ICS 33.040.40
CCS M32

YD

中 华 人 民 共 和 国 通 信 行 业 标 准

YD/T 4303—2023

基于 IPSec 协议的量子保密通信应用设备技术规范

Technical specification of quantum secure communication application equipment based on IPSec protocol

2023-04-21 发布　　2023-08-01 实施

中华人民共和国工业和信息化部　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中国信息通信研究院、南京易科腾信息技术有限公司、科大国盾量子技术股份有限公司、国科量子通信网络有限公司、安徽问天量子科技股份有限公司、中国电子科技网络信息安全有限公司、数据通信科学技术研究所、华为技术有限公司、中移系统集成有限公司、信通数智量子科技有限公司、浙江九州量子信息技术股份有限公司。

本文件主要起草人：赖俊森、林晨、王敬、晏志文、黄强、马彰超、陈传亮、徐兵杰、党金哲、潘伟、王昀、高有军、魏瑛、丁胜建。

基于 IPSec 协议的量子保密通信应用设备技术规范

1 范围

本文件规定了基于 IPSec 协议的量子保密通信应用网关设备和终端设备的技术协议、功能性能要求及相关测试方法。

本文件适用于基于 IPSec 协议的量子保密通信应用网关设备和终端设备的研制、检测、使用和管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 15843.2 信息技术安全技术实体鉴别第 2 部分：采用对称加密算法的机制

GB/T 16262.1 信息技术抽象语法记法-（ASN.1）第 1 部分：基本记法规范

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32915 信息安全技术二元序列随机性检测方法

GB/T 32918（所有部分）信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 32922 信息安全技术 IPSec VPN 安全接入基本要求与实施指南

GB/T 36968—2018 信息安全技术 IPSec VPN 技术规范

GM/T 0028—2014 密码模块安全技术要求

GM/T 0062—2018 密码产品随机数检测要求

YD/T 1466—2006 IP 安全协议（IPSec）技术要求

YD/T 3834（所有部分）量子密钥分发（QKD）系统技术要求

IETF RFC8784 在互联网密钥交换协议第 2 版（IKEv2）中混合预共享密钥以实现后量子安全（Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security）

3 术语和定义

GB/T 36968—2018 界定的以及下列术语和定义适用于本文件。

3.1

量子密钥分发　quantum key distribution

通信双方通过传送量子态的方法实现对称密钥生成，在理论协议层面具备信息论安全性，简称为QKD，也称量子密钥分配。

3.2

量子密钥　quantum key

通信双方基于QKD协议直接生成的对称密钥，在理论协议层面可被证明具备信息论安全性。

3.3

量子保密通信　quantum secure communication

基于量子通信，利用量子不可分割、量子态不可克隆和量子纠缠等特性保护秘密消息，进而保证信息传输安全的通信方法。

注1：秘密消息包括密钥、口令、敏感信息等任何需要保护其机密性、完整性的信息或数据。

注2：结合量子密钥分发和对称密码技术的加密通信是一种典型的量子保密通信实现方案。

3.4

IPSec协议　internet protocol security

一种开放标准的框架结构，通过使用加密的安全服务以确保在公开网络上进行保密而安全的通信，可以端到端的层面上提供数据完整性保护、数据源鉴别、载荷机密性和抗重放攻击等安全服务。

3.5

量子加密服务密钥　quantum encryption service key

基于QKD系统生成的量子密钥，通过QKD网络中继转发或终端密钥协商服务等方式生成，为基于IPSec协议的量子保密通信应用设备提供的端到端密钥。直接使用QKD系统为基于IPSec协议的量子保密通信应用设备提供密钥时，量子密钥即为量子加密服务密钥。

3.6

终端密钥协商服务　terminal key agreement service

用于支持在量子保密通信应用网关设备和终端设备之间获取量子加密服务密钥的服务。与网关设备之间基于QKD系统或QKD网络生成量子加密服务密钥，再使用终端充注密钥对量子加密服务密钥进行加密，实现终端设备对量子加密服务密钥的获取。

3.7

终端充注密钥　terminal charging key

通过密钥存储介质充注或在线更新，加载到终端设备中预存使用的密钥，可用于终端设备与终端密钥协商服务之间，获取量子加密服务密钥过程的加密。

3.8

终端密钥信封　terminal key envelope

在终端密钥协商服务中，使用终端充注密钥对量子加密服务密钥进行加密，产生终端密钥信封。其中包含加密后的量子加密服务密钥，以及加密所使用的终端充注密钥的索引和验证信息，用于在终端设备中，作为解密模块的输入参数，还原恢复出量子加密服务密钥。

3.9

量子加密服务协商　quantum encryption service agreement

在 IPSec 协议密钥交换协议中使用量子加密服务密钥时，交换服务模式、参数、密钥融合方式等信息的协商过程。

4　缩略语

下列缩略语适用于本文件。

AH	鉴别头	Authentication Header
CBC	密文分组链接	Cipher Block Chaining
DOI	解释域	Domain of Interpretation
ESP	封装安全载荷	Encapsulated Security Payload
IPSec	IP 安全协议	Internet Protocol Security
IPv4	互联网通信协议第四版	Internet Protocol version 4
IPv6	互联网通信协议第六版	Internet Protocol version 6
ISAKMP	互联网安全关联密钥管理协议	Internet Security Association and Key Management Protocol
MAC	消息认证码	Message Authentication Code
NAT	网络地址转换	Network Address Translation
QKD	量子密钥分发	Quantum Key Distribution
SA	安全联盟	Security Association
SPI	安全参数索引	Security Parameter Index
VPN	虚拟专用网络	Virtual Private Network

5　量子保密通信系统概述

量子保密通信系统的一种典型实现方案是使用量子加密服务密钥，与 IPSec 协议进行融合，为收发双方提供通信加密安全服务。生成量子密钥的 QKD 系统的技术要求见 YD/T 3834，IPSec 协议技术规范见 GB/T 36968，IPSec 协议框架结构、工作原理、实现方式和工作模式见 YD/T 1466—2006 第 4 章，IPSec VPN 安全接入的应用场景见 GB/T 32922。

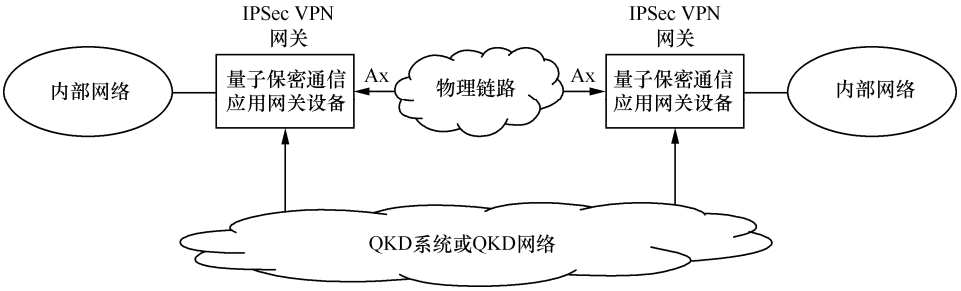

图 1　量子保密通信系统网关到网关应用模式

基于 IPSec 协议和 QKD 的量子保密通信系统，在网关到网关安全接入场景中的应用模式如图 1 所示。其中，量子保密通信应用网关设备，简称网关设备，宜与 QKD 系统或 QKD 网络直接通信，以在线方式获取量子加密服务密钥。

网关设备作为 IPSec VPN 网关，使用量子加密服务密钥，与 IPSec 密钥交换协议相结合，在用户网络之间的物理链路中，建立双向 SA，提供安全性增强的加密传输通道。网关设备之间的密钥交换与加密业务报文传输接口为 Ax。

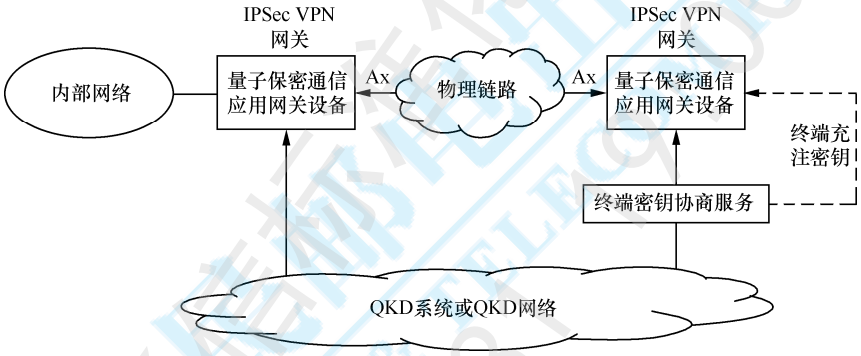

图 2　量子保密通信系统终端到网关应用模式

基于 IPSec 协议和 QKD 的量子保密通信系统，在终端到网关安全接入场景中的应用模式如图 2 所示。其中，量子保密通信应用终端设备，简称终端设备，与 QKD 系统或 QKD 网络通过终端密钥协商服务获取量子加密服务密钥。具体方式为，终端密钥协商服务与 QKD 系统或 QKD 网络直接通信，以在线方式获取量子加密服务密钥。终端设备通过加载密钥存储介质或在线更新获取终端充注密钥。终端密钥加密服务与终端设备在传输量子加密服务密钥时，通过终端充注密钥对量子加密服务密钥进行加密保护。

终端设备和网关设备之间，使用量子加密服务密钥，与 IPSec 密钥交换协议相结合，建立双向 SA，提供安全性增强的加密传输通道。终端设备和网关设备之间的密钥交换与加密业务报文传输接口为 Ax。

6　密码算法和密钥种类

6.1　密码算法

基于 IPSec 协议的量子保密通信应用网关设备和终端设备，应支持国家密码管理主管部门批准的非对称密码算法、对称密码算法、密码杂凑算法和随机数生成算法。各算法及使用要求如下。

——非对称密码算法应支持 SM2 椭圆曲线密码算法，用于身份鉴别、数字签名和数字信封等，SM2 算法的使用应符合 GB/T 32918 的要求。

——对称密码算法应支持 SM4 分组密码算法，用于密钥交换数据的加密保护和报文数据的加密保护。

——算法的工作模式应支持 CBC 模式，SM4 算法的使用应符合 GB/T 32907 的要求。

——密码杂凑算法应支持 SM3 密码杂凑算法，用于消息摘要生成和完整性校验。SM3 算法的使用应符合 GB/T 32905 的要求。

——随机数生成算法生成的随机数应能通过 GB/T 32915 规定的检测。

6.2 密钥种类

基于 IPSec 协议的量子保密通信应用网关设备和终端设备，在业务加密过程中使用下列密钥。

——设备密钥：可使用基于非对称密码算法的公私钥对，包括签名密钥对和加密密钥对，用于身份鉴别、数字签名和数字信封等。也可使用预置对称密钥，用于基于对称密钥的设备身份鉴别和密钥协商。

——工作密钥：在密钥交换一阶段得到的密钥，用于会话密钥交换过程的保护。

——会话密钥：在密钥交换二阶段得到的密钥，用于数据报文及报文 MAC 的加密。

——量子加密服务密钥：基于 QKD 系统生成的量子密钥，通过 QKD 网络中继转发或终端密钥协商服务等方式生成，为基于 IPSec 协议的量子保密通信应用设备提供的端到端密钥，用于在密钥交换协议中，辅助生成工作密钥和会话密钥，增强 IPSec 协议和保密通信的安全性。

——终端充注密钥：通过密钥存储介质充注或在线更新，加载到终端设备中预存使用的密钥，可用于终端设备与终端密钥协商服务之间，获取量子加密服务密钥过程的加密。

7 协议

7.1 量子加密服务密钥获取协议

7.1.1 协议交互流程

7.1.1.1 网关到网关

网关设备到网关设备应用模式中，量子加密服务密钥获取的协议交互流程如图 3 所示。

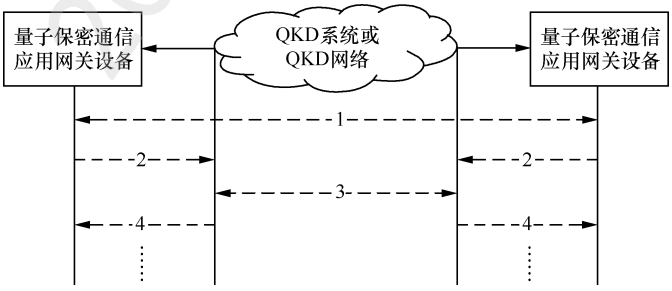

图 3 网关设备到网关设备的量子加密服务密钥获取协议交互流程

图 3 中协议交互步骤与实现功能如下。

——步骤 1：基于 IPSec 协议在通信双方的网关设备之间完成身份鉴别，基于量子加密服务协商消息，完成使用量子加密服务密钥的请求和响应，协议内容见 7.2 节。

——步骤 2：通信双方网关设备分别向 QKD 系统或 QKD 网络发送量子加密服务密钥请求。

——步骤 3：QKD 系统或 QKD 网络接收到量子加密服务密钥请求后，通过其内部协议处理，生成端到端的量子加密服务密钥。

——步骤 4：QKD 系统或 QKD 网络向通信双方网关设备分别发送量子加密服务密钥响应。

网关设备的量子加密服务密钥获取过程，采用请求—响应模式，请求者和响应者应首先完成身份鉴别，身份鉴别应符合 GB/T 15843.2 的规定，再通过协议交互流程和协议报文完成密钥获取。

步骤 2 至步骤 4 构成一个量子加密服务密钥请求—响应流程。量子加密服务密钥应按一定周期进行更新。当结束通信时，应通过会话销毁消息，释放密钥资源。

7.1.1.2 终端到网关

终端设备到网关设备应用模式中，量子加密服务密钥获取的协议交互流程如图 4 所示。

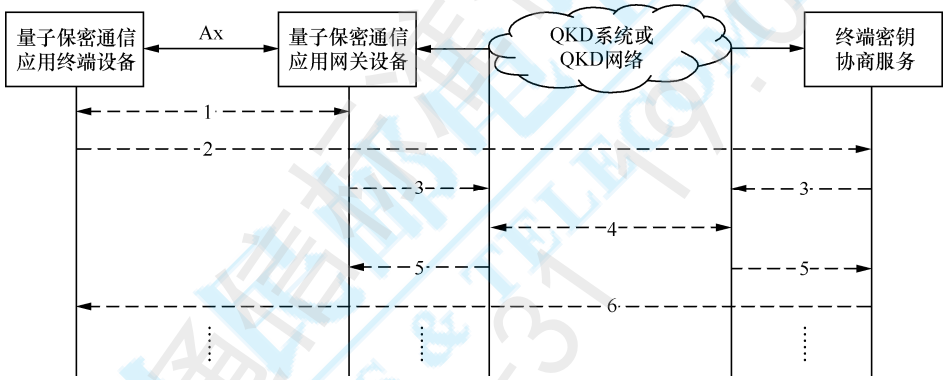

图 4 终端设备到网关设备的量子加密服务密钥获取协议交互流程

图 4 中协议交互步骤与实现功能如下。

——步骤 1：基于 IPSec 协议在通信双方的终端设备和网关设备之间完成身份鉴别，基于量子加密服务协商消息，完成使用量子加密服务密钥的请求和响应，协议内容见 7.2 节。

——步骤 2：终端设备和网关设备，向终端密钥协商服务发送使用终端密钥协商服务的请求。

——步骤 3：网关设备和终端密钥协商服务分别向 QKD 系统或 QKD 网络发送获取量子加密服务密钥的请求。

——步骤 4：QKD 系统或 QKD 网络通过其内部协议处理，生成端到端的量子加密服务密钥。

——步骤 5：QKD 系统或 QKD 网络向网关设备和终端密钥协商服务发送量子加密服务密钥的响应。

——步骤 6：终端密钥协商服务向终端设备发送终端密钥信封的响应。

网关设备和终端设备的量子加密服务密钥获取过程，采用请求—响应模式，请求者和响应者应首先完成身份鉴别，身份鉴别应符合 GB/T 15843.2 的规定，再通过协议交互流程和协议报文完成密钥获取。

步骤 3 至步骤 5 构成一个量子加密服务密钥请求—响应流程。量子加密服务密钥应按一定周期进行更新。当结束通信时，应通过会话销毁消息，释放密钥资源。

7.1.2 协议报文格式

网关设备和终端密钥协商服务从 QKD 系统或 QKD 网络中获取量子加密服务密钥。

量子加密服务密钥获取的具体协议与报文格式不在本文件中规范。

7.2 密钥交换协议

7.2.1 概述

本节在 GB/T 36968—2018 第 6.1 节密钥交换协议定义的协商、建立、修改、删除安全联盟的过程和报文格式基础上，增加使用量子加密服务密钥作为密钥参数，参与 SA 建立的过程和报文格式。

本章用到的符号如下。

HDR：一个 ISAKMP 头。

HDR*：表示 ISAKMP 头后面的载荷是加密的。

SA：带有一个或多个建议载荷的安全联盟载荷。

IDi：发起方的标识载荷。

IDr：响应方的标识载荷。

HASHi：发起方的杂凑载荷。

HASHr：响应方的杂凑载荷。

HASH_<n>：双方进行协商交互时的中间 Hash 数据。

SIGi：发起方的签名载荷。

SIGr：响应方的签名载荷。

XCHi：发起方的交换载荷。

XCHr：响应方的交换载荷。

CERT_sig_r：签名证书载荷。

CERT_enc_r：加密证书载荷。

Ni：发起方的 nonce 载荷。

Nr：响应方的 nonce 载荷。

<p>_b：载荷<p>的主体，指没有 ISAKMP 通用头的载荷。

pub_i：发起方公钥。

pub_r：响应方公钥。

prv_i：发起方私钥。

prv_r：响应方私钥。

CKY-I：ISAKMP 头中的发起方 cookie。

CKY-R：ISAKMP 头中的响应方 cookie。

x | y：x 与 y 串接。

[x]：x 为可选。

HASH（msg）：使用密码杂凑算法对 msg 进行数据摘要运算。

PRF（key，msg）：使用密钥 key 对消息 msg 进行数据摘要运算。

N()：通知载荷

USE_QKD：量子加密服务协商通知载荷

7.2.2 协议交互流程

7.2.2.1 第一阶段

IPSec 协议密钥交换协议第一阶段协商基本流程应按照 GB/T 36968—2018 第 6.1.3.2 节的要求执行。

在第一阶段交互流程中，增加量子加密服务协商通知载荷，使得通信双方能够实现量子加密服务的协商，量子加密服务密钥属性的交换，以及量子加密服务密钥获取结果的通知。

量子加密服务协商通知载荷分别添加在第一阶段交换过程中消息 1、消息 2 和消息 3 的载荷之后，第一阶段交互过程如下。

消息序列	发起方 i	方向	响应方 R
1	HDR, SA, N(USE_QKDi)	————>	
2		<————	HDR, SA,CERT_sig_r,CERT_enc_r, N(USE_QKDr)
3	HDR, XCHi, SIGi, N(USE_QKDs)	————>	
4		<————	HDR, XCHr, SIGr
5	HDR*, HASHi	————>	
6		<————	HDR*, HASHr

消息 1 中的 USE_QKDi 通知载荷用于使用量子加密服务的协商请求：

USE_QKDi =Usage[|Mode|Vendor|Version]

当发起端支持多个 QKD 厂家的接口时，USE_QKDi 可以重复发送多个。

消息 2 中的 USE_QKDr 通知载荷用于使用量子加密服务的协商应答和响应方量子加密服务密钥属性的交换、以及量子加密服务密钥获取结果的通知：

USE_QKDr = Usage[|Mode|Vendor|Version|Config|KeyID|KeyLen|Envelope]|Status

消息 3 中的 USE_QKDs 通知载荷用于请求方量子加密服务密钥获取结果的通知：

USE_QKDs = Status

消息 3 和消息 4 交互完成后，参与通信的双方生成基本密钥参数 SKEYID，以生成后续密钥 SKEYID_d、SKEYID_a、SKEYID_e，计算方法分别如下：

SKEYID = PRF(HASH(Ni_b | Nr_b), CKY-I | CKY-R)

SKEYID_d = PRF(SKEYID, CKY-I | CKY-R | 0)

SKEYID_a = PRF(SKEYID, SKEYID_d | CKY-I | CKY-R | 1)

SKEYID_e = PRF(SKEYID, SKEYID_a | CKY-I | CKY-R | 2)

上述计算公式中的值 0，1，2 是单个字节的数值。

SKEYID_e 是 ISAKMP SA 用来保护其消息机密性所使用的工作密钥。SKEYID_a 是 ISAKMP SA 用来验证其消息完整性以及数据源身份所使用的工作密钥。SKEYID_d 用于会话密钥的产生。

所有 SKEYID 的长度都由 PRF 函数的输出长度决定。如果 PRF 函数的输出长度太短，不能作为一个密钥来使用，则 SKEYID_e 应进行扩展。例如，HMAC 的一个 PRF 可产生 128 比特的输出，但密码

算法要求用到大于 128 比特的密钥的时候，SKEYID_e 就需要利用反馈及连接方法加以扩展，直到满足对密钥长度的要求为止。反馈及连接方法如下：

K = K1 | K2 | K3…

K1 = PRF(SKEYID_e, 0)

K2 = PRF(SKEYID_e, K1)

K3 = PRF(SKEYID_e, K2)

…

最后从 K 的起始位置开始取密码算法的密钥所需要的位数。

在量子加密服务协商成功时，在第一阶段协商生成原始工作密钥 SKEYID_d、SKEYID_a、SKEYID_e 后，使用量子加密服务密钥 QK，与原始工作密钥进行融合，可选实现方案如下。

方案一：使用量子加密服务密钥 QK 作为密钥参数，对原始工作密钥进行数据摘要运算，生成量子融合工作密钥。基于密钥参数混合方式，增强 IPSec 协议安全性的原理与实现方法见 IETF RFC8784。具体计算方式如下：

QSKEYID_d = prf+(QK_d, SKEYID_d)

QSKEYID_a = prf+(QK_a, SKEYID_a)

QSKEYID_e = prf+(QK_e, SKEYID_e)

上述计算公式中的 prf+定义为：

prf+(K,S) = T1 | T2 | T3 | T4 | ...

T1 = prf (K, S | 0x01)

T2 = prf (K, T1 | S | 0x02)

T3 = prf (K, T2 | S | 0x03)

T4 = prf (K, T3 | S | 0x04)

...

持续计算到直到所有需要密钥材料长度足够为止。QK_d，QK_a 和 QK_e 分别为不同的量子加密服务密钥。

方案二：使用量子加密服务密钥 QK 对原始工作密钥进行异或运算，生成量子融合工作密钥。具体计算方式如下：

QSKEYID_d = QK_d⊕SKEYID_d

QSKEYID_a = QK_a⊕SKEYID_a

QSKEYID_e = QK_e⊕SKEYID_e

其中，x⊕y 表示 x 与 y 进行异或。QK_d，QK_a 和 QK_e 分别为不同的量子加密服务密钥。QK_d 与 SKEYID_d 长度相同，QK_a 与 SKEYID_a 长度相同，QK_e 与 SKEYID_e 长度相同。

在量子加密服务协商成功时，基于上述方案生成 QSKEYID_d、QSKEYID_a 和 QSKEYID_e，并使用 QSKEYID_d 替代 IPSec 协议原有的 SKEYID_d 作为会话密钥的派生密钥，使用 QSKEYID_a 替代 SKEYID_a 作为工作密钥的认证密钥，使用 QSKEYID_e 替代 SKEYID_e 作为工作密钥的加密密钥。

当量子加密服务协商失败时，如果量子加密服务密钥使用模式为强制，则 IPSec 密钥协商失败，如果量子加密服务密钥使用模式为优选，则使用原始工作密钥作为工作密钥。

7.2.2.2 第二阶段

IPSec 协议密钥交换协议第二阶段协商基本流程应按照 GB/T 36968—2018 第 6.1.3.3 节的要求执行。

在第二阶段交互流程中，增加量子加密服务协商通知载荷，使得通信双方能够实现量子加密服务密钥属性的交换、以及量子加密服务密钥获取结果的通知。

量子加密服务协商通知载荷分别添加在第一阶段交换过程中消息 1、消息 2 和消息 3 的载荷之后，第二阶段交互过程如下：

消息序列	发起方	方向	响应方
1	HDR*, HASH_1, SA, Ni [, IDci, IDcr], N(USE_QKDi)	————>	
2		<————	HDR*, HASH_2, SA, Nr [, IDci, IDcr], N(USE_QKDr)
3	HDR*, HASH_3, N(USE_QKDs)	————>	

消息 1 中的 USE_QKDi 通知载荷用于量子加密服务协商的请求：

USE_QKDi = Usage[|Mode|Vendor|Version]

当发起端支持多个 QKD 厂家的接口时，USE_QKDi 可以重复发送多个。

消息 2 中的 USE_QKDr 通知载荷用于量子加密服务协商的应答，以及响应端量子加密服务密钥属性的交换、以及量子加密服务密钥获取结果的通知：

USE_QKDr =Usage[|Vendor|Version|Mode|Config|KeyID|KeyLen|Envelope]|Status

消息 3 中的 USE_QKDs 通知载荷用于量子加密服务协商请求端量子加密服务密钥获取结果的通知：

USE_QKDs = Status

会话密钥素材定义为：

KEYMAT = PRF(SKEYID_d, protocol | SPI | Ni_b | Nr_b)

其中，protocol 和 SPI 是从协商得到的 ISAKMP 建议载荷中选取。

用于加密的会话密钥和用于完整性校验的会话密钥按照算法要求的长度从 KEYMAT 中依次选取。先选取用于加密的会话密钥，后选取用于完整性校验的会话密钥。

当 PRF 函数的输出长度小于 KEYMAT 需要的密钥素材长度时，需要利用反馈及连接方法加以扩展，直到满足对密钥长度的要求为止。即：

KEYMAT = K1 | K2 | K3 | ...

其中：

K1 = PRF(SKEYID_d, protocol | SPI | Ni_b | Nr_b)

K2 = PRF(SKEYID_d, K1 | protocol | SPI | Ni_b | Nr_b)

K3 = PRF(SKEYID_d, K2 | protocol | SPI | Ni_b | Nr_b)

…

单个 SA 协商产生两个安全联盟，一个入，一个出。每个 SA（一个由发起方选择，另一个由响应方选择）的不同的 SPI 保证了每个方向都有一个不同的 KEYMAT。由 SA 的目的地选择的 SPI，被用于衍生该 SA 的 KEYMAT。

在量子加密服务协商成功时，使用多个量子加密服务密钥 QK1、QK2、QK3……QKn，与原始会话密钥进行融合，可选实现方案如下。

方案一：使用量子加密服务密钥 QK 作为密钥参数，对原始会话密钥进行数据摘要运算，生成量子融合会话密钥。基于密钥参数混合方式，增强 IPSec 协议安全性的原理与实现方法见 IETF RFC8784。具体计算方式如下：

QKEYMAT1 = prf+(QK1,KEYMAT)

QKEYMAT2 = prf+(QK2,KEYMAT)

QKEYMAT3 = prf+(QK3,KEYMAT)

……

QKEYMATn = prf+(QKn,KEYMAT)

prf+定义见 7.2.2.1 节。

方案二：使用量子加密服务密钥 QK 对原始会话密钥进行异或运算，生成量子融合会话密钥。具体计算方式如下：

QKEYMAT1 = QK1⊕KEYMAT

QKEYMAT2 = QK2⊕KEYMAT

QKEYMAT3 = QK3⊕KEYMAT

……

QKEYMATn = QKn⊕KEYMAT

其中，x⊕y 表示 x 与 y 进行异或。QK1，QK2，QK3，…，QKn 分别为不同的量子加密服务密钥，各自长度均与 KEYMAT 长度相同。

在量子加密服务协商成功时，基于上述方案生成 QKEYMAT，并使用 QKEYMAT 替代 IPSec 协议原有的 KEYMAT，用于协商产生 SA，每个 QKEYMAT 产生两个 SA，一个入，一个出，*n* 个 QKEYMAT 共产生 *n* 对 SA。

当量子加密服务协商失败时，如果量子加密服务密钥使用模式为强制，则 IPSec 密钥协商失败，如果量子加密服务密钥使用模式为优选，则使用原始会话密钥作为会话密钥。

7.2.3 协议报文格式

在 IPSec 协议中增加量子加密服务协商的报文，采用通知载荷，通知载荷的格式如图 5 所示。

<table>
<tr><td>下一个载荷</td><td>保留</td><td>载荷长度</td></tr>
<tr><td colspan="3">解释域（DOI）</td></tr>
<tr><td>协议 ID</td><td>SPI 长度</td><td>通知消息类型</td></tr>
<tr><td colspan="3">安全参数索引（SPI）</td></tr>
<tr><td colspan="3">通知数据</td></tr>
</table>

图 5 通知载荷格式

图 5 中各字段含义说明如下。

— 下一个载荷：这个字段的长度为 1 个字节，标识了本载荷后下一个载荷的类型。如果当前载荷是最后一个，则该字段将被置为 0。载荷类型定义见 GB/T 36968—2018 的表 1。
— 保留：这个字段的长度为 1 个字节，其值为 0。
— 载荷长度：这个字段的长度为 2 个字节，长度数值以字节为单位，用于表示包含通用载荷头在内的整个载荷长度。
— 解释域（DOI）：这个字段的长度为 4 个字节，这个字段的值为 1。
— 协议 ID：这个字段的长度为 1 个字节，用于表示协议标识符。协议标识符的定义见表 3。
— SPI 长度：这个字段的长度为 1 个字节，长度数值以字节为单位，用于表示 SPI 的长度。在第一阶段该长度为 0，在第二阶段该长度为 4。
— 通知消息类型：这个字段的长度为 2 个字节，用于表示通知消息类型。量子加密服务协商消息类型为 40959。
— 通知数据：这个字段是变长的，用于传送通知消息类型对应的通知数据。

量子加密服务协商有关的通知数据的协议采用抽象语法表示，描述记法要求应符合 GB/T 16262.1—2006 的规定，格式和内容如下：

```
USE_QKD::=SET{
    usage       Usage OPTIONAL,
    mode        Mode OPTIONAL,
    vendor      Vendor OPTIONAL,
    version     Version OPTIONAL,
    config      Config OPTIONAL,
    keyid       KeyID OPTIONAL,
    keylen      KeyLen OPTIONAL,
    envelope    Envelope OPTIONAL,
    status      Status OPTIONAL
}
其中
Usage::=SEQUENCE{
    type        INTERER(1),
    length      INTERER,
    mode        ENUMERATED{force(1), optimization(2)}
}
Mode::=SEQUENCE{
    type        INTERER(2),
    length      INTERER,
    mixMode     ENUMERATED{PRF(1), XOR(2)}
}
Vendor::=SEQUENCE{
```

```
        type            INTERER(3),
        length          INTERER,
        vendorName      OCTET STRING(Size(4..16))
}
Version::=SEQUENCE{
        type            INTERER(4),
        length          INTERER,
        versionStr      OCTET STRING(Size(2..8))
}
Config::=SEQUENCE{
        type            INTERER(5),
        length          INTERER,
        parameters      OCTET STRING(Size(1..64))
}
KeyID::=SEQUENCE{
        type            INTERER(6),
        length          INTERER,
        identity        OCTET STRING(Size(4..16))
}
KeyLen::=SEQUENCE{
        type            INTERER(7),
        length          INTERER,
        keyLength       INTERER
}
Envelope::=SEQUENCE{
        type            INTERER(8),
        length          INTERER,
        envelopeData    OCTET STRING
}
Status::=SEQUENCE{
        type            INTERER(9),
        length          INTERER,
        errorNum        INTERER
}
```

量子加密服务协商消息类型的说明见表 1。

表 1　量子加密服务协商消息类型说明

类型	说明	Type	Length	Value
Usage	量子加密服务密钥使用模式	1	4	无符号整数，1 表示强制、2 表示优选
Mode	量子加密服务密钥融合模式	2	4	无符号整数，1 表示 PRF 推导、2 表示 XOR 异或
Vendor	厂家标识	3	变长	字符串
Version	协议版本	4	变长	字符串
Config	配置参数	5	变长	参数字符串形式
KeyID	量子加密服务密钥标识	6	变长	二进制数值
KeyLen	量子加密服务密钥长度	7	4	无符号整数
Envelope	终端密钥信封	8	变长	二进制数值
Status	量子加密服务密钥状态	9	4	无符号整数，0 表示成功，非 0 表示错误代码

量子加密服务协商消息的具体说明如下。

——Usage：用于标识量子加密服务密钥使用模式：1 强制、2 优选。通信双方均为强制模式时，若量子加密服务密钥获取失败，则 IKE 协商失败。一方为强制模式，另一方为优选模式时，协商按照强制模式执行。两端均为优选模式时，若量子加密服务密钥获取成功，则使用量子加密服务密钥按照 7.1.1.1 节方式进行密钥交换，若量子加密服务密钥获取失败，则使用原始 IPSec 协议的 IKE 协商，协议应符合 GB/T 36968—2018 的第 6.1 节。

——Mode：用于标识量子加密服务密钥与 IPSec 协商密钥的融合模式，1 表示采用 PRF 推导方式，2 表示采用 XOR 异或方式。

——Vendor：用于标识本端使用 QKD 设备厂商信息，验证 QKD 系统或 QKD 网络的兼容性。

——Version：用于标识本端使用 QKD 设备协议信息，验证 QKD 系统或 QKD 网络的兼容性。

——Config：用于标识本端量子加密服务密钥获取的参数配置，为 URL 字符形式，表示连接 QKD 的协议类型、地址和端口号。当两端独立配置 QKD 参数时，该字段为可选。当两端为主从关系时，如网关设备作为主端，终端设备作为从端，主端将 QKD 的密钥获取参数配置发给从端。

——KeyID：用于标识网关设备所采用的量子加密服务密钥 ID，该字段为变长的二进制数值。

——KeyLen：用于标识网关设备所采用的量子加密服务密钥长度，该字段为 UINT32 数值。

——Envelope：用于标识终端设备和终端密钥协商服务中所采用的终端密钥信封。

——Status：用于标识本端的量子加密服务密钥获取状态，0 表示成功，非 0 表示错误。

7.3　安全报文协议

网关设备和终端设备的安全报文协议按照 GB/T 36968—2018 第 6.2 节的要求执行。

8 设备功能性能要求

8.1 设备功能要求

8.1.1 随机数生成

网关设备应具有随机数生成功能，可采用基于物理原理的随机数生成方案，如量子随机数发生器。在使用随机数前，应能够根据安全级别与使用场景要求，对生成的随机数进行检测。应提供检测接口，能通过检测接口对网关设备所生成的随机数进行样本采集，随机性检测应符合 GB/T 32915 的要求。

终端设备应具有随机数生成功能，可采用随机数发生器芯片。在使用随机数前，应能够根据安全级别与使用场景要求，对生成的随机数进行检测。应提供检测接口，能通过检测接口对终端设备所生成的随机数进行样本采集，随机性检测应符合 GB/T 32915 的要求，不同形态产品的随机数检测应符合 GM/T 0062 的要求。

8.1.2 密码算法

网关设备和终端设备应支持国密 SM2、SM3、SM4 算法，并将国密算法作为默认密码套件使用。对于 SM4 密码算法，应支持 CBC 工作模式。

8.1.3 工作模式

网关设备和终端设备工作模式应支持隧道模式和传输模式。其中隧道模式是必备功能，用于网关设备和终端设备实现；传输模式是可选功能，仅用于终端设备实现。

8.1.4 密钥获取

网关设备应支持基于以太网口的量子加密服务密钥输入接口。终端设备应支持基于密钥存储介质加载的终端充注密钥输入接口。

网关设备应支持从 QKD 系统或 QKD 网络获取量子加密服务密钥，终端设备应支持基于终端密钥协商服务的终端充注密钥获取功能，以及量子加密密钥获取功能，协议应符合第 7.1 节的要求。

网关设备和终端设备的密码模块应符合国家密码管理主管部门的管理规定，密码模块的安全技术要求应按照 GM/T 0028—2014 第 7 章执行，密码模块安全等级应不低于网关设备和终端设备的安全等级。

8.1.5 密钥交换

网关设备和终端设备应支持 IPSec 密钥交换和量子加密服务密钥增强的 IPSec 密钥交换两种工作模式，默认使用量子加密服务密钥增强的 IPSec 密钥交换协议作为主用模式，在量子加密服务密钥不可用时，应能够自动切换到 IPSec 密钥交换协议的备用模式。在量子加密服务密钥恢复后，可自动或人工切换回到主用模式。

IPSec 密钥交换通过协商产生工作密钥和会话密钥，协议应符合 GB/T 36968—2018 第 6.1 节要求。

量子加密服务密钥增强的 IPSec 密钥交换，使用量子加密服务密钥参与 IPSec 密钥交换的协商流程。使用 IPSec 密钥交换协议第一阶段产生的密钥材料与量子加密服务密钥进行摘要运算或异或运算，产生工作密钥。使用 IPSec 密钥交换协议第二阶段产生的密钥材料与量子加密服务密钥进行摘要运算或异或

运算，产生会话密钥，协议应符合第 7.2 节的要求。

8.1.6 密钥使用

网关设备和终端设备使用量子加密服务密钥增强的 IPSec 密钥交换功能时，应支持在第二阶段融合量子加密服务密钥一次性产生多个会话密钥，其数量由网关设备和终端设备获取的量子加密服务密钥量和所使用的对称加密算法的密钥分组长度共同决定。网关设备和终端设备应使用这些会话密钥，一次性协商产生多对相应的 SA。在之后业务加密过程中，发送方应将业务报文根据一定的时间周期或报文流量规则进行划分，分摊到不同 SA 中进行传输。基于上述方式，量子保密通信应用设备借助量子加密服务密钥的密钥量和更新速率优势，间接提升对称加密算法中的会话密钥更新速率，从而增强安全性。

8.1.7 密钥更新

网关设备和终端设备中量子加密服务密钥的更新频率与更新量，应满足用户网络对量子保密通信应用的加密能力和安全性要求。

网关设备和终端设备在使用量子加密服务密钥增强的 IPSec 密钥交换功能时，应支持根据一定的时间周期或报文流量规则，进行工作密钥和会话密钥更新。根据时间周期规则进行密钥更新为必备功能，根据报文流量规则进行密钥更新为可选功能。其中：

——网关设备工作密钥最大更新周期宜不大于 4h，会话密钥最大更新周期宜不大于 10min。

——终端设备工作密钥最大更新周期宜不大于 12h，会话密钥最大更新周期宜不大于 30min。

网关设备和终端设备在使用 IPSec 密钥交换功能时，密钥更新要求应按照 GB/T 36968—2018 第 7.1.10 节的要求执行。

8.1.8 安全报文封装

网关设备和终端设备的安全报文封装协议分为 AH 协议和 ESP。AH 协议应与 ESP 嵌套使用，这种情况下不启用 ESP 中的验证操作。ESP 可单独使用，这种情况下应启用 ESP 中的验证操作。

安全报文封装协议应按照 GB/T 36968—2018 第 6.2 节的要求执行。

8.1.9 NAT 穿越

网关设备和终端设备应支持 ESP 单独使用时 NAT 穿越。

NAT 穿越协议应按照 GB/T 36968—2018 第 6.2.3 节的要求执行。

8.1.10 鉴别方式

网关设备和终端设备应具备实体鉴别功能，身份鉴别数据应支持数字证书方式。

8.1.11 IP 协议版本支持

网关设备和终端设备应支持 IPv4 和 IPv6 两种协议版本。

8.1.12 抗重放攻击

网关设备和终端设备在安全报文传输阶段应具有对抗重放攻击的功能。

8.2 设备性能参数

8.2.1 量子加密服务密钥更新速率

量子加密服务密钥更新速率是指量子保密通信应用网关设备和终端设备在一定的时间周期内获取的量子加密服务密钥的比特数，除以该时间周期的秒数。

网关设备和终端设备应满足用户网络环境对量子加密服务密钥更新速率的要求。

8.2.2 加解密吞吐率

加解密吞吐率是指分别在 64 字节以太帧长和 1428 字节（IPv6 是 1408 字节）以太帧长时，IPSecVPN 产品在丢包率为 0 的条件下，内网口上达到的双向数据最大流量。

网关设备和终端设备应满足用户网络环境对业务数据的加解密吞吐率的要求。

8.2.3 加解密时延

加解密时延是指分别在 64 字节以太帧长和 1428 字节（IPv6 是 1408 字节）以太帧长时，IPSecVPN 产品在丢包率为 0 的条件下，一个明文数据流经加密变为密文，再由密文解密还原为明文所消耗的平均时间。

网关设备和终端设备应满足用户网络环境对业务数据的加解密时延的要求。

8.2.4 加解密丢包率

加解密丢包率是指分别在 64 字节以太帧长和 1428 字节（IPv6 是 1408 字节）以太帧长时，IPSecVPN 产品在内网口处于线速情况下，单位时间内错误或丢失的数据包占总发数据包数量的百分比。

网关设备和终端设备应满足用户网络环境对业务数据的加解密丢包率的要求。

8.2.5 每秒新建隧道数

每秒新建隧道数是指网关设备和终端设备在 1s 时间内能够建立隧道数目的最大值。

网关设备和终端设备应满足用户网络环境对每秒新建隧道数的要求。

8.2.6 最大并发隧道数

最大并发隧道数是指网关设备和终端设备能够支持同时并存的 IPSec VPN 隧道数目的最大值。

网关设备和终端设备应满足用户网络环境对最大并发隧道数的要求。

8.2.7 单隧道最大并发连接数

单隧道最大并发连接数是指网关设备和终端设备中，单条 IPSec VPN 隧道能够支持并发建立的 TCP 连接数目的最大值。

网关设备和终端设备应满足用户网络环境对单隧道最大并发连接数的要求。

8.3 安全管理要求

8.3.1 密钥管理

网关设备和终端设备的设备密钥、工作密钥和会话密钥的管理，应按照 GB/T 36968—2018 第 7.3.1

节的要求执行。

量子加密服务密钥的管理要求，参照工作密钥的管理要求执行。

终端充注密钥的管理要求，参照设备密钥的管理要求执行。

8.3.2 数据管理

网关设备和终端设备的配置数据和日志的数据管理，应按照 GB/T 36968—2018 第 7.3.2 节的要求执行。

8.3.3 管理员角色管理

网关设备和终端设备的管理员角色管理，应按照 GB/T 36968—2018 第 7.3.3 节的要求执行。

8.3.4 设备管理

网关设备和终端设备的硬件安全、软件安全、设备初始化、注册和监控、设备自检以及设备物理安全防护的设备管理，应按照 GB/T 36968—2018 第 7.3.4 节的要求执行。

网关设备和终端密钥协商服务中的密钥管理设备与密钥充注设备，应与 QKD 系统或 QKD 网络中的密钥管理设备处于同一安全管理域内。

网关设备的密钥输入接口、终端密钥协商服务的密钥输入与输出接口、终端设备的密钥输入接口，应与其他业务和管理接口进行隔离，不能泄露设备内部敏感信息。

9 设备测试方法

9.1 设备功能检测

9.1.1 随机数功能

按照 GB/T 32915 的要求，提取网关设备或终端设备生成的随机数样本，进行随机性检测，检测结果应合格。

9.1.2 密码算法

网关设备或终端设备在出厂状态下，建立一条 IPSec 配置，查看其密码套件配置选项，默认使用的算法应为国密算法。

9.1.3 工作模式

将测试设备与被测的网关设备或终端设备均设置为隧道模式，应能成功完成密钥交换，建立 IPSec 隧道进行通信。当被测的网关设备或终端设备支持传输模式时，将测试设备和被测设备均设置为传输模式，应能成功完成密钥交换，进行通信。将测试设备和被测设备一方设置为隧道模式，另一方设置为传输模式，则密钥交换应失败，无法建立 IPSec 隧道进行通信。

9.1.4 密钥获取

将网关设备与 QKD 系统或 QKD 网络的密钥管理设备连接，配置密钥获取、存储与更新的功能及

流程，查看量子加密服务密钥获取状态，应能正常获取、存储和更新量子加密服务密钥。配置与 QKD 系统或 QKD 网络连接的终端密钥协商服务进行密钥获取和离线充注，在终端设备中查看终端充注密钥的获取状态，应能正常实现终端充注密钥获取和存储功能。配置终端密钥协商服务与终端设备的量子加密服务密钥获取、存储与更新的功能及流程，在终端设备或网关设备和网管系统中查看量子加密服务密钥获取状态，应能正常获取、存储和更新量子加密服务密钥。

对密钥获取过程进行网络数据截获，查看其过程应符合 7.1 节的要求，应能正确进行加解密传输。该项测试通过，可间接验证网关设备和终端设备在密钥获取过程中采用的对称密码算法、非对称密码算法和密码杂凑算法的实现正确性。

9.1.5 密钥交换

密钥交换检测步骤按照 9.1.3 节进行。对密钥交换过程进行网络数据截获，查看其过程应符合 7.2 节的要求，应能正确进行加解密通信。该项测试通过，可间接验证网关设备和终端设备在密钥交换过程中采用的对称密码算法、非对称密码算法和密码杂凑算法的实现正确性。

9.1.6 密钥使用

使用量子加密服务密钥增强的 IPSec 密钥交换功能时，将测试设备与被测的网关设备或终端设备，均设置为隧道模式，应能成功完成密钥交换，建立 IPSec 隧道进行通信。查看被测设备中的量子加密服务密钥使用情况和消耗量，IPSec 协议会话密钥生成情况与数量，以及 SA 建立情况与数量，应能在一次协商过程中，通过使用量子加密服务密钥，生成多个会话密钥，并建立多个相应的 SA。通过对业务加密隧道进行网络数据截获，查看业务数据流在不同 SA 中划分和传输的实现情况，应能实现业数据流在不同 SA 中的划分和传输。

9.1.7 密钥更新

在使用量子加密服务密钥增强的 IPSec 密钥交换功能时，网关设备和终端设备的量子加密服务密钥更新检测见第 9.1.4 节。

在网关设备或终端设备中，分别设定工作密钥和会话密钥的更新周期或按照业务流量更新条件，当满足更新条件时，使用网络报文截获工具进行业务信道抓包，应能查看到 IPSec 协议的密钥协商过程，应能查看到在相同明文报文条件下，使用不同密钥加密产生的密文状态变化。

9.1.8 安全报文封装

按照 GB/T 36968—2018 第 8.1.5 节的要求进行检测。

9.1.9 NAT 穿越

按照 GB/T 36968—2018 第 8.1.6 节的要求进行检测。

9.1.10 鉴别方式

按照 GB/T 36968—2018 第 8.1.7 节的要求进行检测。

9.1.11 IP 协议版本支持

按照 GB/T 36968—2018 第 8.1.8 节的要求进行检测。

9.1.12 抗重放攻击

按照 GB/T 36968—2018 第 8.1.9 节的要求进行检测。

9.2 设备性能检测

9.2.1 量子加密服务密钥更新速率

按照第 8.2.1 节的要求进行测试，记录测试结果。

9.2.2 加解密吞吐率

按照第 8.2.2 节的要求进行测试，记录测试结果。

9.2.3 加解密时延

按照第 8.2.3 节的要求进行测试，记录测试结果。

9.2.4 加解密丢包率

按照第 8.2.4 节的要求进行测试，记录测试结果。

9.2.5 每秒新建隧道数

按照第 8.2.5 节的要求进行测试，统计时间为 1min，记录测试结果。

9.2.6 最大并发隧道数

按照第 8.2.6 节的要求进行测试，记录测试结果。

9.2.7 单隧道最大并发连接数

按照第 8.2.7 节的要求进行测试，记录测试结果。

9.3 安全管理检测

9.3.1 密钥管理

按照 GB/T 36968—2018 第 8.3.1 节的要求进行检测。

9.3.2 数据管理

按照 GB/T 36968—2018 第 8.3.2 节的要求进行检测。

9.3.3 管理员角色管理

按照 GB/T 36968—2018 第 8.3.3 节的要求进行检测。