(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110213257 A
(43)申请公布日 2019.09.06

(21)申请号 201910452106.8

(22)申请日 2019.05.28

(71)申请人 中国电子科技集团公司第三十研究所
地址 610000 四川省成都市高新区创业路6号

(72)发明人 李大双 徐兵杰 何远杭 田波

(74)专利代理机构 成都九鼎天元知识产权代理有限公司 51214
代理人 邓世燕

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/08(2006.01)
H04L 9/06(2006.01)

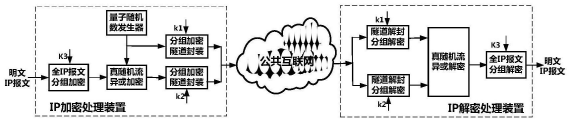
权利要求书1页 说明书4页 附图1页

(54)发明名称

基于真随机流异或加密的高安全IP保密通信方法

(57)摘要

本发明公开了一种基于真随机流异或加密的高安全IP保密通信方法，包括IP加密处理装置和IP解密处理装置，其中：所述IP加密处理装置包括全IP格式隐藏加密模块、量子随机数发生器模块、真随机流异或加密模块和两个分组加密隧道封装模块；所述IP解密处理装置包括两个隧道解封分组解密模块、真随机流异或解密模块和全IP格式隐藏解密模块。本发明能够在公共互联网上以低成本代价建立高安全的保密通信IP网络，能够抵御现有的各种密码分析破译技术的攻击威胁，并且能够非常有效地对抗具有强大运算能力的量子计算机的破译分析攻击，既可用于具有极高安全需求的党政军机密通信，也可用于具有较高安全需求的商用保密通信。



CN 110213257 A

1.一种基于真随机流异或加密的高安全IP保密通信方法,其特征在于:包括IP加密处理装置和IP解密处理装置,其中:所述IP加密处理装置包括全IP格式隐藏加密模块、量子随机数发生器模块、真随机流异或加密模块和两个分组加密隧道封装模块,量子随机数发生器模块分别和真随机流异或加密模块及一个分组加密隧道封装模块连接,全IP格式隐藏加密模块、真随机流异或加密模块和另一个分组加密隧道封装模块依次连接;所述IP解密处理装置包括两个隧道解封分组解密模块、真随机流异或解密模块和全IP格式隐藏解密模块,两个隧道解封分组解密模块均和真随机流异或解密模块连接,真随机流异或解密模块和全IP格式隐藏解密模块连接。

2.根据权利要求1所述的基于真随机流异或加密的高安全IP保密通信方法,其特征在于:对于每个明文IP报文,分别实施全IP格式隐藏加密、真随机化异或加密、分组加密三重传输保护机制:首先,以分组加密算法对需要传输的整个明文IP报文实施分组加密,形成一个与明文IP报文等长的密态掩盖数据块;其次,基于量子真随机数将密态掩盖数据块以与明文IP报文等长的量子真随机数据块进行逐字节的异或加密运算,形成一个真随机化数据块,并将量子真随机数据块作为另一个真随机化数据块;随后,分别基于为链路传输加密独立协商的两个不同的加密密钥,采用分组加密算法对这两个真随机化数据块进行分组加密,形成两个分组加密数据块。

3.根据权利要求2所述的基于真随机流异或加密的高安全IP保密通信方法,其特征在于:所述IP加密处理装置对一个明文IP报文执行IP加密时,采取以下处理步骤:

第一步、基于分组加密密钥k3,对包括IP头在内的整个明文IP报文进行隐藏格式的分组加密,形成一个与明文IP报文长度相同的密态掩盖数据块;

第二步、以量子随机数发生器实时产生的与明文IP报文长度相同的量子真随机数据块作为链路传输分组加密输入的一个真随机化数据块;同时以量子真随机数据块逐字节对密态掩盖数据块进行异或加密运算,形成链路传输分组加密输入的另一个真随机化数据块;

第三步、分别基于分组加密密钥k1、k2,对真随机化数据块实施分组加密形成链路传输的IP报文的密文载荷数据,重新加封标准的IP协议头,形成两个IP密态报文,其中,将使用k1加密的IP密态报文序号值域设置为递增的奇序号值,将使用k2加密的IP密态报文序号值域设置为递增的偶序号值,并且这两个IP密态报文序号的差值为1;然后,将这两个IP密态报文发送到公共互联网中,通过路由中继转发传输到目的IP密码机。

4.根据权利要求1所述的基于真随机流异或加密的高安全IP保密通信方法,其特征在于:所述IP解密处理装置在接收到IP密态报文时,采取以下步骤:

第一步、剥离掉隧道传输封装的IP头;

第二步、对于奇序号对应的IP密态报文,基于密钥k1对其密文载荷实施分组解密运算,获得链路传输分组解密输出的一个真随机化数据块;对于偶序号对应的IP密态报文,基于密钥k2对其密文载荷实施分组解密运算,获得链路传输分组解密输出的另一个真随机化数据块;

第三步、对两个奇偶序号已收齐的链路传输真随机化数据块执行逐字节的逻辑“异或”解密运算,恢复出全IP分组加密数据块;

第四步、基于密钥k3,对由异或解密运算获得的全IP分组加密数据块进行分组解密运算,恢复出明文IP报文。

基于真随机流异或加密的高安全IP保密通信方法

技术领域

[0001] 本发明涉及一种基于真随机流异或加密的高安全IP保密通信方法。

背景技术

[0002] 目前,量子计算技术发展迅速,将为密码分析破译技术提供了一种新的指数加速运算途径。量子计算与密码分析技术的结合使用将对现有保密通信系统形成严重的安全挑战。

[0003] 在现有的公共互联网中,各种网络设备总是存在一些安全漏洞,容易被敌手通过网络攻击手段植入监听木马,很容易获取IP子网之间的通信数据。而且即使IP子网之间基于专用的光缆直接连接,光纤中传输的光信号也容易被监听,通过信号解码恢复出IP报文数据。

[0004] 在现有的IP保密通信网络中,IP加密采用人工预置的或由密钥分发协议动态分配的加密密钥,在下一次密钥更换之前使用的是同一个固定不变的加密密钥,高速保密通信系统在此期间将产生大量的相同密钥的明-密文对,并且在一次加密运算过程中加密算法的输入数据也是固定不变的,在密钥和输入的明文数据都相同的情况下,加密所产生的密文是相同的,从而给予敌手利用明-密文对照的密码分析技术实施破译的机会。

发明内容

[0005] 为了克服现有技术的上述缺点,本发明提出了一种基于真随机流异或加密的高安全IP保密通信方法,将真随机流异或加密机制嵌入到IP报文的加密过程中,使保密通信系统的加密算法的输入真随机化,使其加密输出的密文流也呈现出真随机化的特性,将极大地提升现有保密通信系统的安全性,能够非常有效地对抗基于量子计算强大算力的密码分析破译攻击。

[0006] 本发明解决其技术问题所采用的技术方案是:一种基于真随机流异或加密的高安全IP保密通信方法,包括IP加密处理装置和IP解密处理装置,其中:所述IP加密处理装置包括全IP格式隐藏加密模块、量子随机数发生器模块、真随机流异或加密模块和两个分组加密隧道封装模块,量子随机数发生器模块分别和真随机流异或加密模块及一个分组加密隧道封装模块连接,全IP格式隐藏加密模块、真随机流异或加密模块和另一个分组加密隧道封装模块依次连接;所述IP解密处理装置包括两个隧道解封分组解密模块、真随机流异或解密模块和全IP格式隐藏解密模块,两个隧道解封分组解密模块均和真随机流异或解密模块连接,真随机流异或解密模块和全IP格式隐藏解密模块连接。

[0007] 与现有技术相比,本发明的积极效果是:

[0008] 在现有的公共互联网中,各种网络设备总是存在一些安全漏洞,容易被敌手通过网络攻击手段植入监听木马,很容易获取IP子网之间的通信数据。

[0009] 本发明设计的基于真随机流异或加密的高安全IP保密通信方法,采取全IP格式隐藏加密、量子真随机流异或加密以及链路传输分组加密三种通信保护机制,即使IP加密处

理装置的输入为连续相同的明文IP报文，其输出的IP密态报文的密文载荷也会呈现出真随机变化的特性，使得敌手很难通过监听通信数据内容分析破译获得IP明文内容。

[0010] 本发明设计的基于真随机流异或的高安全IP保密通信方法，能够在公共互联网上以较低的成本代价建立高安全的IP保密通信网络，能够抵御现有的各种密码分析破译技术的攻击威胁，并且能够非常有效地对抗具有强大运算能力的量子计算机的破译分析攻击，既可用于具有极高安全需求的党政军机密通信，也可用于具有较高安全需求的商用保密通信。

附图说明

[0011] 本发明将通过例子并参照附图的方式说明，其中：

[0012] 图1为本发明方法的实现架构。

[0013] 图2为IP加密隧道传输报文格式。

具体实施方式

[0014] 本发明涉及以下几个专用术语：

[0015] 密态掩盖数据块：整个明文IP报文(包括IP头在内)执行分组加密后，形成的与明文IP报文等长的数据块。

[0016] 真随机化数据块：以量子真随机数进行异或加密运算后，形成的数据块。

[0017] 密文载荷数据：将真随机化数据块按奇偶字节进行分割后形成的数据，通过封装标准的IP协议头，则形成IP密态报文。

[0018] 本发明提出了一种联合采取隐藏IP报文数据格式的分组加密、真随机流异或加密以及链路传输分组加密三重保护机制的高安全保密通信方法。这种高安全的IP保密通信方法，以真随机流异或加密技术为核心，并以全IP格式隐藏加密和链路传输分组加密来增强真随机流异或加密机制的安全完备性。首先，以分组加密算法对需要传输的整个明文IP报文(包括IP头在内)实施分组加密，形成一个与明文IP报文等长的密态掩盖数据块；其次，基于量子真随机数将密态掩盖数据块以与明文IP报文等长的量子真随机数据块进行逐字节的异或加密运算，形成一个真随机化数据块，并将量子真随机数据块作为另一个真随机化数据块；随后，分别基于为链路传输加密独立协商的两个不同的加密密钥，采用分组加密算法对这两个真随机化数据块进行分组加密，形成两个分组加密数据块；最后，分别将这两个分组加密数据块封装为标准的IPSec报文(即IP密态报文)，经由公共互联网传输到目的地IP密码设备。

[0019] 采用本发明提出的这种基于真随机流异或加密的高安全的IP保密通信方法，由于传输链路的两路分组加密算法的输入都为真随机的数据流，使得传输链路的分组加密输出也都成为真随机化的密文流，已有的所有密码分析攻击方法都无法奏效。即使保密通信系统采用公开的分组密码算法，也能够迫使敌手必须进行遍历三重密钥空间的穷举运算，因此敌手进行密码分析解密的运算量至少超过分组密钥空间的上限，其密码分析解密运算需要的计算时间量和存储空间量在工程实现上都是不可行的。

[0020] 因而本发明的方法具有对抗敌手运用网络监听和量子计算等强大算力实施破译分析攻击的能力。采取本发明提供的技术，能够基于公共互联网建立高安全的保密通信网

络。

[0021] 以下结合附图对本发明方法详细说明如下：

[0022] (一)基于真随机流异或加密的高安全IP保密通信方法的技术框架

[0023] 本发明提出基于真随机流异或加密的高安全IP保密通信方法，其设计理念是以IP报文内容真随机异或加密传输技术为核心，并以全IP格式隐藏加密和链路传输分组加密来增强其真随机流异或加密技术的安全完备性。对于每个明文IP报文，分别实施了隐藏IP明文格式的全IP格式隐藏加密、密态掩盖数据块的真随机化异或加密、真随机化数据块的分组加密三重传输保护机制。

[0024] 本发明不涉及IP加密机之间的动态密钥协商、IP密码机之间的IPSec报文封装的具体实现。

[0025] 1、基于真随机流异或加密的高安全IP保密通信方法的实现架构设计

[0026] 本发明提出的基于真随机流异或加密的高安全IP保密通信方法中，其保密通信实现架构设计如图1所示。IP加密处理功能主要由全IP格式隐藏加密模块、量子随机数发生器模块、真随机流异或加密模块、两个分组加密隧道封装模块共5个模块组成。IP解密处理主要由两个隧道解封分组解密模块、真随机流异或解密模块、全IP格式隐藏解密模块共4个模块组成。

[0027] 我们提出的这种基于真随机流异或加密的高安全IP保密通信方法中，IP加密设备针对要传输的每个明文IP分组，首先对包括IP头在内的整个报文采用全IP格式隐藏加密，基于实时产生的量子真随机数进行逐字节的异或加密，形成一个与原IP报文长度相同的真随机化数据块，用于异或加密的量子真随机数据块作为另一个真随机化数据块，这两个真随机化数据块经过分组加密算法加密后，重新封装为两个新的IP密态报文，然后从互联网接入链路上传送出去，经由互联网传输到接收的IP解密设备，去掉它们的封装后，通过异或解密运算与全IP格式隐藏解密运算，恢复出明文IP报文。

[0028] 链路传输加密使用的分组加密密钥(k1、k2)和全IP格式隐藏加密使用的密钥(k3)由动态密钥分发协议协商产生，这三个密钥彼此不相关，要求不能通过彼此派生推算获得。

[0029] 2、加密输入真随机化与分组加密结合极大地提高了抗密码分析破译的能力

[0030] 本发明提出的基于真随机流异或加密的高安全IP保密通信方法，其核心思想是将链路传输分组加密算法的输入内容通过真随机流异或加密运算达到真随机化，并且使链路传输分组加密产生的密文流也真随机化，以此来对抗已有的各种密码分析破译方法。真随机化异或加密机制将要经过公共互联网传输的IP报文内容，基于实时动态产生的与IP报文长度相同的量子真随机数，逐字节进行真随机化异或加密运算，获得一个内容完全随机化的随机化数据块，经过分组算法加密后，重新封装为一个IP密态报文。同时，将用于真随机化异或加密的与IP报文长度相同的量子真随机数据，经过分组算法加密后，封装为另一个IP密态报文。这两个IP密态报文的IP序号以递增的方式产生，且差值为1。由于链路传输分组加密算法的输入与输出都是真随机化数据流，不再具有任何可以被密码分析技术利用的特征，所以，这种方法能够对抗现有的那些采取明-密文对比分析、神经网络深度学习特征分析的所有密码分析破译方法。

[0031] 3、格式隐藏加密提升了敌手穷举破译运算量的下限

[0032] 在本发明提出的基于真随机流异或加密的高安全保密通信方法中，在执行真随机

化异或加密IP报文之前，对整个IP报文(包括IP头在内)采取了格式隐藏加密保护，使得敌手对两个奇偶序号关联的IP分组加密报文联合实施穷举解密的异或运算破译时，在其输出数据中找不到任何明文特征，迫使敌手对分组解密的穷举运算量将超过遍历单个密钥空间的解密运算上限。即使在算法公开的情况下，敌手若要破解整个密码系统，必须首先针对每一种链路传输分组加密密钥组合(k1,k2)实施分组解密运算，然后再进行IP格式隐藏解密的穷举运算。最后，即使敌手在两个密钥空间执行完一遍分组算法的穷举运算，因为针对每一对分组密钥组合的“解密”运算结果的异或解密输出都为密态掩盖数据，也无法破译出明文IP报文，还必须进行针对IP格式隐藏加密算法的密码分析破译运算。这种必须在三重密钥空间联合进行组合解密的破译运算，所需要的存储空间量在工程上也是根本无法实现的。

[0033] (二)工作流程

[0034] 1、IP加密处理工作流程

[0035] 当IP加密处理装置对一个明文IP报文执行IP加密时，采取以下处理步骤：

[0036] 第一步、基于密钥分发协议协商的分组加密密钥k3，对包括IP头在内的整个明文IP报文进行隐藏格式的分组加密，形成一个与明文IP报文长度相同的密态掩盖数据块；

[0037] 第二步、从量子随机数发生器获取实时产生的与明文IP报文长度相同的量子真随机数据块；

[0038] 第三步、以量子真随机数据块逐字节对密态掩盖数据块进行异或加密运算，形成一个真随机化数据块，作为链路传输分组加密输入的一个真随机化数据块，同时将量子真随机数据块作为链路传输分组加密输入的另一个真随机化数据块；

[0039] 第四步、分别基于分组加密密钥k1、k2，对真随机化数据块实施分组加密形成链路传输的IP报文的密文载荷数据，重新加封标准的IP协议头，形成两个IP密态报文。其中，将使用k1加密的IP密态报文序号值域设置为递增的奇序号值，将使用k2加密的IP密态报文序号值域设置为递增的偶序号值，并且这两个IP密态报文序号的差值为1。然后，将这两个IP密态报文发送到公共互联网中，通过路由中继转发传输到目的IP密码机。图2为IP加密隧道传输报文格式。

[0040] 至此，IP密码加密装置就完成了对明文IP报文的加密处理流程。

[0041] 2、IP解密处理工作流程

[0042] 当地IP解密处理装置接收到IP密态报文时，采取以下步骤：

[0043] 第一步、剥离掉隧道传输封装的IP头；

[0044] 第二步、对于奇序号对应的IP密态报文，基于密钥k1对其密文载荷实施分组解密运算，获得链路传输分组解密输出的一个真随机化数据块。对于偶序号对应的IP密态报文，基于密钥k2对其密文载荷实施分组解密运算，获得链路传输分组解密输出的另一个真随机化数据块；

[0045] 第三步：对两个奇偶序号已收齐(即序号关联的且差值为1)的链路传输真随机化数据块执行逐字节的逻辑“异或”解密运算，恢复出全IP分组加密数据块；

[0046] 第四步：基于密钥k3，对由异或解密运算获得的全IP分组加密数据块进行分组解密运算，恢复出明文IP报文。

[0047] 至此，IP解密处理装置就完成了对IP密态报文的解密处理流程。

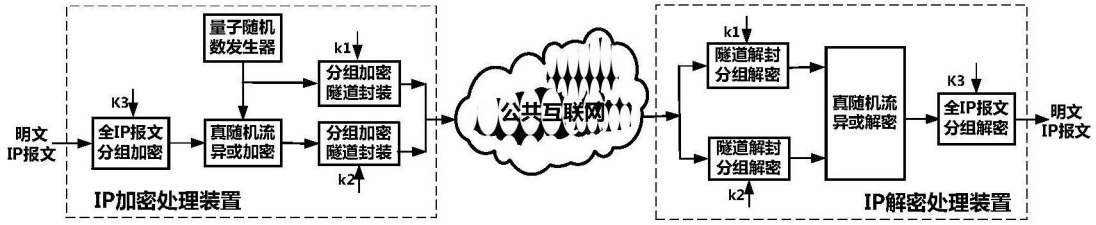

量子随机
数发生器
k1
分组加密
隧道封装
K3
明文
IP报文
全IP报文
分组加密
真随机流
异或加密
分组加密
隧道封装
k2
IP加密处理装置
公共互联网
k1
隧道解封
分组解密
真随机流
异或解密
K3
全IP报文
分组解密
明文
IP报文
隧道解封
分组解密
k2
IP解密处理装置

图1

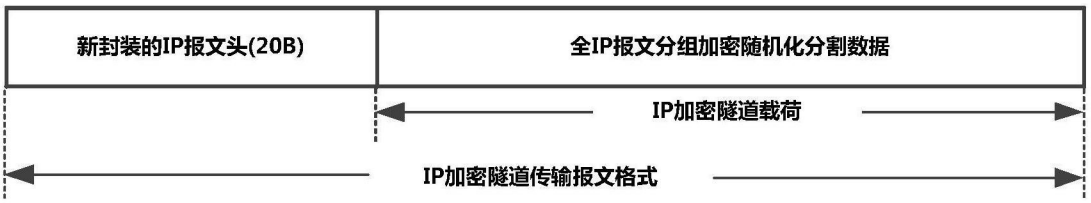

新封装的IP报文头(20B)
全IP报文分组加密随机化分割数据
IP加密隧道载荷
IP加密隧道传输报文格式

图2