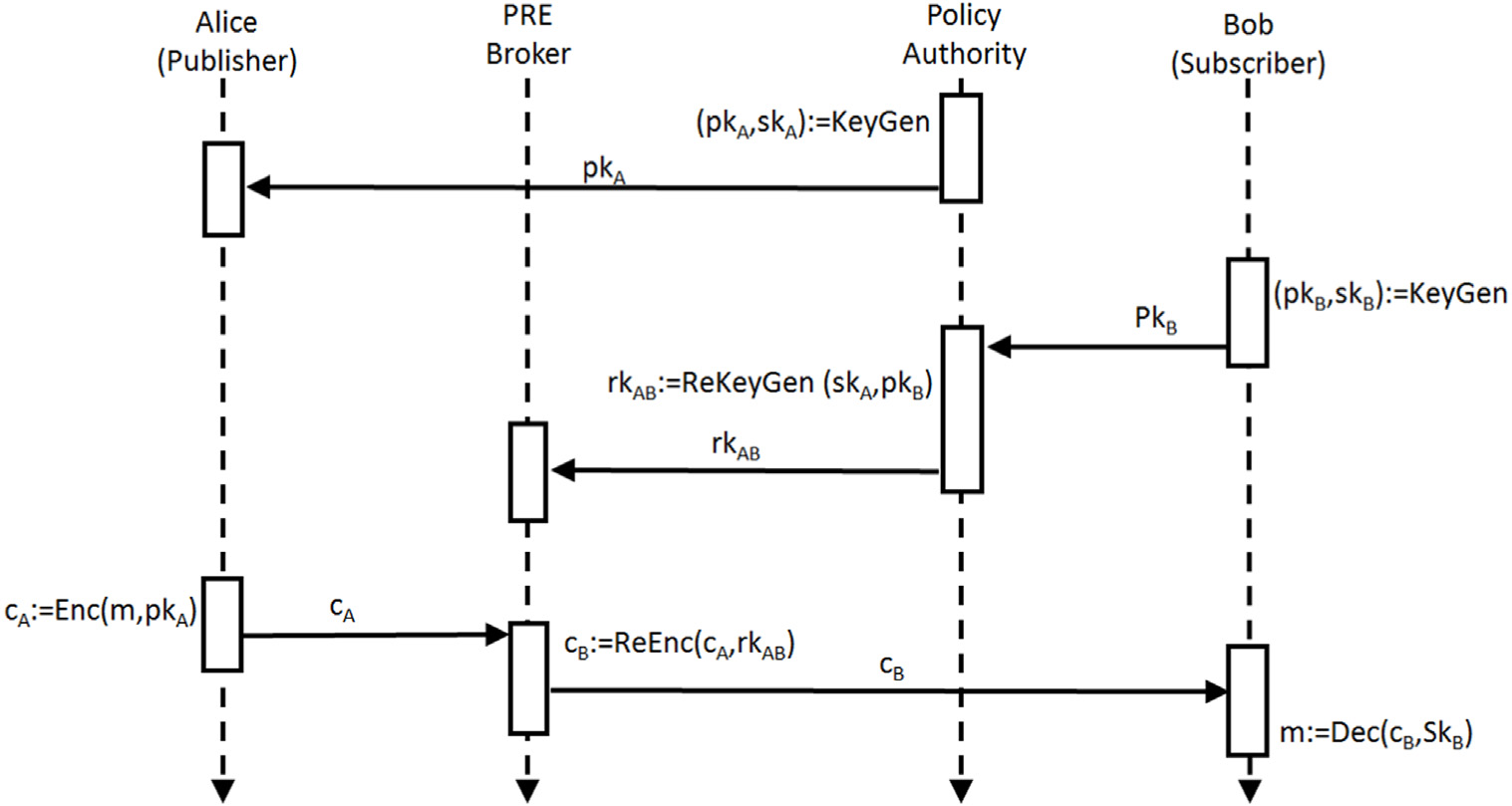
3.PRE加密系统

本节介绍PICADOR的新颖PRE密码系统。我们

首先讨论现有PRE方案在Pub/Sub系统中考虑时所面临的挑战。接下来，我们将概述我们的解决方案，并解释它如何解决现有PRE方案的已知挑战。在涵盖理论之前

180C.Borcea等。/FutureGenerationComputerSystems71（2017）177-191





在我们的解决方案的各个方面，我们介绍了在提出的PRE方案中使用的一些格子加密的概念。然后，该部分继续对我们的解决方案进行正式描述，最后讨论所提出的PRE方案的参数选择。

3.1。现有PRE计划的挑战

PRE方案通常分为双向[15,20,21]

和单向的[8,9,22-24]。在双向方案中，重新加密密钥不仅可以用于将加密数据从发布者加密转换为用户加密，而且可以反过来从订阅者加密转换为发布者加密。大多数双向方案需要在重新加密密钥生成期间预共享密钥。单向方案保证重新加密仅以一种方式工作：它将发布者密文（使用发布者密钥加密）转换为订户密文（可以使用订户的私钥解密）。单向方案通常不需要预共享。

PICADOR需要一个不允许的单向方案

密钥生成期间的预共享（最小信任模型）。我们的Pub/Sub系统还需要高效的加密，重新加密和解密操作。虽然我们专注于信息被重新加密一次的操作（也称为单跳或单跳重新加密），但我们的Pub/Sub模型进行了概括，以便密文可以多次重新加密（也称为多跳重新加密）-加密）。[8]中提出的单向方案需要预共享。[9]中提出的方案是不可转移的（单跳），理论上不能支持额外的跳。在[22-24]中开发的PRE方案尚未实现，并且基于已知的学习错误（LWE）结构，与基于理想（循环）格子的网格结构相比，已知具有更高的渐近复杂度（和实际运行时间），即多项式环。因此，

现有的单向方案都不适用于我们的Pub/Sub模型。

3.2。解决方案概述

我们提出了一种新颖的单向PRE方案组合

可证明安全的Stehlé-SteinfeldNTRU方案[10]和Albrecht等人提出的NTRU免疫约束。[25]。Stehlé-Steinfeld加密方案及其安全性分析分别见附录A.1和A.2。

我们的方案基于高效且安全的网格基元

（理想格子）。与PRE的其他已知方法相反，格子加密方法，例如我们的方法，通常被认为是后量子[11,12]，也就是说，除了具有经典的对手之外，甚至可以防止来自具有实际量子计算设备的对手的攻击。计算设备[13]。此外，网格加密方案渐近地比其他公钥加密方案（如Paillier加密和RSA）更快。

所提出的PRE方案的另一个优点是基于

在支持以下同态操作的部分同态加密方案上：加法，索引和乘法。因此，本文开发的Pub/Sub模型可以扩展为支持：（1）添加不同发布者发布的加密数据，（2）通过索引查询特定密文数据，以及（3）多个发布的加密密文的乘法出版商。

3.3。我们的PRE方案的格子加密概念

我们的方法是基于格的加密方案。一般

关于基于格的方案设计的调查可以在[26]中找到。基于格的密码学的数学预备可以在[27]中找到，但我们在这里提供了一个高级概述。

C.Borcea等。/FutureGenerationComputerSystems71（2017）177-191181

我们的基于格的密码系统提供核心公钥

密钥生成的加密原语（KeyGen→（pk，sk）），加密（Enc（pk，μ）→c）和解密（Dec（sk，c）→μ），其中pk是公钥，sk是密钥，μ是明文，c是密文。

具体地说，我们将明文和密文表示为向量

无符号整数。我们在我们的密码系统中使用2次幂的cyclotomics，这意味着明文和密文向量代表多项式mod（xn+1）的系数，其中n是2的幂[27]。我们在纯文本和密文上需要支持的几乎所有操作都是线性变换，并且通过将自身限制为2维幂，我们大大降低了我们的密码系统所需的实现复杂性。这直接转化为更有效的实施。目前针对非2次幂循环分析设计的实现可以支持更多通用功能，但我们有意选择专注于简化方案，以改善有限深度应用的运行时间。

从[27]和基于格的加密的一般领域来看

在2的幂下，我们定义环R=Z[x]/⟨xn+1⟩（即，整数多项式为模xn+1）。对于任何正整数q，我们定义密文空间Rq=R/qR（即，整数多项式模xn+1，具有mod-q系数）。对于某个整数p≥2，明文空间是Rp，这意味着明文是整数模p的长度为n的向量。

一般会讨论密码系统的实际安全性

就“工作因素”而言，这是从加密数据中恢复可用信息的相对计算工作[26]。工作因素通常通过对密码系统安全性证明中使用的潜在计算硬度问题的困难实验密码分析来确定。密码系统的安全性源自许多网格加密方案的已知硬计算问题的硬度的减少证明[26,27]。

工作因素很难转化为有意义的具体内容

参数设置。密码学家经常使用（有时是人为的）标量安全参数来表示这些问题的硬度和派生密码系统的安全性。实际上，密码学家通过保证这些安全参数满足提供基本安全级别的特定最小值来保证安全系统。

基于格的密码系统的安全性通常在下文中讨论

根Hermite因子δ的术语或安全表示的位[26-29]。我们关注安全的根Hermite因子表示。目前的安全性估计表明，根Hermite因子δ<1.006对应于100位安全性和实际安全性的适当工作因子[28-30]。

3.4。NTRU-RLWEPRE方案

我们的NTRU-RLWEPRE方案使用

以下数量：

•对应的安全参数（根Hermite因子）δ

最短向量问题[28]，

•密文模数q，•环维数n，•明文模数p，•Bk-有界离散高斯（密钥生成）分布χk

在多项式环上R=Z[n]/⟨xn+1⟩，标准偏差σk，

•有限离散高斯（误差）分布χe

多项式环R，标准偏差σe，

•重新线性化窗口r以优化重新加密运行-

时间，

•根据经验选择保证措施α以最小化钻头

q的长度（在我们的方案中引入以获得更好的性能）。

就像Stehlé-Steinfeld计划一样，我们支持a

明文空间M={0,1，...。。，p-1}n，其中p是明文模数。密文的所有操作都在环Rq≡R/qR中进行。多项式中的每个系数表示为

范围-q

2,.。。，q

2.

该计划包括以下操作：

•KeyGen：样本多项式f'，g←χk并设置f：=pf'+1到

满足f≡1（modp）。如果f在Rq中没有模乘法逆，则重新采样f'。设置公钥pk和私钥sk：sk：=f∈R，

pk：=h=pgf-1∈Rq。

•Enc（pk=h，m∈M）：样本多项式s，e←χe。计算

密文：

c：=hs+pe+m∈rq。

•Dec（sk=f，c）：计算密文错误b：=f·c∈Rq。

输出m'：=b（modp）。

•ReKeyGen（pk=h\*，sk=f）：对于每个i=0,1，....。。，

⌊log（q）/r⌋，样本多项式si和ei并计算

γi=h\*si+pei+f·2ri∈Rq，

并设置重新加密密钥

rk：=γ=γγ0，γ1，。。。，c∈log（q）/rc。

•ReEnc（rk=γ，c）：计算密文

c'=

⌊log（q）/r⌋⌋

i=0（ci·γi），

哪里

这里={h·s+pe+m}i

和

c=

⌊log（q）/r⌋⌋

i=0ci·2ri.ReKeyGen和ReEnc操作基于重新线性化过程[31]，其定义方式与[32]相同。只要在解密的最后阶段没有环绕模q，该方案是正确的。实际上，对于解密重新加密数据的情况，我们有

f\*·c'=f\*·



我ci·γi



=

我ci·（f\*·γi）

=p

我ci·Ei+

和cif\*f·2ri

=p

我ci·Ei+f\*fc

哪里

否=g\*si+f\*否。

可以看出

f\*·c'=f\*fc=m（modp），

即，如果密文错误f\*·c'不是太大而不能缠绕q，则解密是正确的。

与[32]中的推导类似，我们可以设计出

使用无穷大规范解密重新加密的密文的正确性约束，上限Bk和Be

182C.Borcea等。/FutureGenerationComputerSystems71（2017）177-191

使用离散高斯分布生成的系数，以及基于中心极限定理的多项式乘法的平均情况分析。单跳重新加密的正确性约束要求f\*·c'=p

ici·Ei+f\*fc<q/2。（1）

鉴于Bk，Be»1，无穷大规范可以表示为

∥ci∥∞≤2r-1，

∥Ei∥∞≤√

n（BkBe+（pBk+1）Be）≈√

nBkBe（p+1），

∥fc∥∞≤√

n（pBkBe+p（pBk+1）Be+（pBk+1）（p-1））≈√

npBkBe（p+1），f\*fc∞≤√

n（pBk+1）∥fc∥∞≈np2Bk2Be（p+1）。

将无穷小规范的表达式代入不等式

（1），应用基于Bk，Be»1的近似值，并将估计的范数乘以因子2（以补偿所有近似值），得到q>4np2BkBe2r-1（⌊log2（q）/r⌋+1）+pBk。（2）

边界Bk和Be表示为σk√α和σe√α，重新

具体而言，α是[32]中引入的经验保证措施。它对应于2-α+1的概率，即离散高斯分布的系数超过束缚Bi，其中i∈{k，e}。对于每个多项式乘法，超出约束的概率急剧下降（单跳代理重新加密需要两次多项式乘法）。

将表达式替换为不等式（2）

yieldq>4np2ασkσe2r-1（⌊log2（q）/r⌋+1）+p√ασk。（3）

选择明文攻击下的不可区分性（IND-CPA）

从[10]中的定理4得出。注意，我们的方案使用[10]中的结构，但是来自[25]的改进的NTRU免疫约束可以保留[10]中IND-CPA的证明。

提出了所提出的PRE方案的安全性分析

在附录A.3中。

3.5。参数选择

格子加密方案的一个普遍问题是它们

参数化比其他加密方案系列更复杂。参数选择主要取决于正确性条件（特定于所分析的方案）和安全条件。在这种情况下的正确性约束由表达式（3）给出，并且安全条件分别是NTRU和RLWE假设的不等式（A.3）和（A.4）。所有三个不等式都必须通过PRE密码系统的参数来满足。

最重要的是具有的参数n和q

对计划运行时间的最大直接影响。n的值应保持尽可能小，因为对于所有操作，运行时间在n中至少是线性的。q的值确定需要通过计算机操作的整数的大小，并且通常应保持尽可能小。不等式（A.4）意味着n的值随q的位长度线性增长。

我们开始使用安全性进行参数选择

参数δ，也称为根Hermite因子。[28]中提出的启发式论证表明，根本Hermite因子δ=1.006可以提供足够的安全性（大约100位安全级别）。因此，我们选择δ=1.006。

离散高斯误差分布χe的界限是

表示为Be=σe√α，其中σe是标准偏差

误差分布和α确定使用离散高斯分布（或离散高斯的乘积）产生的系数超过约束Be[32]的有效概率。σe的值通常选择在3到6的范围内，我们将σe的值设置为4，如[33]中所示。我们将α设置为9，对于使用离散高斯分布生成的整数的情况，对应于最多2-8的理论概率

选择超过上限Be的值。这个α值的选择经验验证了35,000次加密/解密迭代[32]。相同的α值用于密钥生成分布χk。

在选择δ，σe和α之后，我们可以选择n和

实验上使用表达式（A.3），（A.4）和（3）来最小化再运行化/最大化重新线性化窗口r和明文模数p的各种值的吞吐量。

表1列出了环尺寸n，位长的最小值

密文模数q和密文展开因子β作为明文模数p和再线性化窗口r的函数。增加p的值以减少β（从而增加吞吐量）并且增加r的值以减少重新加密操作的计算和空间复杂性。可以看出，对于p=2，密文扩展因子很高，这意味着它不应该用于需要达到最大吞吐量的情况，这就是PICADOR的情况。r的最高值（最多16）通常是最佳的，只要没有环尺寸增加或需要明显的密文模数位长度增加[32]。表1的分析可归纳如下：

•对于案例p=，预期最低的加密/解密延迟

2，r=1，

•对于p=2，r=8的情况，预期最低的重新加密延迟，•对于p=16，r=16或者预期最高吞吐量

p=256，r=16.第5节提供了r=16的吞吐量的实验评估。

4.原型架构和实现

我们实施了PICADOR原型来探索设计贸易-

关闭并通过实验评估我们的系统性能。Pub/Sub体系结构用Java实现，PRE加密实现为C++格子加密库。我们实现了体系结构的所有组件，包括发布者，订阅者，启用PRE的Pub/Sub代理以及基于Java的框架中的策略权限，并调用C++加密库。

在下文中，我们首先讨论PRE的实现

第4.1节。然后，我们在4.2节中介绍Pub/Sub实现。

4.1。PRE实施

密钥生成，加密，重新加密和解密

我们的PAL方案库为格式加密启用了PRE方案的操作.2我们选择建立PALISADEC++库，因为它定义明确的加密API并优化了格/算术运算。为方便起见，我们使用PALISADE作为PALISADE-PRE参考我们实施的NTRU-RLWEPRE方案。

使用PALISADE-PRE生成公钥/私钥对

政策机构（即出版商）和订户的KeyGenAPI。PALISADE-PRE支持将密钥和密文序列化和反序列化为JavaScriptObjectNotation（JSON）文件。PICADOR使用密文和密钥的JSON序列化

2PALISADE库是在BSD开源许可下发布的。

C.Borcea等。/FutureGenerationComputerSystems71（2017）177-191183

表1明文模数p和再线性化窗口r对环尺寸n，密文模数q和密文展开因子β的影响。

prnlog2qβ

2110243434281024383821620484848

1612048521316820485213161620485715

2561409677102568409677102561640967710

其组件之间的通信以及存储。选择JSON是因为它是轻量级的，可编程访问的，并且通过避免第三方数据管理系统的集成和资源需求来提供快速开发和部署。

4.2。发布/订阅实现

PICADOR是使用JavaServerPages（JSP）实现的，

JavaServlet，Java消息服务（JMS），Java本机接口（JNI）API，消息驱动的EnterpriseJavaBean（MDEJB）以及伴随Wildfly9应用程序服务器中运行的所有资源的随附Java类。PICADOR的基于Java的组件使用JNI框架与其C++PALISADE-PRE库进行交互。选择Java是为了开发原型，因为它支持跨平台，通过JNI进行C++集成的可靠API，通过JMS进行消息传递以及安全支持。选择Wildfly9的支持JMS的消息传递系统来实现PICADOR的组件通信，因为它具有快速部署，易于扩展，性能和可扩展性。

图3显示了我们的原型和主要组件

他们的沟通。原型包括发布者，启用PRE的代理和订阅者。尽管图中仅示出了每个实例，但是可以存在许多发布者实例和订户的许多实例。这些组件中的每一个都驻留在Wildfly9容器中。该实现可以作为Wildfly的单个实例进行部署，所有组件都处于活动状态并在使用中，或者可以将其实现为Wildfly的多个实例，每个实例运行三个组件的子集。我们注意到，由于组件之间的通信使用HTTPPOST和GET，因此组件可以分开，并且在某些情况下可能使用较小的实现构建，如果这样的部署证明是有用的。

虽然我们使用PICADOR进行设计，实例化和实验

作为单个代理Pub/Sub系统，我们的架构也可以通用化，以支持多个代理，以提高可扩展性和容错能力。通过使用分布式系统技术（如一致性哈希和复制），可以跨多个代理分区主题，同时为每个主题数据结构维护给定的复制因子。这些数据结构是订户及其公钥之间的映射，以及发布者/订阅者对与重新加密密钥之间的映射。由于它们都不经​​常更新，因此复制和一致性的成本预计会很低。由于内容是只读的，因此其复制很简单。如[34]所示，消息可以在O（1）中路由，代价是网络拓扑维护的开销略高。因此，预计延迟与我们当前的原型相似。在本文中，我们不关注多个布鲁克设计，我们主要将其留给未来的工作。

这些组件可以访问PALISADE-PRE的功能。

通过库的JNI包装器进行编辑。每个组件都执行

加密/重新加密/解密周期中的一个单独步骤。他们的交互是通过中央内容存储库和共享使用发布者队列。

发布者通过发送加密内容来发布文件

被指定用于代理的特定队列。队列特定于内容的主题。队列可以即时添加。PRE代理将已发布的内容存储在存储库中，更新相应的队列，并通知任何订阅者队列的更新。当通知内容已添加到其队列时，订户请求下载已发布的内容。PRE代理执行重新加密并将重新加密的内容发送给订户。订户执行解密，重新组装内容，并保存发布的内容文件。

4.3。Publisher工作流程

可以通过publisherIndexJSP访问发布者。该

用户将自己标识为发布者，选择（或创建）要发布内容的队列（即主题），选择要发布的内容，并将内容上载到PublisherFileServlet。

PublisherFileServlet通过分区处理内容

它成了明文块。这些块中的每一个都可以单独处理，允许实现在多个独立线程中并行化加密和发布。发布者可以根据发布者的可用处理能力选择块的大小和并行度。然而，如所指出的，就最小化密文扩展因子而言，最有效的块大小是n（PRE环维度）的函数。

PublisherFileServlet中的每个线程都会加密块

明文，将它们转换为密文的JSON数据结构，并为JSON数据结构添加一个标记，指示整个内容中块的位置顺序。每个线程将这些标记的JSON结构组装成HTTPPOST。

HTTPPOST包含一个标志，通知代理哪个

基于主题的JMS队列与发布的内容相关。帖子的主体由一系列加密的密文块组成，包含：（1）密文的JSON数据结构的一部分，以及（2）一个标志，指示密文的整个JSON数据中的块的JSON部分的索引结构体。代理使用这些项来存储每个块。为了有效利用网络带宽，JSON数据结构在使用JavaJDK中的ZIP压缩类发送到代理之前进行压缩。

当发布者处理完所有块时

并且所有POST线程都已完成，发布者发出一条消息，指示发布已完成。当代理收到此“发布完成”POST时，它会向其为已发布内容管理的JMS队列发送单个“发布通知”。此通知由内容标识符和内容的JMS队列主题的标志组成。通过使用部署在每个订户客户端上的MDEJB来实现通知，该客户端配置为监视通知的特定队列，并将每个通知存储到订户的发布通知存储库（PNR）。

4.4。订阅者工作流程

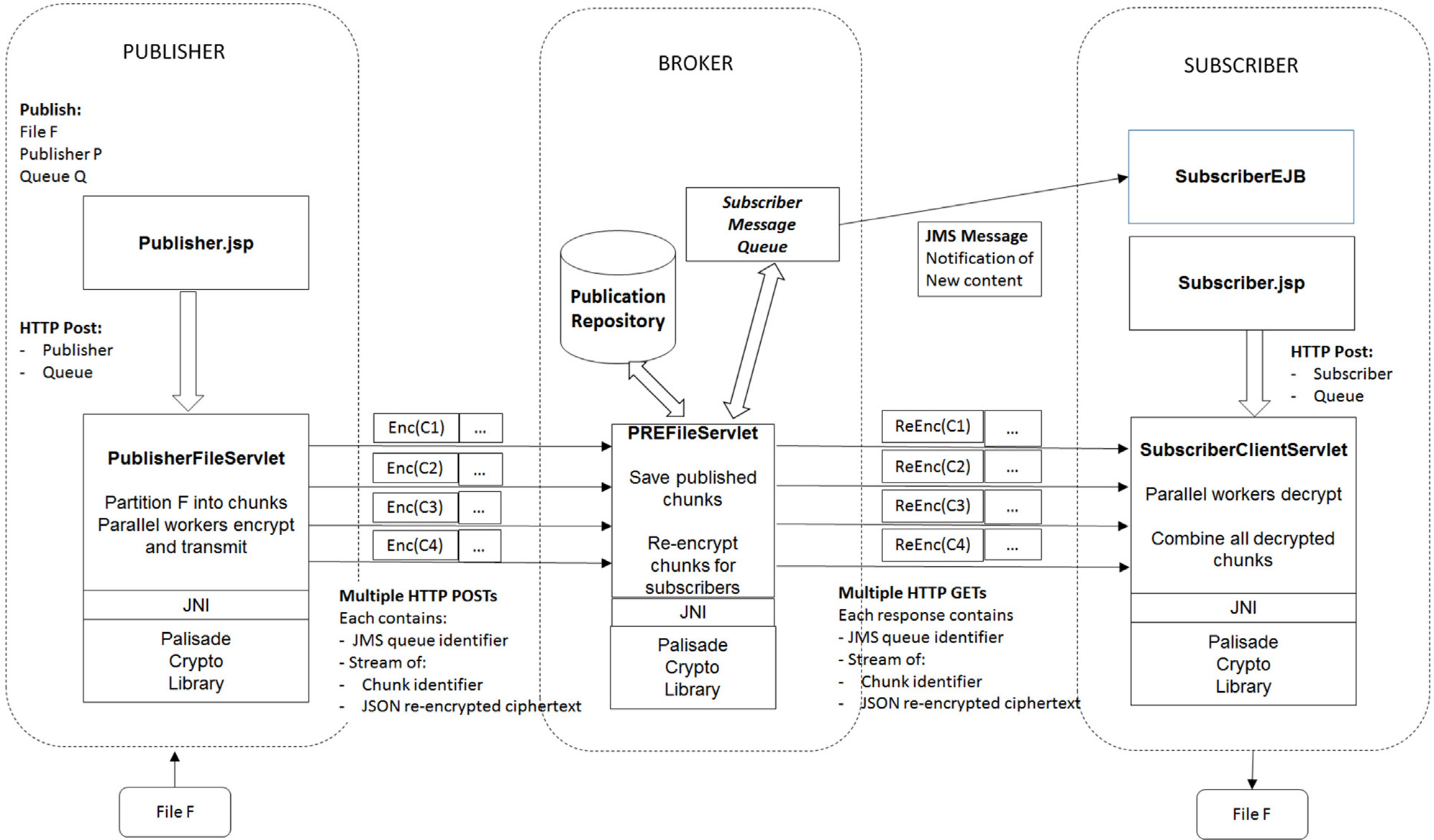
订户实现可以使用到达

发布通知消息，以启动提取已订阅内容的过程。然而，应该注意，订户还可以查看其队列的内容，并且在任何时候启动拉取内容的过程。

代理维护一个PRE关键映射，该映射关联每个PRE

使用特定JMS队列和订户重新加密密钥

184C.Borcea等。/FutureGenerationComputerSystems71（2017）177-191



公钥。以这种方式，适当的订户可以在接收到发布通知时检索内容。具体而言，订户客户端的JSP接口列出了存储在其PNR中的发布通知，这些通知是从代理管理的JMS队列接收的，用于订阅者的订阅。

订户客户端请求与a对应的内容

通过向Subscriber-ClientServlet发送HTTPPOST来发出特定通知。该请求包含（1）订户的ID，（2）内容的主题，以及（3）相关JMS队列的标志。

SubscriberClientServlet提交已发布的请求

内容到PREBroker。在收到订户的请求后，代理检查以确保允许订户接收该信息。如果订户被授权，则代理通过检索内容的密文块，重新加密每个块，然后将这些PRE密文块发送给订户来回复内容请求。返回的每个密文块包含（1）PRE密文JSON数据结构，以及（2）反映原始密文的整个JSON数据结构中的块的索引的标志。

代理解压缩压缩的JSON数据结构

在重新加密之前，然后在将其发送给代理之前对其进行压缩。订阅者还必须在解密之前对压缩的JSON数据结构进行解压缩。

订户解密每个接收到的PRE密文块

使用其私钥来恢复已发布内容的一部分，并使用每个块的索引值来重建和存储已发布的内容。

SubscriberClientServlet可以选择并行化

从PREBroker获取订阅的内容。该决定可以独立于加密参数或发布细节而做出，并且仅基于订户资源。这是通过以循环方式跨线程分发块的简单方法来实现的。

5.实验

我们通过实验评估PICADOR来探索它

配置-性能权衡和可扩展性，并确定

它可能支持的应用程序类型。实现和使用基于格的密码系统的主要实际挑战是性能之一。典型的实现需要调整诸如多线程，明文编码和相关参数之类的设置，所有这些都是我们通过实验检查的。

在改变配置参数的同时找到最佳设置-

我们在实验过程中修复了安全参数，以提供符合当前最佳实践的基本安全级别，并提供高级别的安全性。我们选择安全参数δ=1.006，它根据当前的理解提供高度安全性[28,29]。降低安全性参数会使密码系统变得不安全，并且将安全设置提高到可接受的阈值可能会过度设计密码系统的安全性，同时会对运行时性能产生负面影响。

5.1。方法

我们根据以下指标评估效果，

与相关的PRE工作[9,20]中使用的相似：

1.吞吐量：可以发布多少个明文位或

为各种设置代理。

2.有效负载扩展：需要多少（摊销）位

表示明文（有效载荷）的每一位。

我们使用吞吐量来评估明文数据的数量

可以按单位时间的实施进行处理。吞吐量测量特定pub-PRE-sub操作的处理时间，该处理时间按照在每个密文中加密的明文位数进行摊销。

吞吐量与有效载荷扩展因子有关。这个

因子是底层加密方案的密文扩展和通信基础设施在传输数据时执行的编码/解码的伪像。

我们进行了多次实验来评估对其的影响

性能：（i）明文模数;（ii）块大小;（iii）有效载荷

C.Borcea等。/FutureGenerationComputerSystems71（2017）177-191185

表2不同的明文模数对发布者和订阅者吞吐量的影响。

明文模数p发布者吞吐量，kB/s订阅者吞吐量，kB/s

26.41.61621.44.925633.86.4

尺寸;（iv）单主机设置的并行化;（v）多主机设置的并行化;（vi）订户数量。除了涉及多主机设置中的并行化的实验以及订户数量的影响之外的所有实验都在单个主机上运行。

序列化的密文数据之前使用GZip压缩

被传输到启用PRE的代理以减少带宽使用。一旦收到，代理就解压缩密文文件，执行重新加密，然后压缩用户的密文文件。我们通过实验观察到密文文件中的平均压缩比低于1.6，这意味着在Pub/Sub操作期间使用的带宽较少。然而，我们观察到代理处的压缩和解压缩操作将延迟平均增加了15％。因此，对于带宽是非问题且低延迟是高优先级的设置，可以禁用压缩。

5.2。测试平台

为了实验评估性能，我们部署了

位于Supermicro1U机架式服务器上的PICADORPub/Sub代理，带有Intel（R）Xeon（R）CPUE5-2660，内核为8x2.20GHz（每个2个逻辑处理器），内存为32GB。服务器运行VmWareESXi6.0。最多8个内核和16GBRAM的虚拟机（VM）用于模拟启用PRE的代理功能。VM配置了Windows764位。

我们使用商品DellLatitude笔记本电脑来模拟发布-

多主机实验中的用户和订户。笔记本电脑配备了In-tel（R）Core（TM）i7-3520MCPU，内核为2x2.90GHz（每个核心2个逻辑处理器）和8GBRAM。笔记本电脑配置了Windows764位。

Pub/Sub客户端通过有线连接到服务器

以太网交换机，带100Mbps端口。我们使用术语“发布者吞吐量”来表示明文数据加密并发布到发布/订阅代理的速率，以及术语“订阅者吞吐量”来表示接收此明文数据的速率。订户，包括它被重新加密，发送给订户，然后由订户解密。

5.3。明文模数

明文可以假设影响性能，因为

较大的明文模数可能能够更有效地将数据打包成需要传输的密文。我们通过多个明文选择实验评估了这个假设：p∈{2,16,256}。表2列出了对发布者和订阅者吞吐量的影响结果。

我们观察到吞吐量通常随着增大而增加

明文模数。这支持了我们的假设，即较大的模量可以导致更有效的数据打包。但是，我们希望使用多大的明文模数是有限的。随着明文模数的增加，密文模数必须相应地增加以保证正确的解密。当密文模数增加时，由于RLWE安全约束，环维度也增加。最终达到一个点，其中进一步的明文模数增加开始导致性能下降。

原型明文编码实现支持

对于明文的字节编码，明文模数高达p=256。进一步的分析表明，将p增加到更高的值可以提供额外的性能改进，但净效应还将取决于重新线性化窗口的值。这种基于明文模数和重新线性化窗口的多参数优化超出了本研究的范围，应该在已知具体应用要求时进行。

5.4。块大小对性能的影响

我们通过实验评估了块大小对其影响

性能。我们进行了实验，块大小从4kB到1024kB不等，所有其他变量保持不变。实验结果如图4所示。

获得的吞吐量可用于应用程序处理

需要低延迟的文本或小尺寸数据。这些值表明PICADOR也可以支持照片或其他类型的大数据，但是在没有严格延迟限制的应用程序中。此外，第5.6节显示通过并行化可以显着提高吞吐量。因此，我们得出结论，医疗保健和军事等领域的许多有用应用可以保证与PICADOR的端到端有效载荷保密性，同时实现良好的性能。

我们观察到发布者和订阅者吞吐量达到

块大小高于32kB的平台。块大小小于32kB的较低吞吐量可能是由C++包装器对加密操作所需的内部预处理步骤引起的。可以优化包装器实现以减少此影响，但订阅者操作​​比单线程设置的发布步骤慢得多。这是因为重新加密是限制性延迟因素，是用户操作的一部分。基于这些实验观察，我们的结论是，块大小应该足够大，足以摊销启动成本，但不能大于此。较大的块大小可能会导致延迟问题，这在安全关键或移动应用程序中可能会出现问题。

5.5。有效载荷大小对性能的影响

我们对有效载荷进行了实验观察

100kB至50MB，所有其他参数保持不变。

该实验的结果可以在图5中看到

他们确认PICADOR能够很好地适应有效载荷大小。该图显示发布者和订阅者吞吐量通常独立于有效载荷大小，除非非常小的有效载荷大小，其中启动成本未摊销。缺乏依赖性可能是由于面向流的数据处理（如块），这使得PICADOR具有良好的可扩展性。

5.6。并行化对单主机设置性能的影响

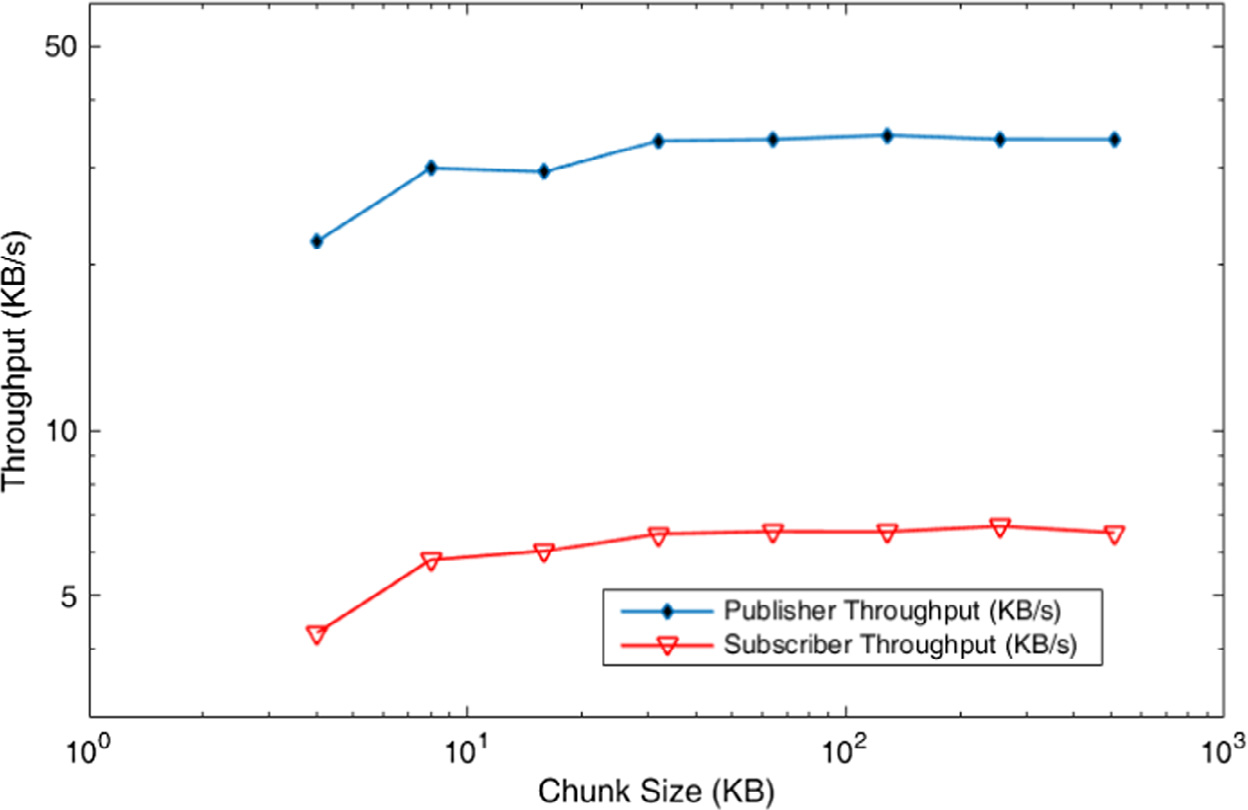
这些实验评估了多线程的影响

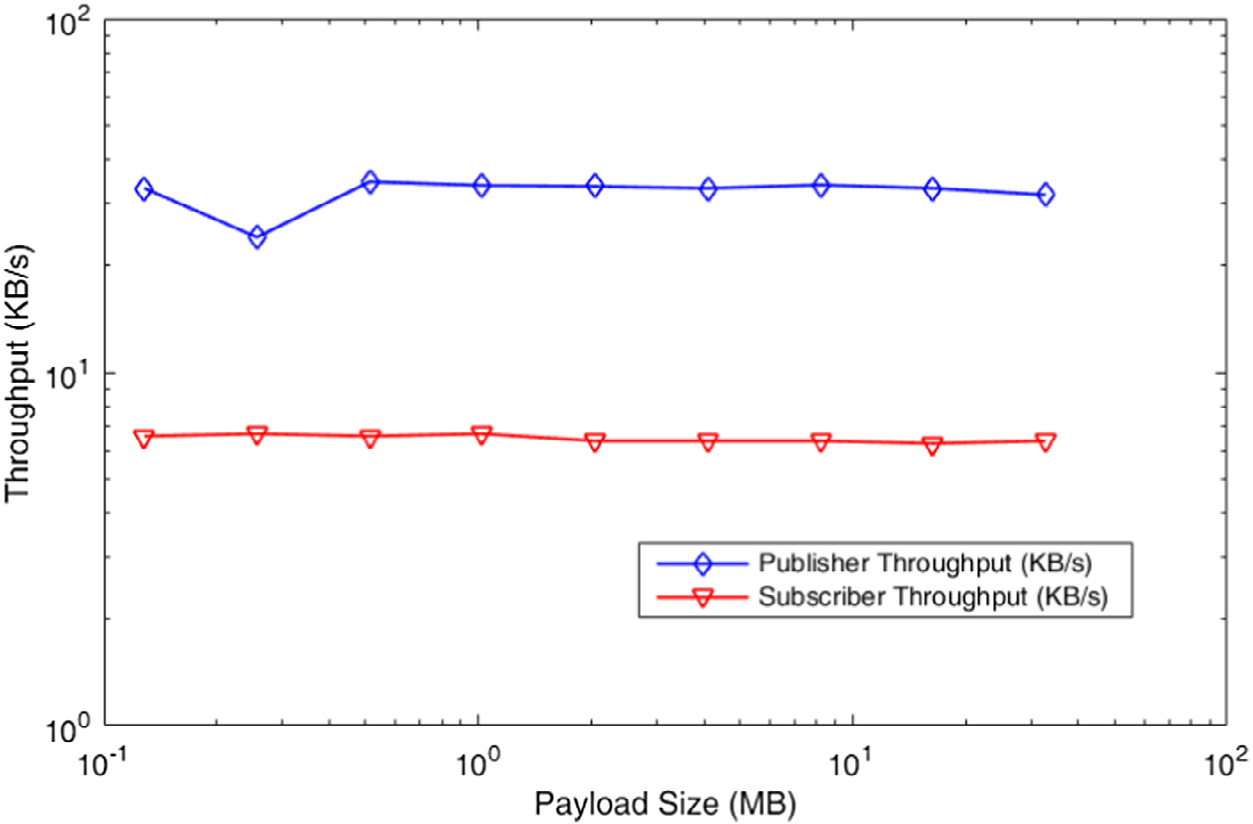
关于吞吐量。正如我们在第4节中所述，发布者和订阅者使用多个线程进行并行上传和下载到代理或从代理下载。通过我们的基线参数集和有效负载大小固定为10MB，我们将启用PRE的代理可用的线程数从1更改为16。

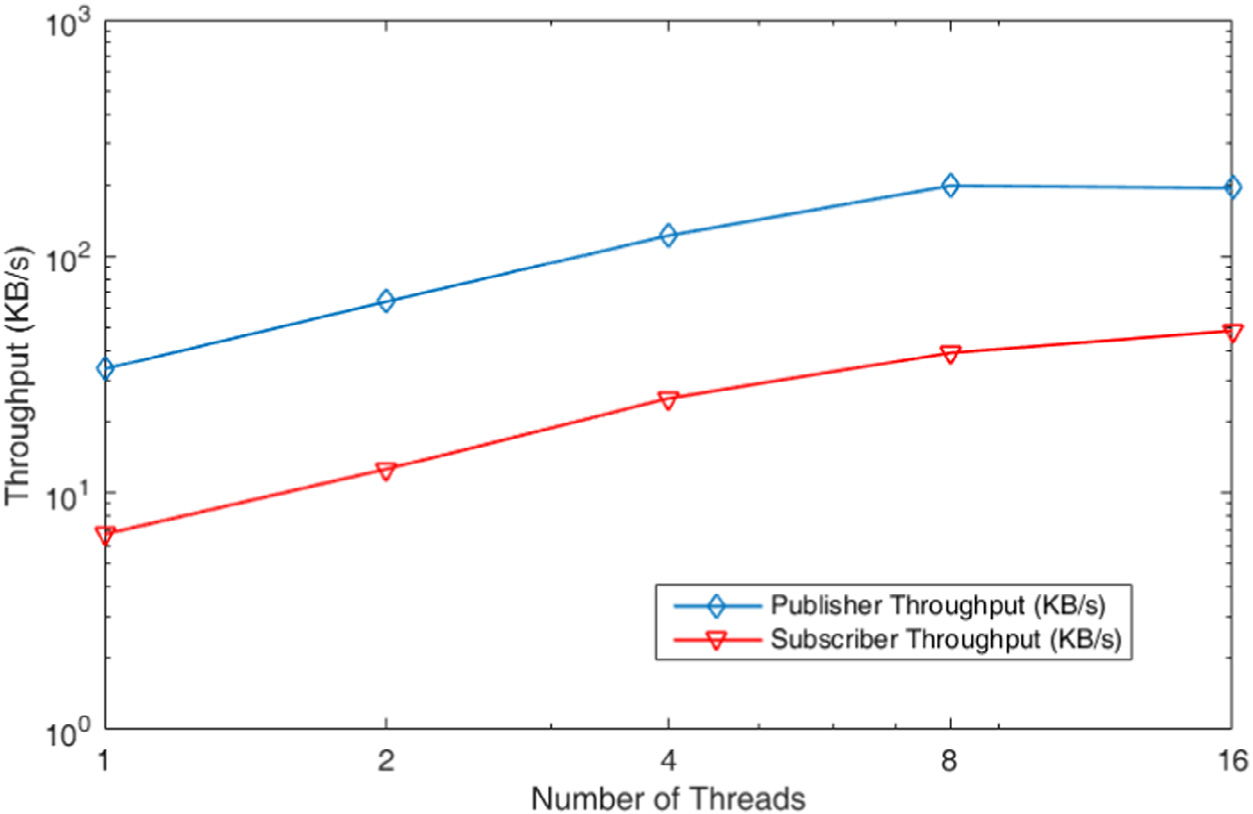
结果如图6所示，显示出显着的增加

随着线程数量的增加，吞吐量也随之增加。发布吞吐量增加了5.9倍，而订阅吞吐量增加了5.8倍。但是，当我们将线程数增加到8以上时吞吐量会降低，因为我们的服务器有8个内核。尽管未在图中显示，但8个线程的加密时间减少了6.3倍。

186C.Borcea等。/FutureGenerationComputerSystems71（2017）177-191







C.Borcea等。/FutureGenerationComputerSystems71（2017）177-191187

表3多核执行对吞吐量的影响。

每个客户端的线程数服务器核心数发布者吞吐量（kB/s）订阅者吞吐量（kB/s）

4194.93.54295.76.64495.416.04895.123.72872.816.41841.59.4

5.7。并行化对多主机设置性能的影响

我们评估了多核业务对以下方面的影响-

当商用笔记本电脑用于模拟发布/订阅客户端时，表现为性能，服务器虚拟机作为PRE经纪人操作。尽管PICADOR设计用于交叉发布/订阅操作，但我们执行了非交错发布和订阅操作，以直接单独测量每个操作的效果。两个笔记本电脑客户端同时发布内容或通过订阅下载内容到单个PRE代理。

改变线程数以检查两种效果

并行化和可伸缩性。使用虚拟机的设置更改了启用PRE的代理上的实际核心数，以检查可伸缩性。实验结果见表3。

我们观察到发布者的吞吐量仅取决于

发行商客户而非经纪人的表现。这是合理的，因为由于加密操作，计算瓶颈在发布者客户端上。当4核主机笔记本电脑上的发布者客户端线程数从1增加到4时，吞吐量增加2.3倍。

相反，用户吞吐量取决于

代理和订户客户端的计算能力。可以看出，当服务器核心数量从1增加到8时，用户吞吐量增加了6.8倍。客户端和代理之间的线程同步有明显的效果。当客户端线程数为1且PRE服务器核心数为8时，代理仅使用两个核心（每个客户端一个）。

5.8。多主机设置中用户数量对性能的影响

我们通过检查实验的可扩展性来结束实验

PRE服务器作为订户数量的函数。作为PRE服务器的基本配置，我们使用了8核虚拟机。所有发布/订阅操作都以单线程模式运行。我们交错发布和订阅操作以检查可伸缩性限制。同时启动订户工作流以检查并发订户会话的影响。我们使用的块大小和有效负载大小分别为128kB和10MB。

图7显示PRE服务器相对较好地扩展到8

订阅者，与PRE服务器中的核心数量相同，当并发用户数量从1增加到8时，单位用户吞吐量仅减少13％。当用户数量增加到16时，吞吐量降低了与8个订户的情况相比，超过38％。这表明PRE服务器中的核心数是我们实验设置中的主要可扩展性瓶颈。还可以观察到，由于所有计算上昂贵的步骤都由发布者执行，因此高PRE服务器CPU利用率（由于大量订户）对发布者吞吐量的影响相对较小。例如，当订阅者的数量时，发布者吞吐量仅减少12％

对应于PRE服务器上正在运行的线程数，从1增加到16。

我们通过执行额外的验证来验证上述结论

实验，其中PRE服务器中的核心数或发布者数量是变化的。

5.9。分析和权衡建议

根据我们的实验结果，我们已经确定了

应用PICADOR或设计类似系统时应考虑的潜在性能瓶颈：

•有效负载扩展：需要设置参数，包括

明文模数，密文模数和块大小，以最大限度地减少有效负载扩展。这极大地减少了带宽使用并减少了与加密操作相关的计算开销。

•代理延迟：与有效负载扩展，代理相关

延迟由代理的有效负载扩展和计算资源驱动。实际上，这可以通过多核服务器上的多线程来解决，因为我们的PRE方案支持并行重新加密数据块。

•可扩展性：我们当前的架构是集中式的，并且具有

可扩展性限制。但是，如第4节所述，可以使用标准分布式系统技术（如一致性散列和复制）设计可扩展的多代理PICADOR版本。预计该版本将扩展，因为与维持一致性相关的开销应该较低（即，不经常添加新订户或新主题）。

•订阅流失：PICADOR不是为高度设计的

挥发性环境，订阅流失率高。为了以可扩展的方式支持这种情况，需要重新设计PICADOR架构的一部分，包括策略机构。

基于我们的实验分析和鉴定

瓶颈，我们就PICADOR原型的配置提出以下建议：

•尽可能使用尽可能大的明文模数

密文模数位宽小于客户端或代理上所有处理器的位宽。

•不对有效载荷大小进行调整。•使用足够大的块大小来分摊加密操作

启动费用，如果有的话。

•使用尽可能多的多线程和限制

factor是机器上的核心数。

6.相关工作

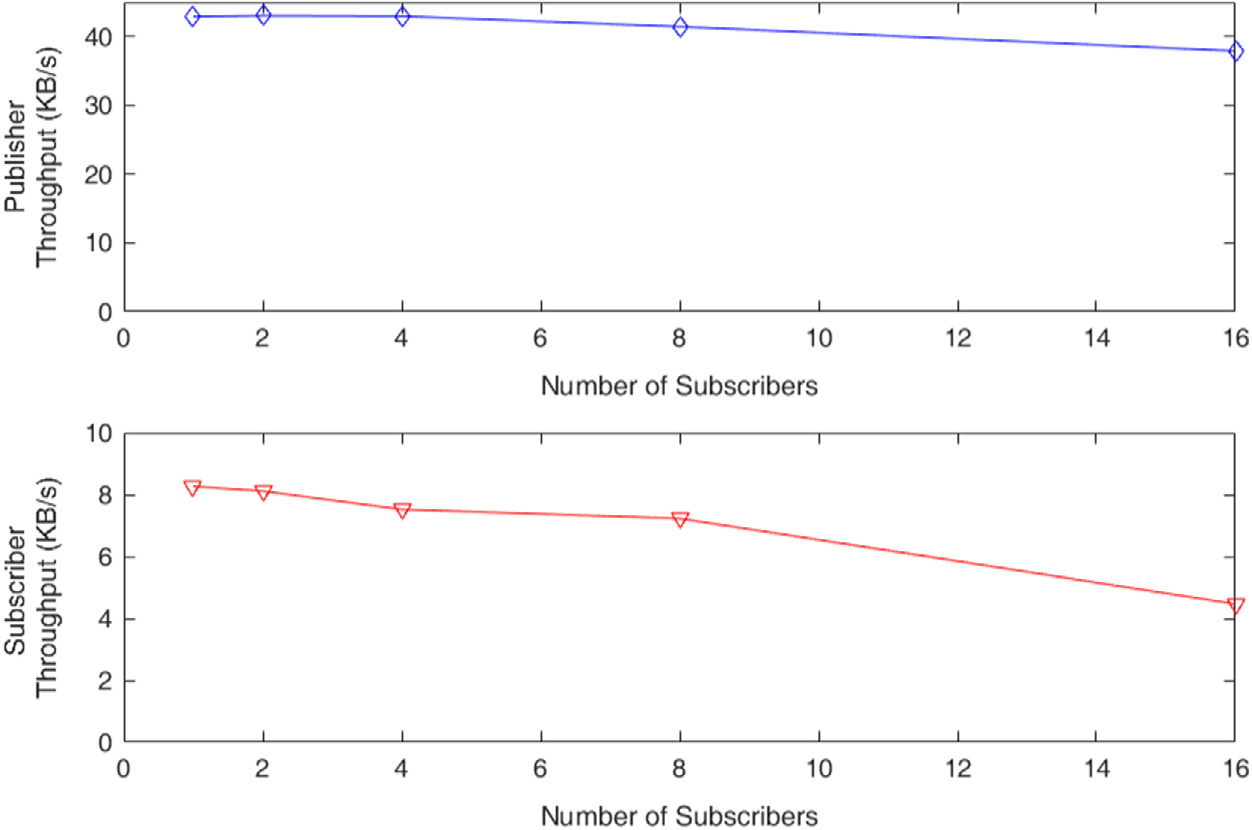
虽然Pub/Sub信息分发一直很积极

研究和使用[1]，对Pub/Sub操作的安全性进行了有限的调查。[6,35]已经确定了此类系统中的一般安全挑战，特别是机密性和密钥管理，这是我们在本文中的贡献。之前对Pub/Sub操作的加密解决方案所面临挑战的概述见[36,37]。[38]中讨论的系统提出了一种在基于内容的Pub/Sub系统中更新发布者加密密钥以加密订阅的方法。PICADOR没有解决这个先前的更一般的能力。PICADOR专注于基于主题的发布/订阅系统，其中订阅信息未加密，并且在密钥交换而不是密钥更新中，如[38]中所述。

基于主题的机密性和其他安全性问题

与基于内容的发布/订阅系统相比，诸如PICADOR之类的发布/订阅系统可能存在不同的安全问题和权衡。以前有过关于机密性的大量先前工作

188C.Borcea等。/FutureGenerationComputerSystems71（2017）177-191



基于内容的Pub/Sub框架，其中代理需要对内容进行一定程度的可见性以支持代理[39-41]。如[39]所示，基于对称密钥加密的解决方案要求在Pub/Sub代理处进行解密，要么在发布者和订阅者之间建立先验共享对称密钥。在[40]中提出的具有高度可扩展密钥管理解决方案的保密发布/订阅系统的一般方法可以覆盖在基于内容的一般发布/订阅信息基板上。

PICADOR专注于保护已发布的隐私

内容;它没有解决主题元数据的隐私问题。但是，[14,41]中提出的解决方案提供了一种方法，可以通过加密订阅信息来保护订阅的机密性。除了信息有效载荷的机密性之外，PICADOR中的PRE技术可以与[14]中的技术相结合，以保护订阅的隐私。

先前基于安全主题的Pub/Sub设计[6]依赖于sym-

度量标准加密，用于实施端到端内容机密性，并侧重于身份管理，以确保只有经过批准的用户才能接收信息。此外，[42]提供了一个相关的基于主题的发布-订阅框架，侧重于端到端加密的身份管理。这些作品对PICADOR非常有用，因为它们解决了我们关注的身份管理问题。

适用的工作越来越多

基于属性的加密（ABE）[43]支持相关的基于ABE的访问控制[44]和基于ABE的Pub/Sub[45,46]。基于ABE的方法很有吸引力，因为数据加密取决于预期数据接收者的属性，包括接收者感兴趣的主题，而不依赖于特定接收者。这一系列研究显示了为主题提供额外机密性的潜在承诺，尽管它可能尚未完全通用和实用。基于ABE的方法的一般挑战是其加密操作的复杂性，这可能难以在有限的发布者硬件上有效地支持，例如在移动设备上遇到的硬件。ABE性能限制在[45,46]中得到了解决，但ABE方法通常比基于PRE的方法需要更多的计算工作量和发布者带宽。此外，ABE不提供我们利用PRE的通用访问委派功能，它具有加密访问委派功能。

代理重新加密的应用有限

（PRE）在Publish-Subscribe系统的域中。最相关的

是[47]没有实现，并使用基于Paillier的PRE方案[48]而不是我们工作中使用的基于格的方法。我们基于格的PRE的一个重要特征是它是单向的，并提供更严格的控制，可以对密文进行重新加密以及向谁进行重新加密。此外，我们的基于格的方案是后量子的，并且允许更一般的同态加密属性。与PRE相关的工作在开始时详细讨论。

第3节

7.结论和未来的工作

我们提供了PICADOR，一个安全的基于主题的Pub/Sub信息-

具有端到端加密的体系结构，使用基于格的代理重新加密（PRE）变体来委托信息访问。PICADOR支持灵活的Pub/Sub异步通信，因为它可以防止信息生产者和消费者需要先验共享信息。此外，它确保Pub/Sub代理无法访问未受保护的信息。实验结果表明PICADOR具有实用可行性。它为许多没有严格实时要求的应用提供了足够的性能，同时传输了大量数据.PICADOR的端到端基于格的重要优势

加密方案是，它使用户能够安全地使用低成本的云计算环境来共享数据，同时还能显着降低内部人员攻击的漏洞。例如，我们的架构仅限于具有解密密钥的系统管理员的数据访问，即使加密计算托管在专有服务器上也是如此。此外，我们的体系结构会阻止对解密数据的访问，直到它到达预期的收件人。因此，我们的架构带来的好处将降低高度监管行业（如医疗保健和军事行业）的运营成本，而监管合规性此前已限制了将数据安全计算外包给低成本云计算环境的能力。尽管我们关注隐私和保密问题，

我们的架构可以增强，以提供完整性和可用性保护，从而满足CIA三元组。例如，标准数字签名方法，如RSA签名或椭圆曲线数字签名算法，可以满足完整性要求。例如，使用主动/主动群集实现的服务复制可以满足可用性要求

C.Borcea等。/FutureGenerationComputerSystems71（2017）177-191189

针对硬件问题和拒绝服务攻击。还可以扩充proto-type的以策略授权为中心的密钥分发方案，以允许对传输的公钥和PRE密钥进行认证。

PICADOR实施基于NTRU-RLWE

支持最多两跳重新加密的PRE方案（两个加密数据委托或两个串联连接的代理）。如果需要更多数量的重新加密，则可以使用其他网格加密方案，例如BGV[30]和FV[49]。这些方案可以使用PICADOR原型使用的PALISADEC++库来实现。

致谢

作者希望感谢与沙菲教授的对话

来自麻省理工学院的Goldwasser和VinodVaikuntanathan教授支持这项工作。

附录

A.1。Stehlé-Steinfeld加密方案

我们的PRE方案基于Stehlé-Steinfeld加密

方案[10]，总结如下。Stehlé-Steinfeld方案使用以下数量进行参数化：

•对应的安全参数（根Hermite因子）δ

最短向量问题[28]，

•密文模数q，•环维数n，•明文模数p，•Bk-有界离散高斯（密钥生成）分布χk

在多项式环上R=Z[n]/⟨xn+1⟩，标准偏差σk，

•有限离散高斯（误差）分布χe

多项式环R，标准偏差σe。

该方案支持明文空间M={0,1，...。。，

p-1}n，其中p是明文模数。密文的所有操作都在环Rq≡R/qR中进行。每个系数

在多项式中，在-q范围内表示

2,.。。，q

2.

该方案包括以下操作：•KeyGen：样本多项式f'，g←χk并设置f：=pf'+1到

满足f≡1（modp）。如果f在Rq中没有模乘法逆，则重新采样f'。设置公钥pk和私钥sk：

sk：=f∈R

pk：=h=pgf-1∈Rq。

•Enc（pk=h，m∈M）：样本多项式s，e←χe。计算

密文：

c：=hs+pe+m∈rq。

•Dec（sk=f，c）：计算密文错误b：=f·c∈Rq。

输出m'：=b（modp）。

只要没有环绕，该方案是正确的

模数q。确实，

b=f·c=f（hs+pe+m）=pgs+pfe+fm

如果b的值没有包围模q，那么

b=pgs+pfe+fm（modp）=fm（modp）=m（modp）。

与[32,31]中的推导类似，可以设计出

使用无穷大规范解密密文的正确性约束∥。。.∥∞，使用离散高斯分布生成的系数的上界Bk和Be，以及平均情况

基于中心极限定理的多项式乘法分析。加密方案的正确性约束要求

f·c=pgs+pfe+fm<q/2。（A.1）

鉴于Bk，Be»1，无穷大范数可表示为

∥f·c∥∞≤√

n{pBkBe+p（pBk+1）Be

+（pBk+1）（p-1）}≈√

np（p+1）BkBe。

将无穷大范数的表达式代入不等式

（A.1）并将估计的范数乘以因子2（以补偿所有近似值），我们得到

q>4√

np（p+1）BkBe。（A2）

A2。Stehlé-Steinfeld加密方案的安全性分析

Stehlé-Steinfeld计划的安全性基于

NTRU和'带错误的环学习'（RLWE）假设[10,31]。

NTRU的问题是要区分以下内容

两个分布：具有f和g的多项式f/g，其从分布χk（假设g在Rq上是可逆的）中采样，并且多项式h在Rq上随机均匀地采样。当σk=ωq1/2[10]时，这些分布在Φm（x）=xn+1时在统计上无法区分。一旦证实了NTRU问题的硬度

（即，不能将公钥与均匀分布的随机多项式区分开），RLWE假设开始证明加密方案的语义安全性。该逻辑用于表明由操作KeyGen，Enc和Dec以及约束σk=ωq1/2定义的Stehlé-Steinfeld方案是

IND-CPA安全[10]。

A.3。NTRU-RLWEPRE方案的安全性分析和约束

虽然证明是安全的，但最初的Stehlé-Steinfeld计划

对于代理重新加密或任何需要从分布χk生成的两个多项式的至少一个乘法的同态加密方案是不切实际的。在这种情况下，q的正确性不等式永远不会成立，因为我们在表达式的右边有B2kασ2k=ω（q），即

q>ω（q）。

出于实际原因，约束σk=ωq1/2是-

通过论证得到的决策小多项式比（DSPR）问题对所有已知的实际攻击都是安全的，可以用对应于误差分布χe的较小值替换[31]。这个假设最近通过两个子场点阵攻击[25,50]对一些参数范围无效，它们能够减小受影响的密码系统的环维度并解决n=512或更低的最短向量问题。

Albrecht等。[25]提出了一个新的实际约束

σk基于NTRU对子场晶格攻击的免疫力，推测Stehlé-Steinfeld证明可以扩展到这种情况：

σk>

2q

NPE

1/4。（A.3）

我们的代理重加密方案，称为NTRU-RLWE

PRE，使用此约束。与最初的Stehlé-Steinfeld方案相比，我们的方案支持ReKeyGen，ReEnc和同态索引和乘法运算。

满足RLWE加密的安全要求

方案，我们使用[33]中导出的不等式，即

n≥log2（q/σe）

4log2（δ）。（A.4）

190C.Borcea等。/FutureGenerationComputerSystems71（2017）177-191

[1]P.T.Eugster，P.A。Felber，R。Guerraoui，A.-M。Kermarrec，很多面孔

发布/订阅，ACMComput。监测网。35（2）（2003）114-131。http：//dx.doi.org/10.1145/857076.857078，URLhttp://doi.acm.org/10.1145/857076。857078。

[2]A.King，S。Procter，D。Andresen，J。Hatcliff，S。Warren，W。Spees，R。Jetley，

P.Jones，S。Weininger，一种用于医疗设备互操作性的发布-订阅体系结构和基于组件的编程模型，SIGBEDRev.6（2）（2009）7：1-7：10。http://dx.doi.org/10.1145/1859823.1859830，URL

HTTP://doi.ACM.org/10.1145/1859823.1859830.

[3]A.King，S。Procter，D。Andresen，J。Hatcliff，S。Warren，W。Spees，R。Jetley，

P.Jones，S。Weininger，医疗设备集成和协调的开放式测试平台，载于：软件工程-伴随卷，2009年，第31届ICSE-Companion2009国际会议。2009年，第141-151页。http://dx.doi.org/10.1109/ICSE-COMPANION.2009.5070972。

[4]V.T.Combs，M.H。Linderman，基于Jini的发布和订阅功能，Proc。

SPIE4863（2002）59-69。http://dx.doi.org/10.1117/12.472945。

[5]J.P.Loyall，M。Carvalho，A。MartignoniIII，D。Schmidt，A。Sinclair，M。Gillen，

J.Edmondson，L。Bunch，D。Corman，QoS支持在发布-订阅-查询信息代理中发布托管信息对象，Proc。SPIE7350（2009）http://dx.doi.org/10.1117/12.818744,73500M-73500M-12。

[6]S.Pallickara，M。Pierce，H。Gadgil，G。Fox，Y。Yan，Y。Huang，Aframework

在发布/订阅系统中安全地端到端地传递消息，参见：第7届IEEE/ACM网格计算国际会议论文集，GRID'06，IEEE计算机学会，华盛顿特区，美国，​​2006年，第215页-222。http://dx.doi.org/10.1109/ICGRID.2006.311018。

[7]E.Orakwue，私有云：安全管理服务，Inf。SECUR。J。：Glob。每-

SPECT。19（6）（2010）295-298。http://dx.doi.org/10.1080/19393550903482924。

[8]A.-A.Ivan，Y。Dodis，代理加密重访，在：Proceedingsofthe

网络和分布式系统安全研讨会，NDSS，2003年。

[9]G.Ateniese，K。Fu，M。Green，S。Hohenberger，改进的代理重加密方案，应用程序用于保护分布式存储，ACMTrans。天道酬勤。SYST。SECUR。（TISSEC）9（1）（2006）1-30。

[10]D.Stelhé，R。Steinfeld，使NTRU与理想格子上的最坏情况问题一样安全，见：K.G。Paterson（Ed。），密码学进展-EUROCRYPT2011：第30届密码技术理论与应用国际会议，爱沙尼亚塔林，2011年5月15日至19日。会议录，柏林施普林格，海德堡，柏林，海德堡，2011年，第27-47页。

[11]D.Micciancio，O。Regev，Lattice-basedcryptography，in：PostQuantumCryptography，Springer，2009，pp.147-191。

[12]O.Regev，量子计算和晶格问题，SIAMJ.Comput。33（3）（2004）738-760。FOCS2002的初步版本。

[13]D.Micciancio，Lattice-basedcryptography，in：EncyclopediaofCryptographyandSecurity，Springer，2011，pp.713-715。

[14]R.Barazzutti，P。Felber，H。Mercier，E。Onica，E.Rivière，Thriftyprivacy：Efficient

支持隐私保护发布/订阅，参见：第六届ACM国际分布式事件系统会议论文集，DEBS'12，ACM，纽约，纽约，美国，2012年，第225-236页。http://dx.doi.org/10.1145/2335484.2335509，URLhttp://doi.acm.org/10.1145/2335484.2335509。

[15]M.Blaze，G。Bleumer，M。Strauss，Divertibleprotocolsandatomicproxycryptography，in：AdvancesinCryptologyEUROCRYPT'98，Springer，1998，pp.127-144。

[16]Z.Miklos，面向广域发布的访问控制机制

lish/subscribesystems，in：第22届分布式计算系统研讨会国际会议，2002年。会议录。2002年，第516-521页。http://dx.doi.org/10.1109/ICDCSW.2002.1030820。

[17]A.Belokosztolszki，D.M。Eyers，P.R。Pietzuch，J。Bacon，K。Moody，基于角色

发布/订阅中间件体系结构的访问控制，参见：第2届国际分布式事件系统研讨会，DEBS'03，ACM，纽约，纽约，美国，2003年，第1-8页。http://dx.doi.org/10.1145/966618.966622，URLhttp://doi.acm.org/10.1145/966618.966622。

[18]J.Hoffert，D。Schmidt，A。Gokhale，一种QoS策略配置建模

发布/订阅中间件平台的语言，参见：2007年首届分布式事件系统国际会议论文集，DEBS'07，ACM，纽约，纽约，美国，2007年，第140-145页。http://dx.doi.org/10。1145/1266894.1266922，URLhttp://doi.acm.org/10.1145/1266894.1266922。

[19]信息技术实验室，FIPSPub186-4数字签名标准

（DSS），国家标准与技术研究所联邦信息处理标准出版物。

[20]D.Nuñez，I。Agudo，J。Lopez，NTRUReEncrypt：一种基于NTRU的高效代理重加密方案，载于：第10届ACM信息，计算机和通信安全研讨会论文集，ACM，2015，pp。179-189。

[21]R.Canetti，S。Hohenberger，Chosen-ciphertext安全代理重新加密，

in：第14届ACM计算机与通信安全会议论文集，CCS'07，ACM，纽约，纽约，美国，2007年，第185-194页。http：//dx.doi.org/10.1145/1315245.1315269,URLhttp://doi.acm.org/10.1145/

1315245.1315269.

[22]Y.Aono，X。Boyen，L。Wang，etal。，LWE下的密钥-私有代理重新加密，在：密码学进展-INDOCRYPT2013，Springer，2013，第1-18页。

[23]E.Kirshanova，来自格子的代理重新加密，在：Public-KeyCryptogra-phy-PKC2014，Springer，2014，pp.77-94。

[24]X.Fan，F.-H。刘，格子的各种代理重加密方案，

CryptologyePrintArchive，Report2016/278,2016，URLhttp://eprint.iacr.org/。

[25]L.D.马丁阿尔布雷希特，施白，对过度拉伸的NTRU的子场格子攻击

假设：一些FHE和分级编码方案的密码分析，CryptologyePrintArchive，Report2016/127,2016，URLhttp://eprint.iacr.org/。

[30]C.Gentry，S。Halevi，N.P。AES电路的智能，同态评估，见：密码学进展-CRYPTO2012，Springer，2012，pp.850-867。

[31]A.López-Alt，E。Tromer，V。Vaikuntanathan，即时多方计算机

[32]Y.Polyakov，K。Rohloff，G。Sahu，V。Vaikuntanathan，Fastproxyre-encryption

[33]C.Gentry，S。Halevi，N。Smart，AES电路的同态评估，R：Safavi-Naini，R。Canetti（编辑），密码学进展，CRYPTO2012，in：LectureNotesin计算机科学，第一卷7417，Springer，Berlin，Heidelberg，2012，pp.850-867。

[34]G.DeCandle，D。Hoster，M。Jampani，G。Kolakupathi，那。拉克斯曼，那。呼吸，s。

[35]A.Rowstron，A.-M。Kermarrec，M。Castro，P。Druschel，Scribe：TheDesignofthe

[36]P.Nikander，G.F。Marias，了解纯粹的发布/订阅

[37]T.H.Yuen，W。Susilo，Y。Mu，迈向加密治疗

[38]E.Onica，P。Felber，H。Mercier，E。Riviere，通过有效的关键更新

[39]H.Khurana，基于内容的可扩展安全和会计服务

发布/订阅系统，参见：2005年ACM应用计算研讨会论文集，SAC'05，ACM，纽约，纽约，美国，2005年，第801-807页。http://dx.doi.org/10.1145/1066677.1066862，URLhttp：//doi。

[40]M.Srivatsa，L。Liu，A。Iyengar，Eventguard：一个系统架构

[41]M.Nabeel，N。Shang，E。Bertino，基于高效的隐私保护内容

发布订阅系统，参见：第17届ACM访问控制模型和技术研讨会论文集，SACMAT'12，ACM，纽约，纽约，美国，2012年，第133-144页。http://dx.doi.org/10.1145/2295136.2295164，URL

[42]M.A.Rajan，A。Varghese，N。Narendra，M。Singh，V.L。Shivraj，G。Chan-

[43]J.Bethencourt，A。Sahai，B。Waters，Ciphertext-policyattribute-baseden-

[44]V.Goyal，O。Pandey，A。Sahai，B。Waters，基于属性的加密

[45]M.Ion，G。Russello，B。Crispo，在基于内容的出版/订阅系统中提供保密性：2010年国际安全和密码学会议论文集（SECRYPT），IEEE，2010，pp.1-6。

[46]P.Pal，G。Lauer，J。Khoury，N。Hoff，J。Loyall，P3S：隐私保护公

[47]K.R.Rohloff，M.J。Gillen，J.P。Loyall，使用代理的信息管理

加密，美国专利申请US2015/0271153A1（2015年9月24日）。

C.Borcea等。/FutureGenerationComputerSystems71（2017）177-191191

[48]G.Ateniese，K。Fu，M。Green，S。Hohenberger，改进的代理重加密

具有应用程序以保护分布式存储的方案，ACMTrans。天道酬勤。SYST。SECUR。9（1）（2006）1-30。http://dx.doi.org/10.1145/1127345.1127346，URLhttp://doi.acm.org/10.1145/1127345.1127346。

[49]J.Fan，F。Vercauteren，Somewhatpractical完全同态加密，

CryptologyePrintArchive，Report2012/144,2012，URLhttp://eprint.iacr.org/。

[50]C.L.JungHeeCheon，JinhyuckJeong，NTRU问题和算法的算法

密码分析没有零级编码的GGH多线性映射，密码学ePrintArchive，Report2016/139,2016，URLhttp://eprint.iacr.org/。



CristianBorcea是新泽西理工学院计算机科学系的教授。他还是日本东京国立信息学研究所的客座教授。他的研究兴趣是移动计算和传感，adhoc和车载网络，分布式系统和云计算。Borcea获得博士学位。他是罗格斯大学的学位，并且是ACM，IEEE和USENIX的成员。



Arnab''Bobby''DebGupta是NJIT网络安全研究中心的研究生。他获得了他的硕士学位。HJIT的计算机科学学位。他获得了卡内基梅隆大学的本科学位。



YuriyPolyakov是NJIT网络安全研究中心的副研究员。他还是麻省理工学院计算机科学与人工智能实验室的研究科学家。他的主要研究兴趣是应用基于格的加密，加密计算和程序混淆。他获得了博士学位。来自莫斯科国立环境工程大学和D.Sc.来自卡尔波夫物理化学研究所。



KurtRohloff是NJIT网络安全研究中心和副主任。新泽西理工学院计算机科学系教授。在加入NJIT之前，他是RaytheonBBNTechnologies的资深科学家。他是多个大型多学科DARPA资助的研发团队的PI。他的专长是控制工程，应用密码学和加密计算。他在佐治亚理工学院获得电气工程学士学位，并获得了硕士学位。和博士在密歇根大学的电气工程专业。



GerardRyan是新泽西理工学院计算机科学系的高级大学讲师。在加入NJIT之前，他曾在AT＆T贝尔实验室，朗讯科技，Avaya和摩托罗拉担任过多个职位。他在软件开发，软件和系统架构以及项目管理方面拥有广泛的背景。他持有硕士学位。罗格斯大学计算机科学系和B.E.在库珀联盟的电气工程。