**一种改进的隐私认证协议，用于**

**5G移动网络**

**玛丽亚・瓦伊萨（Mariya Ouaissa）**

***ENSAM数学与计算机科学实验室***

**穆莱伊斯梅尔大学**

**梅克内斯，莫鲁科**

**mariya.ouaissa@edu.umi.ac.ma ，mariyam.ouaissa@edu.umi.ac.ma**

***抽象的*—移动通信网络始终**

**自从仅作为电话网络推出以来，经历了持续快速的发展。从一代到下一代，服务已经成倍增加和多样化，以先包含数据，然后包含视频和许多其他服务。在此进展之后，用户和移动设备的数量呈指数级增长，因此，数据流量也呈指数级增长。第五代（5G）是新一代的移动电话标准。通过支持一系列要求，例如服务质量，新服务集成的性能和网络安全性，这项无线电信技术有望彻底改变世界的通信方式。第三代合作伙伴计划（3GPP）为5G网络提出了名为5G‑AKA的身份验证和密钥协议（AKA）协议，以提高安全性要求并克服第四代（4G）网络的EPS‑AKA协议中存在的漏洞。在这项工作中，我们提出了一种针对5G移动网络的改进，高效的身份验证和密钥协商协议，该协议克服了现有5G‑AKA中发现的弱点，并使用了轻量级的加密方法来增加不同实体的计算成本。为了验证和验证我们提出的建议，我们使用Internet安全协议和应用程序的自动验证（AVISPA）工具来演示已验证身份验证和安全性的目标。此外，**

***关键字‑5G，5G‑AKA，3GPP，身份验证，隐私。***

**一世。一世简介**

**近年来，我们目睹了健康，媒体，工业，运输，能源等领域的新应用和技术的指数级发展。这种发展与新服务的出现密切相关，新服务的出现与连接对象的激增相关[1]。连接着一切的世界变得越来越数字化。这些对象将在互联网上与数十亿人彼此连接。尽管当前基于长期演进（LTE）标准[4]的第四代（4G）网络带来了许多解决方案，例如与老一代相比速度和带宽增加，但是这种增长需要在移动电信系统上取得许多进步。移动网络。4G使用IP技术，可通过智能手机，平板电脑或笔记本电脑舒适地浏览互联网。**

**面对这些问题，移动通信系统的新标准宣布了新的革命，称为第五代（5G）。该标准为满足当前需求以及未来需求提供了视角，届时我们将拥有数千亿个互联对象和自动驾驶汽车。面对所有这些要求，下一代移动电信系统将必须结合多种技术才能拥有可以满足期望的移动网络[3]。5G网络当然容易受到攻击。罪犯一次又一次地能够在将设备连接到网络的同时访问通信，以拦截对话或窃取数据。**

**为了支持安全性，设备和网络在连接时必须能够相互认证。同时，必须对用户数据，身份和位置保密。为此，自第三代（3G）标准引入以来，已经实现了称为身份验证和密钥协商（AKA）[4]的通信协议，该标准通过协商和建立用于对电话和蜂窝网络之间的通信进行加密的密钥来工作。但是，为5G协议设计的AKA版本（也称为第三代合作伙伴计划（3GPP）标准化的5G‑AKA）经过专门设计，旨在通过增强的身份验证协商系统来阻止国际移动用户身份（IMSI）收集 。**

**与3G和4G相比，通过5G高速传输的数据的保护得到了改善。5G‑AKA协议的概念是在4G网络中标准化的EPS‑AKA协议的改进的安全版本，但是此新的身份验证协议中存在一些弱点，这些弱点将影响5G网络中用户的隐私和数据安全性。因此，有必要增强5G‑AKA协议以建立强大的认证程序[5]。**

**在本文中，我们提出了5G系统认证和密钥协商协议的增强版本，以克服5G‑AKA标准中存在的局限性。我们提出的目的是保证移动用户身份的隐私保护，避免IMSI捕获 ，并在网络设备之间交换密钥K，并且还使用一组轻量级的加密方法以增加不同实体中的计算成本。**

**本文的其余部分安排如下：下一部分介绍了背景，包括系统体系结构，现有协议5G‑AKA的描述及其弱点。在第3节中，我们提出了改进的安全性**

**978‑1‑7281‑9785‑2 / 20 / $ 31.00©2020 IEEE**

**136**

**授权使用仅限于：哥德堡大学。从IEEE Xplore在2020年12月18日世界标准时间19:07:11下载。有限制条件。**

|  |  |  |
| --- | --- | --- |
| **5G网络的协议。第四部分使用形式验证来分析我们提议的安全** | **对于5G核心网络，传输计划功能由用户平面功能（UPF）负** |  |
| **性，并评估现有协议的性能以及我们的主张。最后，我们在第5节** | **责。通过策略计费功能（PCF）实体，既可以在SMF实体级别也可** |  |
| **中得出结论。** | **以在AMF实体级别上控制流，从而能够在考虑到移动台位置的情** |  |
|  | **况下，在授权流上提供更好的粒度UE。移动设备的注册要求使用** |  |
| **二。乙周围** | **AUthentication服务 功能（AUSF）提供的身份验证矢量在AMF** |  |
| **实体和移动UE的级别执行双重身份验证。** |  |
| **在本节中，我们将介绍5G通信的系统架构，并介绍现有协议** |  |  |
| **5G‑AKA及其弱点** |  |  |

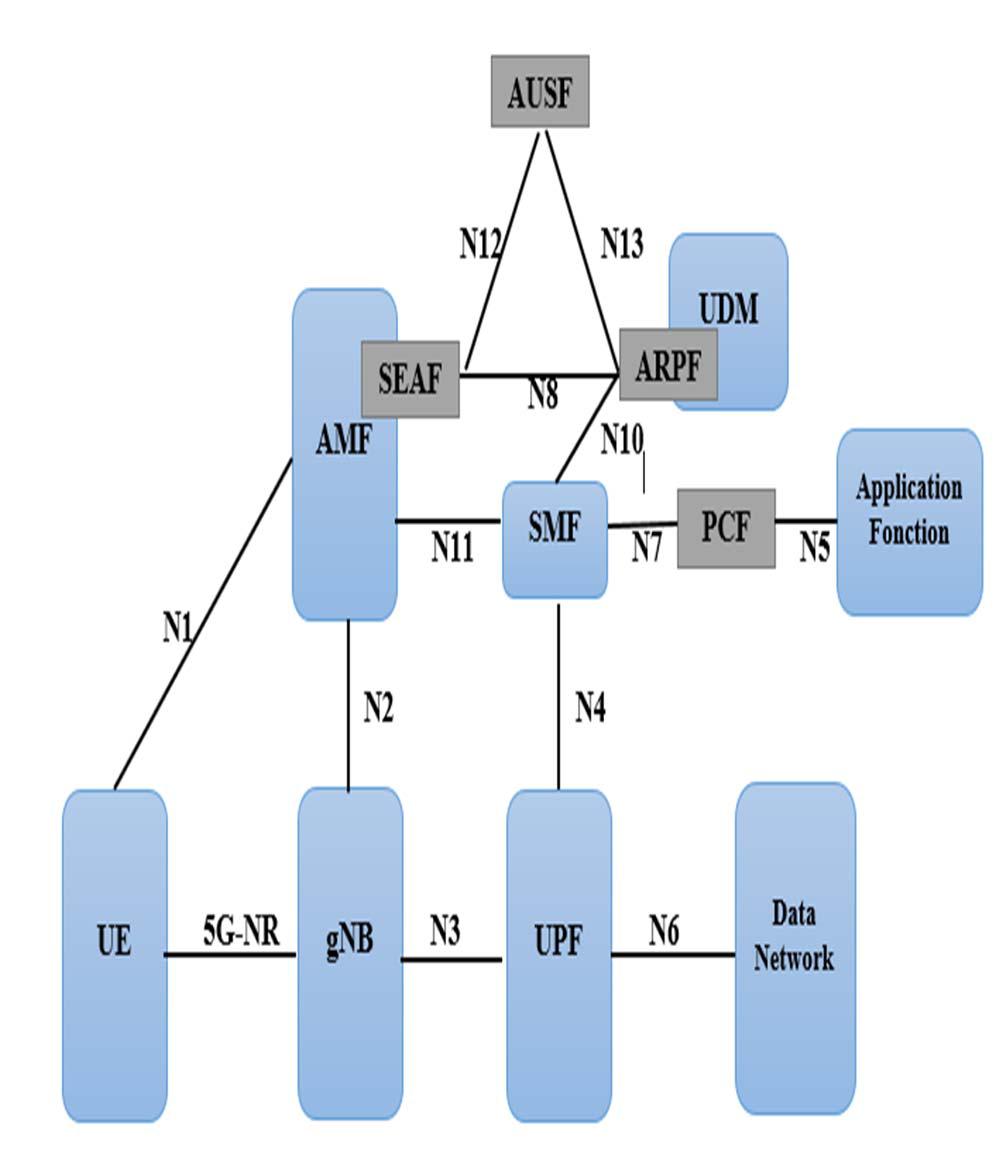
***A.系统架构***

**5G网络由新一代无线接入网络（NG‑RAN）和5G核心（5GC）网络组成。图1显示了5G架构以及每个实体之间的接口[6]。**

**5G无线电接入由新一代基站组成，这些基站形成了具有5GC网络的移动设备的连接节点。用户设备（UE）移动台通过称为生成节点基站（gNB）站的5G无线电链路与基站进行通信。gNB基站的功能与演进型NB（eNB）实体非常相似。但是，差异涉及按流而不是按介质对服务质量的管理以及无线接口上的网络切片的管理。**

**5G核心网络适用于网络虚拟化，并且基于控制平面和用户平面的划分。因此，在5G中管理移动设备的附着，位置和承载的创建的实体是，访问和移动性管理功能（AMF）实体与UE移动设备建立NAS连接，并具有注册UE移动设备的作用。在3GPP和非3GPP网络上管理移动设备的位置。AMF与SEcurity锚定功能**

**（SEAF）并置，该功能包含被称为访问网络锚定键的根密钥，会话管理功能（SMF）实体用于控制分组数据网络（PDN）会话。**



**用户配置文件保存在可通过统一数据管理（UDM）实体访问的统一数据存储库（UDR）数据库中。UDM实体保留UE移动设备所附接的数据会话和AMF实体的配置文件。身份验证凭证存储库和处理功能（ARPF）与UDM并置，并存储诸如密钥K之类的长期安全凭证。**

***B.现有的5G‑AKA协议***

**由于不同代移动网络的进步，该体系结构一直并且一直在发展，并且仍然提出了新机制和协议以通过关注认证服务来提高网络安全性，特别是无线电接入部分。为此，自3G标准引入以来，已实施了3GPP提出的协议AKA，并且一直演进到出现5G移动标准的新版本为止。**

**用于实现4G网络中用户与网络之间相互认证的AKA版本 [Evolved Packet System（EPS‑AKA）[7]]知道几个问题，包括IMSI的清晰传输，中间人（MITM）攻击。攻击者获取IMSI，然后尝试向基站注册拒绝服务（DoS）攻击，该攻击使服务不可用，以防止服务的合法用户使用该服务。EPS‑AKA \* [8]是针对5G提出的一种身份验证协议，它对EPS‑AKA进行了一些修改，但是这两种协议的主要困难在于UE从未针对其对身份SNid的观点进行过密码可验证的声明。服务网络。**

**实际上，5G移动通信标准当前基于3GPP在技术规范33.501 [9]中提出的5G‑AKA协议。与3G和4G技术相比，新协议将大大改善数据保护。特别是，由于他，IMSI拦截 先前利用的缺陷已得到解决。使用这些设备，可以读取移动电话卡的国际移动用户身份，以确定移动设备的位置并跟踪用户。为此，设备仅需要侦听移动电话和移动网络天线之间的传输。使用5G‑AKA不再可能。**

**图2显示了包含四个实体的标准5G‑AKA协议的过程，涉及设备设备UE，服务网络SEAF中的功能安全性以及安全功能驻留在本地网络AUSF和ARPF中。UE和ARPF共享秘密对称密钥K。**

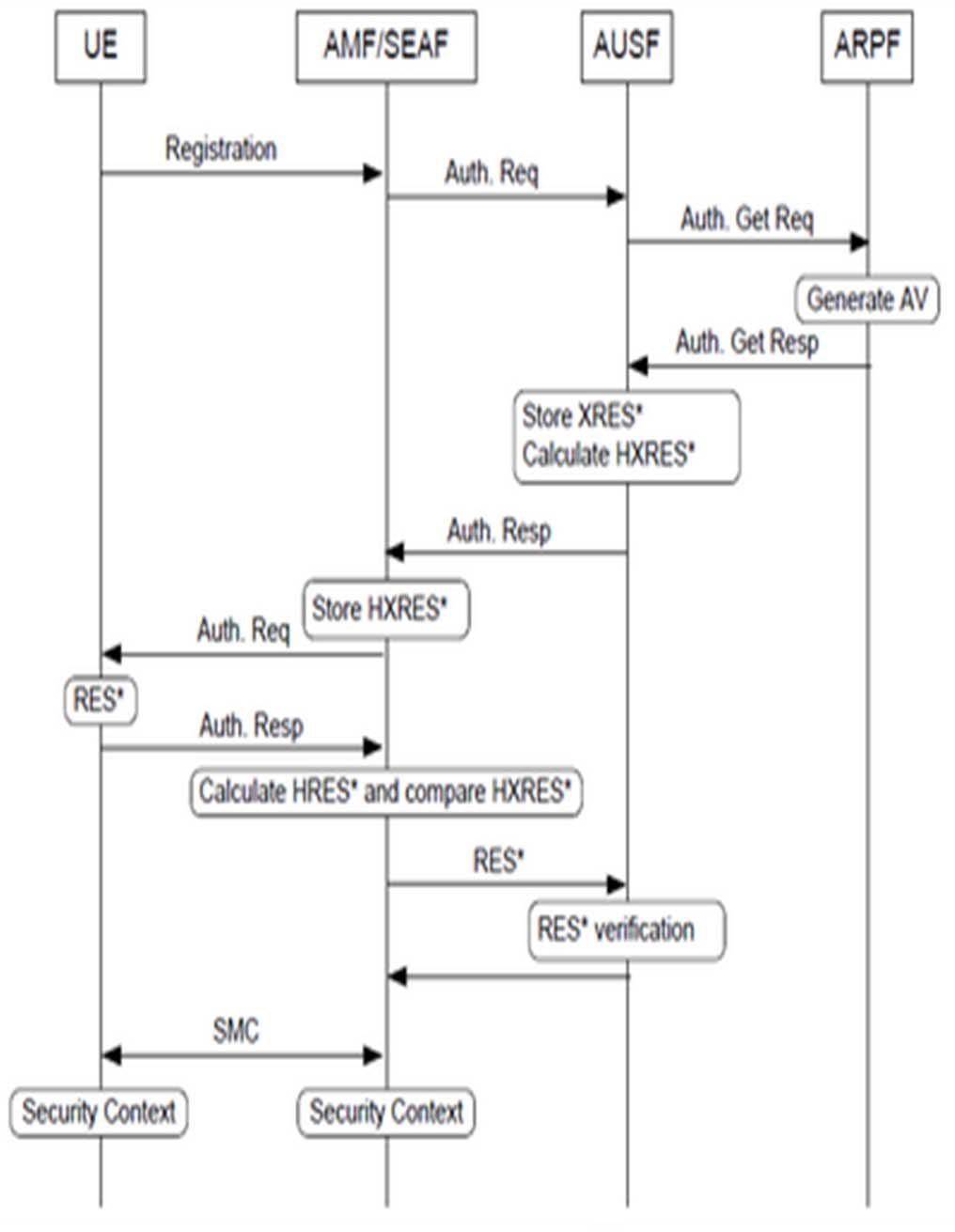
***C.5G‑AKA协议的局限性***

**尽管与前几代产品相比，5G安全性得到了改善，但已经确定了某些系统限制，这些限制对于安全协议和机制至关重要，这使5G系统容易受到多种攻击的影响。**

**图1.系统架构**

**137**

**授权使用仅限于：哥德堡大学。从IEEE Xplore在2020年12月18日世界标准时间19:07:11下载。有限制条件。**



**图2. 5G‑AKA身份验证过程**

**攻击。然后，我们列举其中一些局限性[10]：**

* **为了保护和提供隐私保护，**

**UE身份的5G‑AKA协议中的全球唯一订阅永久标识符**

**（SUPI），3GPP提议实施椭圆曲线集成加密方案（ECIES）[11]加密，这可能导致高计算开销，主要是在无法支持的智能对象中非对称加密。**

* **另外，该协议遭受高**

**核心网络中的通信和计算开销是由归属网络实体之间计算出的认证向量的数量引起的。**

* **在5G‑AKA中，完整性验证在**

**ARPF实体以及此后的实体都无法向UE进行身份验证，在这种情况下，可以使用UE的私有身份在网络中对任何入侵者进行身份验证。然后，该协议面临多种安全攻击，例如MITM，重播和DoS攻击。**

**Ø同步问题是最多的问题之一**

**在UE和ARPF之间建立序列号时，在5G身份验证过程中已知。**

|  |  |  |
| --- | --- | --- |
| **表一** | **Ť他 d不同的 ñ适用于 Ť他 P滚转** |  |
| **符号** | **描述** |  |
| **SUPI / SUCI** | **SUPI订阅永久标识符，隐藏的订阅标识符，** |  |
| **隐藏的** |  |
|  | **苏皮** |  |
| **MAC / XMAC** | **消息验证码** |  |
|  |  |  |
| **东南亚ID** | **SEAF的身份** |  |
|  |  |  |
| **CK / IK** | **x生成的密码/完整性密钥** |  |
|  |  |  |
| **ķAUSF /ķ海豚/ķAMF** | **由ARPF，AUSF，SEAF生成的密钥** |  |
|  |  |  |
| **XRES \* / HXRES \*** | **预期响应值** |  |
|  |  |  |
| **RES \* / HRES \*** | **认证响应值** |  |

**影音** **验证向量**

**兰德** **随机数**

**加密函数用于计算**

**f1⋯⋯f6** **认证参数**

***A.初始化阶段***

**我们提出的协议中的身份验证和密钥协商过程是在架构实体UE，AMF / SEAF，AUSF和UDM / ARPF之间实现的。**

**每个移动台由称为SUPI的永久身份标识，该身份应由提供商安装，以允许用户在核心网络3GPP中进行注册。**

**为了保护用户身份SUPI的隐私并避免IMSI捕获 ，并在UE和SEAF或UE和ARPF之间交换密钥K，我们考虑了密钥协议协议 Elliptic Curve Diffie Hellman（ECDH）[12]，该协议允许两个双方，每个方都有一条椭圆曲线和公用/专用密钥对，以在不安全的通道上建立共享的机密，我们使用对称加密操作对身份进行加密，以获得隐藏了身份的隐藏的身份订阅隐藏标识符（SUCI）。UE计算的SUPI。**

**此外，我们假设核心网络实体和安全功能（AMF / AUSF / ARPF）之间的通信是安全的，并在指定方之间通过建立通道维护长期IPSec，（D）TLS或DIAMETER会话。**

**此外，当UE在ARPF上成功通过身份验证时，我们的协议允许在ARPF中对AUSF / SEAF进行身份验证。**

|  |  |  |
| --- | --- | --- |
| **三，P定位 P滚转** | ***B.认证程序*** |  |
| **根据5G‑AKA协议中存在的不同限制并在上一节中进行了讨** | **图3显示了我们提出的认证过程，每个消息的详细说明如下：** |  |
| **论，我们提出了一种改进且有效的身份验证和密钥协商协议，该** |  |  |
| **协议遵循5G蜂窝网络的网络架构，并克服了诸如重播攻击，重定** | **M1： UE •AMF / SEAF：附加请求** |  |
| **向攻击，人为攻击等多种攻击方式中间攻击和DoS攻击。表1列出** |  |
| **了此过程中使用的参数的长度以及密码功能。** | **为了启动身份验证过程，用户** |  |
|  | **设备生成随机数RANDUE 并发送其** |  |
|  | **除了SUCI实体对SEAF实体的身份。** |  |

**138**

**授权使用仅限于：哥德堡大学。从IEEE Xplore在2020年12月18日世界标准时间19:07:11下载。有限制条件。**

**M2： AMF / SEAF •UE：附加请求**

**收到拟合信息后，SEAF将**

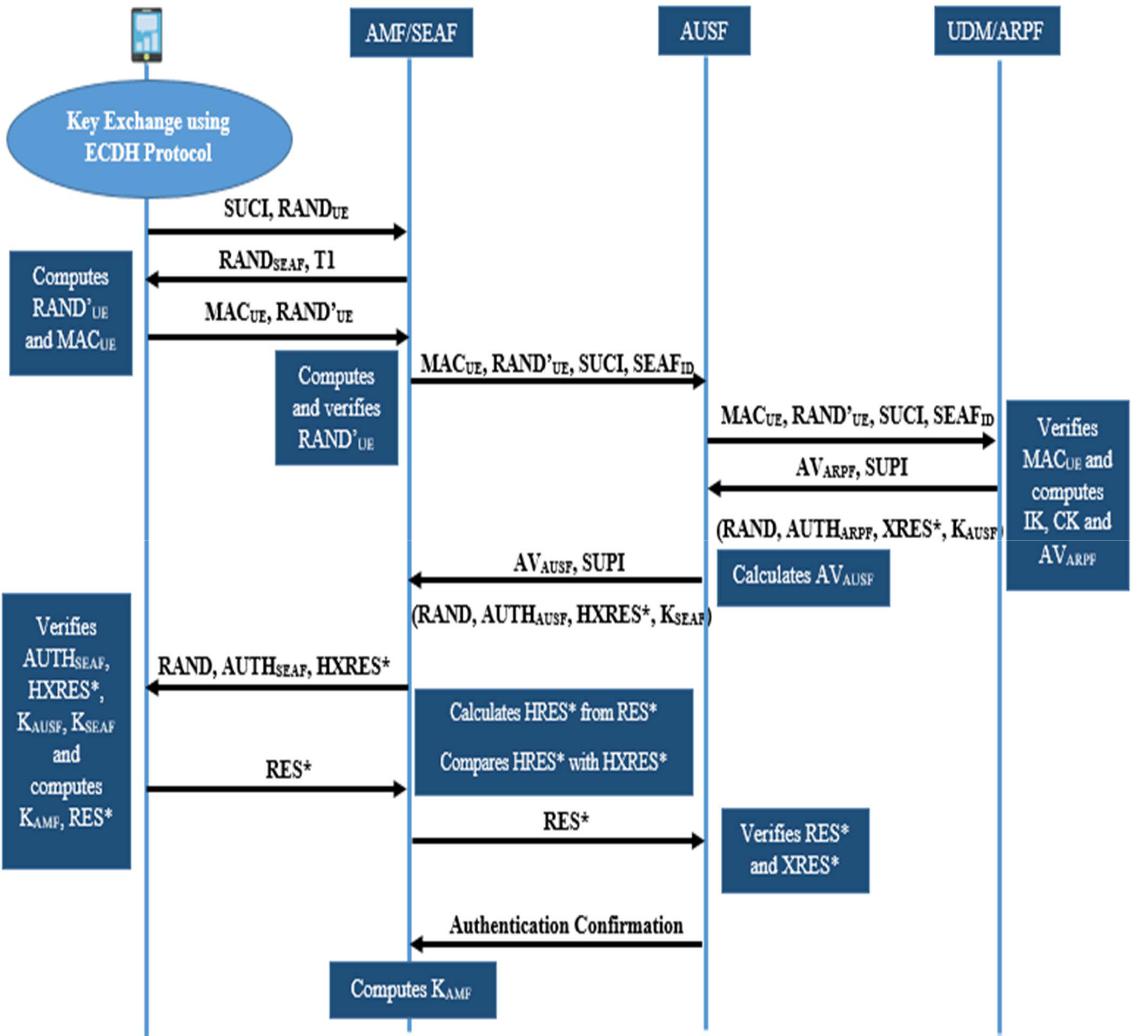
**随机数RAND东南亚 和时间戳T1，以验证UE是否在操作中，并定义**

**UE的到期时间**

**下一个回应。**

|  |  |  |
| --- | --- | --- |
| **M3： UE •AMF / SEAF：附加请求** |  |  |
| **UE计算自己的认证消息MACUE** |  |  |
| **并生成随机参数RAND'UE 并发送给他们** |  |  |
| **到SEAF。** | **（1）** |  |
| **苹果电脑UE =11K（苏克兰德UE）** |  |
| **兰德UE = f2K（兰德UE， 兰德东南亚）** | **（2）** |  |
| **M4： AMF / SEAF• AUSF / UDM / ARPF：身份验证请求** |  |  |

**SEAF会验证随机数和SUCI是否匹配，然后通过AUSF将参数发送给ARPF。**



**图3.拟议协议**

**M5： UDM / ARPF •AUSF：身份验证响应**

**UDM / ARPF收到认证请求消息后，首先通过生成密钥K来启动，然后**

**比较接收到的消息认证码MACUE**

**与XMACUE。 如果这些值相同，则UE被认证。然后，ARPF在对SEAF进行身份验证之后**

**SEAF的验证ID。 而且，ARPF会生成自己的随机RANDARPF 和一个随机数RAND。然后，它计算MACARPF， 并依次计算CK，IK，XRES \*，AUTHARPF， ķ美国空军 并转移影音ARPF与SUPI一起**

|  |  |  |
| --- | --- | --- |
| **AUSF。** | **（3）** |  |
| **苹果电脑ARPF = 11K（兰德UE， 兰德）** |  |
| **CK = f3K（兰德ARPF）** | **（4）** |  |
| **IK = f4K（兰德ARPF）** | **（5）** |  |
| **XRES \* = f5K（兰德UE， 兰德ARPF， 兰德）** | **（6）** |  |
| **AUTNARPF =（兰德（MAC）ARPF， 兰德ARPF）** | **（7）** |  |

**139**

**授权使用仅限于：哥德堡大学。从IEEE Xplore在2020年12月18日世界标准时间19:07:11下载。有限制条件。**

**（16）**

**（17）**

|  |  |
| --- | --- |
| **ķAUSF = KDF（CK，IK，兰德ARPF， SUCI）** | **（8）** |
| **影音ARPF =（兰德（AUTN）ARPF， XRES∗， ķAUSF）** | **（9）** |

**M6： 美国空军•AMF / SEAF：身份验证响应收到上一条消息后，AUSF存储**

**XRES \*和KAUSF， 然后选择RANDAUSF。 进一步计算HXRES \*，AUTHAUSF， ķAUSF， HXRES \*是哈希值（如果为XRES \*），并将所有参数传输到**

**SEAF。**

**HXRES \* = f6K（XRE∗，兰德AUSF，兰德ARPF，兰德）（10）AUTN**

|  |  |  |
| --- | --- | --- |
| **AUSF =（兰德，兰德ARPF， 兰德AUSF）** | **（11）** |  |
| **ķSEAF = KDF（KAUSF， 兰德AUSF， 兰德UE， 东南亚ID）** | **（12）** |  |
| **影音AUSF =（兰德（AUTN）AUSF，高解析度∗，ķ东南亚）** | **（13）** |  |
| **M7： AMF / SEAF •UE：身份验证请求** |  |  |
| **收到来自AUSF的消息后，SEAF会进行计算** |  |  |
| **苹果电脑东南亚 并传输参数RAND，AUTH东南亚 和** |  |  |
| **HXRES到UE。** |  |  |
| **苹果电脑SEAF =f2瑞典空军（兰德SEAF，东南亚ID，兰德** | **（14）** |  |
| **苹果电脑ARPF）** |  |
| **认证SEAF =（苹果电脑SEAF， 兰德SEAF， 东南亚ID）** | **（15）** |  |

**M8： UE •AMF / SEAF：身份验证响应首先，UE检查MAC的验证ARPF 和MAC东南亚**

**为了确保UE对ARPF和SEAF进行身份验证实体。UE比较接收到的值之后**

**HXRES \*，XRES \*，KAUSF， ķ东南亚如果这些值匹配，则UE对ARPF和AUSF进行认证。还可以**

**计算K** **AMF 和将要发送给SEAF的RES \*。**

**ķAMF = KDF（SUCI，K东南亚）**

**RES\* = f5K（兰德UE， 兰德ARPF， 兰德）**

**M9： AMF / SEAF•AUSF：身份验证请求**

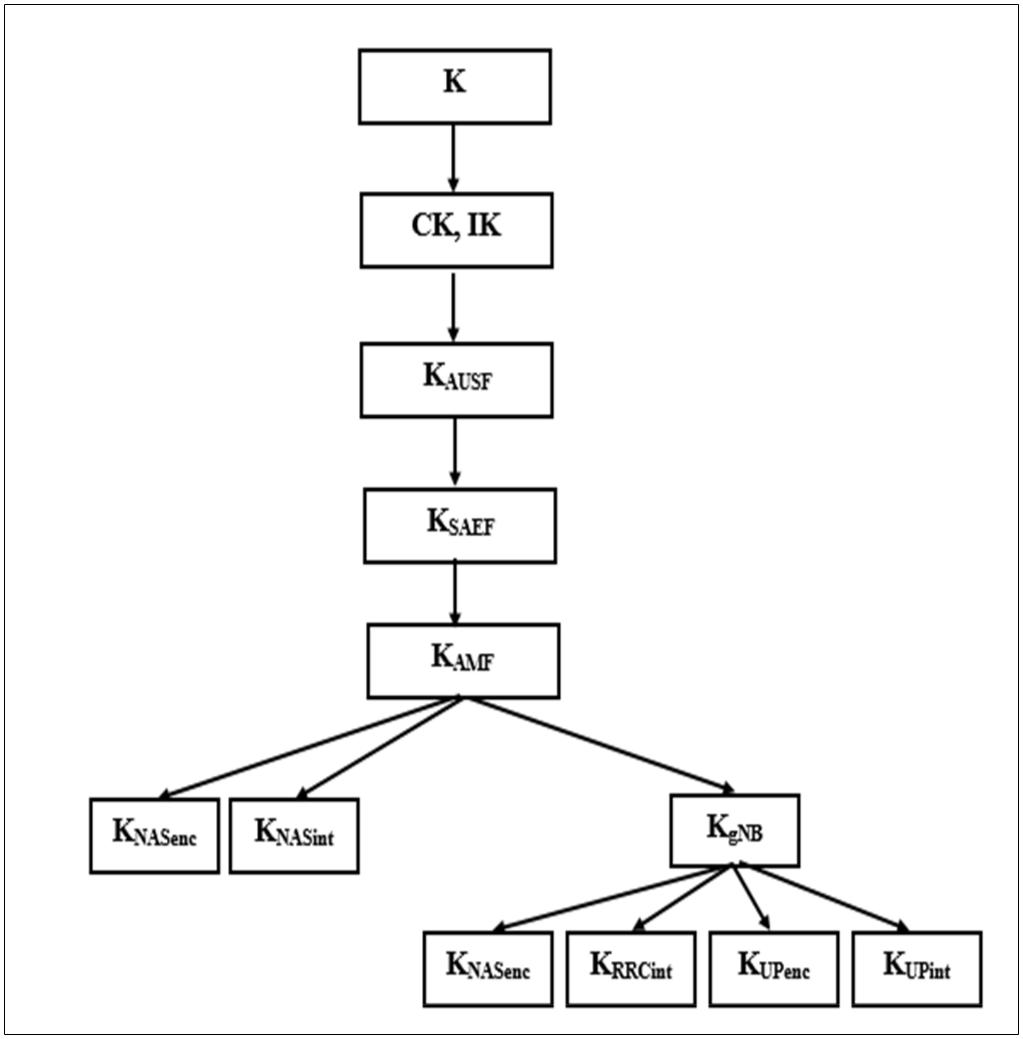
**如果已验证值HXRES \*，则SEAF将在UE中成功进行身份验证，并且在AUSF接收到RES \*之后，它将把参数的值与XRES \*进行比较。**

**HRES\* =f6K（RES∗，兰德AUSF， 兰德ARPF， 兰德）（18）M10： 美国空军 •AMF / SEAF：确认消息**

**AUSF将包含结果和SUPI的身份验证确认消息发送给SEAF，稍后再发送**

**计算KAMF。**

**图4. 5G系统中的密钥层次结构**

****

**IV。伏特替代和 E估值**

**本节评估我们的表现**

**身份验证协议根据安全性进行分析，并与其他现有协议进行性能评估。**

***A.安全性分析***

**在这一部分中，我们将对安全性分析和形式验证进行分析，以说明我们的模型可以达到安全性目标和要求。**

***1）正式验证***

**此解决方案已通过安全协议验证工具Internet安全协议和应用程序的自动验证（AVISPA）[13]进行了检查，它表明它是一个非常安全的级别。该工具的主要优点是能够在同一协议规范上使用不同的验证技术。协议设计者通过在高级协议规范语言**

**（HLPSL）中指定安全问题来与该工具进行交互。该协议的规范用作四个不同后端的输入：动态模型检查 （OFMC），基于CL的攻击搜索 （CL‑AtSe），基于SAT的模型检查 （SATMC）和基于树自动机的协议分析 （TA4SP）。这些后端对包含结果的输出执行分析和格式化。**

**在验证了所有过程之后，我们可以认为我们的身份验证和密钥协商过程已成功完成**

***C.我们的系统5G中的关键层次结构***

**认证成功后，每个用户设备和**

**服务网络共享密钥KAMF 作为衍生以下密钥的必要工具。按键中的层次结构**

**5G系统如图4所示。**

**5G中的密钥层次结构比4G中的密钥层次结构更长，因为5G引入两个中间键，K美国空军 和KAMF。 ķ东南亚 是**

**5G中的锚键，等效于K美国机械工程师学会 在4G中。**

**我们提出的方案的主要目标是在UE设备与服务网络和家庭网络的实体之间提供所有安全要求。我们需要验证所提出的协议可以通过使用后端服务 在UE，SEAF，AUSF和ARPF之间提供成功的相互认证。**

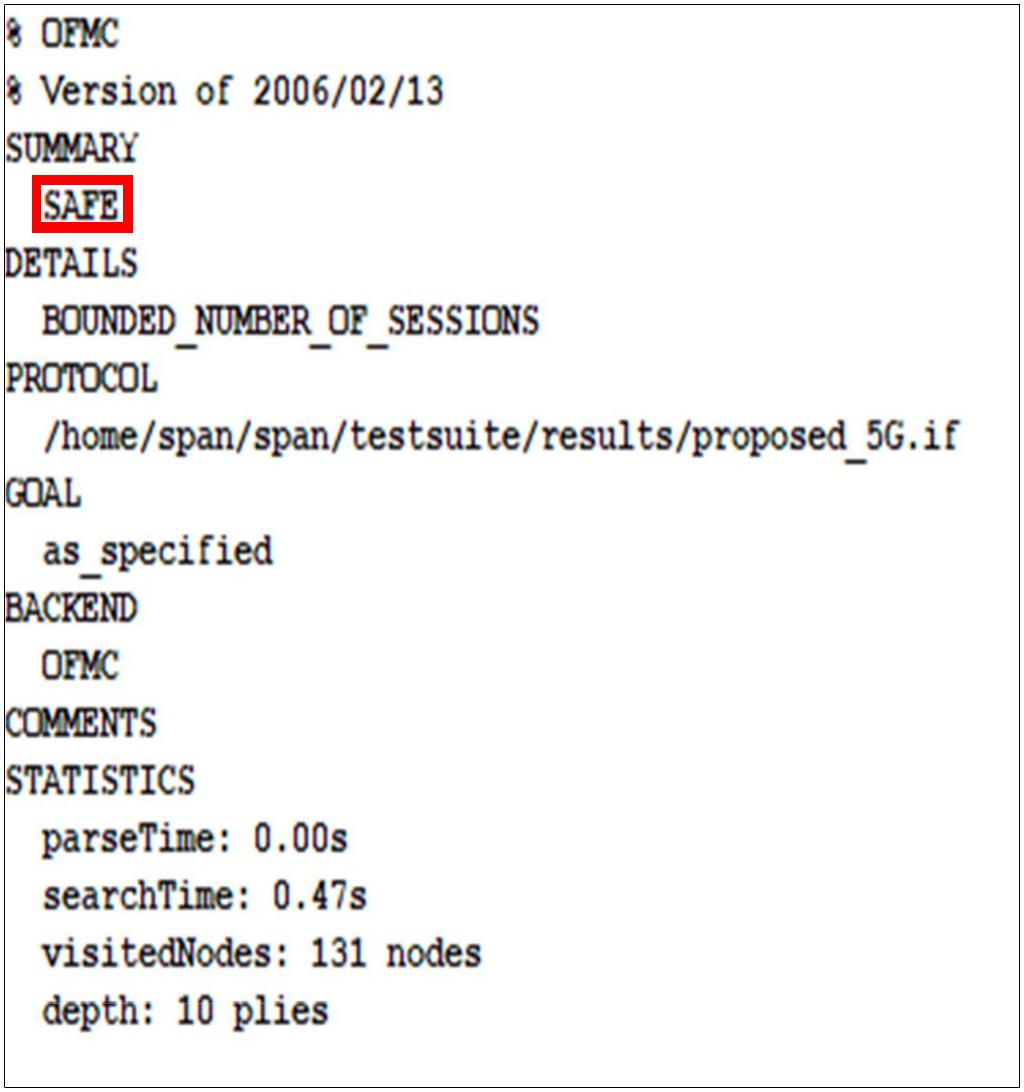
**在使用OFMC和CLAtSe后端运行此规范之后，我们可以得出结论，提出的解决方案可以实现我们的目标，并且可以抵抗那些恶意攻击，例如重播攻击，保密攻击， 和DoS攻击，**

**MITMattacks⋯经过AVISPA的测试。模型检查结果的输出在图2和图3中示出。5和6。**

**140**

**授权使用仅限于：哥德堡大学。从IEEE Xplore在2020年12月18日世界标准时间19:07:11下载。有限制条件。**

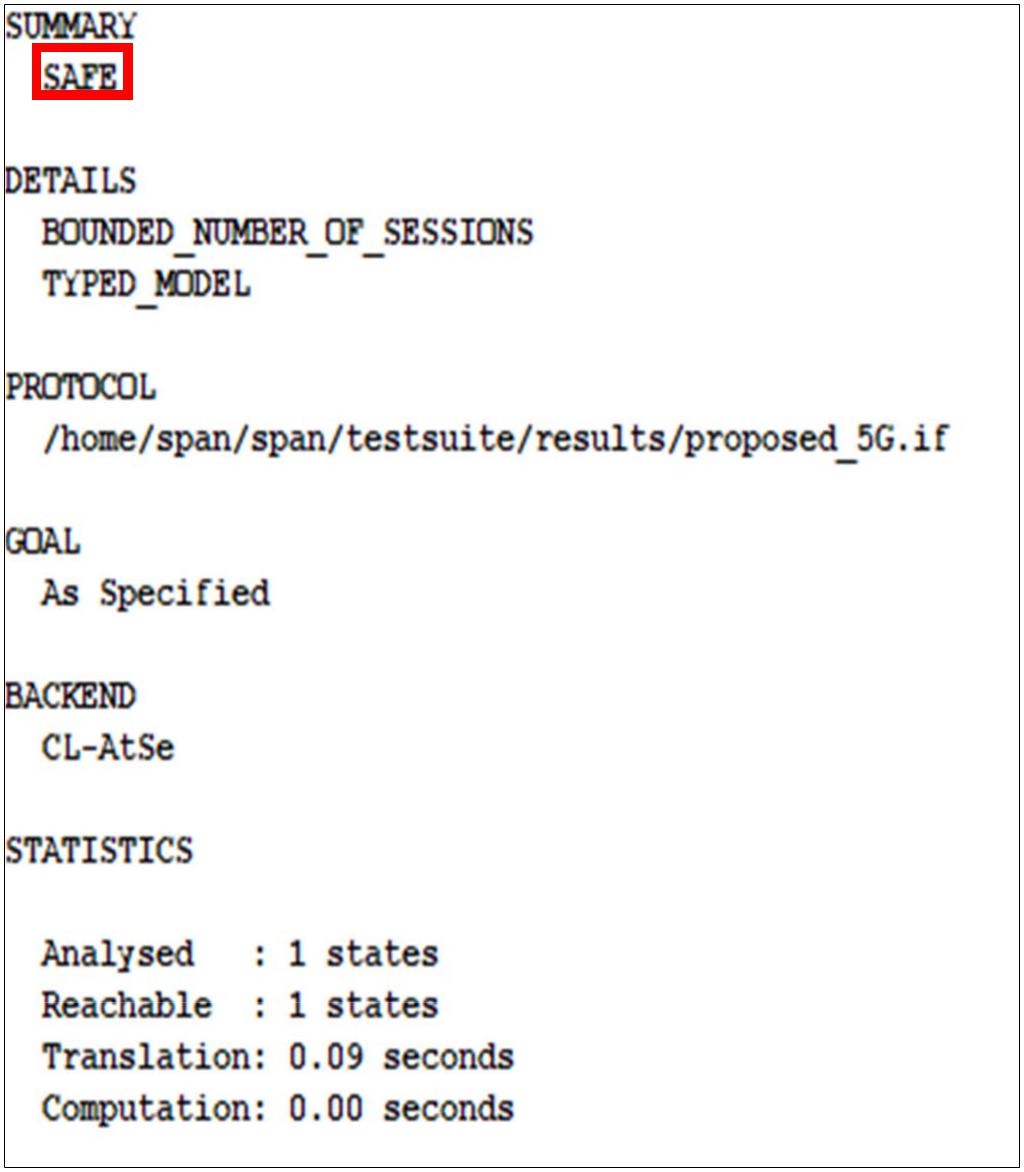
***3）抵抗攻击***



**Ø** ***重播攻击***

**所提出的协议可以抵抗重播攻击，入侵者无法计算有效的会话密钥并重播相同的消息，这是由于每个实体RAND中都生成了随机**

|  |  |  |
| --- | --- | --- |
|  | **数UE， 兰德SEAF， 兰德美国空军 和** |  |
|  | **兰德ARPF以及交易参数的验证** |  |
|  | **XRES \*，K美国空军和允许** |  |
|  | **UE对ARPF和AUSF的身份验证。** |  |
|  | **Ø*DoS攻击*** |  |
|  | **我们的解决方案可以通过限制向访问和核心网络中的实体传输** |  |
|  | **错误的消息请求来减少DoS攻击的影响，因为每个设备都会生成** |  |
|  | **自己的消息身份验证代码并对其进行验证** |  |
|  | **通过计算XMAC在ARPF实体中UE， 然后通过相同的方法，UE对** |  |
|  | **AUSF进行身份验证，但这一次是通过验证** |  |
|  | **XRES \*和HXRES \*。** |  |
|  | **Ø*中间人攻击*** |  |
|  | **共享密钥KAUSF，ķSEAF，ķAMF在5G系统中实体之间的通信中进行** |  |
| **图5. OFMC后端报告的结果** | **计算和验证** |  |
| **克服了窃听的问题，避免了任何对手计算认证消息。** |  |
|  | **Ø*重定向攻击*** |  |
|  | **我们的协议具有抵御重定向攻击的能力，入侵者无法承受此攻** |  |
|  | **击以获得用户信息，因为UE的SUPI身份不会在不安全的运河上传** |  |
|  | **输** |  |
|  | **以及对SEAF身份的验证ID 由...实现** |  |
|  | **ARPF。** |  |
|  | ***B.绩效评估*** |  |
|  | **在这一部分中，我们根据通信开销和计算开销来评估所提出协** |  |
|  | **议的性能。** |  |



**图6. CL‑AtSe后端报告的结果**

***2） 相互认证***

**在提出的协议中，所有实体UE，ARPF，SEAF和AUSF之间的通信执行并实现相互认证和密钥协议以及使用它们自己的MAC的协议。UE在验证MAC之后对SEAF和ARPF进行身份验证UE 计算byUE并传输到ARPF，还通过检查MAC的有效性来进行计算ARPF**

**和MAC东南亚 并验证接收到的RES \*值。然后，设备通过生成并验证密钥KAUSF。**

***1）*** ***通讯开销***

**为了评估我们提出的协议和其他AKA协议的通信开销，基于消息中传递的每个参数，我们计算了实体之间传输的此类消息中的位数。的大小**

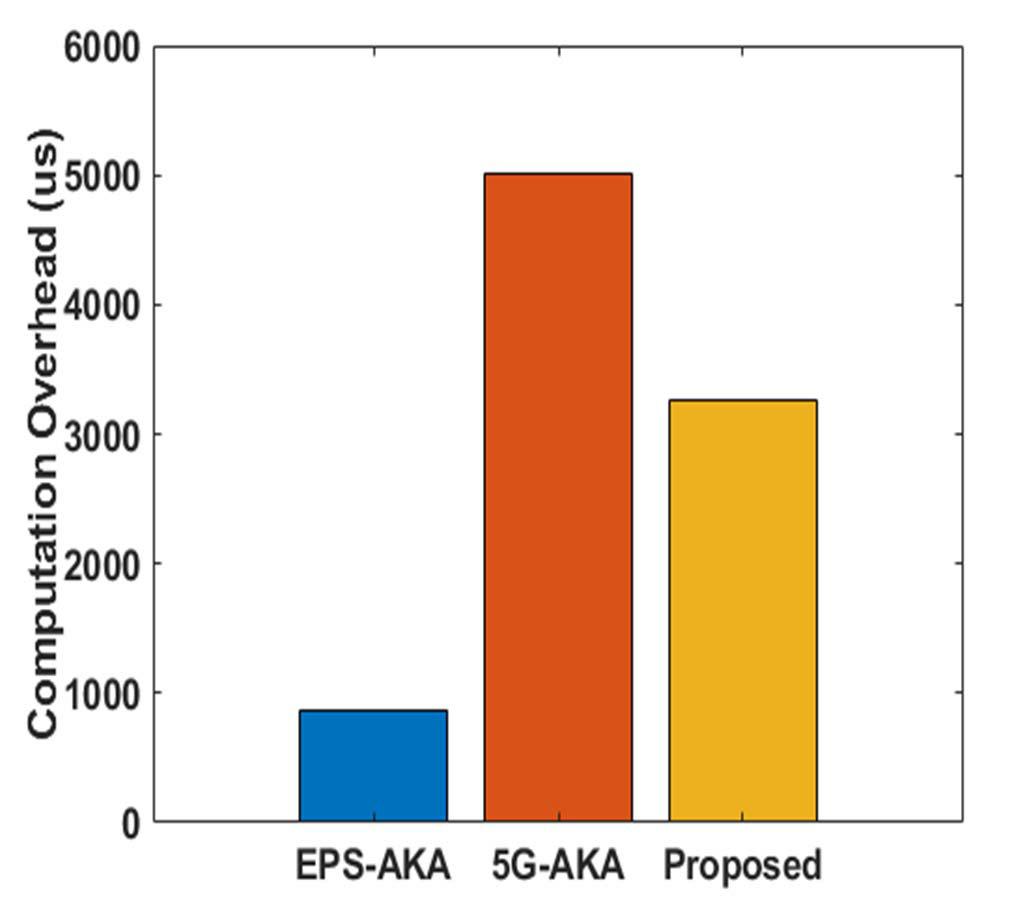
**位中的参数如表2所示。**

|  |  |  |  |
| --- | --- | --- | --- |
| **表II。** | **小号参数大小** |  |  |
|  | **参数** | **大小（位）** |  |
| **SUPI / SUCI / SEAFID** | | **128** |  |
| **兰德/兰德UE /兰德UE /兰德SEAF /兰德AUSF /** | | **128** |  |
|  | **兰德ARPF** |  |
| **CK / IK / AK / K** | | **128** |  |
|  | **AUTN** | **多变的** |  |
| **影音/影音ARPF /影音美国空军** | | **多变的** |  |
| **MAC / XMAC** | | **64** |  |
| **K A中小企业/ķ澳洲空军/ķ海豚/ķAMF** | | **256** |  |
| **RES / XRES / RES \* / XRES \* / HRES \* / HXRES \*** | | **64** |  |

**141**

**授权使用仅限于：哥德堡大学。从IEEE Xplore在2020年12月18日世界标准时间19:07:11下载。有限制条件。**

**在每个AKA协议中，分为三个阶段，第一阶段是设备与核心网络建立通信时，第二阶段是本地网络发送将存储在服务网络中的n个身份验证向量（AV），以及**



**第三阶段是在**

**服务网络与UE之间的通信，n是身份验证请求的数量（表3）。**

**步骤1中的位数= ∑消息（阶段1 +阶段2）步骤2中的位数= ∑消息（阶段3 \* n）**

**传输的比特总数= ∑消息（阶段1 +阶段2）+ ∑消息（阶段3 \* n）**

***2）*** ***计算开销***

**我们评估了我们的协议，4G EPS‑AKA的标准协议和现有5G‑AKA的计算开销。在这种情况下，我们选择使用Crypto ++ Library [14]来实现这些单一操作的执行时间值，这些值是通过在Ubuntu上使用2.1 GHz处理 的测试平台上运行的测量获得的。表4说明了这些操作及其计算开销。**

**图7.计算开销**

**在我们提出的建议中，为了确保第一个附加请求的安全，我们假设使用ECDH协议来保护实体之间的密钥秘密交换和加密，我们研究了对称加密操作AES‑CTR的使用[15]。考虑的性质**

**具有低功率容量和能量约束的智能设备。**

**然后，对于密钥派生，生成和哈希函数，我们使用HMAC‑SHA256和SHA‑256函数。**

**我们在图7中演示了计算开销。可以观察到，与EPS‑AKA相比，我们的协议提供了更大的延迟，这是因为我们的解决方案使用了更多的操作，这些操作提供了更好的安全性并增强了系统安全性和隐私保护。。另外我们提出的比5G‑AKA协议要快得多，原因是选择轻量级的操作来使相互之间**

**验证**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **表III。** | **C通讯方式 Ø佛黑德** | | | | | |  |
|  | **AKA协议** |  | **通讯开销** | | | |  |  |
|  |  |  |  |
|  | **每股收益** |  |  | **276 + 1088n** | | |  |  |
|  |  |  |  |  |  |  |  |  |
|  | **5G‑AKA** |  |  | **2787 + 2147n** | | |  |  |
|  | **建议的** |  |  | **2240 + 1024n** | | |  |  |
|  |  | |  |  |  |  |  |  |
| **表IV。** | **C运用 Ø佛得角 小号单人 ØPERATION** | | | | | | |  |
|  | **运作方式** |  |  | **时间（我们）** |  |  |  |  |
|  |  |  |  |  |
|  | **ECDH** |  |  | **1290** |  |  |  |  |
|  | **ECIES / EN** |  |  | **2580** |  |  |  |  |
|  | **ECIES / DE** |  |  | **1750** |  |  |  |  |
|  | **哈希（SHA‑256）** |  |  | **3.8** |  |  |  |  |
|  | **HMAC SHA256** |  |  | **67** |  |  |  |  |
|  | **AES‑CTR** |  |  | **0.47** |  |  |  |  |

1. **C列入**

**在本文中，我们提出了一种改进**

**基于5G网络的隐私保护的身份验证和密钥协商协议。我们协议的主要目标是克服5G‑AKA标准协议中存在的各种弱点。使用AVISPA工具进行的正式验证表明，该解决方案可以满足总体安全要求，并且可以抵御多种攻击。此外，我们从通信开销和计算延迟方面评估了EPS‑AKA，5G‑AKA和我们的建议的性能，结果表明我们的协议在性能上优于其他协议。**

**[R参会**

1. **M. Ouaissa，M。Ouaissa和A. Rhattoy，“针对物联网系统的LTE移动网络的高效且安全的身份验证和密钥协议，”《国际智能工程与系统杂志》（IJIES），第1卷。12号 2019年4月，第212‑222页。**
2. **M. Ouaissa，A。Rhattoy和M. Lahmer，“控制长期演进系统中机对机应用拥塞的新方法，”国际通信天线与传播杂志（I.Re.CAP），第一卷。8号 2018年4月，第355‑363页。**
3. **N. Panwar，S。Sharma和AK Singh，“关于5G的调查：下一代移动**

**通信”，《物理通信》，第1卷。**

**2016年第18页，第64‑84页。**

1. **M. Ouaissa和A. Rhattoy，“一种用于LTE网络上的机 类型通信的基于组的AKA的新方案，” Int J Electric Comput Eng（IJECE），第1卷。8号 2018年2月，第1169–1181页。**
2. **X. Zhang，A。Kunz和S. Schroder，“ 3GPP中的5G安全概述”，IEEE通信和网络标准会议（CSCN），第181‑186页，2017年。**
3. **A. Gupta和RK Jha，“ 5G网络调查：架构和新兴技术”，IEEE Access，第1卷。2015年3月，第1206‑1232页。**
4. **M. Ouaissa，A。Rhattoy和I. Chana，“ LTE移动网络上IoT的身份验证和密钥协议协议的新安全级别”，第六届无线网络和移动通信国际会议（WINCOM），第1页– 2018年6月。**

**[8]第三代合作伙伴计划（3GPP）TR 33.899 V1.3.0“研究下一代系统的安全性。草案”，8月。**

**2017。**

**[9]第三代合作伙伴计划（3GPP）TS 33.501，“技术规范组服务和系统方面；5G系统的安全架构和程序”，V.16.2.0，2020年3月。**

1. **M. Dehnel‑Wild和C.Cremers，“ 5G‑AKA草案中的安全漏洞”，2018年2月**

**142**

**授权使用仅限于：哥德堡大学。从IEEE Xplore在2020年12月18日世界标准时间19:07:11下载。有限制条件。**

**[11] V. GayosoMartínez，L。HernándezEncinas和A. Queiruga**

**Dios，“在实现椭圆曲线集成加密方案时的安全性和实际考虑”，**

**Cryptologia，第一卷。39，没有3，**

**2015年，第244‑269页。**

* 1. **AP Fournaris，I。Zafeirakis，C。Koulamas，N。Sklavos和O. Koufopavlou，“为嵌入式系统设计有效的椭圆曲线Diffie‑Hellman**

**加速 ”，IEEE国际电路与系统专题讨论会（ISCAS），pp。2025‑2028年，2015年。**

* 1. **AVISPA项目：http：//www.avispa‑project.org/**
  2. **Crypto ++库：http：//www.cryptopp.com/**

1. **S. Heron，“高级加密标准（AES）”，《网络安全》，否。2009年12月，第8‑12页。**

**143**

**授权使用仅限于：哥德堡大学。从IEEE Xplore在2020年12月18日世界标准时间19:07:11下载。有限制条件。**