TLS混合客户端证书简介的安全分析

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	14 条：14 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

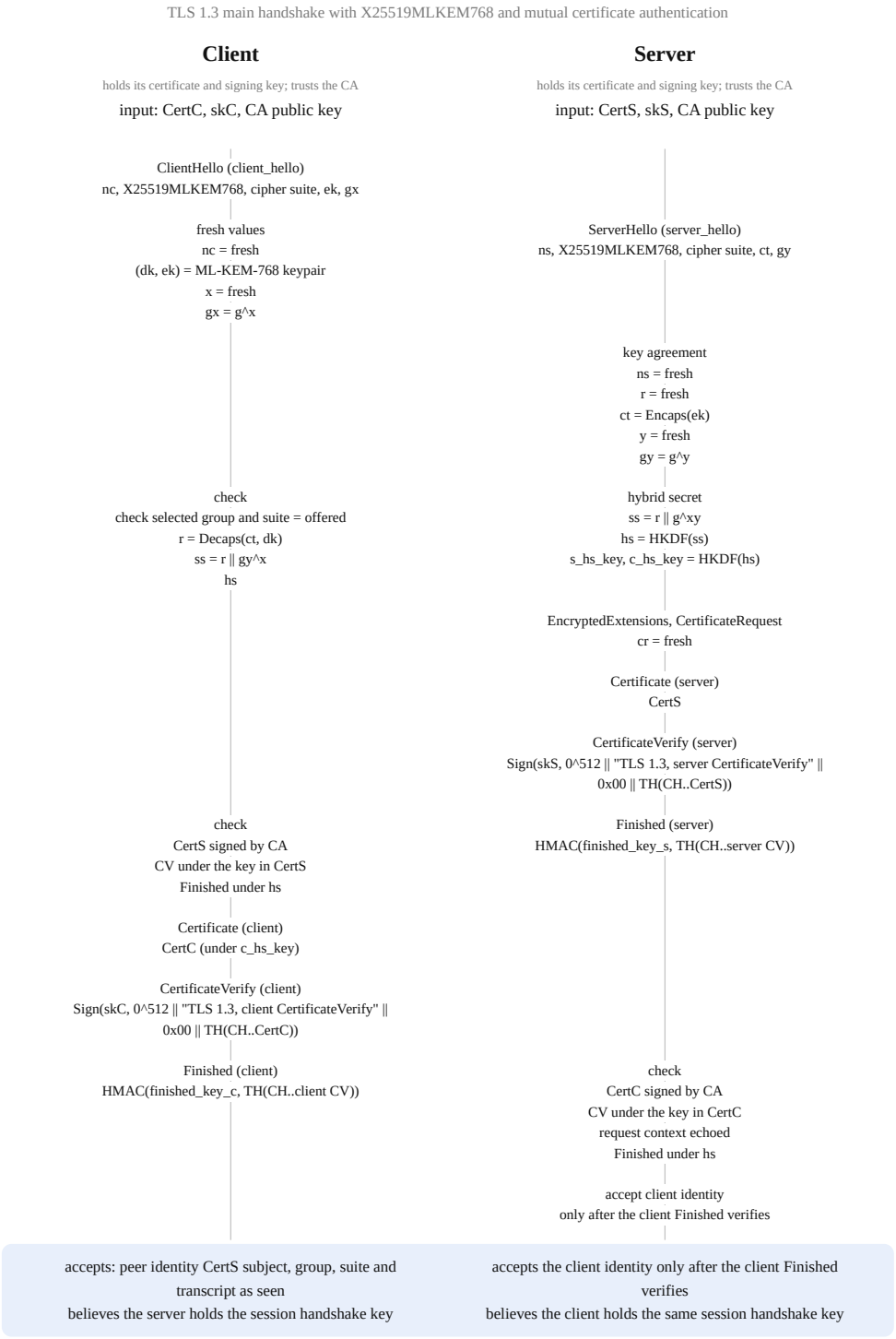
剖面图确定了一个关键协议,X25519MLKEM768,和证书认证双向TLS1.3握个手 一个客户端和一个服务器各持有一个证书及其签名密钥,两者都信任一个证书权威. 客户端发送ML-KEM封装密钥和一个X25519共享; 服务器用一个ML-KEM密码和它自己的X25519每一方都从两部分获得一个秘密。

服务器然后用CertificateVerify的签名和完成的检查值来证明它的身份; 客户端检查和以自己的证书(CertificateVerify)回复,并完成,服务器只有在验证客户端完成后才接受客户端的身份。 当交换结束时,客户端确定服务器的身份和记录誊本,服务器确定客户端的身份,谈判参数和共享会话密钥.

双方:

- **客户**:持有其证书和签名密钥; 信任CA号. 持有:CertC,skC,CA公用密钥.
- **公务员**:持有证书和签名密钥; 信任CA号. 持有:CertS,skS,CA公用密钥.

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。

在模拟范围内,简介做了它要做的事:相互认证、就身份、组别、套件和记录稿达成协议、注入协议、关键确认、角色区别、长期密钥和会话密钥的保密、前向保密和针对一个破碎的密钥协定组成部分的混合安全,所有这些在任何会议上都得到了证明。 未报告调查结果; 所检查的每个财产都是文件本身要求的,分析发现文件没有说明攻击。 证据依赖于理想化的原始物(一种不透明ML-KEM,X25519,只有g^xy = g^yx),在证书路径上验证模型摘要离开. 有两个警告限制了其影响范围:几个认证证明没有控制能力,在泄露的-服务器-键世界中,攻击者也没有获得绑定键的证书,因为这个世界并没有在ProVerif年终止.

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	**对等点进行相互认证。** 客户端接受服务端证书与 完成 时，服务端确实以该客户端为对象运行过；服务端在验证客户端 完成 后接受客户端身份时，客户端确实以该服务端为对象运行过。	无	成立	中	是
A03	**关于记录和参数的协议。** 客户端接受时与服务端运行在身份、协商组、套件和握手 transcript 上一致；服务端接受客户端身份时与客户端运行在同样的值上一致。 (中文(简体)).	无	成立	中	是
A04	**每种接受的握手方式的独特性。** 服务端每次接受客户端身份、客户端每次接受服务端，都对应不同的对端协议运行，同一握手证据不能被重复接受。	无	成立	低	是
A06	**已完成确认握手键。** 客户端验证服务端 完成 时，服务端确实持有本次会话的握手密钥；服务端验证客户端 完成 时，客户端确实持有同一会话的握手密钥。	无	成立	低	是
A07	**被接受的身份与签名密钥持有人相符。** 接受方认定的对端身份与对端证书主体、以及实际持有签名私钥的实体一致。	无	成立	中	是
A08	**未替换的谈判参数。** 接受方接受的组、套件、CertificateVerify 角色标签与 transcript 对应双方本次提议与协商结果，不被替换或错接。	无	成立	中	是
K01	**长期密钥和交通密钥的保密性。** 客户端与服务端的长期签名私钥、以及本次会话派生的握手与应用流量密钥，除合法持有者外不可被推导。	无	成立	中	是
C01	**过去会话密钥的保密性。** 会话完成并擦除握手秘密之后，泄露双方长期签名私钥不暴露此前会话的流量密钥。	客户端与服务端长期签名私钥 (会话完成并擦除握手秘密之后)	成立	低	是
C02	**关键妥协假冒抵抗。** 客户端长期签名私钥泄露后，攻击者不能冒充服务端使客户端接受；服务端长期签名私钥泄露后，攻击者不能冒充客户端使服务端接受客户端身份。	受害方长期签名私钥 (受害方继续诚实执行的前提下)	成立	中	是
C08	**如果一个组件失败,则安全性差。** 在 X25519 部分或 ML-KEM 部分之一失效（其共享秘密被攻击者获得）时，双方认证与流量密钥保密仍成立。	X25519 或 ML-KEM 共享秘密 (握手期间)	成立	中	是
U01	**CertificateVerify 角色分离.** 客户端与服务端各自接受对端 CertificateVerify 时，签名由对端以对端角色标签对本次 transcript 生成，不可反射或跨方向混用。 (中文(简体)).	无	成立	中	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
A06.12	**服务器接受意味着客户持有密钥。** 服务端验证客户端 完成 并接受客户端身份时，客户端确实持有本次会话的握手密钥。	无	成立	低	是
C02.13	**单侧长期密钥泄漏.** 分别泄露客户端或服务端长期签名私钥时，攻击者不能冒充未泄露的对端使对方接受。	客户端或服务端长期签名私钥 (单端泄露，另一端未泄露)	成立	中	是
X01	**从网络中隐藏客户证书。** 对手握网络（可读可写全部握手记录）的攻击者，客户端证书的值不出现在他能获得的数据中；即客户端身份在主动攻击者面前也受保护。	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: 双向身份认证不可反射/混用签名方向	这两个方向不能混为一谈:双方在笔录上分别签上不同的上下文字符串,每个方向都用对等证书的密钥进行验证,所以一个角色的签名在另一个角色中从未被接受; ProVerif 证明这一点,任何会议次数。	U01, A02
Q2: 客户端认证完成条件与会话密钥绑定	服务器仅在客户端完成验证后才接受客户端身份,在会话下手握键下检查值为HMAC,因此接受意味着客户端持有相同的手握键; 这已经证明。	A06.12, A06
Q3: 仅泄露一端长期认证密钥的影响分别检查	泄露客户端的长期签名密钥不会让攻击者冒充服务器给该客户端,泄露服务器密钥不会让其冒充客户端给服务器; 两者都得到证明,第二个是持有密钥但不能装订密钥的证书的攻击者。	C02, C02.13, K01

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:

- ML-KEM部分是一个不透明的封装:模型对计算或后量子安全,密码长度,封装-键检查或解封失败都只字未提.
- X25519系仿照单定律g^xy=g^yx; 2. 全零和低序检查不是模拟的。
- 证书有CA个身份和密钥签名; 路径验证,撤销,名称限制和密钥使用被抽象化,双方信任一个CA.
- 只有客户机飞行受模型中记录层的保护; 2. 服务器飞行是纯文本,所以端点识别保护只要求客户端证书.
- 一个组和一个密码套件是模拟的,因为配置图可以固定它们; 无法在模型中降低到另一组或套房的等级。
- 手摇后认证,HelloRetryRequest,PSK,0-RTT,KeyUpdate,会场门票和警报不在模型范围之内,因此无法分析可区分的故障行为.
- 在折中作用中,一个角色实例的会话共享瞬间密钥-协议值,这使得攻击者比协议中更强大.
- 在泄露的服务器键世界中,攻击者持有签名键,但不持有将其与服务器身份相连的证书; 给予它证书使得ProVerif的搜索没有终止,所以答案是针对一个略微弱的攻击者.
- 时机、可得性和资源消耗不要求采用这一模式。

主持人记录的是什么:

- 没带对照查询的证明（附录 C）：A02: auth_client, A02: auth_server, A03: auth_client, A03: auth_server, A04: inj_client, A04: inj_server, A06: auth_client, A06: auth_server, A07: auth_client, A07: auth_server, A08: auth_client, A08: auth_server, K01: sess_secret, C01: sess_secret, C02: auth_client_x, C02:

auth_server_leakedsrv, C08: kem_broken, C08: dh_broken, C08: auth_client, C08: auth_server_any, A06.12: auth_server, C02.13: auth_client_x, C02.13: auth_server_leakedsrv。 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:对等方相互认证

客户端接受服务端证书与 完成 时，服务端确实以该客户端为对象运行过；服务端在验证客户端 完成 后接受客户端身份时，客户端确实以该服务端为对象运行过。

两个方向都坚持住。 一个接受服务器的客户端已经与一个真正用同样的记录进行握手的服务器进行了交谈,服务器只有在拥有该证书的客户端运行之后才接受客户端身份. 客户端无法得知服务器接受其证书,因为TLS 1.3没有发出确认函.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:剖面图的中央保证,机器检查过任意一个会话,但在理想化的原始人和抽象的PKI上
- 在文件中说明:是的。 文件上说:rfc9846:6490
- 休息:客户机飞行作为加密处理,服务器飞行作为模型中的普通文本处理; 所有证书都是CA-签发的,路径验证是抽象的; KEM的秘密只有用斩首密钥才能找到; X25519 仅含 g^xy = g^yx
- 下一步:无

A03:就记录和参数达成协议

客户端接受时与服务端运行在身份、协商组、套件和握手 transcript 上一致；服务端接受客户端身份时与客户端运行在同样的值上一致。 (英语).

客户端和服务器在相同的身份,组,套件和笔录上结束运行. 由于签名和两个完成值都覆盖了笔录散列,改变任何握手消息的一方必须产生一个值,在同行证书密钥下进行验证.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:这是配置文件所依赖、经机械证明的绑定值; 固定组是指在模型中不能出现降级到另一个组的情况
- 在文件中说明:是的。 文件上说:rfc9846:6499
- 以简洁文本握手信息上的散列链为模型的语录; 模型中的固定组和套房
- 下一步:无

A04:每个被接受的握手的独特性

服务端每次接受客户端身份、客户端每次接受服务端，都对应不同的对端协议运行，同一握手证据不能被重复接受。

每种接受都与对等方的不同:不能两次接受握手证据,无论是哪种方向。 这取决于双方在笔录上 刚开始的无名小卒

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:独特性直接来自新鲜的无色和装订的文字记录; 它确认而不是添加
- 在文件中说明:是的。 文件上说:rfc9846:6495
- 休息:新非名作为绑定名称模式

- 下一步:无

A06: 完成确认握手键

客户端验证服务端 完成 时，服务端确实持有本次会话的握手密钥；服务端验证客户端 完成 时，客户端确实持有同一会话的握手密钥。

验证对等者完成的证明是,对等者在双向计算同一会话的握手键。 支票值为HMAC,在笔录上从会话秘密中衍生出来的密钥下.

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:建筑完工的直接后果,证明财产明确
- 在文件中说明:是的。 文件上写着:s0398,s0408
- 休息时间:关键时间表倒塌,从混合秘密中跌至HKDF步; 混合密钥不透明
- 下一步:无

A07:接受身份与签名密钥持有人相符

接受方认定的对端身份与对端证书主体、以及实际持有签名私钥的实体一致。

当事人接受的身份是其核实的证书的主题,它所核对的签名是用该证书的密钥作出的,所以所接受的身份属于私钥的持有人. 这是双向的。

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:身份约束是证书认证的目的; PKI 被抽象化
- 在文件中说明:是的。 文件上说:rfc9846:6490
- 证书是CA个身份和密钥签名; 未检查密钥用途和名称限制
- 下一步:无

A08:谈判参数未替换

接受方接受的组、套件、CertificateVerify 角色标签与 transcript 对应双方本次提议与协商结果，不被替换或错接。 (中文(简体)).

各方所接受的组合、套间和角色上下文串是各方输入记录誊本的,记录散列在每一个签名和完成值之内。 一个替代他们的政党需要同行的签名密钥或会话密钥.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质: 配置文件承诺参数不能被替换, 证明了它实际谈判的参数
- 在文件中说明:是的。 文件上说:rfc9846:6499
- 休息时间:一个组和一个套房,因为配置文件可以固定它们; 角色上下文字符串是不同的常数
- 打开: 降级到另一个组或套件无法测试, 因为配置文件同时修正
- 下一步: 如果配置文件允许提供替代组的客户端建模

K01:长期密钥和交通密钥

客户端与服务端的长期签名私钥、以及本次会话派生的握手与应用流量密钥，除合法持有者外不可被推导。

网络上的攻击者从未获得长期签名密钥或会话握手密钥,因此衍生的交通密钥一直保密. 控件显示,一旦一个密钥被披露,查询可能会失败.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:密钥保密为中心; 证据在于抽象的KEM 和单人法的迪菲-赫尔曼
- 在文件中说明:是的。 文件上说:rfc9846:6483
- 休息时间:混合秘密不透明,来源于两部分; 交通密钥来自会话密钥, 没有破坏器
- 下一步:无

C01:过去会话密钥的远期保密

会话完成并擦除握手秘密之后， 泄露双方长期签名私钥不暴露此前会话的流量密钥。

在握手后揭示两个长期的签名密钥并不暴露会话的握手密钥,完成会话后,会话的握手密钥不会暴露. 会话秘诀只来自两个瞬间密钥协议部分,模型与会话一同丢弃.

- 结果:持有; 回答问题:是的; 可用备注
- 值低:从新鲜的麻黄部分开始前向保密,没有显示出什么令人惊讶之处。
- 在文件中说明:是的。 文件上说:rfc9846:6504
- 休息时间:phase-1 显示会后密钥泄漏的模型; 届会结束后,不保留任何秘密
- 打开: 没有控件显示查询会失败, 因为没有角色会公布两个密钥协议的秘密
- 下一步:增加一个角色,公布两个组件的机密,以见证控制

C02:关键妥协假冒阻力

客户端长期签名私钥泄露后， 攻击者不能冒充服务端使客户端接受； 服务端长期签名私钥泄露后， 攻击者不能冒充客户端使服务端接受客户端身份。

这两半财产都没有落空。 由于客户端的签名密钥已知,该客户端仍然只接受真服务器; 有服务器的签名密钥已知,服务器对客户端的接受仍然对应真实的客户端运行. 泄露的密钥不是同行认证所依赖的密钥.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质: 已声明属性的双向得到证明, 缺少证书时会提醒服务器键的答案
- 在文件中说明:是的。 文件上说:rfc9846:6522
- 休息:通过发布持续运行的第二个客户身份的密钥来模拟泄露的客户端密钥; 泄露的服务器密钥通过发布没有绑定它的证书的密钥来建模
- 打开: 在服务器键的方向中, 攻击者没有获得将密钥绑定在服务器身份上的证书, 所以答案是针对一个略弱的攻击者
- 下一步:攻击者完成服务器握手的模型,或Tamarin+ Agent,可以解决缺少证书的案件

C08: 如果一个组件失败, 混合安全

在 X25519 部分或 ML-KEM 部分之一失效（其共享秘密被攻击者获得）时， 双方认证与流量密钥保密仍成立。

当只有ML-KEM部分失败时,当只有X25519部分失败时,会话握手键会保密,两个认证方向仍然维持不变. 攻击者需要两个组件的秘密才能到达会话密钥,这就是配置图所构建的混合属性.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:混合组的中心前景,机械显示; 组合器是自由函数,所以只检查结构

- 在文件中说明:是的。 文件中说:rfc9954:550,主:268
- 休息:通过公布一个客户身份的解封密钥和另一个客户身份的X25519代表,模拟组件故障; 结合器是一种不透明的函数,所以没有说真正的结合器的强度
- 打开: 没有控件显示会话密钥查询会失败, 因为没有角色会公布两个组件的秘密 。
- 下一步:增加一个发布两个组件机密的角色作为控制

U01:CertificateVerify 角色分离

客户端与服务端各自接受对端 CertificateVerify 时， 签名由对端以对端角色标签对本次 transcript 生成， 不可反射或跨方向混用。 (中文(简体)).

CertificateVerify的值曾经满足客户端-角色和服务器-角色检查:两个上下文字符串不同,两个键是不同的. ProVerif显示客户端从未验证过其在客户端角色中所做的签名,服务器也从未验证过其在服务器角色中所做的签名.

- 结果:持有; 回答问题:是的; 可用
- 值介质: profile 角色标签要求用机械检查, 答案不依赖于简化的原始
- 在文件中说明:是的。 文件上说: s0383
- 休息: 角色上下文字符串是不同的常数, 如配置文件所指定的
- 下一步:无

A06.12:服务器接受意味着客户端持有密钥

服务端验证客户端 完成 并接受客户端身份时， 客户端确实持有本次会话的握手密钥。

当服务器接受客户端身份时,客户端必须持有同一会话握手键,因为客户端只在该密钥下通过笔录验证. 此配置文件的规则是,客户端身份只有在客户端完成后才被接受.

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:完成施工和接受活动所在地的直接后果
- 在文件中说明:是的。 文件上写着:s0398、s0402、s0408
- 休息时间:关键时间表崩溃到HKDF步
- 下一步:无

C02.13:单侧长期密钥泄漏.

分别泄露客户端或服务端长期签名私钥时， 攻击者不能冒充未泄露的对端使对方接受。

内容与C02相同:由于客户端的签名密钥已知客户端仍然只接受真服务器,而服务器的签名密钥已知服务器仍然只接受真客户端运行.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:内容与C02相同,双向均用服务器键提醒证明
- 在文件中说明:是的。 文件上说:rfc9846:6522
- 休息:通过发布第二个客户身份的密钥来模拟泄露的客户端密钥; 已泄露的服务器密钥在没有证书的情况下模拟
- 打开: 未向攻击者提供匹配证书而解答了服务器密钥的一半
- 下一步: Tamarin+ Agent, 或与服务器握手的模型抽象化, 用于缺失的证书大小写

X01:向网络隐瞒客户证书

对手握网络（可读可写全部握手记录）的攻击者，客户端证书的值不出现在他能获得的数据中；即客户端身份在主动攻击者面前也受保护。

客户端的证书从未出现在网络攻击者可以获得的数据中:客户端证书消息在客户端握手交通密钥下,攻击者无法从中获取. 服务器的证书在本模型中作为公共数据处理.

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:由于客户航班加密,财产持有; 模型无法显示被动观察者可以随着时间的推移链接到什么
- 在文件中说明:是的。 文件上说:rfc9846:6530
- 休息:模型中只加密了客户航班,所以这里讲的是客户证书; 证书值未以其他方式公布
- 打开: 不询问客户端身份在会话之间的不关联性
- 下一步:就两个客户身份进行互不干涉查询,以解决可链接性问题

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_client			证明:2
A03	proved		auth_client			证明:2
A04	proved		inj_client			证明:2
A06	proved		auth_client			证明:2
A07	proved		auth_client			证明:2
A08	proved		auth_client			证明:2
K01	proved		secret_skC	3中的2人		证明:3
C01	proved		sess_secret			证明:1
C02	proved		auth_client_x			证明:2
C08	proved		kem_broken			证明:4
U01	proved		role_client	检查		证明:2
A06.12	proved		auth_server			证明:1
C02.13	proved		auth_client_x			证明:2
X01	proved		cert_hidden	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
A02	客户端接受服务端证书与 完成 时，服务端确实运行过该会话（对端身份与 特朗普 一致）	network	proved	auth_client	无
A02	服务端验证客户端 完成 并接受客户端身份时，客户端确实运行过该会话（对端身份与 特朗普 一致）	network	proved	auth_server	无
A03	客户端接受的服务端运行在身份、协商组、套件与 transcript 上与其一致 (英语).	network	proved	auth_client	无
A03	服务端接受客户端身份时与客户端运行在身份、协商组、套件与 transcript 上一致 (英语).	network	proved	auth_server	无
A04	每一次客户端接受服务端都对应一次不同的服务端运行，旧 飞行 不能被再次接受	network	proved	inj_client	无
A04	每一次服务端接受客户端身份都对应一次不同的客户端运行,握手证据不能被重复接受	network	proved	inj_server	无
A06	客户端验证服务端 完成 时服务端确实持有本次会话的握手密钥	network	proved	auth_client	无
A06	服务端验证客户端 完成 时客户端确实持有同一会话的握手密钥	network	proved	auth_server	无
A07	客户端认定的服务端身份与服务端证书主体一致，且签名由该证书私钥持有者生成	network	proved	auth_client	无
A07	服务端认定的客户端身份与客户端证书主体一致，且签名由该证书私钥持有者生成	network	proved	auth_server	无

目标	主张	攻击者	回答	查询	对照
A08	客户端接受的组与套件是其在 ClientHello 中提议的值，并绑定在被验证的 transcript 中 (中文(简体)).	network	proved	auth_client	无
A08	服务端接受的组、套件与 transcript 与客户端本次运行一致，未被替换 (英语).	network	proved	auth_server	无
K01	本次会话派生的握手流量密钥不可被网络攻击者推导	network	proved	sess_secret	无
K01	客户端长期签名私钥不可被网络攻击者推导	network	proved	secret_skC	检查
K01	服务端长期签名私钥不可被网络攻击者推导	network	proved	secret_skS	检查
C01	会话完成并擦除握手秘密之后泄露双方长期签名私钥，不暴露此前会话的流量密钥	ltk_after_session	proved	sess_secret	无
C02	客户端长期签名私钥泄露后（攻击者持有该私钥），攻击者不能冒充服务端使该客户端接受	leaked_client_key	proved	auth_client_x	无
C02	服务端长期签名私钥泄露后（攻击者持有该私钥；模型未一并给其该证书，故其能力弱于文档所述），攻击者不能冒充客户端使服务端接受客户端身份	leaked_server_key	proved	auth_server_leakedsrv	无
C08	ML-KEM 部分失效（攻击者获得该部分共享秘密）时，本次会话的流量密钥仍不可被推导	kem_broken	proved	kem_broken	无
C08	X25519 部分失效（攻击者获得该部分共享秘密）时，本次会话的流量密钥仍不可被推导	dh_broken	proved	dh_broken	无
C08	单一密钥交换组件失效时，客户端接受的服务端身份与运行仍为真实服务端	kem_broken	proved	auth_client	无
C08	单一密钥交换组件失效时，服务端接受的客户端身份仍对应真实的客户端运行	kem_broken	proved	auth_server_any	无
U01	客户端接受的服务端 CertificateVerify 由服务端角色生成，客户端自己的签名不会被当作服务端签名接受	network	proved	role_client	检查
U01	服务端接受的客户端 CertificateVerify 由客户端角色生成，服务端自己的签名不会被当作客户端签名接受	network	proved	role_server	检查
A06.12	服务端验证客户端 完成 并接受客户端身份时，客户端确实持有本次会话的握手密钥	network	proved	auth_server	无
C02.13	客户端长期签名私钥泄露后（攻击者持有该私钥），攻击者不能冒充服务端使该客户端接受	leaked_client_key	proved	auth_client_x	无
C02.13	服务端长期签名私钥泄露后（攻击者持有该私钥；模型未一并给其该证书，故其能力弱于文档所述），攻击者不能冒充客户端使服务端接受客户端身份	leaked_server_key	proved	auth_server_leakedsrv	无
X01	客户端证书不出现在网络攻击者能获得的数据中（客户端身份对主动攻击者亦受保护）	network	proved	cert_hidden	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-20261115T080743, 2026-11-15. 状态: 完成 。 型号:deepseek-v4-1-flash-261017. 台阶:71,校对:405 s,壁24 min,耗资0.177 USD.

ProVerif:163 证明运行,154 决定,9 未答,200 s,33 答录.

分析了什么

协议	TLS 混合客户端证书简介
版本	rfc10024
分析范围	固定 X25519MLKEM768及双方证书认证，双方 CertificateVerify角色标签及完整 记录服务端仅在验证客户端 完成(E)后接受客户端身份；排除 手动震动后验证/HRR/PSK。
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
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

文稿	章节	标题
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:固定 X25519MLKEM768及双方证书认证，双方 CertificateVerify角色标签及完整 记录服务端仅在验证客户端 完成(E)后接受客户端身份；排除 手动震动后验证/HRR/PSK。

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	相互认证对等点	客户端接受的服务端身份来自服务端证书与 CertificateVerify 完成; 服务端接受的客户端身份来自客户端证书与 CertificateVerify 完成,且在验证客户端 完成, 之后才接受（s0402 完成,完成,完成,完成,完成,完成.	rfc9846 附录 E 明列 佩尔认证:客户端的对端身份视图应反映服务端身份，若客户端被认证，服务端的对端身份视图应与客户端身份相符。（rfc9846:6490)	rfc9846:6490, s0372, s0392, s0398, s0402
A03	关于记录和参数的协议	客户端接受的服务端运行与服务端接受时的客户端运行在身份、组、套件和 transcript 上一致。 (英语).	rfc9846 明列 下级保护:密码参数在两侧应相同，且应与无攻击时相同（rfc9846:6499); CertificateVerify 覆盖 Transcript-Hash(s0376),完成覆盖 transcript(s0408).	rfc9846:6499, s0376, s0408, s0026, s0031
A04	每个接受的握手方式的独特性	每一次客户端接受服务端、服务端接受客户端身份，对应一个不同的对端协议运行；同一握手证据不能被第二次接受。	rfc9846 明列 会话唯一性 键: 任意两次不同握手应产生不同且无关的会话密钥（rfc9846: 6495); 完成 必须被校验（s0399 (中文(简体)).	rfc9846:6495, s0399, s0408
A06	完成确认握手键	服务端验证客户端 完成 时，客户端确实持有同一会话的握手密钥；客户端验证服务端 完成 时，服务端确实持有该密钥。	完成了是认证块的最后一条消息, 用于认证握手与已计算的密钥（s0398); verify_data=HMAC(finished_key),笔录(s0408).	s0398, s0399, s0404, s0408
A07	已接受的身份与签名密钥持有人匹配	接受方认定的对端身份与对端证书主体一致，且与真正持有该证书签名私钥的实体一致。	CertificateVerify用于证明端点持有其证书对应的私钥，接收方必须用证书中终端实体证书的公钥验证签名（s0372、s0392..s0396）； 同行认证要求对端身份视图相符（rfc9846:6490）。	rfc9846:6490, s0372, s0392, s0393, s0394, s0395, s0396
A08	未替换的谈判参数	接受方接受的组、套件、CertificateVerify 角色标签与 transcript 对应双方本次协商结果，不被替换或错接。 (中文(简体)).	降级保护(rfc9846:6499); 角色 康文本字符串 用于区分不同上下文的签名（s0383 ; 笔录 覆盖全部握手消息（s0026 s0031).	rfc9846:6499, s0383, s0026, s0031, s0408
K01	长期密钥和交通密钥的保密	客户端与服务端的长期签名私钥，以及本次会话派生的握手流量密钥，除合法持有者外不可被推导。	rfc9846 明列 会话密钥:共享会话密钥应只被通信双方知道（rfc9846:6483); 密钥调度见 s0455、s0474。	rfc9846:6483, s0455, s0474
C01	以往会话密钥的转发密钥	会话完成并擦除握手秘密之后，泄露双方长期签名私钥不暴露此前会话的流量密钥。	rfc9846 明列 远期密钥的前方密钥:握手完成后长期密钥被泄露不危及会话密钥，只要会话密钥及可重建它的材料已擦除（rfc9846: 6504. . 6514； s0479）。	rfc9846:6504, s0479, s0484, s0474
C02	密钥折叠性假冒阻力	泄露一端长期签名私钥后，该端对其对端的认证不被破坏：攻击者不能冒充对端使泄露方接受，也不能冒充泄露方使对端接受。	rfc9846 明列 凯伊妥协冒名顶替(KCI)阻力:在双向证书认证连接中，泄露一方的长期秘密不应破坏该方对端在该连接中的认证（rfc9846:6522. . 6528）。	rfc9846:6522, s0372, s0383

ID	简称	对象	文稿怎么说	出处
C08	如果一个组件失败, 则混合安全	X25519 部分或 ML-KEM 部分之一失效（其共享秘密落到攻击者手中）时，会话流量密钥保密与双方认证仍成立。	RFC 9954 的 hybrid 性质：只要至少一个组件密钥交换算法未被攻破，结果秘密即安全（rfc9954:550 (中文(简体)). . 553）； RFC 10024 继承同一安全考虑（main:268););););););););); 共享秘密为两部分拼接（s0015）。	rfc9954:550,主机:268,s0001,s0015,s0018
U01	CertificateVerify 角色分离	客户端与服务端各自接受对端 CertificateVerify 时，签名以对端角色标签对本次 transcript 生成，不可反射或跨方向混用。 (中文(简体)).	服务端 上下文字符串为 "TLS1.3,服务器CertificateVerify"，客户端为 "TLS1.3客户端CertificateVerify"，用于区分不同上下文的签名以防跨协议/跨方向攻击（s0383）。	s0372, s0383, s0376
A06.12	服务器接受意味着客户端持有密钥	服务端验证客户端 完成 并接受客户端身份时，客户端确实持有本次会话的握手密钥。	完成 的构造与校验要求（s0398 s0399 s0408); 服务端在验证客户端 完成 前无对端身份与活性保证（s0402 (中文(简体)).	s0398, s0399, s0402, s0408
C02.13	单侧长期密钥泄漏	分别泄露客户端或服务端长期签名私钥时，攻击者不能冒充未泄露的对端使对方接受。	KCI抗战(rfc9846:6522. . 6528）。	rfc9846:6522, s0372, s0383
X01	从网络中隐藏客户端证书	客户端证书（终端实体证书）；服务端证书同理但文档只要求对被动攻击者保护。	rfc9846明列 保护终点身份:服务端证书应对被动攻击者受保护，客户端证书应对被动与主动攻击者都受保护，因为客户端 证书在握手流量密钥下加密发送（rfc9846:6530. .6535、s0413）。	rfc9846:6530, s0413, s0402

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 40 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 4 段，没选 36 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	C08, A03	
P02	主机: 273-276	证明器问不了	NIST SP800-227 的实现指导与侧信道防护建议，非符号模型可判定的协议性质。
P03	主机: 278-280	证明器问不了	固定长度的公钥/密文/共享秘密是编码与长度性质，符号模型不含长度。
P04	主机: 282-287	证明器问不了	ML-KEM 封装随机数 m 被客户端恢复、以及它对 RNG 其他输出的影响，属于 RNG 质量与计算层性质。
P05	主机: 289-297	证明器问不了	不安全 RNG 输出被用于破坏 RNG 状态（DUALECTLS）属于随机数生成的实现性质。
P06	主机: 299-306	`dh_broken`	
P07	主机: 308-310	证明器问不了	两个算法共用同一不安全 RNG 的相互影响属实现层随机数性质。
P08	rfc5280:5226-5231	没有陈述目标	说明证书与 CRL 无需保密、可匿名获取；不构成对本协议的要求。

段落	出处	定为	不选的原因
P09	rfc5280:5233-5236	不在范围内	规范之外影响 保证金 的证书管理因素，任务范围只到主握手消息流。
P10	rfc5280:5238-5240	不在范围内	CA/RA 对主体身份与公钥绑定的核验流程，属 PKI 实践；模型把 CA 签发的证书视为合法。
P11	rfc5280:5246-5248	不在范围内	同上，依赖方查阅 CA 认证实践声明，属 PKI 实践。
P12	rfc5280:5250-5259	不在范围内	对密钥持有者的密钥用途分离建议，不是本协议消息流的性质。
P13	rfc5280:5261-5274	A07, C02, `leaked_client_key`, `leaked_server_key`	
P14	rfc5280:5276-5280	不在范围内	CA 私钥丢失与备份，属 PKI 运营。
P15	rfc5280:5282-5302	不在范围内	撤销信息的新鲜度与 CRL 处理，任务未包含撤销检查。
P16	rfc5280:5304-5311	不在范围内	信任锚的分发是带外过程，任务未包含。
P17	rfc5280:5313-5318	不在范围内	受信 CA 密钥泄露后的信任信息更新，属 PKI 运营。
P18	rfc5280:5320-5326	不在范围内	证书处理实现质量与路径验证实现，属 PKI 实现。
P19	rfc5280:5328-5334	证明器问不了	密钥长度与散列强度对绑定的限制是计算安全性质。
P20	rfc5280:5336-5339	不在范围内	名称比较规则，属 PKIX 路径验证细节。
P21	rfc5280:5347-5349	不在范围内	DN 编码一致性，属 PKIX 路径验证细节。
P22	rfc5280:5351-5356	不在范围内	nameConstraints 编码，属 PKIX 路径验证细节。
P23	rfc5280:5358-5365	不在范围内	不同名称形式之间的约束覆盖，属 PKIX 路径验证细节。
P24	rfc5280:5367-5369	不在范围内	签发者名称冲突，属 PKIX 运营。
P25	rfc5280:5371-5381	不在范围内	emailAddress 大小写匹配，属 PKIX 名称处理。
P26	rfc5280:5383-5391	不在范围内	CRL 分发点/扩展中的恶意链接，属 PKIX 客户端实现。
P27	rfc5280:5393-5397	不在范围内	https URI 造成的循环依赖，属 PKIX 实现。 请检查isbn=值 (帮助).
P28	rfc5280:5399-5406	不在范围内	CA 不应在扩展中使用 https URI,属 PKIX 运营。
P29	rfc5280:5408-5416	不在范围内	自签发证书的用途，属 PKIX 运营。
P30	rfc5280:5418-5428	不在范围内	TeletexString/Latin1String 编码差异，属 PKIX 名称处理。

段落	出处	定为	不选的原因
P31	rfc5280:5430-5437	不在范围内	字符串视觉表示混淆，属界面/PKIX 名称处理。
P32	rfc5280:5439-5449	不在范围内	同上，名称视觉混淆。
P33	rfc9846:4676-4677	没有陈述目标	该段只指向附录 C/E/F；其中实际列出的目标已由 A02、A03、A04、A06、A08、K01、C01、C02、U01 与新增目标覆盖。
P34	rfc9954:550-558	C08, `kem_broken`, `dh_broken`	
P35	rfc9954:560-569	证明器问不了	KEM 的 IND-CCA2/FO 变换与公钥重用下的安全性是计算层假设。
P36	rfc9954:571-574	证明器问不了	定长公钥/密文/秘密属于编码与长度性质。
P37	rfc9954:576-582	证明器问不了	变长秘密导致散列块处理时间侧信道，属实现层时序。
P38	rfc9954:584-586	证明器问不了	散列不再抗碰撞时变长拼接的风险，属计算层假设。
P39	rfc9954:588-592	证明器问不了	拼接需单射编码，属编码层性质。
P40	rfc9954:594-597	证明器问不了	只可与定长共享秘密的算法一起使用，属编码/长度要求。

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 22 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 6 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	参与方	`leaked_client_key`	
S02	服务端	参与方	`leaked_server_key`	
S03	证书颁发者	参与方	按定义全部失守	攻击者控制证书颁发者即可为任意身份签发证书，本处所问的全部认证性质按定义不再成立；文档假定 PKI 正常工作（rfc5280:5233、5311）。
S04	攻击者	参与方	攻击者得不到更多	它就是攻击者本身，不额外给出信息。
S05	对端身份	值	攻击者得不到更多	对端身份是公开名称，证书本身是公开数据（rfc5280:5226）； 新增的“客户端证书不被网络获知”目标是证书值不出现在线上，而非名称不被知悉。
S06	协商参数	值	攻击者得不到更多	协商参数（组、套件）在握手中明文交换，属公开值。
S07	握手 图文	值	攻击者得不到更多	记录 由握手消息构成，均可公开观察，知道它不泄漏秘密。
S08	握手流量密钥	值	按定义全部失守	持有本次握手的流量密钥即按定义失去该会话的机密性与完成 可靠性，文档未在其下要求任何性质。
S09	CertificateVerify 签名	值	攻击者得不到更多	CertificateVerify 签名在握手中发送，是公开值；其价值在于不可伪造而非保密。
S10	已完成 校验值	值	攻击者得不到更多	已完成 校验值在握手中发送，是公开值。
S11	终端实体证书	值	攻击者得不到更多	证书是公开可验证数据（rfc5280:5226）； 在 TLS 1.3 中只是不在线上明文出现。
S12	签名私钥	值	`leaked_client_key`, `leaked_server_key`, `ltk_after_session`	
S13	协商组	值	攻击者得不到更多	协商组名在 ClientHello/ServerHello 中明文交换。

ID	参与方或值	类别	攻击者条件	不设的原因
S14	套件	值	攻击者得不到更多	套件名在握手中明文交换。
S15	角色标签	值	攻击者得不到更多	角色标签是公开的固定字符串常量（s0383）。
S16	笔录	值	攻击者得不到更多	同 S07,图文由公开消息构成。
S17	客户端签名私钥	值	`leaked_client_key`, `ltk_after_session`	
S18	服务端签名私钥	值	`leaked_server_key`, `ltk_after_session`	
S19	应用流量密钥	值	按定义全部失守	应用流量密钥由握手秘密派生，持有它即该连接机密性按定义丧失，文档未在其下要求其它性质。
S20	历史会话流量密钥	值	按定义全部失守	持有某个历史会话的流量密钥即该会话机密性按定义丧失；前向保密问的是长期密钥泄露后它是否可得，而非持有它时还成立什么。
S21	对端认证	值	`leaked_client_key`, `leaked_server_key`	
S22	会话流量密钥	值	按定义全部失守	同 S08/S19，持有会话流量密钥即该会话按定义暴露。

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		
`leaked_client_key`	客户端证书对应的长期签名私钥，握手中即可使用（会话进行中已持有）。	KCI阻力 讨论了一方长期秘密被泄露的情形（rfc9846:6522. . 6528）； 私钥未受保护则攻击者可冒充（rfc5280:5261）。	rfc9846:6522, rfc5280:5261, s0372
`leaked_server_key`	服务端证书对应的长期签名私钥，握手中即可使用。	同上（rfc9846:6522、rfc5280:5261）。	rfc9846:6522, rfc5280:5261, s0372
`kem_broken`	本次会话 ML-KEM 部分的共享秘密（ML-KEM 被攻破），握手期间即可计算它。	RFC 9954 要求混合构造在至少一个组件未破时仍安全，故须分别考察单一组件被破（rfc9954:550. . 553）。	rfc9954:550, s0015, s0008
`dh_broken`	本次会话 X25519 部分的共享秘密（X25519 被攻破，例如由密码相关量子计算机从临时公钥恢复标量并在会话中可用）。	RFC 9954 的 hybrid 性质（rfc9954:550 (中文(简体)). . 553）； RFC 10024 指出被动观察者可借 CRQC 恢复 ECDH 标量（main:299. . 302）。	rfc9954:550,主机:299,s0015,s0003,s0018
`ltk_after_session`	双方长期签名私钥，在会话完成且握手秘密已擦除之后才获得。	远期密钥的前进密钥(rfc9846:6504. . 6514)，并注明需擦除的中间值（s0479）。	rfc9846:6504, s0479

ID	`network`	`leaked_client_key`	`leaked_server_key`	`kem_broken`	`dh_broken`	`ltk_after_session`
A02	成立					
A03	成立					
A04	成立					

ID	network	leaked_client_key	leaked_server_key	kem_broken	dh_broken	ltk_after_session
A06	成立					
A07	成立					
A08	成立					
K01	成立					
C01						成立
C02		成立	成立			
C08				成立	成立	
U01	成立					
A06.12	成立					
C02.13		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：
54	A02, A03, A04, A06, A07, A08, K01, C01, C02, C08, U01, A06.12, C02.13, X01	plain_primitives, many_sessions	所有答案都来自散列式、HMAC/HKDF、客户飞行的公用密钥加密、有证书检查的签名、以及X25519, 仿照与单一定律g^xy=g^yx的普通Diffie-Hellman密钥协议; ML-KEM部分是一个不透明封装,带有攻击者-不可访问共享的秘密,混合组合器是一个自由的功能. 会话密钥来自两部分,所以除了g^xy = g^yx之外,没有使用代数定律,也没有答案取决于一个跨消息变化的值(没有计数器,序列号或替换的密钥是模型化的:后手摇动的auth,HRR,PSK和复发都超出了范围). 要求属性为每个角色设置任何次数的会话.

分析员的结语

该模型覆盖主TLS1.3握手此简介 -ClientHello,ServerHello与X25519MLKEM768份额,EncryptedExtensions,CertificateRequest,两个证书/CertificateVerify/完成飞行——每个签名和完成值内都有记录片散列,两个角色上下文字符串,客户机在客户机握握交通键下的客户机. 它运行,正常运行被找到;28答案记录在最后文本上,所有答案仍然保留(检查点已核实)。

除了一种警告之外,每个目标的所有声称都得到答复:13个14个目标的答复是肯定的,C02/C02.13个目标也得到答复,漏掉的服务器密钥半部分被证明是持有密钥的攻击者所持有的,而不是捆绑密钥的证书(给予它证书使ProVerif的搜索超过了10的限度). 证明任何会议次数:相互认证(双向),身份/组/套/图书协议,注入协议,关键确认两种方式,身份对签名的密钥绑定,谈判参数不替换,长期签名密钥和会话握手密钥保密,会后长期密钥泄露后提前保密,只有ML-KEM部分或只有X25519部分失败时的混合安保(保密和认证),两者角色标签分离CertificateVerify方向,服务器仅在客户端完成后才接受客户端身份,并且隐藏网络攻击者提供的客户端证书.

没有发现 : 没有属性失败, 因此与文件没有新的关系, 这些文件规定了所有这些目标(同侪认证、 独特性、 降级保护、 会话密钥、 前向保密、 KCI 阻力、 端点识别保护、 混合安全) 。 其余的空白,全部记录在报告内:由于攻击者完成服务器握手的世界没有在ProVerif年终止,一些认证证明没有控制能力; C01/C08的会话关键证明也没有控制权(需要公布两个关键协议的秘密); 每次读数都基于不透明ML-KEM,X25519,只有g^xy=g^yx,一个抽象的PKI没有撤销,一个固定的组和套件,排除了PSK,0-RTT,HRR,后手摇动剂和警报. Tamarin+ Agent将解决服务器认证案件,并给出缺失的控件.