TLS混合型PSK-DHE恢复情况的安全分析

rfc10024 — ProVerif+ 代理 报告

文稿	量子后传统(PQ/T) TLS 1.3(协议定义）; 运输层安全(TLS)协议版本1.3(辅助))
检查的性质	12 条：12 条成立，0 条不成立
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

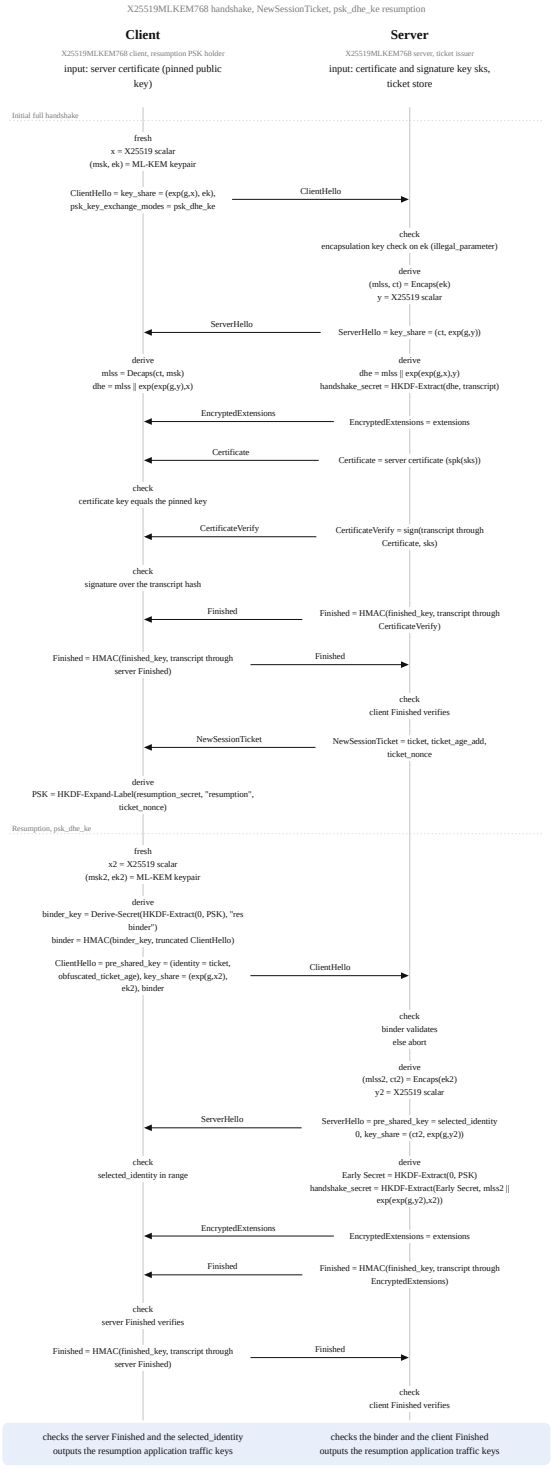
简介与TLS 1.3恢复了X25519MLKEM768密钥交换. 客户端和服务器首先运行由服务器证书认证的全握手方式; 2. 服务器再发放一张票, 接下来的连接恢复到psk_dhe_ke 使用票面代表的PSK。 客户端持有被绑定的服务器证书密钥,其ephemeral X25519 scalars及其ML-KEM密钥对; 2. 服务器持有其证书和签名密钥及其签发的门票。

每次交换结束时,双方握有相同的握手和应用程序交通密钥,知道相同的车票身份,并确认同行计算了相同的笔录. 在恢复时,客户端确定它正在和它在原始握手方式中检查证书的服务器交谈,服务器确定客户端持有罚单和绑定器,尽管证书和签名都没有再次发送.

双方:

- **客户**:X25519MLKEM768客户端,恢复PSK持卡人. holds:服务器证书(绑定公钥).
- **Server**:X25519MLKEM768服务器,售票员. 持有:证书和签名密钥滑雪,售票店.

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。

在所分析的范围内,概况将目标要求的每一个财产都保留下来:所有12个目标都得到证实,没有一个是伪造的,没有发现。 文件对协议、保密、恢复PSK的远期保密、单一泄露的关键交换部件下的混合财产以及票和绑定器装订等内容,在一次完全握手后机械地复制,然后是一次恢复。 结果依赖于模型的简化:一个客户端和一个服务器运行,一个定型的KEM,攻击者无法应用的单向散列函数,以及没有重播商店. 需要证明服务器保存整个会话门票的模型,然后才能说出重复使用一张门票的情况。

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
A03	**恢复会议关键协议。** 每当客户端（或服务器）在psk_dhe_ke恢复握手中接受会话，就存在一个匹配的对端运行，双方对相互身份、所选 PSK身份、协商组与 key_share、以及 笔录派生的握手密钥一致。	无	成立	中	是
A04	**不重播复航航班。** 每次恢复握手成功接受都对应一个不同的对端运行；同一 ClientHello- 宾德或同一 完成(E)不能被接受两次。	无	成立	低	是
A08	**不可替换参数。** 恢复握手接受的协商参数（组、key_share PSK 身份、transcript) 对应本次会话的提议与上下文，不能被替换为其他会话或其他 PSK 的值。	无	成立	中	是
K01	**secree of PSK and traffic keys.** 攻击者不能推导 恢复 PSK binder_key 握手流量密钥或应用流量密钥。	无	成立	中	是
C01	**PSK漏气为较早的届会所用。** 在恢复会话完成后泄露 重置 PSK 不暴露此前完成的会话密钥或应用数据。	恢复PSK(会话完成之后)	成立	中	是
C03	**从PSK和原始密钥中分离出重置密钥。** 泄露 重置 PSK 或原始会话应用流量密钥，不暴露恢复会话的应用流量密钥。	恢复 PSK 或原始会话应用流量密钥 (恢复握手期间或之后)	成立	中	是
C04	**一个破损的KEX组件备用密钥。** 泄露恢复握手中的 X25519 临时私钥或 ML-KEM 私钥之一，恢复会话密钥仍保密。	X25519 临时私钥或 ML-KEM 私钥 (恢复握手期间)	成立	中	是
S04	**恢复继承了原来的上下文。** 恢复会话的身份、PSK 与密钥上下文正确继承自原始握手，不被错接到其他会话。	无	成立	低	是
A08.9	**PSK和捆绑在服务器和文字记录上。** 恢复握手中接受的 PSK/binder 绑定到原服务器身份与恢复 transcript.	无	成立	中	是
U01	**单一泄漏会留下恢复密钥的秘密。** 分别泄露 重置 PSK 或单个新 KEX 分量，恢复会话密钥是否仍保密。	PSK 或单个新 KEX 分量 (恢复握手期间)	成立	中	是
C03.11	**连接间隔离的应用密钥。** 恢复会话应用密钥与原始会话应用密钥相互隔离，泄露一方不暴露另一方。	原始会话或恢复会话应用流量密钥 (恢复握手期间或之后)	成立	中	是
X01	**握手会给出不同的会话键。** 没有两个不同的会话产生相同的恢复应用程序流量密钥:如果客户端的会话和服务器的会话命名为同一个密钥,则这两个会话是同一个会话.	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: 恢复 PSK/binder 与原服务器身份和恢复 transcript 绑定(中文(简体)).	是:服务器接受的绑定器精确地绑定了客户端发送的ClientHello,客户端只从一个会话中提取一个PSK,其中验证了服务器的证书密钥和CertificateVerify签名,因此PSK和绑定器被绑定在原始服务器身份和恢复记录上.	A08.9, S04, A08
Q2: PSK 或单个新 KEX 分量泄露的独立影响	单是泄漏了恢复PSK号,单是X25519号麻黄板,或单是ML-KEM号解封密钥就从来不给恢复会话密钥,因为握手密钥是从PSK号中提取的,密钥交换结果和笔录的调和.	U01, C04, C01
Q3: 恢复与原始会话应用密钥隔离	两种连接通过单向导出从不同的主密钥中获取其应用流量密钥,因此持有原连接的应用程序流量密钥不会给恢复连接的密钥,持有恢复密钥不会给原服务器对客户端的密钥; 2. 其余方向没有回答。	C03.11, C03, C01

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:

- 一个客户端进程和一个服务器进程,没有复制:重放ClientHello,装订器或完成器进入第二个会话,以及重新使用一张票来进行几次恢复,都不属于模型范围.
- KEM型具有定型(封装不随机性),其解封密钥是一个普通的名称,因此KEM型断层攻击,密码长检查和封装密钥检查的模型不能超越中止.
- KDF型机车所用的散装、装配和散装是攻击者自己无法应用的私人功能; 因此,攻击者在所了解的价值观上略弱于现实。
- X25519是单定律g^xy=g^yx的模型; 2. 没有显示曲线的其他代数属性,也没有全零共享的秘密检查。
- 票龄携带但未检查:ticket_lifetime,除污obfuscated_ticket_age及任何验收窗口均不仿制,不设目标.
- 0-RTT,跨组售票,基于证书的客户端认证,关键更新和手摇后信息不属于任务范围,没有建模.
- PSK,X25519scalar,ML-KEM拆卸密钥和交通密钥在运行后分别分期放置,每一次漏漏查询也包括了梯子较早的漏漏漏; 攻击者在会话中取得价值并干扰其作用的,只是大致的.
- 恢复的交通密钥泄露的方向和原始连接的客户端对服务器密钥必须保密,没有回答; 2. 只有原始连接的服务器对客户端密钥被覆盖在那里,因为一个模型不能泄露一个值并同时保密.

主持人记录的是什么:

- 解读后答案有变:A04,K01,C03,U01.

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.

A03:续会关键协议

每当客户端（或服务器）在 psk_dhe_ke恢复握手中接受会话，就存在一个匹配的对端运行，双方对相互身份、所选 PSK身份、协商组与 key_share、以及 笔录派生的握手密钥一致。

在恢复中,双方以同一握手键结束,该键来自PSK,既有关键股,也有全部笔录,因此双方同意选择的PSK身份,股份和笔录衍生的密钥. 服务器的接受意味着客户端运行匹配交换机,客户端的接受意味着服务器在同一密钥下发送完成,控制显示当客户端的消息从未到达服务器时,查询能够失败.

- 结果:持有; 回答问题:是的; 可用备注
- 数值介质:RFC 9846 附录F.1要求完成握手后在两侧输出相同的会话键; 2. 模型证实它恢复,没有增加任何弱点。
- 在文件中说明:是的。 文件上说:rfc9846:6478
- 休息:一个客户端和一个服务器进程,不重复运行; X25519 by g^xy = g^yx; 仅由 g^xy = g^yx ; 记录是私人散列 攻击者无法重算
- 下一步:一个同时举行几次届会的模式将测试各届会是否达成同样的协议

A04:不重播复航航班.

每次恢复握手成功接受都对应一个不同的对端运行；同一 ClientHello/binder 或同一 完成 不能被接受两次。

此目标的答案在此读取后有所改变.

每一次服务器接受一个客户端完成对应一个不同的客户端运行,所以在模式交换中一个完成没有接受两次. 该型号有一个单一的服务器会话,没有售票店,所以它没有说客户端重放一个ClientHello和装订器,或一张票,进入第二个会话.

- 结果:持有; 回答问题:部分; 可用备注
- 低值:RFC 9846 附录F.1 要求不同握手之间有独特的会话键; 这里的注入协议来自每个会话的新鲜密钥股份,而不是来自重播检查.
- 在文件中说明:是的。 文件上说:rfc9846:6495
- 休息:一个服务器进程,不复制; 没有售票店,也没有单一用途的执法模式,因为任务将重新播放存储超出范围
- 打开: 在两次服务器会话中接受相同的票和绑定器
- 下一步: 解开一个服务器, 将一个售票店保存在多个恢复站上

A08:无法替换的恢复参数

恢复握手接受的协商参数（组、key_share、PSK身份、记录)对应本次会话的提议与上下文，不能被替换为其他会话或其他 PSK的值。

服务器只有在其绑定器验证时才接受ClientHello,绑定器是MAC,在PSK衍生出的密钥下超过截断的ClientHello,因此密钥股,售票身份和模糊的年限都无法不经过检测而改变. 恢复ServerHello的参数也包含在同样的论证中,因为握手键双方都会得到整本记录稿的校正.

- 结果:持有; 回答问题:是的; 可用备注
- 中值:RFC 9846要求在PSK关键单位之前验证装订器,并声明完成的MAC防止降级; 模型显示替换失败 。
- 在文件中说明:是的。 文件上说:rfc9846:6499
- 休息:装订本和记录,模拟为MAC份,在公共领域使用散列链; 只有X25519MLKEM768组是谈判的,所以降级到另一个组不是模拟的
- 下一步:无

K01: 保密 PSK和交通密钥

攻击者不能推导 恢复 PSK binder_key 握手流量密钥或应用流量密钥。

此目标的答案在此读取后有所改变.

PSK,绑定键和两种连接的应用流量键都远离只控制网络的攻击者. 他必须倒置KDF或获得密钥共享秘密,在模型中也不可能.

- 结果:持有; 回答问题:是的; 可用备注
- 数值介质:RFC 9846 附录F.1规定,共享的会话密钥只应告知通报方; 2. 这就是询问所证实的。
- 在文件中说明:是的。 文件上说:rfc9846:6483
- 休息:KDF和记录散列是攻击者不能适用于已知输入的单向函数; X25519 由 g^xy = 仅 g^yx ; KEM是决定性的 它的斩首由客户的种子按键
- 下一步:无

C01: PSK 较早开庭时的漏气零部件

在恢复会话完成后泄露 恢复 PSK 不暴露此前完成的会话密钥或应用数据。

原连接完成后所学的PSK恢复功能并不暴露该连接的应用流量密钥. PSK号机车来自复机密令,该密令仅从一个方向从主机密令中降下,因此交通密钥无法从中重算.

- 结果:持有; 回答问题:是的; 可用备注
- 数值介质:RFC 9846 附录F.1指出,连接N的恢复密钥与连接N的交通密钥是分开的,因此后来的妥协没有达到它们.
- 在文件中说明:是的。 文件上说:rfc9846:6504
- 休息时间:PSK型机车在运行后被泄露,处于单独阶段; KDF号是单向的; 单凭PSK型机车,没有交通密钥
- 下一步:无

C03:与PSK和原密钥分离的恢复键

泄露 恢复 PSK 或原始会话应用流量密钥， 不暴露恢复会话的应用流量密钥。

此目标的答案在此读取后有所改变.

恢复的PSK和原连接的应用流量键都没有给出恢复连接的应用流量键. 恢复主密钥将PSK号机身与新混合共享密钥和新抄本混为一谈,因此已知的PSK号机身或已知的早期密钥不复制.

- 结果:持有; 回答问题:是的; 可用备注

- 数值介质:RFC 9846 附录F.1准确描述了连接之间的这种分离; 证据证实了它的侧写。
- 在文件中说明:是的。 文件上说:rfc9846:6551
- 休息:恢复密钥股票是新产生的,在这些查询中从未漏出; KDF是单向的
- 下一步:无

C04:一个破损的KEX元件零部件密钥

泄露恢复握手中的 X25519 临时私钥或 ML-KEM 私钥之一， 恢复会话密钥仍保密。

泄露客户端的X25519麻黄石板,或复刊的ML-KEM解封密钥,并不给复刊会话密钥,因为握手密钥是从两个关键交换结果与PSK和笔录的交接中提取出来的,没有单个组件决定. 这是配置所依赖的混合属性 。

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:RFC 9954 第6节要求混合共享秘密保持安全,同时一个组件密钥交换没有中断,RFC 10024则依赖它进行X25519MLKEM768.
- 在文件中说明:是的。 文件上说:rfc9954:550
- 休息:每个泄露的值在运行后给出; ML-KEM的查询还提供了PSK和X25519号标尺; 混合密钥是两个组成密钥的简单缩合,没有长度前缀或进一步混合
- 下一步:无

S04:恢复继承原上下文.

恢复会话的身份、PSK 与密钥上下文正确继承自原始握手， 不被错接到其他会话。

PSK名客户在复会中主动提出,这是在一次已完成的握手式NewSessionTicket中收到的,而罚单和PSK是从这一联系的复会秘密中衍生出来的,所以复会继承了原来的上下文,而不是另一届的上下文. 客户端还将票绑定到它认证的服务器上.

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:RFC 9846 附录F.1指出,绑定器将PSK绑定在它建立时的会话上,这是查询通过结构证实的.
- 在文件中说明:是的。 文件上说:rfc9846:6585
- 休息时间:每台服务器运行一票; 服务器从 PSK 本身获得, 因此没有模拟整个会话的门票查询
- 下一步:无

A08.9:PSK和捆绑在服务器和记录稿上

恢复握手中接受的 PSK/binder 绑定到原服务器身份与恢复 transcript. [永久失效連結] (中文(简体)).

服务器接受的绑定器是客户端所发送的ClientHello的MAC,因此PSK与恢复式的笔录捆绑在一起,客户端仅在其核实服务器证书和CertificateVerify的会话中接受一张罚单. 因此,一张票仍然附着在发行该票的服务器上,并附着在它的握手方式上.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:RFC 9846 附录 F.1规定,绑定器将PSK绑定在目前的握手架和建立它的会话上,并警告说与第二个端点共用的PSK是不安全的.
- 在文件中说明:是的。 文件上说:rfc9846:6585,rfc9846:6600
- 休息: 单一绑定的服务器证书密钥; 一个客户端和一个服务器进程
- 下一步 两台服务器接受对方的罚单 将直接测试PSK-FINISHED警告

U01:单漏叶恢复密钥

分别泄露 恢复PSK或单个新 KEX分量，恢复会话密钥是否仍保密。

此目标的答案在此读取后有所改变.

PSK恢复中的任何单次泄漏,客户端的X25519麻黄板和ML-KEM解首键都留下了恢复会话的关键秘诀. 因为每个查询也把攻击者交给了梯子上较早的径流,所以答案一次覆盖了不止一个漏出的值.

- 结果:持有; 回答问题:是的; 可用备注
- 中值:RFC 9846 附录F.1和RFC 9954 第6节规定了向一个方向泄漏的这些限制; 模型证实它们恢复使用。
- 在文件中说明:是的。 文件上说:rfc9846:6562,rfc9954:550
- 休息:在运行后分不同阶段进行漏泄; 编号KEM是决定性的,其共同的秘密是服务器所选择的新值; 编号PSK-仅查询处于一个阶段,即X25519斯卡拉还不知道,但是...ProVerif相位计数也承认后期的漏水
- 打开:每个查询也包括阶梯较早的泄漏,所以答案比一次泄露更强
- 下一步:每个漏漏的漏漏

C03.11: 连接间分离的应用程序密钥

恢复会话应用密钥与原始会话应用密钥相互隔离，泄露一方不暴露另一方。

原连接的应用程序流量密钥不给出恢复连接的应用程序流量密钥,恢复密钥不给出原连接的服务器对客户端密钥. 两把密钥通过单向衍生而来自不同的主密.

- 结果:持有; 回答问题:是的; 可用备注
- 数值介质:RFC 9846 附录F.1指出连接之间的分离; 模式可以同时维持的两个方向都得到证明。
- 在文件中说明:是的。 文件上说:rfc9846:6551
- 休息:第二个方向是原连接的服务器对客户端密钥的回答,模型不会泄露; KDF是单向的
- 下一步:无

X01:不同的握手会给出不同的会话键

没有两个不同的会话获得相同的恢复应用程序流量密钥:如果客户端的会话和服务器的会话命名为同一个密钥,那么这两个会话是同一个会话.

两个名为同一应用程序流量密钥的复会是同一会话. 每个运行中新鲜的混合密钥股份使得密钥不同.

- 结果:持有; 回答问题:是的; 可用备注
- 数值低:RFC 9846 附录F.1要求不同的握手产生不同的,无关的会话键.
- 在文件中说明:是的。 文件上说:rfc9846:6495

- 休息:会议名称是会议最后记录; 一个客户端和一个服务器进程
- 下一步:无

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
A03	proved		a03_srv	检查		证明:2
A04	proved		a04_inj	检查		证明:2
A08	proved		a08_sub	检查		证明:1
K01	proved		k01_psk	检查		证明:5
C01	proved		c01	检查		证明:1
C03	proved		c03	检查		证明:3
C04	proved		c04_x	检查		证明:2
S04	proved		s04	检查		证明:1
A08.9	proved		a08_sub	检查		证明:2
U01	proved		u01_psk	检查		证明:4
C03.11	proved		c03	检查		证明:2
X01	proved		x01	检查		证明:1

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
A03	服务器侧协议:当服务器接受恢复(客户端完成验证)时,一个客户端用相同的PSK和相同的握手键hs2运行恢复,该键修正了记录,选择的PSK身份和两个关键股	network	proved	a03_srv	检查
A03	客户端协议:当客户端接受服务器恢复后完成,服务器以相同的PSK和相同的握手键hs2发送,因此双方就PSK的身份,密钥股份和笔录衍生的密钥达成一致.	network	proved	a03_cli	检查
A04	关于恢复的注入协议:服务器对一个客户端的每次接受完成都对应不同的客户端运行; 在模拟交换中,无法接受两次完成的相同数据。	network	proved	a04_inj	检查
A04	关于恢复的注入协议:服务器对一个客户端的每次接受完成都对应不同的客户端运行; 同一完成的无法接受两次	network	proved	a04_inj	检查
A08	使用有效绑定器接受的 ClientHello 服务器完全是一个客户端发送的:绑定器和两个密钥共享都无法替换	network	proved	a08_sub	检查
K01	PSK的恢复被双方所知 仅针对网络上的攻击者	network	proved	k01_psk	检查
K01	PSK的绑定键是针对网络攻击者的秘密	network	proved	k01_binder	检查
K01	原始连接的应用程序流量密钥是针对网络攻击者的秘密	network	proved	k01_orig	检查
K01	恢复连接的握手和应用程序交通密钥是针对网络攻击者的秘密	network	proved	k01_res	检查
K01	恢复连接(手摇和应用程序)的应用程序流量密钥是针对网络攻击者的秘密	network	proved	k01_res	检查
C01	原连接的应用流量密钥在攻击者持有在连接完成后学到的 PSK 恢复时保密	psk_leak	proved	c01	检查

目标	主张	攻击者	回答	查询	对照
C03	当攻击者持有恢复的PSK时,恢复连接的应用流量密钥将保密(在此查询中,恢复密钥份额的私人一半也将保密)	psk_leak	proved	c03	检查
C03	当攻击者持有原始连接的应用程序流量密钥时,恢复连接的应用程序流量密钥将保密	orig_app_key_leak	proved	c03	检查
C03	当攻击者持有恢复的PSK时,恢复连接的应用交通密钥将保密(在本查询中,还有恢复的X25519号标尺和ML-KEM号标尺)	psk_leak	proved	c03	检查
C04	当攻击者持有客户端的X25519 ephemeral scalar 恢复密钥份额时,恢复应用程序流量密钥将保密(在本次查询中,还持有PSK的恢复)	x25519_scalar_leak	proved	c04_x	检查
C04	当攻击者持有客户恢复密钥份额的ML-KEM解首密钥时,恢复应用程序流量密钥将保密(在本查询中,还有PSK和X25519scalar)	mlkem_sk_leak	proved	c04_kem	检查
S04	PSK客户在恢复时使用 是在完成握手的NewSessionTicket中收到的 所以恢复继承了原来的背景 而不是另一个会话	network	proved	s04	检查
A08.9	服务器接受的绑定器 绑定客户端发送的确切的ClientHello(笔录), 所以PSK 和绑定器 绑定在恢复记录中	network	proved	a08_sub	检查
A08.9	客户端接受PSK输入 aNewSessionTicket只在它验证服务器证书密钥和证书的会话中CertificateVerify签名,所以PSK与原始服务器身份绑定	network	proved	a089_srv	检查
U01	恢复会话键在恢复会话漏漏的X25519平时保密(本查询中的攻击者也持有PSK)	x25519_scalar_leak	proved	c04_x	检查
U01	当恢复漏水的ML-KEM解首键(本查询中的攻击者还持有PSK和X25519 scalar)时,恢复会话键会保密.	mlkem_sk_leak	proved	c04_kem	检查
U01	当PSK次复会泄露时,恢复会话密钥将保密	psk_leak	proved	u01_psk	检查
U01	复会密钥在PSK次复会被泄露时保密	psk_leak	proved	u01_psk	检查
C03.11	泄露恢复连接的应用程序流量密钥不会暴露原连接的应用程序流量密钥(服务器对客户端方向,从不泄露)	res_app_key_leak	proved	c0311b	检查
C03.11	泄露原连接的应用程序流量密钥不会暴露恢复连接的应用程序流量密钥	orig_app_key_leak	proved	c03	检查
X01	获得相同恢复应用程序流量密钥的两会是同一会话	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-20261115T080741, 2026-11-15. 状态: 完成 。 型号:deepseek-v4-1-flash-261017. 台阶:66,校对:311 s,壁19 min,耗资0.158 USD.

背景:主机从谈话中移除了1时间(s),总共删除了453010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:93 证明运行,93 决定,0 未答,230 s,45 答录.

分析了什么

协议	TLS 混合型 PSK-DHE 恢复型简介
版本	rfc10024
分析范围	一次完整 X25519MLKEM768 握手得到 重置 PSK 再一次 psk_dhe_ke 恢复；保留 年龄/身份 binder.transcript 和新 key_share; 2. 不包含 0-RTT,样板 跨集群分发、抗重放存储的无界保证。
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512个编号段落(135022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	4	谈判小组
主体	4.1	客户份额
主体	4.2	服务器共享
主体	4.3	共享机密
rfc9846	4	握手协议
rfc9846	4.1	译名哈什
rfc9846	4.2	密钥交换信件
rfc9846	4.2.1	密码谈判
rfc9846	4.2.2	客户端 你好
rfc9846	4.2.3	服务器 你好
rfc9846	4.2.4	你好 重试请求
rfc9846	4.3	扩展
rfc9846	4.3.1	已支持的版本
rfc9846	4.3.2	饼干
rfc9846	4.3.3	签名算法
rfc9846	4.3.4	证书管理机关
rfc9846	4.3.5	OID 滤镜

文稿	章节	标题
rfc9846	4.3.6	手摇后基于证书的客户端认证
rfc9846	4.3.7	支助团体
rfc9846	4.3.8	密钥共享
rfc9846	4.3.8.1	迪菲-地狱人参数
rfc9846	4.3.8.2	ECDHE 参数
rfc9846	4.3.9	共享前密钥交换模式
rfc9846	4.3.10	早期数据指示
rfc9846	4.3.11	共享前密钥扩展
rfc9846	4.3.11.1	售票时间
rfc9846	4.3.11.2	PSK 宾德尔
rfc9846	4.3.11.3	处理顺序
rfc9846	4.4	服务器参数
rfc9846	4.4.1	加密扩展
rfc9846	4.4.2	证书请求
rfc9846	4.5	认证信件
rfc9846	4.5.1	证书
rfc9846	4.5.1.1	OCSP 现状和SCT 延期
rfc9846	4.5.1.2	证书选择
rfc9846	4.5.1.3	接收证书信件
rfc9846	4.5.2	证书验证
rfc9846	4.5.3	完成(E)
rfc9846	4.6	早期数据的结束
rfc9846	4.7	手摇后信件
rfc9846	4.7.1	新建会话车票消息
rfc9846	4.7.2	手摇后验证
rfc9846	4.7.3	键和初始化矢量更新
rfc9846	7	密码计算
rfc9846	7.1	密钥时间表
rfc9846	7.2	更新交通秘密
rfc9846	7.3	交通密钥计算
rfc9846	7.4	非对称共享秘密计算
rfc9846	7.4.1	自由球场迪菲-地狱人
rfc9846	7.4.2	椭圆曲线 迪菲-地狱人
rfc9846	7.5	出口商

协议的目的是在文档中将其定位为源步骤:一次完整 X25519MLKEM768握手得到 恢复PSK，再一次psk_dhe_ke恢复；保留 售票年龄/身份、binder、transcript和新 key_share；不包含 0-RTT盘点跨集群分发、抗重放存储的无界保证。

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
A03	复会关键协议	客户端和服务器同意PSK身份,关键股权,笔录和他们从psk_dhe_ke恢复中获得的握手密钥	RFC 9846 附录F.1要求握手方式在每个端点完成时,双方输出相同的一组会话键.	rfc9846:6478
A04	没有恢复飞行的重播	每一次被接受的恢复都对应不同的同行运行; ClientHello 个装有装有装有的装有的装有的装有的装有的装满的装有的装的装的装的装有的装有的装的装的装的装的装的装有的装有的装有的装有的装的装有的装的装有的装的装有的装有的装的装有的装的装的装的装的装的装的装有的装有的装有的装的装的装的装有的装的装的装有的装有的装有的装的装的装有的装有的装的装的装有的装的装的装的装的装的装的装的的装有的装的	RFC 9846 附录F.1 要求在明显的握手之间提供独特的会话键,第4.5.3节要求接受者拒绝一个不验证的完成的会话键.	rfc9846:6495, s0399
A08	不可替换的恢复参数	在复会中接受的PSK个身份和笔录 是本届会议的,不是另一届会的,也不是另一张罚单的	RFC 9846要求降级保护(双方的密码参数相同),并声明完成的MAC防止降级; 4. 绑定器将PSK绑在目前的握手架上.	rfc9846:6499, rfc9846:6627, rfc9846:6585
K01	保密 PSK和交通密钥	恢复 PSK 绑定键 握手和应用程序 交通键只为双方所知	RFC 9846 附录F.1:共享的会话密钥应只为通信方所知,而非攻击方所知.	rfc9846:6483

ID	简称	对象	文稿怎么说	出处
C01	PSK 早会时的漏气	连接完成后获得的恢复 PSK 并不显示原始连接的密钥或应用数据	RFC 9846 附录 F.1 将恢复式 PSK 视为长期密钥材料,对此需要预先保密,并指出恢复式连接的密钥N与连接式N的交通密钥是分开的.	rfc9846:6504, rfc9846:6551
C03	与PSK和原始密钥隔离的还原密钥	恢复连接的应用流量密钥,当攻击者知道恢复 PSK 或原连接的应用流量密钥时	RFC 9846 附录 F.1:连接N+1所需的恢复密钥与连接N的交通密钥是分开的,因此连接控件之间的前向密钥,在较早时的妥协在不对称密钥机构重新运行时不会在稍后时给出密钥.	rfc9846:6551, rfc9846:6562
C04	一个破损的 KEX 元件配件密钥	恢复会话键,当攻击者持有X25519平方尺或恢复会话键的ML-KEM解首键时	RFC 9954 第6节: 只要至少有一个元件密钥交换算法没有断裂,混合共享密钥是安全的; 2. RFC 10024 以此为根据的 X25519MLKEM 768.	rfc9954:550, s0015, s0018
S04	恢复继承原上下文	车票身份 PSK 以及恢复使用的关键上下文是原始的握手方式 而不是另一张连接或另一张车票	RFC 9846 附录 F.1:绑定器在PSK号,目前的握手式和PSK号的成立会期之间形成约束,过渡性地包括了握手式的原始记录.	rfc9846:6585
A08.9	PSK和捆绑在服务器和记录稿上	PSK和装订器 恢复接受 与签发罚单的服务器身份 和恢复记录	RFC 9846 附录 F.1规定,绑定器将PSK绑定在目前的握手架和建立它的会议上,并警告说,一个与第二个终点共用的PSK是不安全的(PSK-FINISHED建造).	rfc9846:6585, rfc9846:6600
U01	单漏漏漏漏漏漏漏漏漏漏漏漏漏漏	恢复会话键 一旦攻击者掌握了PSK的恢复键之一, 客户端的X25519 麻黄板, 或客户端的ML-KEM 斩首键	RFC 9846 附录 F.1 修正一个方向的泄漏给定的东西(在T1妥协时,当不对称的密钥机构重新运行时,在T2不给密钥) RFC 9954 第6节给出了混合要求.	rfc9846:6562, rfc9954:550

ID	简称	对象	文稿怎么说	出处
C03.11	连接间分离的应用程序密钥	原始连接和恢复连接的应用程序流量密钥,一个针对另一个的泄漏	RFC 9846 附录F.1:连接N的恢复密钥与连接N使用的交通密钥分开,提供连接之间的前方密钥.	rfc9846:6551, rfc9846:6573
X01	不同的握手会给出不同的会话键	关于恢复握手程序流量密钥的客户端和服务器	RFC 9846 附录F.1:任何两种不同的握手方式都应产生不同的,无关的会话密钥,由握手方式生成的单个会话密钥应不同且独立.	rfc9846:6495

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 15 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 3 段，没选 12 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: 268-271	A03, A08, S04, A08.9	
P02	主机: 273-276	证明器问不了	指导侧通道耐药性实施; 附带渠道和执行质量不在象征性协议模式之外
P03	主机: 278-280	证明器问不了	公共密钥、密码和共享秘密的固定长度:编码财产,无任何痕迹
P04	主机: 282-287	证明器问不了	向客户披露ML-KEM封装的随机性,并载有RNG号产出; 模型理想化,不能说RNG状态
P05	主机: 289-297	证明器问不了	攻击始于公布无保障的RNG的产量; 随机性质量没有建模
P06	主机: 299-306	C04, U01, `x25519_scalar_leak`	
P07	主机: 308-310	证明器问不了	两种算法共用一个不安全的RNG: 大约RNG状态,不可建模
P08	rfc9846:4676-4677	没有陈述目标	附录C、E和F的指针; 说明没有自己的财产;
P09	rfc9954:550-558	C04, U01, `x25519_scalar_leak`, `mlkem_sk_leak`	
P10 至 P15	rfc9954:560-597	证明器问不了	IND-CCA2安全 KEM,恒长编码,以及散列和KDF的定时或碰撞抵抗特性:密码假设和执行属性,没有一个符号跟踪模型可以决定

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 23 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 10 项，没设的 13 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	参与方	攻击者得不到更多	被损坏的客户端只持有自己的PSK和自己的会话键; 没有目标询问其他当事人对客户的保证, 因为此配置文件不认证客户
S02	服务器	参与方	`psk_leak`	
S03	恢复 PSK	值	`psk_leak`	
S04	绑定器	值	攻击者得不到更多	绑定器在ClientHello的清晰度中发出, 所以握住它除了网络攻击者之外什么也给不了。
S05	笔录	值	攻击者得不到更多	记录稿是用公开握手信息制作的
S06	key_share	值	攻击者得不到更多	关键份额是公开的; 它们是S18和S19的条目
S07	握手流量密钥	值	按定义全部失守	K01只要求网络攻击者不能获得握手交通密钥; 一旦这些密钥被给出,这被定义为丢失了,没有文件要求针对已经持有这些密钥的攻击者提供保护
S08	完成(E)	值	攻击者得不到更多	完成值在电线上,是攻击者没有的密钥下的MAC
S09	车票身份	值	攻击者得不到更多	车票身份为PSK人身份; 没有目标要求连接不能连接
S10	协商组	值	攻击者得不到更多	谈判小组是公开的
S11	PSK 身份	值	攻击者得不到更多	PSK的身份是罚单,在清空时发出
S12	binder_key	值	按定义全部失守	K01要求绑定键不能由网络攻击者得出; 从定义上说,放弃它就失去它,没有文件要求更多
S13	应用流量密钥	值	`orig_app_key_leak`, `res_app_key_leak`	
S14	会话密钥	值	`orig_app_key_leak`, `res_app_key_leak`	
S15	应用数据	值	`orig_app_key_leak`, `res_app_key_leak`	
S16	原始会话应用流量密钥	值	`orig_app_key_leak`	
S17	恢复会话应用流量密钥	值	`res_app_key_leak`	
S18	X25519 临时私钥	值	`x25519_scalar_leak`	
S19	ML-KEM 私钥	值	`mlkem_sk_leak`	
S20	恢复会话密钥	值	按定义全部失守	C04和U01要求当一个关键交换组件泄露时,恢复会话密钥应保密; 一个持有会话的攻击者 自己会失去它 顾名思义,没有文件要求它
S21	PSK	值	`psk_leak`	
S22	会话上下文	值	攻击者得不到更多	会议背景包括公开握手信息
S23	服务器身份	值	攻击者得不到更多	服务器的证书是公开的

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		
psk_leak	(a) 从服务器的售票店或从连接完成后得知的连接恢复PSK; PSK的恢复是超过连接的长期密钥材料	RFC 9846 附录 F.1 将外部或恢复的PSK视为长期密钥材料,其握手后的妥协不得打破会话密钥,并讨论存储在数据库中的门票.	rfc9846:6504, rfc9846:6547
x25519_scalar_leak	从端点获得的或由被动观察者用加密相关量子计算机回收的恢复握手键份额的 X25519 电子平面 私人平面	RFC 10024 第6节规定,任何带有量子计算机的被动观察者都可以回收ECDH 麻黄石板,RFC 9954 第6节要求混合密钥在一个部件断裂时保持安全.	主机:299,rfc9954:550
mlkem_sk_leak	属于客户在恢复握手中的关键份额的 ML-KEM 拆弹密钥	RFC 9954 第6节要求混合共享秘密保持安全,只要两个元件的密钥交换器之一没有断裂,这就是这个泄漏测试的方法.	rfc9954:550, s0015
orig_app_key_leak	原始连接的应用程序流量密钥, 在连接完成后获得	RFC 9846 附录 F.1限制密钥泄漏在一个方向的影响,并声明在交通秘密泄露后,保护重新运行的不对称密钥机构。	rfc9846:6562, rfc9846:6573
res_app_key_leak	恢复连接的应用程序流量密钥,在它完成后获得	RFC 9846 附录F.1指出,在后期折中一个密钥不会在更早时给出一些密钥.	rfc9846:6562

ID	network	psk_leak	x25519_scalar_leak	mlkem_sk_leak	orig_app_key_leak	res_app_key_leak
A03	成立					
A04	成立					
A08	成立					
K01	成立					
C01		成立				
C03		成立			成立	
C04			成立	成立		
S04	成立					
A08.9	成立					
U01		成立	成立	成立		
C03.11					成立	成立
X01	成立					

关于证明和模型的说明

分析师给目标取了什么名字?

步骤	目标	特性	原因 :
55	A03, A04, A08, K01, C01, C03, C04, S04, A08.9, U01, C03.11, X01	plain_primitives, 其他类	每一份答复都以散列、MAC、KDF、KEM和Diffie-Hellman作为与单项法律g^xy=g^yx的简单关键协议; KEM是决定性的(没有封装随机性),记录片散列功能是私密的,因此攻击者既不能自己计算记录片散列,也不能利用分布的KEM. 该模型运行一个客户端和一个服务器进程而不复制,因此重播和跨会话答案(A04,X01,S04)只为该单曲运行而持有,并且对一个保存会话间票的服务器不说任何内容.

分析员的结语

该型号为全X25519MLKEM768握手式,后为psk_dhe_ke恢复型号(型号. pv,一个客户端和一个服务器进程,26事件,找到正常运行. 所有12个目标都得到回答,每个目标都得到ProVerif的证明,没有伪造,每个证明都包含一个模型伪造的控制查询,所以没有发现.

设立:双方商定PSK身份、密钥股份、笔录和衍生密钥(A03(二) 双向; 绑定器不能替换,只有在证书之后才能取票,而且CertificateVerify检查,并恢复PSK总是来自完成的握手(A08,A08.9,S04); 不同的会话给出不同的应用密钥(X01),每个服务器接受匹配一个不同的客户端运行(A04(在一届会议内举行)。 保密性问题PSK,绑定键和交通键对网络攻击者持有(K01). 复会PSK之后学到的不会暴露原始连接的密钥( ) 。C01), aPSK漏出或漏出的原始应用程序密钥不给恢复密钥(C03),而且两者都不是X25519斜线或斜线ML-KEM单是解封密钥就能提供恢复密钥,即使与PSK(C04,U01——混合财产.RFC9954问曰. 两个连接的应用密钥在双向隔离,线性漏漏梯级可以保持(C03.11).

哪些屏蔽了完整答案:模型运行一个客户端和一个服务器而不复制,并且没有保留售票店,所以重放到第二个会话中,再使用一张票(A04,以及X01和S04的交叉会话部分)在它之外; KEM是决定性的,记录和KDF散列是攻击者不能适用的私人功能,X25519只有定律 g^xy = g^yx,票龄和寿命被携带但没有检查. 漏水在运行后分不同阶段放置,每个查询也持有梯子早期的漏水,这使得答案比单次漏水更强,但相伴. 证明复播问题需要使用一个服务器在会话间保存票的模型; 没有任何目标依赖于一个不断变化的计数器,因此不需要有界限的模式,也不需要国家审查。