SSH sntrup761 X25519 简介的安全分析

rfc9941 — ProVerif+ 代理 报告

文稿	安全壳(SSH) 采用混合精简式NTRU Prime sntrup761和X25519的密钥交换法,与SHA-512:sntrup761x25519-sha512(协议定义）; 安全壳(SSH)运输层协议(辅助))
检查的性质	13 条：11 条成立，0 条不成立，2 条没有答案
发现	无

目录

1 协议和范围
2 发现
3 检查过的性质
4 本次分析的局限
附录 A：逐条性质的解读
附录 C：主张和证明器的答案
附录 D：分析是怎么跑的

1 协议和范围

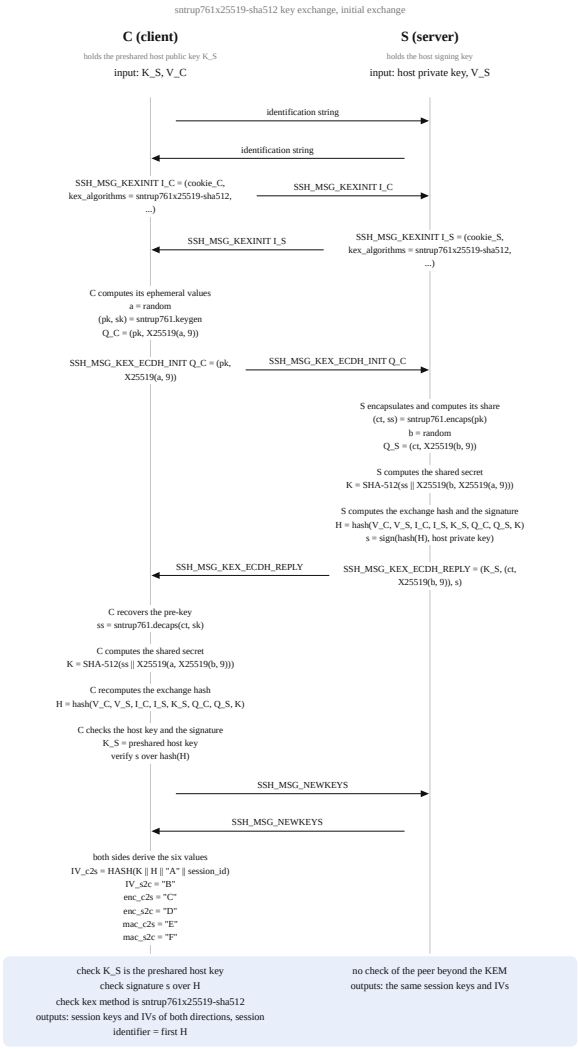
协议是SSH型混合键交换机sntrup761x25519-sha512. 一个客户端和一个服务器同意一种方法,客户端发送一个sntrup761公钥连同其X25519股,服务器以sntrup761密码解答,其X25519股和其主机密钥的签名,双方从中获取会话密钥并用NEWKEYS投入使用. 客户端提前持有服务器的主机公钥,服务器即匹配的私钥.

当交换结束时,客户端确定它持有的密钥属于它已经拥有的主机密钥的服务器,并且它接受的算法名称和交换值是服务器使用的. 服务器确信只有拥有它所处理的sntrup761密钥的客户端才能计算出相同的密钥. 双方都不了解用户是谁:用户认证在本分析之外.

双方:

- **C(客户)**:持有预分摊主机公用密钥K_S. 持有量:K_S,V_C.
- **S(服务器)**:持有主机签名密钥. Holds:主机私钥,V_S.

图1显示交易所,如文件所示。



- 图1。 指定协议 。 *

分析的范围载于附录D:分析的内容、遗漏的内容和文件的章节。

2 发现

没有发现。 分析发现文件没有说明或搁置任何内容。 款次中的表格3对每一个财产都有结果。

协议给出了分析属性所要求的,没有发现. 13个目标中有12个通过初步关键交换的任何会议次数的证明得到答复; 其余两项主张,即泄漏的只有X25519 ephemeral 保存会话键,在ProVerif之前没有答案. 没有发现任何财产受到攻击,因此没有已知的弱点必须复制。 结果依赖于一种理想化的sntrup761,保持X25519的一条定律,并且不包含再交换,关于交换散列本身的协议通过签名的散列和服务器的KEXINIT cookie来回答,而不是直接查询.

3 检查过的性质

每行是一块财产,投入到ProVerif. 结果是ProVerif对分析师的协议模型的回答; 价值以及文件是否已经说明结果是分析员的判断,理由见附录A。

ID	性质	假定的泄露	结果	价值	文稿是否已写
A02	**密钥交换的服务器认证。** 每当客户端完成一次密钥交换并接受会话，就存在一个以该客户端为通信对象的服务器真实运行。	无	成立	中	是
A03	**关于交换散列投入的协议。** 每当客户端接受会话，就存在一个匹配的服务器运行，双方在角色、身份、I_C、I_S、K_S、Q_C、Q_S 与 K 上一致。	无	成立	中	是
A04	**注入性协议和独特的会议编号。** 客户端每次接受会话都对应一个不同的服务器运行（单射匹配），会话标识符不重复。	无	成立	中	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
A08	**固定配置文件绑定了谈判算法**。 客户端接受的算法集合与主机公钥算法对应双方 KEXINIT 提议按协商规则选出的结果，并绑定到本次会话的 交换散列。	无	成立	中	是
K01	**会话密钥和主机密钥**。 攻击者不能推导出共享秘密 K 及由 K、H 派生的会话密钥，也不能获得服务器主机私钥。	无	成立	中	是
K04	**按方向和会话分列**。 客户端到服务器与服务器到客户端的加密密钥、完整性密钥、IV 互不相同，且不同会话的密钥互不相同。	无	成立	中	是
C01	**会话密钥的预先保密**。 会话完成并擦除临时状态后，泄露服务器主机私钥不能使攻击者获得该会话的共享秘密 K 或会话密钥。	服务器主机私钥 (会话完成并擦除临时状态后)	成立	中	是
C04	**hybrid 组件泄漏保留了密钥**. 泄露 X25519 临时私钥或 sntrup761 KEM 私钥之一时，攻击者仍不能获得共享秘密 K 与会话密钥。	单个 KEX 组件（X25519 临时私钥或 sntrup761 KEM 私钥） (密钥交换期间或之后)	无答案	中	否
D01	**接受的签字对交换具有约束力**。 客户端接受的签名覆盖的 外汇散列 与主机公钥确实由声称的服务器生成，未被篡改。	无	成立	中	是
C04.10	**一个组件漏漏保留了密钥**。 泄露 X25519 临时私钥或 sntrup761 KEM 私钥之一时，攻击者仍不能获得共享秘密 K 与会话密钥。	单个 KEX 组件（X25519 临时私钥或 sntrup761 KEM 私钥） (密钥交换期间或之后)	无答案	中	否
A03.11	**主键和散列绑定**。 客户端接受的会话中，主机公钥 K_S 与 交换散列(会话标识符）的绑定与服务器真实运行一致，未被替换。)	无	成立	低	是
A08.12	**与会话绑定的旋律和算法**。 客户端接受的算法集合与角色对应双方 KEXINIT 提议按协商规则选出的结果，并绑定到本次会话的 交换散列,不能被跨会话替换。	无	成立	低	是
X01	**交换散列保密**。 对于已完成的会话,网络上的攻击者不能计算交换散列H, i. e. 该届会的标识符	无	成立	低	是

文稿写明而起草的清单里没有、由分析者补充的目标（见附录 D）：X01.

所问之问,及分析师之答:

问题	回答	依据
Q1: 不同 KEX 组件泄露时密钥保密	仅持有一个密钥交换部件并不能给sntrup761边的会话密钥,这一点已得到证明; 在X25519号一侧,同一主张没有得到答复,因此一半需要另一个证明器。	C04.10, C04
Q2:主机密钥 与 会话 ID/交换散列 绑定	主机公共密钥和会话标识符绑定在产生它们的运行中:客户端仅接受由预共享的主机密钥在它重算的交换散列上签名,它不能从流量中计算散列.	A03.11, A02, X01
Q3: 角色与算法协商字段不可跨会话替换	角色和算法字段不能取自另一个会话:每个会话接受匹配一个不同的服务器运行,客户端从不接受一个会话来命名任何其他算法.	A08.12, A08

4 本次分析的局限

这里的一个结果就是协议模型的结果:它描述了特定的信息和检查给出的或未能给出的,以密码学为理想,没有关于执行的内容.

正如分析师所说,这一分析没有涵盖的内容是:

- 分析仅涵盖初始密钥交换; 重新交换,即会话标识符保留其值和所有密钥被替换的地方,不是不滚动的。
- sntrup761被理想化为公用密钥加密新预键; 2. 未显示其IND-CCA2安全及其计算强度。
- X25519系仿照单定律g^(xy) = g^(yx); 模型给予攻击者少于真正的群体,所以发现的攻击会维持在协议中,但证据是针对较弱的代数攻击者.
- 按规定在错误长度Q_C或Q_S上进行流产,是一种字节级的检查,没有模式化.
- 侧面通道,特别是继承安全考虑中讨论的大纳姆编码,以及随机数据的质量不在符号模型之外.
- 用户认证,记录层的序列号,密码模式和重键策略都在模型交换之外.
- 双方的协议在服务器的KEXINIT cookie上显示,其余的通过签好的交换散列显示; 要求就交换散列值达成协议的查询本身并没有在ProVerif年终止。
- 混合成分分析的一项主张,即只有X25519麻黄保存密钥的泄漏,没有ProVerif的答案; Tamarin+ Agent,即模拟代数的原样,可以解决它.

主持人记录的是什么:

- 无答:C04,C04.10.
- C04,C04.10的答案依赖于该型号简化后的操作(附录D).

- 证明器没有给出结论的查询（附录 C）：C04: c04_xa, C04.10: c04_xa。 这条性质问过了，证明器既没有证明它也没有找到攻击，所以结果写“无答案”。
- 没带对照查询的证明（附录 C）： A02:auth_cs,A03:auth_cs,A04:inj_cs,A08: 降级,A08:auth_cs,K01:k01_k,K01:k01_e,K01:k01_se,K01:k01_ltsk,K04:k04_dir,K04:k04_e,K04:k04_iv,D01:auth_cs,A03.11:auth_cs,A0 对照查询是这条性质的一个必然不成立的变体；没有它，就没有东西表明这条性质照现在的写法在模型里有可能不成立。

附录A中列出了每个财产的开口情况以及解决这些财产的办法。

附录 A：逐条性质的解读

分析师自己对证明器的答案的解读,而不是对证明器的答案:答案对协议的意义,读取的基础,是否可以按原样使用,价值如何.

A02: 密钥交换的服务器认证

每当客户端完成一次密钥交换并接受会话，就存在一个以该客户端为通信对象的服务器真实运行。

一个客户端只有在服务器运行时才接受一个会话,它持有预先共享的主机密钥在客户端计算的交换机上签名. 网络上的攻击者不能让客户端接受一个没有服务器运行的会话 。

- 结果:持有; 回答问题:是的; 可用备注
- 价值介质:通过理想化的混合体证明了中央保障,要求就饼干而不是整个散列达成协议。
- 在文件中说明:是的。 文件中说:rfc4253:812,s0028,s0079,s0082,s0083
- 休息:客户持有并比较预分享的主机公钥; KEM是理想化的,所以只有地址客户端恢复了预键; 协议显示在服务器的KEXINIT cookie 在签名的交换散列中
- Open:关于交换-hash字段本身的协议通过KEXINIT cookie被解答,因为直接查询没有终止.

A03:关于交换散列投入的协议

每当客户端接受会话，就存在一个匹配的服务器运行，双方在角色、身份、I_C、I_S、K_S、Q_C、Q_S 与 K 上一致。

客户端接受的会话是此交换的服务器运行,输入交换散列的算法名称,交换值和密钥是服务器自己的. 从饼干到每个字段的一步 都取决于散列的抗碰撞性 和无人计算散列。

- 结果:持有; 回答问题:部分; 可用备注
- 值介质:实地协议通过签名的散列和饼干证明,但直接的散列查询保持开放.
- 在文件中说明:是的。 文件上说:rfc4253:1176,s0011,s0082,s0091
- 休息时间:散列的碰撞阻力,象征模型假定; 签名覆盖包含所有字段的交换散列; 第KEM号理想化法和第X25519号单一法
- 开放:就交换散列值本身达成协议:双参数函证查询超时30s.

A04: 注入协议和独特的会话 id

客户端每次接受会话都对应一个不同的服务器运行（单射匹配），会话标识符不重复。

每个被接受者计算一个不同的服务器运行,所以一个被记录的服务器交换无法重播为第二个被接受者. 会话标识符来自两侧的新值,不重复.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:重玩握手的阻力得到证明,新鲜度读出注射式的函文.
- 在文件中说明:是的。 文件上说:rfc4251:841,s0035,s0061,s0074
- 休息时间:饼干,KEM预键和X25519 expresents是新鲜的; 在KEXINIT饼干上询问了注射式信件
- 打开:会话标识符的新鲜度显示为对应物的注入性,而不是散列值的区别性.

A08:固定剖面绑定谈判算法

客户端接受的算法集合与主机公钥算法对应双方 KEXINIT 提议按协商规则选出的结果，并绑定到本次会话的 交换散列

客户端从未接受一个KEXINIT命名任何其他密钥交换方法,它接受的有效载荷是服务器自己的,捆绑在已签名的散列中,因此无法从另一个会话中互换. 模式中有一个方法,没有什么可谈判的。

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:固定剖面内部的降级阻力得到证明,但模型没有第二个套件可以向它谈判.
- 在文件中说明:是的。 文件上说:s0003、s0012、s0033、s0034
- 休息:模型中只有固定方法和一个替代名称; 模拟的KEXINIT有效载荷是饼干加固定名称,而不是全名清单

K01:会话密钥和主机密钥

攻击者不能推导出共享秘密 K 及由 K、H 派生的会话密钥，也不能获得服务器主机私钥。

共享的秘密,双向加密密钥,完整性密钥和主机私人密钥远离攻击者手中,用于整个交换. 在模型的后期泄露开始后运行的会话仍然受到保护.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:证明了衍生密钥的保密性,将原始人理想化.

- 在文件中说明:是的。 文件上说:rfc4251:652,s0011,s0063,s0064
- 休息时间:KEM是理想化的,X25519有一条法律,因此保密取决于理想化而不是计算; 在交换过程中,在模型泄露之前,要保密

K04:按方向和会话划分的关键分隔

客户端到服务器与服务器到客户端的加密密钥、完整性密钥、IV 互不相同，且不同会话的密钥互不相同。

这两个方向从未共享过IV,加密密钥或完整性密钥,两个会话也从未获得相同的值,因为每个会话都是会话本身的散列和独特的方向字母.

- 结果:持有; 回答问题:是的; 可用备注
- 数值介质:为模拟会议证明密钥分离; 同一段落的重键分支不是模拟的。
- 在文件中说明:是的。 文件中说:s0064、s0065、s0066、s0067、s0068、s0069
- 依据:文档的六个方向值以K、H和一个字母为模型; 差异通过自由散列来显示,它使不同的术语相隔开
- 开放:c2s加密密钥和c2s IV加密密钥的跨会间分离被询问; 完整性密钥和其他方向遵循相同的构造,但没有给出每个查询。

C01:会话密钥的预先保密

会话完成并擦除临时状态后，泄露服务器主机私钥不能使攻击者获得该会话的共享秘密 K 或会话密钥。

交换后泄露出来的主机私人密钥不打开完成的会话:密钥来自ephemeral KEM预键和X25519协议,而不是主机密钥. 控件显示, 一旦发布会话本身的机密, 同样的查询就会失败 。

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:对主机密钥泄漏的前进密钥通过控制,在理想化原始下得到证明.
- 在文件中说明:是的。 文件上写着:rfc4251:1021,s0061,s0063
- 休息时间:漏泄是按会话的模式,在后期进行; 第KEM号理想化法和第X25519号单一法
- 打开:文件还要求删除麻黄参数; 清除不是模拟的,只是完成的会话没有显示任何东西。

C04:混合部件泄漏保存密钥

泄露 X25519 临时私钥或 sntrup761 KEM 私钥之一时，攻击者仍不能获得共享秘密 K 与会话密钥。

失去sntrup761 KEM的秘密 仍然留下了会话密钥 由X25519 半 保护,这一点已经得到证明。 与此相反的是,失去X25519的电离层使其受到KEM半体的保护,这是建筑所暗示的,但ProVerif既不能证明也不能反驳:它造就了一种衍生物,然后无法重建痕迹。

- 结果:没有答复; 回答问题:部分; 可用备注
- 数值介质:混合成分问题的一半被机械地证明; 另一半留给一个模型代数的验证器。
- 在文件中说明:否。 资料来源:s0004、s0008、s0009、s0011。
- 休息时间:KEM理想化使KEM-号主张通过建筑得到证实; X25519半只与单法模式一样强大; 控件直接发布会话密钥,从而显示查询可能失败,但单是漏泄就够了
- 公开:X25519侧组件问题没有ProVerif的答案.

D01:接受的签字对交易所具有约束力

客户端接受的签名覆盖的 外汇散列 与主机公钥确实由声称的服务器生成，未被篡改。

客户端接受的是服务器在本次运行的交换散列上的签名,对照它已经信任的宿主密钥进行检查,因此在中转时无论是散列还是宿主密钥都无法更改.

- 结果:持有; 回答问题:是的; 可用备注
- 价值介质:在理想化的签名和散列上证明签字具有约束力。
- 在文件中说明:是的。 文件上说:rfc4253:1176,s0082,s0083,s0093
- 休息:签名是不可原谅的,主机密钥是预先共享的; 标本标出H的散列,因为文件要求将签名适用于H

C04.10:一个部件泄漏 保存密钥

泄露 X25519 临时私钥或 sntrup761 KEM 私钥之一时，攻击者仍不能获得共享秘密 K 与会话密钥。

混合体的一个漏出部分没有给sntrup761侧的会话键,这一点已得到证明; X25519的方位没有得到答复。 这些文件描述了混合建筑,但没有说明一个泄露的部件购买了什么。

- 结果:没有答复; 回答问题:部分; 可用备注
- 值介质:这是用户提出的问题; KEM半被证实,X25519半被打开。
- 在文件中说明:否。 资料来源:s0004、s0008、s0009、s0011。
- 休息时间:KEM理想化; 单一法X25519模式; 控件在两个组件会话中直接发布 K
- 公开:泄露X25519麻黄单曲:没有ProVerif的回答.

A03.11:主机密钥和散列装订

客户端接受的会话中，主机公钥 K_S 与 交换散列(会话标识符）的绑定与服务器真实运行一致，未被替换。)

在被接受的会话中,主机公钥和会话标识符是服务器运行的会话:客户端将提供的主机密钥与预共享的密钥进行比较,仅接受其重算的散列上的签名.

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:用户要求重述A02和A03; 它没有增加任何结果 除了他们之外。
- 在文件中说明:是的。 文件上写着:s0061、s0082、s0091
- 休息:主机密钥预先共享和比较; 交换散列包含K_S,所以不同的主机键给出不同的散列

A08.12:与会话绑定的角色和算法

客户端接受的算法集合与角色对应双方 KEXINIT 提议按协商规则选出的结果，并绑定到本次会话的 交换散列 不能被跨会话替换。

一个侧面承担的角色和它接受的算法字段属于产生它们的运行,因为每个侧面接受地图到一个不同的服务器运行,客户端拒绝其他方法名称.

- 结果:持有; 回答问题:是的; 可用备注
- 值低:用户要求的A04和A08的重述.
- 在文件中说明:是的。 文件上说:s0033、s0034、s0036、s0099
- 休息:在模型中,角色是不同的过程; 只有初始交换模式
- 开放:不分析角色不得在重交换上改变的规则,因为重交换不是不滚动的.

X01: 交换散列保密

对于已完成的会话,网络上的攻击者无法计算交换散列H, i. e. 该届会的标识符

交换散列远离攻击者,这是文件要求的; 它的会话标识符和绑定的更高层, 所以它的保密性不仅仅是化妆品。

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:直接源于K的保密性,由文件说明; 保持为选中的入球 显示模型不会通过签名泄露 H 。
- 在文件中说明:是的。 文件上写着:rfc4253:1176,s0092
- 休息:H是K的散文,所以它的秘密来自K的秘密; 模型标记H的散列,所以签名不显示H

附录 C：主张和证明器的答案

证明器对每个目标的记录:所达到的关卡,到达它的查询,是否检查了控制,以及攻击与分析师对每个目标的判决.

目标	级别	界	查询	对照	攻击	主张
A02	proved		auth_cs	2中的1人		证明:2
A03	proved		auth_cs	2中的1人		证明:2
A04	proved		inj_cs	2中的1人		证明:2
A08	proved		降级	4中的2人		证明:4
K01	proved		k01_k	8中的4人		证明:8
K04	proved		k04_dir	6中的3人		证明:6
C01	proved		c01	检查		证明:1
C04	proved		c04_kem	检查		证明1,1 未裁定
D01	proved		auth_cs	2中的1人		证明:2
C04.10	proved		c04_kem	检查		证明1,1 未裁定
A03.11	proved		auth_cs	2中的1人		证明:2
A08.12	proved		inj_cs	2中的1人		证明:2
X01	proved		x01	2中的1人		证明:2

以分析师对每项主张的措辞提出的主张; 每一个答案都是证明器的:

目标	主张	攻击者	回答	查询	对照
A02	每个客户端接受对应此交换的真实服务器运行: 客户端只接受服务器的KEXINIT cookie 在共享的主机密钥已经签名的交换散列内.	network	proved	auth_cs	无
A02	每个客户端接受对应此交换的真正服务器运行.	network	proved	auth_cs	检查
A03	客户端接受的会话是真实服务器运行的会话:服务器的KEXINIT cookie,并通过交换散列客户端验证,角色,I_C,I_S,K_S,Q_C,Q_S和K是服务器自己的值.	network	proved	auth_cs	无
A03	客户端接受的会话是真实的服务器运行,其KEXINIT cookie和其他交换-hash字段的客户端通过服务器的签名验证.	network	proved	auth_cs	检查
A04	每个客户端接受匹配一个截然不同的服务器运行(注射通信):一个服务器运行,客户端接受的交换不计算两次,因此没有接受的会话是重播的服务器运行.	network	proved	inj_cs	无
A04	每个客户端接受匹配一个不同的服务器运行(注射通信),所以一个被接受的会话不是重播的服务器运行.	network	proved	inj_cs	检查
A08	无降级:客户端从未接受一个会话,其KEXINIT命名为sntrup761x25519-sha512以外的算法.	network	proved	降级	无
A08	接受的算法字段I_C和I_S是服务器运行的字段,并捆绑在交换散列中,因此不能从另一个会话中取出.	network	proved	auth_cs	无
A08	不降级:客户端从未接受一个KEXINIT命名除固定方法以外的算法.	network	proved	降级	检查
A08	被接受的算法字段是服务器自己的,并捆绑在已签名的交换散列中.	network	proved	auth_cs	检查
K01	完成会话的共享秘密K在密钥交换期间不为网络攻击者所知,即使模型中其他会话的会话会后泄露.	network	proved	k01_k	无
K01	K和H衍生的客户端对服务器加密密钥,网络上的攻击者并不知情.	network	proved	k01_e	无
K01	服务器对客户端加密密钥不为网络攻击者所知; 完整性密钥的生成方式相同,并被同一查询覆盖。	network	proved	k01_se	无
K01	服务器主机私钥在密钥交换过程中从未为攻击者所知.	network	proved	k01_ltsk	无
K01	完成会话的共享秘密K在交流期间不为网络攻击者所知.	network	proved	k01_k	检查
K01	交换期间网络上的攻击者不知道客户端对服务器的加密密钥.	network	proved	k01_e	检查
K01	服务器对客户端加密密钥和生成同样方式的完整密钥在交换过程中不为网络攻击者所知.	network	proved	k01_se	检查
K01	服务器主机私钥在交换过程中从未为攻击者所知.	network	proved	k01_ltsk	检查
K04	IVs与两个方向的加密和完整性密钥在一个会话中是双向的:衍生出的两个方向从未产生相同的值.	network	proved	k04_dir	无
K04	一个会话的客户端对服务器加密密钥从来不是另一个会话的加密密钥(同一会话的加密密钥也是同样会话的加密密钥):等同的密钥属于同一个会话标识符.	network	proved	k04_e	无
K04	一个会话的客户端对服务器的IV从不是另一个会话的; 2. 服务器对客户的 IV 和完整性密钥 遵循相同的衍生。	network	proved	k04_iv	无

目标	主张	攻击者	回答	查询	对照
K04	这两个方向在会话中从未共享IV或加密或完整性密钥.	network	proved	k04_dir	检查
K04	一个会话的客户端对服务器加密密钥从来不是另一个会话的加密密钥.	network	proved	k04_e	检查
K04	一个会话的客户端到服务器的IV从不是另一个会话.	network	proved	k04_iv	检查
C01	在会话结束后,主机私密密钥被披露,攻击者不会学习K或该会话的会话密钥(前向保密).	host_key_leak	proved	c01	检查
C04	持有一个会话(和整个网络流量)的sntrup761 KEM秘密密钥的攻击者,仍然没有学会那个会话的K.	kem_secret_leak	proved	c04_kem	检查
C04	攻击者持有一个会话的X25519元电平的私人价值,仍然无法从该会话中得知K.	x25519_ephemeral_leak	undecided	c04_xa	
D01	客户端接受的签名是服务器通过这个运行的交换散列,用预先共享的主机密钥制作的; 无论是H型还是K_S型,都无法在过境时改变。	network	proved	auth_cs	无
D01	客户端接受的签名是服务器通过这次运行的交换散列,因此H和K_S都无法更改.	network	proved	auth_cs	检查
C04.10	漏掉一个会话的一个KEX元元件,sntrup761 KEM密钥,不给K或会话密钥:X25519元件仍然保护着它们.	kem_secret_leak	proved	c04_kem	检查
C04.10	仅泄漏X25519的麻黄私人价值并不能给K:sntrup761组件仍然保护它.	x25519_ephemeral_leak	undecided	c04_xa	
A03.11	在被接受的会话中,主机公钥和交换散列(会话标识符)是生成它们的服务器运行的会话; 两者都无法替换。	network	proved	auth_cs	无
A03.11	被接受会话的主机密钥和交换散列是生成它们的服务器运行的密钥和散列.	network	proved	auth_cs	检查
A08.12	双方各自承担的角色和客户端接受的算法字段就是这个运行中的角色,不能被另一个会话所取代,因为每个会话接受匹配一个不同的服务器运行.	network	proved	inj_cs	无
A08.12	客户端接受的角色和算法字段属于此运行,不能从另一个会话中获取.	network	proved	inj_cs	检查
X01	对于已完成的会话,网络上的攻击者无法计算交换散列H,会话标识符.	network	proved	x01	无
X01	已完成会话的交换散列H,会话标识符,不能由网络上的攻击者计算.	network	proved	x01	检查

附录 D：分析是怎么跑的

LLM名分析员从文件中建立了协议模型,将每个财产归入ProVerif; 第3节中的每一个结果都是证明器的答案.

ProVerif+ 代理会话 session-20261115T080525, 2026-11-15. 状态: 完成 。 型号:deepseek-v4-1-flash-261017. 台阶:65,校对:157 s,壁14 min,耗资0.151 USD.

背景:主机从谈话中移除了1时间(s),总共删除了549033个字符(更早的推理,以及最新变化之前显示模型的内容)的僵化部分. 轨迹文件保存了一切

ProVerif:109 证明运行,93 决定,16 未答,151 s,35 答录.

分析了什么

协议	SSH sntrup761 X25519 简介.
版本	rfc9941
分析范围	固定 sntrup761x25519-sha512，与先前 ML-KEMSSH是不同算法配置；完整 SSHKEXINIT交换散列,主机签名和 NEWKEYS；可信主机公钥预置。理想 摇摆KEM不涉及多项式运算或计算安全证明；排除用户认证。
不在范围内	符号模型不证明算法的计算安全或抗量子安全；攻击轨迹只在明确假设下成立，不直接等同规范漏洞。每个性质必须有可达性/正例控制。
原文	以下各节的102个编号段落(22661字节). 本报告中的s0001等参考文献就是其中一段。

文件各节的分析依据如下:

文稿	章节	标题
主体	2	要求 语文
主体	3	密钥交换方法: sntrup761x25519-sha512
主体	4	安全考虑
rfc4253	7	密钥交换
rfc4253	7.1	算法谈判
rfc4253	7.2	密钥交换输出
rfc4253	7.3	将密钥带入使用
rfc4253	8	Diffie- Hellman 密钥交换
rfc4253	8.1	diffie-hellman-group1-sha1
rfc4253	8.2	diffie-hellman-group14-sha1
rfc4253	9	密钥重交换

协议的目的是在文档中将其定位为源步骤:固定 sntrup761x25519-sha512，与先前 ML-KEMSSH是不同算法配置；完整 SSHKEXINIT交换散列,主机签名和 NEWKEYS；可信主机公钥预置。理想 摇摆KEM不涉及多项式运算或计算安全证明；排除用户认证。

对照文稿定性质

在写出查询之前,分析师根据文件本身所说的协议的目的设定了已起草的属性清单. 名称、财产是什么 以及文件上所说的 是分析师的读物; 文档中存在指定位置。

ID	简称	对象	文稿怎么说	出处
A02	密钥交换的服务器认证	客户端 C 被保证持有预共享主机密钥 K_S 的服务器真的运行此密钥交换,客户端只接受此运行	密钥交换使用明确的服务器认证:服务器用其主机密钥在交换散列上签名,客户端对照预先共享的主机密钥进行验证.	rfc4253:812, rfc4253:1430, s0011, s0028, s0079, s0082, s0083
A03	商定交换散列投入	客户端和服务器接受约定角色的会话,I_C,I_S,K_S,Q_C,Q_S和K,均受交换散列H的约束.	交换散列是V_C,V_S,I_C,I_S,K_S的散列,交换值和K,它认证了密钥交换.	rfc4253:1176, s0006, s0011, s0082, s0091
A04	注射协议和独特的会话 id	每个客户端接受对应不同的服务器运行,会话标识符(第一次交换散列)不会在会话中重复	第一个密钥交换的散列是独特的会话标识符; 使用同一会话id的两次会让数据包在它们之间重新播放,因此其独特性就是重新播放保护的基础。	rfc4251:841, rfc4251:857, s0035, s0061, s0074

ID	简称	对象	文稿怎么说	出处
A08	固定配置文件绑定谈判算法	客户只接受KEXINIT有效载荷I_C和I_S命名为sntrup761x25519-sha512的会话,两个有效载荷都装入H,因此无法从另一会话中取走。	方法名称由本文档固定,名称列表先用首选算法订购,KEXINIT有效载荷进入交换散列.	s0003, s0007, s0012, s0033, s0034, s0091
K01	会话密钥和主机密钥	共享的密钥 K, 生成的会话密钥和服务器主机的私密密钥从网络攻击器中保存	加密和完整性密钥为HASH的K,H和一个方向字节; 运输提供保密和完整性保护,并进行服务器主机认证。	rfc4251:652, s0011, s0063, s0064, s0067, s0070
K04	按方向和会话按键分隔	IVs和两个方向的加密和完整性密钥是不同的,一个会话的密钥是不同的,另一个会话的密钥是不同的.	6个值中每个值用自己的字母散列,所有密钥和IVs在重置时重置.	s0064, s0065, s0066, s0067, s0068, s0069, s0100
C01	会话密钥的转发性	在会话结束后获得服务器主机私钥的攻击者不会学习 K 或该会话的会话密钥	SSH密钥交换与ephemeral Diffie-Hellman给出前向保密:会话保持安全,即使私人密钥材料后来被披露,但如果会话密钥被披露,则不会.	rfc4251:1021, rfc4251:1026, s0061, s0063, s0100
C04	混合组件泄漏保存密钥	攻击者获得X25519电子元值或sntrup761 KEM 个会话的秘密密钥 仍然没有学会 K 或该会话的密钥	共享的秘密是...SHA-512散列轴线 sntrup761密钥输出与X25519产出; 文档中写道,披露 Diffie-Hellman 的私人参数会揭示会话密钥,这就是为什么单方询问混合体的一个组件的原因.	s0004, s0008, s0009, s0011, s0015
D01	接受的签名约束交换	客户端接受的签名是服务器通过使用预共享主机密钥制作的运行交换散列的签名,所以H或K_S都无法更改	服务器用主机密钥标出H,客户端验证K_S真的是S的主机密钥,并验证H上的签名,签名应用到H上.	s0011, s0082, s0083, s0093
C04.10	一个部件漏漏保留了密钥	如果攻击者获得一个会话的KEX元元件(X25519电子平面值,或sntrup761 KEM秘密密钥),仍然不学习K或会话密钥.	混合体共享两个元件, 所以每个元件单独留下另一个保护K; 文档中不显示此组件属性。	s0004, s0008, s0009, s0011
A03.11	主机密钥和散列绑定	在被接受的会话中,主机的公用密钥K_S和交换散列(会话标识符)是生成它们的服务器运行的散列; 两者都无法替换	H覆盖了K_S的交换值,客户端对照预先共享的键检查所提供的主机密钥,会话标识符是第一个H.	s0011, s0061, s0082, s0091
A08.12	与会话绑定的角色和算法	双方的角色和算法字段I_C,I_S客户端接受的是此运行中的操作,不能被另一个会话的替换 。	KEXINIT名列表载有发送者的首选算法和随机饼干,有效载荷被捆绑在H,在重新交换时角色不得改变.	s0033, s0034, s0036, s0099
X01	交换散列保密	切换会话的散列 H(会话标识符), 远离网络攻击器	'这个值叫做交换散列,用来验证密钥交换. 交易所的hash SHOULD 被保密。 '	rfc4253:1176, s0092

分析者依据文稿补充的性质：X01.

文稿里的安全表述，逐段去向

宿主把文稿里说明协议保护什么、防什么的章节逐段列出，共 97 段；分析者对每一段说明了去向：定为性质、定为攻击者条件，或者为什么都不选。选了 17 段，没选 80 段。列哪些段落由标准的章节结构决定；每一段的去向是分析者的判断。

段落	出处	定为	不选的原因
P01	主机: 159-160	没有陈述目标	指出RFC4251、RFC5656、RFC7748和RFC8731的安全考虑; 这些文件的每个内容都列在下文自己的条目中。
P02	主机: 162-170	证明器问不了	关于sntrup761(IND-CCA2)的计算强度的主张,符号模型是不能问的.
P03	主机: 172-175	证明器问不了	限制装置的通信规模和计算费用:资源主张,而不是运行财产。
P04	主机: 177-181	证明器问不了	安保水平与curve25519-sha256的比较:计算主张。
P05	主机: 183-188	证明器问不了	K 大纳姆编码的侧通道, 由字符串编码解决 ; 侧式频道在符号模型之外.
P06	主机: 190-193	证明器问不了	安全性取决于适当的随机数据:一种对随机性源的假设,由模型作出而不是检查.
P07	rfc4251:648-650	没有陈述目标	解释如何收集SSH套文件的安全考虑因素; 说不出什么来。
P08	rfc4251:652-655	A02, A03, A04, K01, K04	
P09	rfc4251:657-662	不在范围内	用户认证协议; 任务不包括用户认证。
P10	rfc4251:664-669	不在范围内	连接协议:通道,转发和子系统,在密钥交换之外.
P11 至 P12	rfc4251:673-694	证明器问不了	PRNG型的随机数据的质量和数量:一个象征模型作出的假设,而不是它可以检查的属性.

段落	出处	定为	不选的原因
P13	rfc4251:698-701	不在范围内	向用户显示错误时过滤控制字符; 非密钥交换的一部分。
P14	rfc4251:707-721	不在范围内	批量密码的选择; 传输密码位于任务所选择的固定密钥交换配置文件之外。
P15 至 P32	rfc4251:723-818	不在范围内	"无"密码器和CBC/IV(Rogaway)攻击用他们的TCP例:记录层密码器模式,在任务选择的关键交换器之外.
P33 至 P35	rfc4251:822-835	K01, K04	
P36 至 P38	rfc4251:839-862	A04	
P39	rfc4251:864-887	不在范围内	记录层序列号作为MAC的输入和包装:记录层的计数器不在模型密钥交换之外.
P40 至 P46	rfc4251:891-989	A02, A03, D01, `unverified_host_key`	
P47 至 P49	rfc4251:993-1009	证明器问不了	拒绝提供服务和机会。
P50	rfc4251:1013-1017	证明器问不了	通过贴板和SSH_MSG_IGNORE的隐蔽通道:不能作为模型的财产来表示.
P51	rfc4251:1021-1035	C01, `host_key_leak`	
P52	rfc4251:1037-1042	C04, `x25519_ephemeral_leak`	
P53	rfc4251:1046-1051	没有陈述目标	关于按强度排列算法名称清单的建议; 声明任何必须运行。
P54	rfc4251:1063-1071	证明器问不了	信息长度的流量分析; 长度在符号模型之外,例子涉及用户认证中的密码长度.
P55 至 P57	rfc4251:1075-1090	不在范围内	关于可接受的方法的用户认证协议和服务器政策.
P58 至 P60	rfc4251:1094-1118	不在范围内	假设用户的认证可以计算出它所运行的传输.
P61	rfc4251:1122-1139	不在范围内	用户认证时调试消息 。
P62 至 P64	rfc4251:1143-1169	不在范围内	地方安全政策和对用户请求的授权; 被任务排除在外。
P65 至 P67	rfc4251:1171-1182	不在范围内	假定公钥用户认证(客户端主机和服务器主机私人密钥不失密); 用户认证不在此列。 一个宿主密钥泄漏的运输侧问题被问到C01.
P68 至 P69	rfc4251:1186-1194	不在范围内	密码认证.
P70	rfc4251:1198-1201	不在范围内	基于主机的用户认证.
P71 至 P72	rfc4251:1219-1232	不在范围内	连接协议的终点安全 。
P73 至 P79	rfc4251:1236-1287	不在范围内	代理和X11转发.
P80	rfc4253:1428-1431	A02, A03, A04, K01, K04	
P81	rfc4253:1433-1434	没有陈述目标	说明建筑文件中的全部安全考虑。
P82	rfc5656:708-712	没有陈述目标	继承了SSH项安全考虑; 说明该简介没有补充任何内容。
P83 至 P86	rfc5656:714-751	证明器问不了	椭圆曲线参数的强度和离散对数问题:计算安全.
P87 至 P90	rfc5656:753-786	证明器问不了	曲线和散列大小的匹配:计算强度选择.
P91 至 P92	rfc5656:788-795	证明器问不了	相信建议曲线的安全级别。
P93	rfc5656:797-803	证明器问不了	要求麻黄私密密钥来自适当播种的PRNG:关于随机源的假设.
P94	rfc8731:165-166	没有陈述目标	继承指针.
P95	rfc8731:168-177	证明器问不了	优势为Curve25519和Curve448以及散列选择:计算.
P96	rfc8731:179-185	证明器问不了	来自共享密钥的 mpint 编码的侧通道, 通过字符串编码在本文档中解决 ; 侧式频道在符号模型之外.
P97	rfc8731:187-190	没有陈述目标	建议采用这一曲线和套房; 部署建议。

性质目录，逐条去向

性质是从一份安全和隐私性质目录起草的。起草时有 33 条没选，分析者把它们逐条过了一遍：作为性质在这里检查，或者写明原因不检查。检查了 9 条，没检查 24 条。“文稿没有提到”不能作为不检查的原因。

条目	目录里的性质	作为哪条性质检查	不检查的原因
K02	载荷与端到端保密性	不在范围内	应用有效载荷保密; 任务不包括用户认证和传输上方的数据。
K03	强保密／秘密值不可区分性	证明器问不了	ProVerif年通过不干涉程序使用的自由名称要求严格保密; 这里的会话密钥是从新麻黄中计算出来的,所以不能不修改协议而设置。K01和C04的秘密询问,约束了攻击者对它的了解.
A01	对端曾参与性（ 寿命)	A02	
A05	隐式密钥认证	K01	
A06	显式密钥确认	不适用	协议没有关键确认信息; NEWKEYS开关密钥,文档则声明有明确的服务器认证.
A07	身份—凭据—密钥绑定	A03, D01	
R01	认证／挑战新鲜性	A04	
R02	消息级抗重放	A04	
R03	业务操作至多一次	不适用	密钥交换不会进行最多一次必须进行的业务操作.
R04	消息接受顺序／窗口安全	不在范围内	消息排序和接受窗口属于记录层的序列号,而模型密钥交换不包括这些序列号.
R05	抗降级／安全策略保持	A08	
C02	抗密钥泄露冒充（KCI）	不适用	一个同行的泄露会让攻击者冒充一个未拆开的一方,没有长期的证明:唯一长期的密钥是服务器的主机密钥,其泄露会让攻击者充当同一个服务器.
C03	已知密钥安全／泄露隔离	C04	
C05	泄露后安全恢复（PCS）	不适用	协议没有鼠标或回收机制; 密钥重交换重算密钥,但文件并不声称在妥协后收回担保。
C06	注册凭据泄露后的增强认证	不在范围内	任务不包括用户认证和注册记录.
C07	抗离线字典攻击	不在范围内	没有密码或其他低调的秘密参与模拟密钥交换.
C08	指定原语失效下的目标保持	C04	
Z01	授权执行正确性	不在范围内	业务授权不在密钥交换之外,用户认证不在此列.
Z02	委托权限不扩张	不在范围内	模拟交流中没有授权或代理授权。
Z03	授权与身份／会话／操作绑定	不在范围内	没有模拟授权令牌或服务会话。
Z04	撤销与过期生效	不在范围内	在模拟交换中没有撤销或过期。
Z05	跨租户／跨服务安全隔离	不在范围内	在模拟交换中,没有租户或共享服务。
S01	加密 0nonce 唯一性 (中文(简体)).	不在范围内	AEAD非塞属于记录层的密码,而不是密钥交换.
S02	重传／密钥重安装安全	K04	
S03	抗回滚与状态单调性	不在范围内	密钥交换没有可回滚的版本或柜台; 会话标识符仍按定义固定。
S04	跨阶段安全上下文一致性	不在范围内	在模拟交换中,没有缓存或迁移的安全环境。
S05	终止与旧状态失效	不在范围内	运输的终止和拆卸不在模拟关键交换范围之外。
P01	身份匿名性	不适用	服务器身份是预先共享的主机密钥,不隐藏; 客户身份不在范围。
P02	会话不可关联性	不适用	协议并不声称无法连接,会话共享长期主机密钥.
P03	用户／凭据存在性隐藏	不在范围内	用户和证书的存在属于用户认证,被排除在外.
V01	条件性进展／错误恢复	证明器问不了	密钥交换的有条件进步是活性财产,而不是要求证明器.
V02	无非预期死锁	证明器问不了	不陷入僵局是一种生活财产。
V03	受限资源滥用／抗放大	证明器问不了	资源消耗和放大是数量性质。

参与方和受保护的值，逐项是否设为攻击者条件

宿主把起草的性质里点到的参与方和受保护的值逐项列出，共 19 项；分析者对每一项说明了哪个攻击者条件控制这个参与方或持有这个值，或者为什么不设。设了攻击者条件的 3 项，没设的 16 项。清单来自性质本身；每一项怎么处理是分析者的判断。

ID	参与方或值	类别	攻击者条件	不设的原因
S01	客户端 C	参与方	`x25519_ephemeral_leak`, `kem_secret_leak`	
S02	服务器 S	参与方	`host_key_leak`	
S03	攻击者	参与方	攻击者得不到更多	网络上的攻击者是分析的基线攻击者.

ID	参与方或值	类别	攻击者条件	不设的原因
S04	服务器身份	值	攻击者得不到更多	服务器身份是预先共享的主机公钥,一种公共价值; 在A02和A03中,可以问到什么,客户没有证实其关联的情况是unverified_host_key攻击者,超出侧面假设.
S05	汇兑散列 输入字段	值	攻击者得不到更多	V_C,V_S,I_C和I_S,交换值Q_C和Q_S以及主机公用密钥都是电线上的公用价值.
S06	共享秘密 K	值	按定义全部失守	已经持有一个会话 K 的攻击者从定义上学习该会话的密钥; 2. 文档中说,一旦会话密钥被披露,前端保密就不会存在。
S07	会话标识符	值	攻击者得不到更多	文件规定,会议编号可以公开,而不损害安全; 他们要求的交换散列的秘密 是增加的进球交换散列的秘密。
S08	协商算法字段	值	攻击者得不到更多	商谈的算法名称清单是公开的; 他们的会期是A08人。
S09	KEXINIT 载荷 I_C、I_S	值	攻击者得不到更多	KEXINIT有效载荷在清空中飞行; 它们的约束力是A08和A03。
S10	会话加密密钥	值	按定义全部失守	拥有会话加密密钥的攻击者解密会话; 除会话外,没有其他东西要靠它,因为密钥是按会话分开的(K04).
S11	会话完整性密钥	值	按定义全部失守	持有会话完整性密钥的攻击者可在会话内伪造; 除了那场会议之外,别无他法。
S12	服务器主机私钥	值	`host_key_leak`	
S13	方向密钥	值	按定义全部失守	持有一个会话方向键的攻击者有该会话的交通键; 其他会话由于密钥分离而未受影响(K04).
S14	会话密钥	值	按定义全部失守	举行届会的关键是文件排除了预先保密的妥协。
S15	历史会话密钥	值	按定义全部失守	以往届会的举行仅输掉该届会的密钥; 其他会话的密钥是K04年要求的交叉会话分离.
S16	交换散列 H	值	攻击者得不到更多	H是公共价值的散列物和K; 持有不会暴露会话密钥,文档中称会话id可以公开. 网络攻击者不知道这是 增加的进球交换散列保密。
S17	主机公钥 K_S	值	攻击者得不到更多	主机公钥为公钥,由本剖析的假设预先与客户共享.
S18	签名	值	攻击者得不到更多	一个会话的交换散列的签名是公开的,不转至另一个会话,其散列不同(A04).
S19	角色	值	攻击者得不到更多	每一方的作用由发起交易所的人确定,不是一方持有的价值; 文件的规则是,角色不得改变,为了重新交换,这个模型不会解开。

每条性质在各攻击者条件下的答案

攻击者是分析师的,在写出询问之前设定的; 每一个答案都记录在其中之一下。 牢房是攻击者的财产的证明器答案; "无答"是攻击者设定的,用于证明器未裁定索偿或无记录的财产; 2. 空单元格是分析师没有为财产设定的攻击者。

攻击者	持有什么	依据	出处
`network`	只有网络:它读、丢、更改和发送消息,并且不为一方保密		
`host_key_leak`	服务器的长期主机签名密钥(私人) , 在会议结束后获得 。	远期保密讨论:即使私人密钥材料后来被披露,但会话仍保持安全,但不会被披露; ephemeral 参数可以在交换后丢弃.	rfc4251:1021, rfc4251:1037
`x25519_ephemeral_leak`	在一个会话(客户端,或服务器端,b)中获取的X25519 ephemeral 私人值,该会话在会话期间或之后获得	文档称,如果客户端和服务器的Diffie-Hellman私人参数被披露,会话密钥会被披露.	rfc4251:1037
`kem_secret_leak`	一次客户会的sntrup761 KEM秘密密钥,该密钥在会中或会后获得	KEM型是杂交车的另一部分; 文件上写着它的IND-CCA2目标 但只字不提它的秘密泄露 所以必须问杂交体内部的部件泄露	s0008, s0009, s0011, s0015
`unverified_host_key`	向未验证服务器与其主机密钥之间的关联的客户端提供自己的主机公钥的能力	这些文件指出,如果一个主机与其主机密钥之间没有可靠的联系,协议本身就不安全,容易受到中层人的攻击; 所分析的配置文件假定有一个预共享的可信任主机密钥 。	rfc4251:891, rfc4251:984

ID	`network`	`host_key_leak`	`x25519_ephemeral_leak`	`kem_secret_leak`	`unverified_host_key`
A02	成立				
A03	成立				
A04	成立				
A08	成立				
K01	成立				
K04	成立				
C01		成立			
C04			无答案	成立	

ID	network	host_key_leak	x25519_ephemeral_leak	kem_secret_leak	unverified_host_key
D01	成立				
C04.10			无答案	成立	
A03.11	成立				
A08.12	成立				
X01	成立				

关于证明和模型的说明

- C04:在ProVerif中回答,分析师的名字是dh_algebra。
- C04.10:在ProVerif中回答,分析师的名字是dh_algebra。

一个简化代数的ProVerif型号(xor,dh_algebra,other_algebra)给予攻击者少于实际操作:一个证明有针对较弱攻击者的证据,一个攻击有攻击. 一个ProVerif模式,不检查一个值变化(changing_state),让各方接受更多的:一个证据存在,攻击可能只有缺失的支票. Tamarin + 代理型号是这些。

分析师给目标取了什么名字?

步骤	目标	特性	原因：
56	A02, A03, A04, A08, K01, K04, C01, D01, A03.11, A08.12, X01	plain_primitives, many_sessions	每个答案都基于一个只有散列、MAC、KDF、签名、KEM理想的公用密钥加密和X25519的普通密钥协议的模型; 证明书和一份未答复的主张只要求开庭次数和初步交换时间。
57	C04, C04.10	dh_algebra, plain_primitives	C04和C04.10问一个泄露的密钥交换部件买到什么:一个持有X25519exponent的攻击者是否能够用它来对抗迪菲-赫尔曼值,所以答案取决于DH代数,而这个模型只有g^xy=g^yx. KEM 一半相同的目标 是一个简单的原始。 在那里发现的攻击会维持在协议中,但X25519一方的证据只是针对模型允许的较弱的代数攻击者,这就是为什么这一说法没有结果.

分析员的结语

SSH sntrup761x25519-sha512的13个目标都有答案,没有发现. 为初始密钥交换的任意会话证明11个目标,每个会话有一个控制查询,ProVerif伪造:客户端只接受一个会话,一个使用已签名的共享主机密钥运行的服务器,每个会话接受匹配一个截然不同的服务器运行,客户端从未接受另一个方法名,共享密钥以及衍生的加密和完整性密钥保持秘密,两个方向和不同会话从未共享一个密钥或IV,在会话结束后对一个主机密钥进行前置保密,交换散列则停留在攻击者无法到达的地方. 两个目标(C04和C04.10,用户对一个漏掉的密钥交换组件的提问)只在sntrup761方面得到回答:漏掉KEM密钥仍然留下了由X25519保护的密钥,这一点已经得到证明,但关于漏掉X25519麻黄的反面说法却没有结果,被记录为未定,因此一半需要验证器来模拟代数的原样. 哪些阻断了其余部分:关于交换散列值本身的协议是通过服务器的KEXINIT cookie和签名的散列来解答的,因为直接函证查询并没有在ProVerif(30 s)中终止; 并且没有目标基于一个跨步骤变化的值,所以重交换不在模型之外,在极限中列出.