TLS 1.3 的安全性分析：X25519MLKEM768 混合密钥交换

本报告的其他语言版本：English。

rfc10024 · ProVerif+ Agent 报告

文稿	Post-Quantum Traditional (PQ/T) Hybrid Key Agreement Mechanisms for TLS 1.3 （协议定义）; Hybrid Key Exchange in TLS 1.3 （辅助）; The Transport Layer Security (TLS) Protocol Version 1.3 （辅助）
检查的性质	14 条：11 条成立，2 条不成立（2 个攻击），1 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

该协议是 TLS 1.3 的完整单往返握手，运行于 X25519MLKEM768 混合组。客户端和服务器参与其中，并协商出握手与应用流量密钥。该混合组将一个 ML-KEM-768 密钥封装与一次 X25519 交换相结合，两个共享秘密在进入 TLS 1.3 密钥调度之前被拼接在一起。

交换结束后，客户端确信对端就是其所固定证书密钥的那台服务器，并且双方持有相同的密钥。服务器只确信其对端持有握手密钥，因为没有请求客户端证书。

参与方：

- **客户端**：请求一个经过服务器认证的信道；固定服务器证书密钥。持有：固定的服务器公钥。
- **服务器**：用证书认证自身；不认证客户端。持有：长期签名密钥、证书。

图 1 展示了文稿所规定的交换过程。

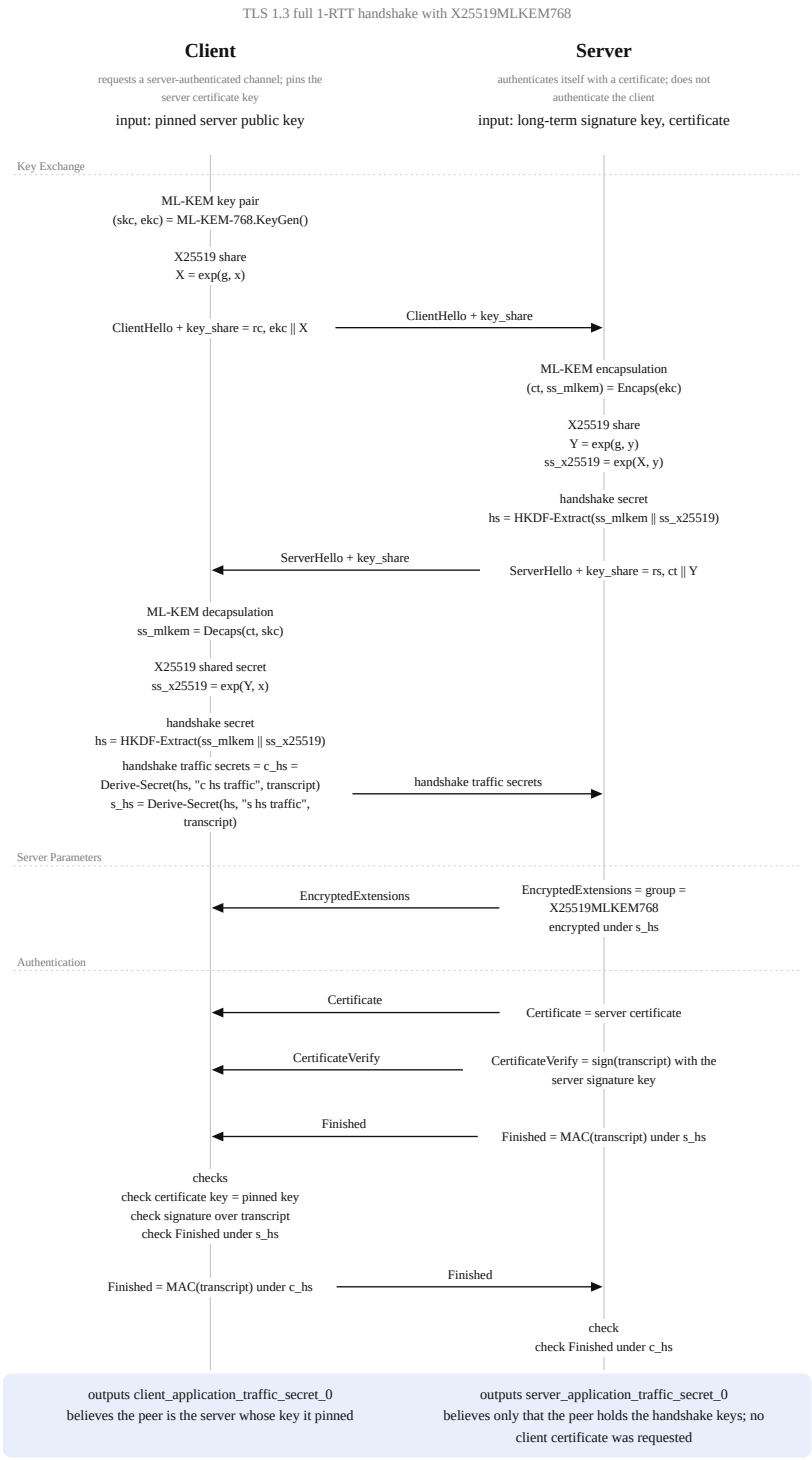


图 1. 文稿所规定的协议。

分析的范围见附录 D：分析了什么、省略了什么，以及它依据的是文稿的哪些章节。

2 发现

没有发现。 分析没有发现任何文稿未已陈述或未已排除的内容。第 3 节的表格给出了每条性质的结果。

在所分析的范围内，X25519MLKEM768 在 TLS 1.3 完整 1-RTT 握手中给出了它应当给出的东西。没有报告任何发现：每一条不成立的性质，要么是文稿已陈述的，要么是模型的产物。两个已知结果被复现：一个组件被攻破时，会话密钥仍然保密；而两个组件共用的一个有故障的随机数生成器会破坏混合性质，这与

主文稿的安全考虑中的警告完全一致。这些答案依赖于理想的密钥封装机制、仅依赖 g^xy = g^yx 这一法则的 Diffie-Hellman，以及理想的密钥调度，因此它们对 ML-KEM 的计算强度或量子强度没有任何说明。十四个目标中有十三个得到了回答；针对被动攻击者的身份保护被留作开放，因为模型中的攻击者是主动的，而证书是公开的。

3 检查过的性质

每一行都是一条交给 ProVerif 的性质。结果是 ProVerif 对分析者的协议模型给出的答案；价值以及文稿是否已陈述该结果，是分析者的判断，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	**客户端对服务器的认证。** 客户端每次接受握手完成时，必须存在一个服务器运行，其意图身份就是该客户端。	无	成立	中	是
A03	**对等方之间的会话密钥协商。** 客户端每次接受时，存在匹配的服务器运行，双方身份、协商组 X25519MLKEM768 与共享秘密一致。	无	成立	中	是
A04	**握手会话的唯一性。** 客户端每次接受对应不同的服务器运行，同一服务器运行不能被重复接受。	无	成立	中	是
A06	**服务器进行的密钥确认。** 客户端在确认点要求服务器已导出同一会话密钥并发送匹配的 Finished。	无	成立	中	是
A08	**转录绑定组与份额。** 客户端接受的协商组与服务器密钥份额必须对应客户端提议的组，且转录绑定双方角色与协商数据。	无	成立	中	是
K01	**混合会话密钥的保密性。** 攻击者不能推导 X25519MLKEM768 共享秘密及由其派生的握手与应用流量密钥。	无	成立	中	是
C01	**针对长期密钥泄漏的前向保密。** 会话完成后泄露服务器长期签名私钥，攻击者仍不能获得此前会话的流量密钥。	服务器 (会话完成之后)	成立	中	是
C04	**单一临时秘密泄漏下密钥仍安全。** 泄露 X25519 临时私钥或 ML-KEM 解封装私钥之一时，共享秘密仍保密。	客户端或服务器 (握手期间或之后)	成立	中	是
C08	**组件被攻破下的混合性质。** 一个组成密钥交换被攻破时，共享秘密仍保密。	组成算法 (握手期间)	攻击成立（文稿已写明）	中	是
K01.10	**本次握手密钥的保密性。** 攻击者不能推导本次握手的会话密钥。	无	成立	中	是
A08.11	**Finished 绑定转录、组与角色。** 客户端接受的 Finished 绑定完整握手转录、协商组 X25519MLKEM768 与双方角色。	无	成立	中	是
C04.12	**单一组件密钥泄漏下密钥仍安全。** 分别泄露 X25519 临时私钥或 ML-KEM 解封装私钥时，会话密钥仍保密。	客户端或服务器 (握手期间或之后)	成立	中	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
X01	**服务器身份对被动攻击者隐藏。** 观察一次诚实握手的被动网络攻击者，永远不会获知服务器的证书公钥；证书以及服务器第二个飞行消息的其余部分只在握手流量密钥下传输。	无	无答案	none	不确定
X02	**共享 RNG 泄漏下混合秘密仍安全。** 当一次会话所用随机数生成器的状态或输出被披露给攻击者，且两个组件算法都从同一生成器取值时，混合共享秘密及由其派生的会话密钥仍然保密。	该会话中两个组件算法共用的随机数生成器的状态或输出，因而也包括该会话的 X25519 临时标量和 ML-KEM 封装随机性	攻击成立（文稿已写明）	低	是

“攻击成立（文稿已写明）”：证明器找到了这个攻击，而文稿自己已经写明它存在。这条性质不成立；这是已知结果，不算发现（附录 B）。

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, X02.

所提出的问题，以及分析者的回答：

问题	回答	依据
Q1: 会话密钥保密	网络攻击者无法推导会话密钥；当任一组件的一次性秘密泄露时，会话密钥仍然保密；只有当两个组件共用一个有故障的生成器时才会被破坏。	K01, K01.10, C04, C08
Q2: Finished 对 transcript/协商组/双方角色的绑定	Finished 是在握手流量密钥下对 hello 转录的 MAC，而该转录携带双方密钥份额与协商组，因此组、份额与双方角色都被绑定；组一旦改变，校验即失败，客户端不会接受。	A06, A08, A08.11
Q3: 不同经典/PQ 密钥泄露条件下分别检查结论	仅泄露 X25519 临时标量，或仅泄露 ML-KEM 解封装密钥，会话密钥仍保密，因为攻击者需要两个组件的秘密才能计算出合并秘密；同时泄露两者才会破坏它们。	C04, C04.12, C08, X02

4 本次分析的局限

这里的结果是协议模型上的结果：它说明规定的消息与检查给出了什么、未能给出什么，其中密码学被视作理想化的，对实现没有任何说明。

正如分析者所述，本次分析不涵盖以下内容：

- ML-KEM 被理想化：一次封装总是解封装出同一个秘密。不主张任何计算安全性、抗量子性，也不主张解封装失败行为。
- Diffie-Hellman 只有 g^xy = g^yx 这一法则。小阶点、贡献性行为，以及文稿要求的全零共享秘密检查，均未被建模。
- 转录哈希只覆盖两条 hello 消息，不覆盖 Certificate 和 CertificateVerify。记录层、其 AEAD nonce、密钥更新与应用数据都在模型之外。
- PSK、恢复、0-RTT 和 HelloRetryRequest 都在本次分析之外，如任务的流程所述。
- 缺少客户端认证，因此服务器对客户端身份的认知无法被认证。
- 随机数生成器警告仅被建模为两个组件秘密同时泄露，而非生成器的状态。
- 模型中只存在一个服务器身份，因此针对被动攻击者的身份保护无法与主动攻击者区分开；该目标仍为开放。
- 攻击者是符号化的：ProVerif 没有计算界，对算法强度没有任何说明。

- 会话密钥协商与单射性答案没有给出对照查询：模型中没有参与方推导出错误的密钥，且每个会话都是一次性的，因此这两条性质没有会不成立的变体。

宿主记录的内容：

- 无答案者：X01。
- 分析者为性质设定了攻击者条件，但既没有证明也没有攻击的（附录 D）：X01 在 `network` 下。
- 没带对照查询的证明（附录 C）：A02: a02_ident, A02: a02_cert, A03: a03_key, A04: a04_inj。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。

每条性质还有哪些开放之处，以及什么能定论，见附录 A。

附录 A：逐条性质的解读

这是分析者自己对证明器答案的解读，而非证明器的答案：这些答案对协议意味着什么、解读依据什么、能否照原样使用，以及它的价值有多大。

A02: 客户端对服务器的认证

客户端每次接受握手完成时，必须存在一个服务器运行，其意图身份就是该客户端。

客户端只接受这样的服务器飞行消息：其证书携带它所固定的密钥，并且该证书是由服务器在同一会话中发送的。持有另一身份有效证书的服务器无法让客户端接受，因此客户端对对端的认知反映了服务器的身份。

- 结果：Holds；是否回答了所问：是；可在有保留的情况下使用
- 价值中：一条核心的、文稿已记载的保证，针对同时持有另一台服务器签名密钥的攻击者得到证明，并带有对照查询：跳过证书检查的客户端会接受攻击者自己的身份。
- 文稿是否已写：是。文稿在哪里说明：rfc9846:6490
- 依据：模型中只有一个可信服务器身份，证书检查是与固定密钥的相等比较；证书链及其验证未被建模；签名与 MAC 方案是理想的；服务器不认证客户端
- 下一步：对证书链与多个可信身份建模，以检验证书验证本身。

A03: 对等方之间的会话密钥协商

客户端每次接受时，存在匹配的服务器运行，双方身份、协商组 X25519MLKEM768 与共享秘密一致。

会话双方最终得到相同的混合派生秘密，因此也得到相同的流量密钥，因为转录绑定了双方的密钥份额，并且 Finished 与签名都在其上校验。

- 结果：成立；是否回答了所问：是；可用但有保留
- 价值 中：文稿将建立相同的会话密钥列为第一条握手性质；证明在理想密钥调度下成立。
- 文稿中已陈述：是。文稿中的位置：rfc9846:6478
- 依赖：转录只覆盖两条 hello；HKDF-Extract 与 HKDF-Expand 是理想单向函数
- 待解决：没有对照查询：模型中没有参与方能从同一会话推导出不同的密钥
- 下一步：把转录扩展到完整握手并重做。

A04: 握手会话的唯一性

客户端每次接受对应不同的服务器运行，同一服务器运行不能被重复接受。

每次客户端接受都由同一会话的服务器运行单射匹配，因此服务器飞行消息不能被重放为第二次接受，一次服务器运行也不能被接受两次。

- 结果：成立；是否回答了所问：是；可用但有保留
- 价值 中：文稿陈述了会话密钥的唯一性；接受的单射性是它的机械形式。
- 文稿中已陈述：是。文稿中的位置：rfc9846:6495
- 依赖：每个协议角色实例只处理一次握手；双方使用新鲜随机数，没有记录层重放窗口
- 待解决：没有对照查询：重放需要某个参与方两次接受同一飞行消息，而模型不包含这种情况
- 下一步：本范围内无。

A06: 服务器进行的密钥确认

客户端在确认点要求服务器已导出同一会话密钥并发送匹配的 Finished。

客户端只有在服务器通过转录上的 Finished 表明自己持有相同握手秘密、因而持有相同会话密钥之后才接受。

- 结果：成立；是否回答了所问：是；可用但有保留
- 价值 中：文稿将 Finished 消息的密钥确认列为握手性质，对照查询显示不带该检查的客户端会接受没有服务器产生的飞行消息。
- 文稿中已陈述：是。文稿中的位置：rfc9846:6483
- 依赖：HMAC 是理想的；Finished 的输入只是 hello 转录
- 下一步：本范围内无。

A08: 转录绑定组与份额

客户端接受的协商组与服务器密钥份额必须对应客户端提议的组，且转录绑定双方角色与协商数据。

客户端接受的密钥份额与组来自同一会话的真实服务器 hello。被替换的份额或被降级的组会改变转录，因此 Finished 与签名不再通过验证。

- 结果：成立；是否回答了所问：是；可用但有保留
- 价值 中：降级保护与转录的作用在 TLS 1.3 安全性质中已有陈述；对照查询显示不做检查的客户端会接受攻击者构造的飞行消息与攻击者构造的份额。
- 文稿中已陈述：是。文稿中的位置：rfc9846:6499, rfc9846:6627
- 依赖：只建模了一个组，因此组检查针对的是固定名称；转录只覆盖 hello 对
- 待解决：要降级到非混合组，模型中需要第二个组
- 下一步：加入一个客户端也会提议的经典组，并询问服务器能否强制使用它。

K01: 混合会话密钥的保密性

攻击者不能推导 X25519MLKEM768 共享秘密及由其派生的握手与应用流量密钥。

攻击者始终无法推导混合共享秘密或诚实会话的流量密钥，即使持有一个组件的秘密也仍然不能。它需要同时持有两个组件才能计算出组合秘密。

- 结果：成立；是否回答了所问：是；可用但有保留
- 价值 中：会话密钥的保密性是文稿陈述的性质，逐组件的回答就是混合性质；两者都在一个已知两个组件秘密的对照查询下得到证明。
- 文稿中已陈述：是。文稿中的位置：rfc9846:6483, rfc9954:550
- 依赖：ML-KEM 是理想的，X25519 只有定律 g^xy = g^yx；由于 HKDF-Extract 是两个秘密的自由函数，组合对两个参数都是单向的；未建模 dual-PRF 论证；没有记录层
- 下一步：KEM 的计算侧需要 Tamarin+ Agent。

C01: 针对长期密钥泄漏的前向保密

会话完成后泄露服务器长期签名私钥，攻击者仍不能获得此前会话的流量密钥。

长期签名密钥不参与密钥调度，因此在握手之后读取它对该会话的流量密钥毫无帮助。

- 结果：成立；是否回答了所问：是；可用但有保留

- 价值 中：关于长期密钥的前向保密在 TLS 1.3 安全性质中已有陈述；证明是结构性的，并在上述保留条件下成立。
- 文稿中已陈述：是。文稿中的位置：rfc9846:6504
- 依赖：密钥调度在不含 PSK 的情况下建模；泄漏建模为密钥在握手后变为公开；假定临时秘密被擦除，模型没有擦除步骤
- 下一步：本范围内无。

C04: 单一临时秘密泄漏下密钥仍安全

泄露 X25519 临时私钥或 ML-KEM 解封装私钥之一时，共享秘密仍保密。

任一临时秘密单独泄漏都不会危及混合共享秘密和会话密钥：攻击者需要两个组件才能计算出组合秘密。这就是符号层面的混合性质。

- 结果：成立；是否回答了所问：是；可用但有保留
- 价值 中：混合性质在两份定义文稿的安全考虑中都有陈述；对照查询显示一旦两个组件秘密都已知，秘密就会失守。
- 文稿中已陈述：是。文稿中的位置：rfc9954:550
- 依赖：组合是两个组件秘密的单向函数，dual-PRF 问题正出在这里；泄漏建模为标量或解封装密钥在会话结束时变为公开；ML-KEM 与 X25519 是理想的
- 下一步：用计算工具解决 dual-PRF 这一步。

C08: 组件被攻破下的混合性质

一个组成密钥交换被攻破时，共享秘密仍保密。

一个组件被攻破不会危及混合秘密，文稿记载的例外也同样成立：当一个故障生成器同时提供两个组件的秘密时，攻击者能计算出组合秘密及由其派生的每一个密钥。

- 结果：攻击成立（文稿中已陈述）；是否回答了所问：是；可用但有保留
- 价值 中：混合性质及其随机数生成器例外都在主文稿中陈述；分析以精确条件复现了每一种情况。
- 文稿中已陈述：是。文稿中的位置：main:128, main:308
- 依赖：泄漏建模为一个或两个组件秘密变为公开；组合是两个秘密的公开函数
- 下一步：建模生成器状态而非两个派生秘密，以更严格地检验该警告。

K01.10：本次握手密钥的保密性

攻击者不能推导本次握手的会话密钥。

单次握手的会话密钥不能被网络攻击者推导，且在任一组件秘密单独泄漏时仍保持保密；只有单个故障生成器同时供给两个组件时才会被攻破。

- 结果：成立；是否回答了所问：是；可用但有保留
- 价值 中：与 K01 相同的性质，按所问针对单次握手作答。
- 文稿中已陈述：是。文稿中的位置：rfc9846:6483
- 依赖：与其他保密性回答相同的理想化
- 下一步：本范围内无。

A08.11：Finished 绑定转录、组与角色

客户端接受的 Finished 绑定完整握手转录、协商组 X25519MLKEM768 与双方角色。

客户端接受的 Finished 是握手流量密钥下对 hello 转录的 MAC，而该转录携带双方的密钥份额与协商组，因此组、份额与双方角色都被绑定，组一旦改变检查就会失败。

- 结果：成立；是否回答了所问：是；可用但有保留
- 价值 中：文稿说明 Finished 的输入是转录哈希，且 Finished 能防止降级；对照查询显示不带该检查的客户端会接受服务器从未产生的组与飞行消息。
- 文稿中已陈述：是。文稿中的位置：rfc9846:6517, rfc9846:6627
- 依赖：转录是两条 hello 的哈希，而不是整个握手的哈希
- 下一步：加入第二个组以检验真正的降级。

C04.12：单一组件密钥泄漏下密钥仍安全

分别泄露 X25519 临时私钥或 ML-KEM 解封装私钥时，会话密钥仍保密。

单独泄露 X25519 临时标量，或单独泄露 ML-KEM 解封装密钥，会话密钥仍保持保密。保护由另一个组件承担。

- 结果：成立；是否回答了所问：是；可用但有保留
- 价值 中：所问的混合性质在安全考虑中已有陈述；逐组件的回答是模型所能给出的。
- 文稿中已陈述：是。文稿中的位置：rfc9954:550
- 依赖：ML-KEM 与 X25519 是理想的，组合对两个参数都是单向的；每个会话建模一次泄漏，在会话结束时公布
- 下一步：用 Tamarin+ Agent 解决计算侧。

X01: 服务器身份对被动攻击者隐藏

被动网络攻击者观察一次诚实握手时，始终无法获知服务器的证书公钥；证书以及服务器第二个飞行消息中的其余内容只在握手流量密钥下传输。

证明器找到的唯一一条踪迹，是攻击者与服务器自行开启一个会话，并像任何客户端一样收到证书。这与目标所指的被动攻击者无关，因此本分析既不能证实也不能否定证书在传输链路上保持隐藏。

- 结果：无答案；回答了所问：否；不可用
- 值 无：用于证伪的踪迹是主动攻击者获取公开信息，因此该结果是攻击者模型的产物，对协议本身没有任何说明。
- 文稿中的陈述：不明确。所依据的原文：rfc9846:6530, s0022
- 依据：模型中只有一个服务器身份和一个主动攻击者，因此只要以客户端身份连接，就总能获得公开证书
- 待解决：被动观察者是否会看到服务器的证书
- 下一步：在一个具有两个候选服务器身份的模型上构建仅被动的攻击者，并询问非干扰问题。

X02: 共享 RNG 泄漏下混合秘密仍安全

当会话所用随机数生成器的状态或输出被泄露给攻击者，且两个组件算法都从同一个生成器取值时，混合共享秘密以及由它导出的会话密钥仍保持秘密。

当同一个有故障的生成器为两个组件的秘密提供输入时，攻击者会算出组合秘密以及由它导出的每一个密钥。这是主文稿安全注意事项中的警告，模型中对其进行了复现。

- 结果：攻击成立（文稿中已陈述）；回答了所问：是；可用但有保留
- 值 低：该失败直接源于假设的失陷，文稿也将其作为对实现者的警告陈述。
- 文稿中的陈述：是。文稿中的位置：main:308
- 依据：泄漏被建模为两个组件的秘密都变为公开；组合是两个秘密的公开函数
- 下一步：对生成器本身建模，以说明该警告的覆盖范围有多大。

附录 C：主张和证明器的答案

证明器为每个目标记录的内容：达到的级别、达到该级别的查询、是否检查了对照，以及攻击及分析者对每项攻击的判定。

目标	级别	界	查询	对照	攻击	主张
A02	proved		a02_ident	6 中的 4		6 proved
A03	proved		a03_key			1 proved
A04	proved		a04_inj			1 proved
A06	proved		a06_fin	checked		1 proved
A08	proved		a08_share	checked		2 proved
K01	proved		k01_hs	checked		5 proved
C01	proved		k01_hs	checked		1 proved
C04	proved		c04_x	checked		2 proved
C08	proved		c04_x	checked	c08_both (holds_in_source)	2 proved, 1 attack
K01.10	proved		k01_hs	checked		3 proved
A08.11	proved		a06_fin	checked		2 proved
C04.12	proved		c04_x	checked		2 proved
X01	none				ident (model_artifact)	1 attack
X02	none				c08_both (holds_in_source)	1 attack

逐条主张，按分析者对每项主张的措辞；每项的答案是证明器给出的：

目标	主张	攻击者	回答	查询	对照
A02	客户端接受结果中的对端身份，就是客户端配置为信任的身份：客户端接受的任何证书公钥都等于服务器自己的公钥，因此客户端眼中的对端反映了服务器的身份（即目标的"预期身份"）。	`network`	proved	a02_ident	none
A02	客户端每一次接受，都有服务器在同一会话中确实发送的证书作为依据，因此该会话存在一次服务器运行。	`network`	proved	a02_cert	none
A02	即使攻击者还持有另一个服务器身份的有效签名密钥和证书，并能用它跑完整个服务器消息流程，客户端也只接受固定的服务器身份。	`rogue_server_key`	proved	a02_ident	checked
A02	客户端所接受的证书来自同一会话中的诚实服务器，而非攻击者自己的服务器身份，即使攻击者持有另一台服务器的签名密钥。	`rogue_server_key`	proved	a02_cert	checked
A02	客户端接受结果中的对端身份，就是客户端配置为信任的身份：客户端接受的任何证书公钥都等于服务器自己的公钥。	`network`	proved	a02_ident	checked
A02	客户端每一次接受，都有服务器在同一会话中确实发送的证书作为依据。	`network`	proved	a02_cert	checked

目标	主张	攻击者	回答	查询	对照
A03	同一握手的客户端会话和服务器会话都完成时，二者持有相同的混合派生握手秘密，因而持有相同的会话密钥和相同的协商 X25519MLKEM768 份额。	`network`	proved	a03_key	none
A04	每一次客户端接受，都与同一会话中通过相同密钥发送了 Finished 的一次服务器角色运行形成单射匹配，因此一次服务器运行不能被接受两次，旧的流程也不能被再次接受。	`network`	proved	a04_inj	none
A06	客户端只在同一会话的服务器运行派生出相同的混合握手秘密、并据此在握手的 transcript 上发送了 Finished 时才接受：即服务器完成了密钥确认。	`network`	proved	a06_fin	checked
A08	客户端接受的 X25519 和 ML-KEM 密钥份额，来自同一会话中真实服务器 hello 的份额；替换份额会改变 transcript 和握手秘密，从而使 Finished 和签名失败。	`network`	proved	a08_share	checked
A08	客户端接受的协商组，是服务器在同一会话中指定的 X25519MLKEM768 组，而不是攻击者选择的组。	`network`	proved	a08_grp	checked
K01	对于不泄露任何临时秘密的诚实会话，攻击者无法获知其混合派生握手秘密（因而也无法获知会话密钥）。	`network`	proved	k01_hs	checked
K01	对于不泄露任何临时秘密的诚实会话，攻击者无法获知由混合共享秘密派生的客户端应用流量密钥。	`network`	proved	k01_ap	checked
K01	攻击者知道客户端的 X25519 临时标量（因而知道该分量的共享秘密），仍然无法获知混合共享秘密或由其派生的密钥。	`x25519_ephemeral_leak`	proved	c04_x	checked
K01	攻击者知道客户端的 ML-KEM 解封装密钥（因而知道 ML-KEM 共享秘密），仍然无法获知混合共享秘密或由其派生的密钥。	`mlkem_leak`	proved	c04_kem	checked
K01	攻击者在握手后读取服务器的长期签名私钥，仍然无法获知已完成会话的会话密钥。	`server_ltk_after`	proved	k01_hs	checked
C01	在握手完成后取得服务器的长期签名私钥，并不能得到该先前会话的流量密钥：密钥调度不以长期密钥为输入。	`server_ltk_after`	proved	k01_hs	checked
C04	客户端的 X25519 临时私标量泄露时，混合共享秘密和会话密钥仍保持秘密，因为 ML-KEM 分量仍在保护它们。	`x25519_ephemeral_leak`	proved	c04_x	checked
C04	客户端的 ML-KEM 解封装私钥泄露时，混合共享秘密和会话密钥仍保持秘密，因为 X25519 分量仍在保护它们。	`mlkem_leak`	proved	c04_kem	checked
C08	X25519 分量密钥交换被攻破（其共享秘密为攻击者所知），混合共享秘密仍保持秘密。	`x25519_ephemeral_leak`	proved	c04_x	checked
C08	ML-KEM 分量密钥交换被攻破（其共享秘密为攻击者所知），混合共享秘密仍保持秘密。	`mlkem_leak`	proved	c04_kem	checked
C08	当该会话所用的随机数生成器状态被泄露、且两个分量算法都从同一生成器取随机数时，混合共享秘密仍保持秘密。	`rng_shared`	attack (holds_in_source)	c08_both (the control of c04_kem)	

目标	主张	攻击者	回答	查询	对照
K01.10	攻击者无法派生此握手的会话密钥（X25519MLKEM768 共享秘密及由其派生的流量密钥）。	`network`	proved	k01_hs	checked
K01.10	X25519 临时标量单独泄露时，会话密钥仍保持秘密。	`x25519_ephemeral_leak`	proved	c04_x	checked
K01.10	ML-KEM 解封装密钥单独泄露时，会话密钥仍保持秘密。	`mlkem_leak`	proved	c04_kem	checked
A08.11	客户端接受的 Finished 是用握手流量密钥在握手 transcript 上计算出来的，因此它同时绑定了两个角色和本会话协商的数据。	`network`	proved	a06_fin	checked
A08.11	被接受的 Finished 绑定到服务器在本会话中指定的 X25519MLKEM768 组，因此降低组不会被接受而不使 Finished 失败。	`network`	proved	a08_grp	checked
C04.12	只有 X25519 临时标量泄露时，会话密钥仍保持秘密。	`x25519_ephemeral_leak`	proved	c04_x	checked
C04.12	只有 ML-KEM 解封装密钥泄露时，会话密钥仍保持秘密。	`mlkem_leak`	proved	c04_kem	checked
X01	观察诚实握手的被动网络攻击者永远不会获知服务器的证书公钥。	`network`	attack (model_artifact)	ident	
X02	当两个分量共享的 RNG 状态泄露给攻击者时，混合共享秘密和会话密钥仍保持秘密。	`rng_shared`	attack (holds_in_source)	c08_both (the control of c04_kem)	

附录 D：分析是怎么跑的

LLM 分析者根据文稿构建协议模型，并把每条性质交给 ProVerif；第 3 节中的每个结果都是证明器的回答。

ProVerif+ Agent 会话 session-20261114T182015，2026-11-14。状态：已完成。模型：deepseek-v4-1-flash-261017。步骤：40，证明器 62 秒，总耗时 18 分钟，费用 0.130 美元。

ProVerif：运行 82 次证明，81 次得出结论，1 次无答案，42 秒，记录 38 个回答。

分析了什么

协议	TLS 1.3：X25519MLKEM768 混合密钥交换
版本	rfc10024
分析范围	固定 X25519MLKEM768；先选一次完整 1-RTT 服务器认证握手，固定认证配置，PSK/0-RTT/恢复/HRR 后续分别加。
不在范围内	扩展只定义 key_share 与共享秘密；完整握手必须读取 TLS 基线；符号 KEM/DH 结论不能作为 ML-KEM 算法计算安全或抗量子证明。仅证明明确模型及攻击者条件下的性质，不能把缺失检查、完整安全信道或全诚实 NF 当作待证结论的替代。
原文	621 个编号原文单元（164414 字节），来自下文列出的章节。本报告中的 s0001 这类引用就是这些单元之一

分析所依据的文稿章节：

文稿	章节	标题
main	4	协商组
main	4.1	客户端份额
main	4.2	服务器份额
main	4.3	共享秘密
main	6	安全考量
rfc9954	3	混合密钥交换的构造
rfc9954	3.1	协商
rfc9954	3.2	传输公钥与密文
rfc9954	3.3	共享秘密计算
rfc9954	6	安全考量
rfc9846	2	协议概述
rfc9846	2.1	不正确的 DHE 份额
rfc9846	2.2	恢复与预共享密钥 (PSK)
rfc9846	2.3	0-RTT 数据
rfc9846	4	握手协议
rfc9846	4.1	转录哈希
rfc9846	4.2	密钥交换消息

文稿	章节	标题
rfc9846	4.2.1	密码协商
rfc9846	4.2.2	Client Hello
rfc9846	4.2.3	Server Hello
rfc9846	4.2.4	Hello Retry Request
rfc9846	4.3	扩展
rfc9846	4.3.1	支持的版本
rfc9846	4.3.2	Cookie
rfc9846	4.3.3	签名算法
rfc9846	4.3.4	证书颁发机构
rfc9846	4.3.5	OID 过滤器
rfc9846	4.3.6	握手后基于证书的客户端认证
rfc9846	4.3.7	支持的组
rfc9846	4.3.8	密钥份额
rfc9846	4.3.8.1	Diffie-Hellman 参数
rfc9846	4.3.8.2	ECDHE 参数
rfc9846	4.3.9	预共享密钥交换模式
rfc9846	4.3.10	早期数据指示
rfc9846	4.3.11	预共享密钥扩展
rfc9846	4.3.11.1	票据年龄
rfc9846	4.3.11.2	PSK 绑定器
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	认证消息
rfc9846	4.5.1	证书
rfc9846	4.5.1.1	OCSP 状态与 SCT 扩展
rfc9846	4.5.1.2	证书选择
rfc9846	4.5.1.3	接收证书消息
rfc9846	4.5.2	Certificate Verify
rfc9846	4.5.3	Finished
rfc9846	4.6	早期数据结束
rfc9846	4.7	握手后消息
rfc9846	4.7.1	新会话票据消息
rfc9846	4.7.2	握手后认证
rfc9846	4.7.3	密钥与初始化向量更新

文稿	章节	标题
rfc9846	7	密码计算
rfc9846	7.1	密钥调度
rfc9846	7.2	更新流量秘密
rfc9846	7.3	流量密钥计算
rfc9846	7.4	非对称共享秘密计算
rfc9846	7.4.1	有限域 Diffie-Hellman
rfc9846	7.4.2	椭圆曲线 Diffie-Hellman
rfc9846	7.5	导出器

源文步骤在文档中定位到的协议目的：固定 X25519MLKEM768；先选一次完整 1-RTT 服务器认证握手，固定认证配置，PSK/0-RTT/恢复/HRR 后续分别加。

对照文稿定性质

在撰写查询之前，分析者将草拟的性质清单与文档本身对协议目的的表述做了对照。名称、性质所涉及的对象以及文档的说法均为分析者的解读；所引用的位置在文档中确实存在。

ID	简称	对象	文稿怎么说	出处
A02	客户端对服务器的认证	客户端在接受时，对其所认证的对等方就是它固定了签名密钥的那台服务器的确信，以及本次会话存在一次服务器运行	rfc9846 附录 F.1：对等方认证意味着客户端对的对等方身份视图反映了服务器的身份；服务器对握手转录的签名以及 Finished MAC 将该会话与服务器身份绑定。	rfc9846:6490, rfc9846:6483, s0065, s0083, s0092
A03	对等方之间的会话密钥协商	同一会话的客户端与服务器最终得到相同的会话密钥和相同的协商组 X25519MLKEM768	rfc9846 附录 F.1：建立相同的会话密钥，握手必须在两侧输出相同的会话密钥；混合共享秘密是 ML-KEM 与 X25519 共享秘密的拼接，被插入 TLS 1.3 密钥调度。	rfc9846:6478, s0015, s0052, s0092
A04	握手会话的唯一性	每次客户端接受都属于一次不同的服务器运行，且一次服务器运行不能被接受两次	rfc9846 附录 F.1：任意两次不同的握手应产生不同且不相关的会话密钥；Finished MAC 与两个 hello 的新鲜随机数可防止被重放的飞行消息再次被接受。	rfc9846:6495, s0092, s0507, s0564
A06	服务器进行的密钥确认	客户端的接受要求服务器已导出相同的会话密钥并发送了匹配的 Finished	rfc9846 附录 F.1 与第 4.5.3 节：Finished 消息为握手中建立的共享秘密提供密钥确认，接收方必须验证其内容。	rfc9846:6483, rfc9846:6507, s0092, s0507, s0513
A08	转录绑定组与份额	客户端接受的组和服务器密钥份额属于协商的 X25519MLKEM768 运行，并由握手转录绑定到双方角色	rfc9846 附录 F.1：降级保护，密码参数应在两侧一致，且如同未发生攻击；Finished MAC 与签名可防止降级攻击。main 第 6 节：本分析关键依赖于 TLS 1.3 消息转录。	rfc9846:6499, rfc9846:6627, main:268, s0003, s0008, s0015, s0092

ID	简称	对象	文稿怎么说	出处
K01	混合会话密钥的保密性	X25519MLKEM768 共享秘密以及由它导出的握手与应用流量密钥，对网络攻击者保密	rfc9846 附录 F.1：会话密钥的保密性，它们应仅为通信双方所知；混合性质要求只要至少一个组件密钥交换未被攻破，秘密就保持安全。	rfc9846:6483, rfc9954:550, s0015, s0052, s0053, s0065
C01	针对长期密钥泄漏的前向保密	已完成握手的会话密钥，对事后获得服务器长期签名私钥的攻击者保密	rfc9846 附录 F.1：关于长期密钥的前向保密，握手完成后签名密钥的泄漏不会危及会话密钥的安全。TLS 1.3 密钥调度不将任何长期密钥作为输入。	rfc9846:6504, s0583
C04	单一临时秘密泄漏下密钥仍安全	混合共享秘密与会话密钥，在客户端的 X25519 临时标量或其 ML-KEM 解封装密钥之一泄漏时仍保持安全	rfc9954 第 6 节：混合性质，只要至少一个组件密钥交换算法未被攻破，所得秘密就是安全的；main 第 6 节讨论了经典标量与 ML-KEM 封装随机数的泄露。	rfc9954:550, main:299, s0025, s0057
C08	组件被攻破下的混合性质	一次会话的混合共享秘密，在一个组件密钥交换（X25519 或 ML-KEM）被攻破而另一个未被攻破时仍保持安全	main 第 3 节将混合定义为：即使其他组件被攻破，只要至少一个组件算法仍然安全；rfc9954 第 6 节陈述了相同要求并指出了 dual-PRF 组合器。	main:128, rfc9954:550, s0020, s0057
K01.10	本次握手密钥的保密性	所分析的这一次握手的会话密钥，对网络攻击者以及获得某一个临时秘密的攻击者保密	rfc9846 附录 F.1 会话密钥的保密性；用户问题 Q1 询问本次握手的会话密钥。	rfc9846:6483, s0015, s0052, s0053
A08.11	Finished 绑定转录、组与角色	客户端接受的 Finished 覆盖握手转录、协商的 X25519MLKEM768 组以及双方角色	rfc9846 第 4.5.3 节：verify_data 是对握手上下文的转录哈希计算的 HMAC；附录 F.1：Finished MAC 可防止降级攻击。用户问题 Q2。	rfc9846:6517, rfc9846:6627, s0092, s0507
C04.12	单一组件密钥泄漏下密钥仍安全	会话密钥，在 X25519 临时标量或 ML-KEM 解封装密钥分别泄漏时仍保持安全	rfc9954 第 6 节混合性质；main 第 6 节关于两个组件秘密。用户问题 Q3。	rfc9954:550, main:299, s0023, s0025, s0057
X01	服务器身份对被动攻击者隐藏	服务器身份（其证书公钥）与被动网络攻击者	rfc9846 附录 F.1：服务器身份（证书）应对被动攻击者受到保护；客户端身份应对被动和主动攻击者受到保护。	rfc9846:6530
X02	共享 RNG 泄漏下混合秘密仍安全	一次会话的 X25519MLKEM768 共享秘密，面对获得两个组件共享的 RNG 输出的攻击者	main 第 6 节警告：若两个算法使用同一个不安全的 RNG，则其中一个算法对状态的泄露也会影响另一个算法的安全；封装随机数是 RNG 输出被泄露的又一个位置。该警告所称已丢失的性质；预期不成立。	main:308, main:282, s0023, s0026

分析者依据文稿补充的性质：X01, X02.

文稿里的安全表述，逐段去向

宿主将文稿中说明协议保护什么、防范什么的章节逐段列出，共 20 段；分析者对每一段说明了去向：定为性质、定为攻击者条件，或者为什么两者都不选。选了 10 段，没选 10 段。列出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	main:268-271	A08, A03	
P02	main:273-276	证明器问不了	面向实现者的抗侧信道 KEM 实现指南，并指向 NIST SP 800-227；侧信道和实现质量超出符号轨迹证明器所能回答的范围。
P03	main:278-280	A03	
P04 至 P05	main:282-297	`rng_shared`	
P06	main:299-306	K01, C04, `x25519_ephemeral_leak`	
P07	main:308-310	X02, `rng_shared`	
P08	rfc7748:783-793	证明器问不了	curve25519 作为原语时的暴力破解安全强度；原语的强度不是轨迹性质。
P09	rfc7748:802-808	证明器问不了	curve25519 与 curve448 之间性能与偏执程度的权衡，以及两者对抗大型量子计算机的强度；这不是轨迹性质。
P10	rfc7748:810-818	证明器问不了	X25519 的贡献性行为：小阶输入点会消除另一方的贡献，并由全零共享密钥检查检测出来。一个只以 g^xy = g^yx 作为 DH 定律的模型无法表示小阶点，因此这项有效性检查被排除在模型之外，并列入限制。
P11	rfc7748:820-825	A08	
P12	rfc7748:827-837	证明器问不了	拒绝扭曲线上的点或非最小域元素的实现可能与 Montgomery 阶梯算法轻易区分开；这是可观察的实现行为，不是协议的轨迹性质。
P13	rfc9846:4676-4677	没有陈述目标	一条指向 rfc9846 附录 C、附录 E 和附录 F 中讨论安全问题的指引；它本身没有陈述任何性质。
P14	rfc9954:550-558	C08, C04, K01	
P15	rfc9954:560-569	证明器问不了	要求此处使用的 KEM 是 IND-CCA2 安全的或带有 Fujisaki-Okamoto 变换，以及某些 IND-CPA KEM 在公钥复用时会被攻破：这是 KEM 的计算安全性，而符号模型假定其为理想。
P16	rfc9954:571-574	A03	
P17	rfc9954:576-582	证明器问不了	哈希函数处理变长秘密时的时序侧信道。模型没有长度或时间的概念。
P18	rfc9954:584-586	证明器问不了	针对变长秘密的时序攻击（Lucky Thirteen、Raccoon）；不是轨迹性质。
P19	rfc9954:588-592	证明器问不了	当 KDF 哈希不具备抗碰撞性时变长秘密的风险；这是关于哈希的计算假设，不是轨迹性质。
P20	rfc9954:594-597	A03	

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 11 条，没检查 22 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	应用数据的载荷与端到端保密性属于记录层；本任务确定该扩展的密钥交换和一次完整的 1-RTT 握手。
K03	强保密／秘密值不可区分性	K01	

条目	目录里的性质	作为哪条性质检查	不检查的原因
K04	密钥用途、方向与会话分离	A03, A04	
D01	消息完整性与数据来源真实性	A03, A08	
A01	对端曾参与性（Aliveness）	A02	
A05	隐式密钥认证	A03, K01	
A07	身份—凭据—密钥绑定	A02	
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	握手不携带任何可能被重复的计费、令牌或分配操作。
R04	消息接受顺序／窗口安全	不在范围内	接受顺序和抗重放窗口是记录层行为；本任务只对握手消息建模。
R05	抗降级／安全策略保持	A08	
C02	抗密钥泄露冒充（KCI）	不在范围内	密钥泄露冒充关注的是被泄露方对其对端的认证；本配置仅做服务器认证，没有客户端长期密钥，因此客户端密钥方向不存在，而服务器密钥方向就是该服务器的普通能力。
C03	已知密钥安全／泄露隔离	A04, K01	
C05	泄露后安全恢复（PCS）	不在范围内	泄露后安全性需要棘轮或恢复机制；PSK、0-RTT、恢复和密钥更新被任务的流程明确推迟。
C06	注册凭据泄露后的增强认证	不适用	TLS 1.3 基于证书的密钥交换中没有注册记录、PAKE 或增强认证。
C07	抗离线字典攻击	不适用	本配置不使用口令或其他低熵共享秘密。
Z01	授权执行正确性	不适用	协议不携带授权决定或受保护资源访问。
Z02	委托权限不扩张	不适用	握手中不存在权限的委托或代理。
Z03	授权与身份／会话／操作绑定	不适用	不签发授权令牌，也不在上下文之间移动令牌。
Z04	撤销与过期生效	不适用	交换中不包含可撤销的权限、过期或配额。
Z05	跨租户／跨服务安全隔离	不适用	握手中不存在多租户或跨服务的授权边界。
S01	加密 nonce 唯一性	不在范围内	AEAD nonce 唯一性是记录层的义务；握手模型推导密钥但不发送记录层流量。
S02	重传／密钥重安装安全	不在范围内	密钥重安装和重传属于记录层和 KeyUpdate，而 KeyUpdate 被任务的流程推迟；握手本身是一次性的，不持有任何可能被重传重置的已安装密钥。
S03	抗回滚与状态单调性	不在范围内	本配置中没有可被旧消息回滚的缓存版本、计数器或恢复状态。
S04	跨阶段安全上下文一致性	不在范围内	跨阶段上下文一致性需要恢复、0-RTT 或迁移，这些都被任务的流程推迟。
S05	终止与旧状态失效	不在范围内	连接拆除和旧状态失效属于记录层，并与 KeyUpdate 一起被推迟。
P01	身份匿名性	X01	
P02	会话不可关联性	不在范围内	会话不可关联性不是 TLS 1.3 的目标，也不在本任务范围内；服务器通过证书认证，因此与同一服务器的两个会话在设计上就是可识别的。
P03	用户／凭据存在性隐藏	不适用	握手中不发生任何用户数据库或凭据查找。
V01	条件性进展／错误恢复	证明器问不了	条件性进展和错误恢复是活性性质；轨迹证明器无法回答一次运行是否总会结束。

条目	目录里的性质	作为哪条性质检查	不检查的原因
V02	无非预期死锁	证明器问不了	无死锁是活性性质，超出 ProVerif 所能回答的范围。
V03	受限资源滥用／抗放大	证明器问不了	资源放大和成本界是定量性质，超出 ProVerif 所能回答的范围。

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 16 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 4 项，没设的 12 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	`x25519_ephemeral_leak`, `mlkem_leak`, `rng_shared`	
S02	服务器	参与方	`server_ltk_after`	
S03	服务器身份	值	攻击者得不到更多	服务器证书是公开信息，任何一方都能在带外获得；持有它对保密性或一致性目标毫无帮助。它是否出现在线路上，是从附录 F.1 新增的独立目标，该目标是在被动网络攻击者下询问的，而不是在已经持有该值的攻击者下询问。
S04	协商组	值	攻击者得不到更多	按设计，协商组在两个 hello 中都以明文传输。
S05	共享秘密	值	按定义全部失守	持有某会话混合共享秘密的一方，按定义就是该会话的参与方；点名该秘密的保密性目标按定义即失守，且文稿并未要求针对持有会话自身密钥的参与方提供任何认证性质。
S06	双方身份	值	攻击者得不到更多	服务器身份是公开的，且在此配置中客户端身份未经认证，因此持有任一方身份都毫无帮助。
S07	会话唯一性	值	攻击者得不到更多	会话唯一性是运行本身的属性，而非攻击者能持有的值；攻击它的方式是重放，已作为 A04 询问。
S08	握手流量密钥	值	按定义全部失守	持有会话的握手流量密钥，正是 K01 和 C04 所否定的；一旦持有，这些性质按定义即失守，且没有文稿在其下进一步询问任何内容。
S09	密钥份额	值	攻击者得不到更多	按设计，两个密钥份额都在 hello 中以明文传输；网络上的攻击者已经拥有它们。
S10	转录	值	攻击者得不到更多	两个 hello 的转录按设计是公开的；网络上的攻击者已经拥有它，而绑定到它正是 A08 所询问的。
S11	ML-KEM 共享秘密	值	`mlkem_leak`	
S12	X25519 共享秘密	值	`x25519_ephemeral_leak`	
S13	应用流量密钥	值	按定义全部失守	应用流量密钥正是 K01 和 C01 所声明其保密性的值；持有它按定义即失去这些，且应用数据保护不在本范围内。
S14	历史会话流量密钥	值	按定义全部失守	历史会话流量密钥正是 C01 所说不得由长期密钥推出的；已经持有它们的攻击者按定义即失去该性质。
S15	会话密钥	值	按定义全部失守	会话密钥是 K01 和 K01.10 的对象；持有它们按定义即失去这些目标。
S16	角色	值	攻击者得不到更多	角色通过 Finished 和签名绑定到转录中；不存在攻击者能持有的独立角色值，而这种绑定已作为 A08 询问。

每条性质在各攻击者条件下的答案

攻击者由分析者在编写查询之前设定；每个答案都在其中之一条件下记录。单元格是证明器在该攻击者下对该性质的答案；“无答案”是指证明器在该攻击者下让某主张处于未决状态、或未记录任何内容的攻击者集合；空单元格是分析者未为该性质设定的攻击者。

攻击者	持有什么	依据	出处
`network`	仅网络：它读取、丢弃、更改和发送消息，不持有任何一方的秘密		
`x25519_ephemeral_leak`	会话中客户端的 X25519 临时私有标量，因而持有该会话的 X25519 共享秘密；在握手期间或之后获得	若一个组件密钥交换被攻破，混合性质仍须成立（rfc9954 第 6 节）；正文第 6 节指出，拥有密码学相关量子计算机的被动观察者能恢复 X25519 标量，该标量来自 RNG 输出。这就是经典组件被攻破的攻击者。	rfc9954:550, main:299, s0025, s0057
`mlkem_leak`	会话中客户端的 ML-KEM-768 解封装私钥，因而持有该会话的 ML-KEM 共享秘密	若一个组件密钥交换被攻破，混合性质仍须成立（rfc9954 第 6 节）；目标 C04 将 ML-KEM 解封装密钥列为两个秘密之一，其单独泄露不得破坏会话。这就是后量子组件被攻破的攻击者。	rfc9954:550, main:128, s0057, s0058
`rng_shared`	两个组件算法为该会话共享的随机数生成器的状态或输出，因而持有该会话的 X25519 临时标量和 ML-KEM 封装随机性	正文第 6 节：封装随机性 m 来自随机比特生成器，并由客户端恢复，因此它是披露给某一方的 RNG 输出；若两个算法使用同一个不安全的 RNG，一方对状态的披露也会影响另一方。	main:308, main:282, main:289, s0023, s0024, s0026
`server_ltk_after`	服务器的长期签名私钥，从服务器存放处读取，读取时机为会话期间或握手完成之后	rfc9846 附录 F.1 要求关于长期密钥的前向保密：握手完成后签名密钥的泄露不得危及会话密钥。长期签名密钥是此配置中唯一的长期密钥。	rfc9846:6504, s0583
`rogue_server_key`	一个有效的签名私钥和证书，其服务器身份不同于客户端配置所接受的身份	对端认证（rfc9846 附录 F.1）是关于客户端对服务器身份之看法的陈述，因此攻击者必须能够出示另一身份的证书；任何服务器都持有自己的一份。	rfc9846:6490

ID	`network`	`x25519_ephemeral_leak`	`mlkem_leak`	`rng_shared`	`server_ltk_after`	`rogue_server_key`
A02	成立					成立
A03	成立					
A04	成立					
A06	成立					
A08	成立					
K01	成立	成立	成立		成立	
C01					成立	
C04		成立	成立			
C08		成立	成立	不成立		
K01.10	成立	成立	成立			
A08.11	成立					
C04.12		成立	成立			
X01	无答案					

ID	network	x25519_ephemeral_leak	mlkem_leak	rng_shared	server_ltk_after	rogue_server_key
X02				不成立		

原文和目标

来源：621 个原文单元，164414 字节，冻结于 source-delivery-01.json。 目标：9 个已批准（A02、A03、A04、A06、A08、K01、C01、C04、C08）；已询问的问题：3 个。 目标清单事先按草稿获批，使用 --approve-targets。

宿主按文档化默认值（任务 `decisions: auto`）做出的决定，供你核对：

- approve_package：批准源文包 protocol-62b1d6c019165ab627bd9496162f

本步骤的自述：1 个请求（1 个失败），0.000 USD，输入 74179 个 token，输出 3987 个，24 秒。

关于证明器和模型的说明

分析者为各目标命名的内容：

步骤	目标	特征	原因
29	A02, A03, A04, A06, A08, K01, C01, C04, C08, K01.10, A08.11, C04.12, X01, X02	plain_primitives	每个答案都建立在理想化原语之上：ML-KEM 视为完美封装（decap(encaps(ek,s))=s，不作计算或量子方面的主张），X25519 视为仅满足 g^xy = g^yx 这一法则的 Diffie-Hellman（不考虑贡献性行为，不考虑小阶点），HKDF-Extract/Expand 视为单向函数，HMAC 和 AEAD 视为理想。混合性质在模型中成立，是因为 HKDF-Extract 是两个组件秘密的公开函数，所以攻击者需要两者；真实安全性所需的 dual-PRF 论证（rfc9954 第 6 节）未被建模，且不存在记录层。要解决计算层面的问题，需要能如实建模这些特征的 Tamarin+ Agent。

分析者的结语

在 ProVerif 中建模了 TLS 1.3 完整 1-RTT 服务器认证握手，使用 X25519MLKEM768 混合组：ClientHello(key_share = ML-KEM ek ‖ X25519 share) / ServerHello(key_share = ct ‖ X25519 share) / 加密的 EncryptedExtensions、Certificate、CertificateVerify、Finished / 客户端 Finished，混合秘密是对两个组件秘密做 HKDF-Extract 的结果，hello 转录作为上下文。先找到的是正常流程；随后模型每次增加一个机制（加密的服务器飞行、X25519 标量、ML-KEM 解封装密钥和单一故障共享 RNG 的泄露族、恶意服务器密钥、握手后长期签名密钥的泄露，以及仅用于控制绑定性质的未校验客户端）。没有任何目标依赖于跨步骤变化的值，因此不需要有界模型，也不需要状态审查。

结果：在 14 个目标上记录了 26 个答案，在最终文本上全部仍然成立。十二个目标已证明：服务器认证与固定身份（带一个对照查询，其中未做检查的客户端会接受攻击者自己的证书）、对同一组会话密钥的一致、接受行为的单射性、通过 Finished 完成的密钥确认、密钥份额与组同真实 server hello 的绑定、混合秘密与流量密钥的保密性、针对长期签名密钥的前向保密，以及——核心结果——混合性质：单独泄露任一组成部分的秘密，共享秘密和会话密钥仍保持保密；这由一个模型证明，其中 HKDF-Extract 需要两个组成部分，并带一个两者均已知的对照查询。有两个结果是文稿自身陈述的攻击：一个共享的故障生成器会破坏混合性质（正文第 6 节），记录为已知结果。有一个目标，即针对被动攻击者的身份保护，仍保持开放：ProVerif 找到的唯一踪迹是主动攻击者像任何客户端一样获得公开证书，这是单服务器身份下主动攻击者模型的产物。

其余部分受阻的原因：对 ML-KEM 和 X25519 的符号化处理（单一 DH 定律，无小阶或全零检查）、仅含 hello 的转录，以及缺少仅被动攻击者模型。混合组合器的计算侧（双 PRF 假设）需要 Tamarin+ Agent；这些答案报告为依赖于上述简化。