TLS 混合 HelloRetryRequest 配置的安全分析

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	16 条：15 条成立，0 条不成立，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 配置，带一次 HelloRetryRequest，并使用固定的混合组 X25519MLKEM768。参与方为客户端和服务器：客户端持有服务器的证书公钥，服务器持有其证书签名密钥和一个 cookie 完整性密钥。服务器先用一个 HelloRetryRequest 回应 ClientHello1，该消息选择组，并携带一个绑定到 ClientHello1 哈希的 cookie；随后客户端发送带有混合密钥份额和 cookie 的 ClientHello2，服务器基于由 message_hash(ClientHello1) 重建的转录，用 Certificate、CertificateVerify 和 Finished 完成认证。

交换结束时，客户端确信自己通信的对象就是其证书所指名的服务器，并且组与转录正是自己提议、服务器回显的那一份。双方持有相同的混合共享秘密和相同的握手与应用流量密钥，网络上的攻击者既不知道共享秘密，也不知道服务器签名密钥。

参与方：

- **客户端**：TLS 客户端，提供 X25519MLKEM768。持有：服务器证书公钥。
- **服务器**：TLS 服务器，发送一次 HelloRetryRequest。持有：证书签名密钥、cookie 完整性密钥。

图 1 展示了文稿所规定的交换过程。

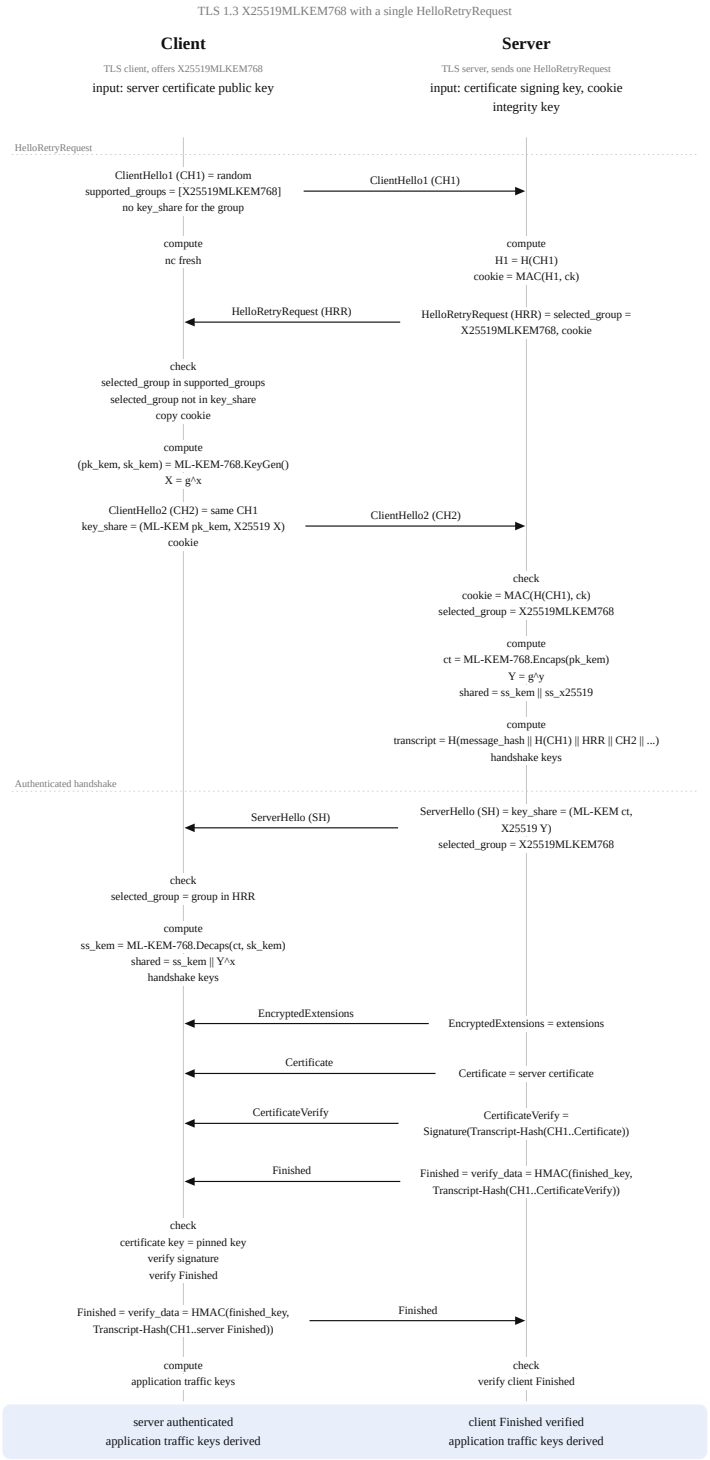


图 1. 文稿所规定的协议。

本次分析的范围见附录 D：分析了什么、略去了什么，以及它依据的文稿章节。

2 发现

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

在符号模型内，该配置提供了它应当提供的保证：重试之后的服务器认证，HRR、cookie 和转录对 ClientHello1 的绑定，对重复或拼接重试的拒绝，共享秘密与密钥的保密性，以及混合与前向保密性质。没有新的发现：所证明的每条保证都已在文稿中针对其所证明的攻击者陈述过，每个被点名的攻击都被排

除。有一条性质尚无定论：共享秘密的强保密性（不可区分性）未被判定，因为带有单一全局选定秘密的符号 KEM 允许攻击者检验一个候选值；这需要带有每会话秘密的 Tamarin+ Agent。这些结果对朴素原语抽象（KEM、满足 g^xy=g^yx 的 Diffie-Hellman、哈希、MAC、签名）成立，并对任意数量的会话成立，但不覆盖记录层、原语的计算强度，也不覆盖 X25519 的全零/小阶点检查。

3 检查过的性质

每一行都是提交给 ProVerif 的一条性质。结果是 ProVerif 对分析者所建协议模型的回答；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
A03	**HRR 后的服务器认证。** 每当客户端在 HRR 流程后接受握手完成，都存在一个真实服务器运行，其身份、协商组 X25519MLKEM768、双方密钥份额与 transcript 与客户端接受的值一致。	无	成立	中	是
A04	**服务器运行不被双重接受。** 每次客户端在 HRR 流程后成功完成握手，都对应一个不同的真实服务器运行；同一服务器运行不能被客户端接受两次。	无	成立	中	是
A08	**HRR 参数绑定到转录。** 客户端接受的 selected_group、cipher suite、selected_version 与 transcript 绑定，均对应其 CH1 提议、HRR 内容及 message_hash(CH1) 重构，攻击者不能替换为未认证的值。	无	成立	低	是
K01	**共享秘密与密钥的保密性。** 攻击者不能推导出 X25519MLKEM768 共享秘密、握手流量密钥、应用流量密钥或服务器长期签名私钥。	无	成立	中	是
K04	**密钥分离与新鲜性。** 客户端与服务器派生的握手/应用流量密钥在方向与用途上分离，不同会话的密钥不意外相同。	无	成立	中	是
R01	**Cookie 绑定到当前 CH1。** 客户端接受的 HRR 及其 cookie 必须对应当前 CH1，旧 HRR/cookie 不能被重放为本次有效认证。	无	成立	中	是
R02	**HRR 或 ClientHello 不可重放。** 同一 HRR 或 CH 消息实例在单连接内至多被接受一次；跨连接拼接的 HRR 不能被接受为有效握手。	无	成立	中	是
C01	**会话密钥的前向保密。** 在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完成会话的握手或应用流量密钥。	服务器长期签名私钥 (会话完成之后)	成立	中	是
C04	**单一坏组件下的混合安全。** 泄露 X25519 临时私钥份额或 ML-KEM 私钥份额之一，攻击者仍不能获得会话共享秘密与流量密钥。	X25519 临时私钥份额或 ML-KEM 私钥份额 (密钥交换期间或之后)	成立	中	是
C08	**X25519 被攻破时 ML-KEM 提供保护。** 在 X25519 原语失效（攻击者获得 X25519 共享秘密）时，ML-KEM 组件仍保护会话共享秘密与流量密钥。	X25519 共享秘密 (密钥交换期间)	成立	中	是
A08.11	**selected_group 与转录绑定。** 客户端接受的 selected_group 与 transcript（message_hash(CH1)、HRR、CH2）绑定，对应其 CH1 提议与 HRR 内容。	无	成立	低	是
R02.12	**HRR 或 ClientHello 的重放。** 同一 HRR 或 CH 消息实例在单连接内至多被接受一次；跨连接拼接的 HRR 不能被接受为有效握手。	无	成立	中	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
A03.13	**服务器运行与应用密钥协商。** 客户端接受握手完成时，存在真实服务器运行，其身份、协商组与密钥份额一致；双方派生的应用流量密钥一致。	无	成立	中	是
X01	**第二次 HelloRetryRequest 后不完成。** 客户端在同一连接中收到第二次 HelloRetryRequest 后绝不会完成握手；收到即强制中止。	无	成立	低	是
X02	**无降级的参数协商。** 客户端接受的协商组、密码套件和 TLS 版本与不存在攻击者时相同，并与双方达成的一致。	无	成立	低	是
X03	**会话共享秘密的强保密性。** 攻击者无法分辨会话共享秘密取两个允许值中的哪一个：该共享秘密不可区分，而不仅仅是不可恢复。	无	只确认可达	none	否

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.

文稿没有提到、由分析者按性质目录补充的性质（见附录 D）：X03 (K03).

所提出的问题及分析者的回答：

问题	回答	依据
Q1: HRR 选择组与 CH1/CH2 transcript 绑定	在模型中，只有当 HRR 选择 X25519MLKEM768，并且其 cookie 与转录绑定到客户端自己的 ClientHello1 时，客户端才会完成；因此攻击者无法替换所选组，也无法把外来 HRR 拼接进本次运行。	A08.11, A08, R01
Q2: 重放/跨连接拼接 HRR 不能导致错误认证	重复的或跨连接的 HRR 不会被接受：客户端的完成与服务器的 HRR 一一对应，且只对应同一会话的 HRR，因此重放不会产生第二个被接受的握手。	R02.12, R02, A04
Q3: 服务器认证及双方应用密钥一致性	当客户端接受完成时，确实有一个真实服务器以匹配的密钥份额运行，且双方派生出相同的应用流量密钥；网络攻击者无法推导出服务器签名密钥。	A03.13, A03, K01

4 本次分析的局限

此处的结果是协议模型上的结果：它说明所规定的消息和检查给出或未能给出什么，密码学被当作理想原语，不涉及任何实现。

据分析者所述，本次分析不覆盖以下内容：

- 模型是符号的：它不证明 ML-KEM-768 或 X25519 的计算安全性，而符号证明是关于抽象的证明。
- X25519 仅以 g^xy=g^yx 定律建模；main s0018 要求、rfc7748 P10 描述的小阶点和全零共享秘密检查无法表示，也未分析。
- 未建模记录层，因此载荷保密性、AEAD nonce 唯一性、服务器证书保密性和端点身份保护不在分析范围内。
- 该配置固定了单一组、密码套件和版本，因此组/密码套件/版本绑定与降级检查是空洞的；模型中没有第二个组可供攻击者替换。
- 未建模 0-RTT、PSK、恢复和 KeyUpdate；安全考虑中的 RNG 质量和变长时序问题不是迹性质。
- 证书链验证不在范围内（rfc9846 s0394）；客户端被固定到单一服务器公钥。
- 共享秘密的强保密性（X03）尚无定论：符号 KEM 和单一全局选定秘密使攻击者作为客户端的相等性测试成为可能，这是模型假象。

- 目标不依赖任何跨步骤保留并改变的值（计数器、序列号、被替换的密钥），因此没有生成展开的有界模型，也没有进行状态审查。

宿主记录的内容：

- 无答案：X03。
- 解读写成之后答案发生变化的性质：X03。
- 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）：X03 在 `network` 下。

每条性质还留有哪些未决之处，以及什么能解决它，见附录 A。

附录 A：逐条性质的解读

以下为分析者本人对证明器回答的解读，而非证明器的回答：这些回答对协议意味着什么、解读依据什么、能否照原样使用，以及它的价值。

A03: HRR 后的服务器认证

每当客户端在 HRR 流程后接受握手完成，都存在一个真实服务器运行，其身份、协商组 X25519MLKEM768、双方密钥份额与 transcript 与客户端接受的值一致。

客户端的完成与在同一会话上发送 Finished 的服务器绑定，且所接受的组就是所提议的 X25519MLKEM768。网络攻击者无法在没有这样一个服务器运行的情况下让客户端接受。

- 结果：Holds；回答所问：是；可用但有附加说明
- 价值 中：文稿将对等认证列为 TLS 目标。
- 文稿中已说明：是。文稿中的位置：rfc9846:6490
- 依据：KEM 与 X25519 是符号原语；仅对 g^xy=g^yx 建模。；转录是嵌套哈希链，message_hash(ClientHello1) 通过哈希 ClientHello1 表示。；只有一个服务器身份，由客户端固定的公钥确定。
- 下一步：此目标无；原语的计算强度超出范围。

A04: 服务器运行不被双重接受

每次客户端在 HRR 流程后成功完成握手，都对应一个不同的真实服务器运行；同一服务器运行不能被客户端接受两次。

客户端完成与服务器 HRR 是一一对应的，因此一个服务器运行不能被接受两次，重放的 HRR 也不会创建第二个会话。这依赖于 cookie 绑定 ClientHello1 的哈希。

- 结果：Holds；回答所问：是；可用但有附加说明
- 价值 中：文稿要求 cookie 绑定 ClientHello1 并禁止第二个 HRR。
- 文稿中已说明：是。文稿中的位置：s0126, s0167, s0168
- 依据：cookie 被建模为使用服务器密钥对 ClientHello1 哈希的 MAC。；转录哈希链的唯一性使不同会话互不相同。
- 下一步：无；源文包中未指定具体的 cookie 完整性算法。

A08: HRR 参数绑定到转录

客户端接受的 selected_group、cipher suite、selected_version 与 transcript 绑定，均对应其 CH1 提议、HRR 内容及 message_hash(CH1) 重构，攻击者不能替换为未认证的值。

客户端只接受 selected_group X25519MLKEM768，且只接受自己会话的 HRR；cipher suite 和 selected_version 在此配置中是固定常量。因此绑定成立，尽管对于固定的单组配置而言是空泛的。

- 结果：Holds；回答所问：是；可用但有附加说明
- 价值 低：文稿明确说明 selected_group 和版本检查。
- 文稿中已说明：是。文稿中的位置：s0057, s0058, s0247, s0251

- 依据：模型中只有一个组，因此无法测试其他 selected_group。；cipher suite 和 selected_version 是常量，不是协商值。
- 下一步：如需非空泛的降级结果，请对第二个组建模。

K01: 共享秘密与密钥的保密性

攻击者不能推导出 X25519MLKEM768 共享秘密、握手流量密钥、应用流量密钥或服务器长期签名私钥。

网络攻击者在握手期间既不能获知混合共享秘密及其派生密钥，也不能获知服务器签名密钥。对照查询表明，泄露两个临时组件（或运行后的签名密钥）确实会泄露它们，因此证明并非空泛。

- 结果：Holds；回答所问：是；可用但有附加说明
- 价值 中：文稿说明只要至少一个组件未被攻破，混合共享秘密就是安全的。
- 文稿中已说明：是。文稿中的位置：rfc9954:550
- 依据：KEM 建模为 decaps(encaps(pk(sk),r),sk)=r。；密钥调度被简化为单向 KDF 和 Finished 密钥函数。；签名密钥是私有自由名称，仅在阶段 2 泄露。
- 下一步：原语强度需要计算性论证，符号模型无法给出。

K04: 密钥分离与新鲜性

客户端与服务器派生的握手/应用流量密钥在方向与用途上分离，不同会话的密钥不意外相同。

握手秘密按会话唯一：会话标识符唯一确定握手秘密，持有一个会话的密钥不会使另一个会话的秘密共享。这由转录绑定的 KDF 得出。

- 结果：Holds；回答所问：是；可用但有附加说明
- 价值 中：文稿说明会话密钥的唯一性。
- 文稿中已说明：是。文稿中的位置：rfc9846:6495
- 依据：在符号模型中，KDF 是单向的且对其输入是单射的。；不同会话使用新鲜 nonce 和新鲜临时份额。
- 下一步：无。

R01: Cookie 绑定到当前 CH1

客户端接受的 HRR 及其 cookie 必须对应当前 CH1，旧 HRR/cookie 不能被重放为本次有效认证。

客户端只接受与其 ClientHello1 属于同一服务器会话的 HRR，因此过时或外来的 cookie 不能认证一次运行。Cookie 的新鲜性通过绑定 ClientHello1 哈希来保证。

- 结果：Holds；回答所问：是；可用但有附加说明
- 价值 中：文稿将 cookie 描述为无状态 HRR 绑定 ClientHello1 哈希。
- 文稿中已说明：是。文稿中的位置：s0167, s0168
- 依据：cookie 是对 ClientHello1 哈希的 MAC。；服务器按文稿描述以无状态方式建模。
- 下一步：无；未指定具体的 cookie 编码。

R02: HRR 或 ClientHello 不可重放

同一 HRR 或 CH 消息实例在单连接内至多被接受一次；跨连接拼接的 HRR 不能被接受为有效握手。

重复的 HRR 不会产生第二次被接受的运行，跨连接拼接的 HRR 会被拒绝，因为客户端只用自己的会话的 HRR 完成。完成与服务器 HRR 单射匹配。

- 结果：Holds；回答所问：是；可用但有附加说明
- 价值 中：文稿要求遇到第二个 HRR 时中止，并将重试绑定到 ClientHello1。
- 文稿中已说明：是。文稿中的位置：s0080, s0126
- 依据：客户端只读取一个 HRR；不存在接受第二个 HRR 的路径。；转录通过 message_hash 将 HRR 绑定到 ClientHello1。
- 下一步：无。

C01: 会话密钥的前向保密

在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完成会话的握手或应用流量密钥。

握手后泄露服务器签名密钥不会暴露过去的会话密钥，因为共享秘密由临时 ML-KEM 和 X25519 材料构建。对照查询表明，泄露两个临时组件确实会泄露秘密。

- 结果：Holds；回答所问：是；可用但有附加说明
- 价值 中：文稿说明相对于长期密钥的前向保密。
- 文稿中已说明：是。文稿中的位置：rfc9846:6504
- 依据：已擦除的临时材料通过阶段分离建模。；KEM 和 DH 是符号的；DH 定律仅为 g^xy=g^yx。
- 下一步：符号模型不能证明计算性前向保密。

C04: 单一坏组件下的混合安全

泄露 X25519 临时私钥份额或 ML-KEM 私钥份额之一，攻击者仍不能获得会话共享秘密与流量密钥。

仅泄露任一临时组件时，共享秘密仍受另一组件保护，只有泄露两者才会暴露它（对照查询）。这是针对两个私钥泄露的混合性质。

- 结果：Holds；回答所问：是；可用但有附加说明
- 价值 中：文稿说明只要至少一个组件未被攻破，混合秘密就是安全的。
- 文稿中已说明：是。文稿中的位置：rfc9954:550
- 依据：在模型中，KEM 共享秘密等于封装随机数。；两个组件通过单向拼接 KDF 组合。
- 下一步：计算性混合安全需要计算性论证。

C08: X25519 被攻破时 ML-KEM 提供保护

在 X25519 原语失效（攻击者获得 X25519 共享秘密）时，ML-KEM 组件仍保护会话共享秘密与流量密钥。

当 X25519 组件被攻破（其共享秘密为攻击者所知）时，ML-KEM-768 仍保护会话秘密和流量密钥。模型仅使用单一 Diffie-Hellman 定律，因此这是混合保护的下界。

- 结果：Holds；回答所问：是；可用但有附加说明
- 价值 中：文稿说明只要一个组件未被攻破，混合秘密就保持安全。
- 文稿中已说明：是。文稿中的位置：rfc9954:550
- 依据：通过将客户端标量交给攻击者来攻破 X25519，使其能计算 X25519 共享秘密。；在符号模型中 KEM 保持单向。
- 下一步：ML-KEM 的计算安全性超出范围。

A08.11: selected_group 与转录绑定

客户端接受的 selected_group 与 transcript（message_hash(CH1)、HRR、CH2）绑定，对应其 CH1 提议与 HRR 内容。

接受的 selected_group 是 X25519MLKEM768，与 ClientHello1 提议匹配，且转录绑定到同一会话的 HRR。由于该配置只有一个组，组部分为空泛的，但转录绑定是真实的。

- 结果：Holds；回答所问：是；可用但有附加说明
- 价值 低：文稿说明 selected_group 和转录重构要求。
- 文稿中已说明：是。文稿中的位置：s0057, s0058, s0247, s0251
- 依据：单一固定组。；转录为嵌套哈希链，含 message_hash(ClientHello1)。
- 下一步：增加第二个组以进行非空泛测试。

R02.12: HRR 或 ClientHello 的重放

同一 HRR 或 CH 消息实例在单连接内至多被接受一次；跨连接拼接的 HRR 不能被接受为有效握手。

重复的 HRR 或 ClientHello 实例至多产生一次被接受的运行，跨连接拼接的 HRR 不被接受。这是对重试的重放要求。

- 结果：Holds；回答所问：是；可用但有附加说明
- 价值 中：文稿要求遇到第二个 HRR 时中止，并禁止握手后重用 ClientHello。
- 文稿中已说明：是。文稿中的位置：s0080, s0087, s0126
- 依据：客户端只读取一次。；cookie 绑定 ClientHello1 哈希。
- 下一步：无。

A03.13: 服务器运行与应用密钥协商

当客户端接受握手完成时，确实有一个真实服务器运行过，其身份、协商组与密钥份额均一致；双方派生出相同的应用流量密钥。

应用密钥与共享的、绑定转录的握手秘密相关联。

- 结果：成立；所问是否有答案：是；有保留地可用
- 价值 中：文稿陈述了对端认证，并说明双方均从共享秘密派生应用秘密。
- 文稿中有陈述：是。文稿中的位置：rfc9846:6490
- 依据：Finished 和 CertificateVerify 是对转录哈希的符号 MAC 和签名。；单一固定的服务器身份。
- 下一步：无。

X01: 第二次 HelloRetryRequest 后不完成

客户端在同一连接中收到第二次 HelloRetryRequest 后，绝不会完成握手；收到一次即强制中止。

客户端只处理恰好一次 HRR，并且只在其后完成，因此不存在接受第二次 HRR 的路径。在这个单次重试配置中，该性质在结构上成立，因为客户端从不读取第二次 HRR，而不是依靠计数器。

- 结果：成立；所问是否有答案：是；有保留地可用
- 价值 低：文稿要求客户端在收到第二次 HRR 时中止。
- 文稿中有陈述：是。文稿中的位置：s0126
- 依据：客户端被写为单次读取的进程；不存在第二次 HRR 路径的构造。；组是固定的。

- 下一步：若需要机械化的第二次 HRR 测试，请建模一个显式的重试计数器。

X02: 无降级的参数协商

客户端接受的协商组、密码套件和 TLS 版本与没有攻击者时相同，并与对端达成的一致。

接受的组是 X25519MLKEM768，不能被攻击者选择的 HRR 替换，并且客户端只在与自身会话匹配的 HRR 下完成。密码套件和版本是固定常量，因此在此配置中降级是空泛的。

- 结果：成立；所问是否有答案：是；有保留地可用
- 价值 低：文稿陈述了降级保护。
- 文稿中有陈述：是。文稿中的位置：rfc9846:6499
- 依据：单一固定的组、密码套件和版本。
- 下一步：为获得非空泛的降级测试，请建模多个套件/版本。

X03: 会话共享秘密的强保密性

攻击者无法分辨会话共享秘密取两个允许值中的哪一个：共享秘密是不可区分的，而不仅仅是不可恢复的。

本目标的答案在本解读写成之后发生了变化。

共享秘密的强保密性（不可区分性）未被判定。ProVerif 的非干扰性失败，仅仅是因为专用副本使用了一个全局选定秘密和一个公开的 KEM 封装，所以充当客户端的攻击者可以解封装它并测试候选值。这是模型产物，不是协议弱点，从本次运行中无法就每会话的强保密性得出任何结论。

- 结果：仅可达；所问是否有答案：未定；不可用
- 价值 无：文稿陈述了保密性和混合性质，但未陈述共享秘密的不可区分性；本次运行无论如何都未判定任何东西。
- 文稿中有陈述：否
- 依据：使用单一的全局选定秘密，而非每会话的秘密。；符号 KEM 让封装密钥持有者能够恢复选定的秘密。
- 未决：每会话的共享秘密是否与另一个允许值不可区分。
- 下一步：使用带每会话秘密的 Tamarin+ Agent，或一个在私有测试密钥下隐藏候选值的非干扰模型。

附录 C：主张和证明器的答案

证明器对每个目标的记录：达到的级别、达到该级别的查询、是否检查了对照，以及附有分析者对各攻击判定的攻击。

目标	级别	界	查询	对照	攻击	主张
A03	proved		auth	checked		2 proved
A04	proved		auth_inj	checked		2 proved
A08	proved		group	checked		2 proved
K01	proved		ss_secret	checked		2 proved
K04	proved		key_sep	checked		2 proved
R01	proved		hrr_bound	checked		1 proved
R02	proved		hrr_inj	checked		2 proved
C01	proved		fs	checked		1 proved
C04	proved		x25519_hybrid	checked		2 proved
C08	proved		x25519_hybrid	checked		1 proved
A08.11	proved		group	checked		2 proved
R02.12	proved		hrr_inj	checked		2 proved
A03.13	proved		auth	checked		2 proved
X01	proved		x01	checked		1 proved
X02	proved		group	checked		2 proved
X03	reachable		ss_reach		strong (model_artifact)	1 attack

逐条主张，按分析者对每条主张的表述；每条主张的答案是证明器给出的：

目标	主张	攻击者	回答	查询	对照
A03	当客户端在 HRR 之后接受握手时，存在一个真实的服务器运行，它为同一会话发送了 Finished；攻击者仅拥有网络。	network	proved	auth	checked
A03	接受协商的组是 CH1 中所提供的 X25519MLKEM768，因此服务器身份/组/密钥共享匹配；攻击者仅拥有网络。	network	proved	group	checked
A04	每个客户端完成都映射到一个不同的真实服务器运行：服务器 Finished 不能被接受两次；攻击者仅拥有网络。	network	proved	auth_inj	checked
A04	服务器运行的给定 HRR 至多产生一个被接受的客户端完成（对 HRR 的单射一致性）；攻击者仅拥有网络。	network	proved	hrr_inj	checked
A08	被接受的 selected_group 是 X25519MLKEM768（密码套件和 selected_version 在此配置中是固定常量），因此攻击者无法替换为未提供的组；攻击者仅拥有网络。	network	proved	group	checked

目标	主张	攻击者	回答	查询	对照
A08	客户端仅以同一会话的 HRR 完成，将 message_hash(CH1)、HRR 和 CH2 绑定到 transcript 中；攻击者仅拥有网络。	`network`	proved	hrr_bound	checked
K01	X25519MLKEM768 共享秘密及其派生的握手/应用流量密钥在握手期间无法被网络攻击者获知；攻击者仅拥有网络。	`network`	proved	ss_secret	checked
K01	服务器长期签名私钥无法被网络攻击者获知；攻击者仅拥有网络。	`network`	proved	sk_secret	checked
K04	不同会话产生不同的握手秘密：会话标识符唯一确定握手秘密，因此不同会话不共享密钥；攻击者仅拥有网络。	`network`	proved	key_sep	checked
K04	即使攻击者拥有一个已完成会话的共享秘密和流量密钥，另一会话的握手秘密也是不同的且不共享；攻击者在网络之外拥有一个会话的密钥。	`one_session_key_leak`	proved	key_sep	checked
R01	客户端接受的 HRR/cookie 对应于当前 CH1：客户端仅以来自服务器会话、绑定到其自身 ClientHello 的 HRR 接受；攻击者仅拥有网络。	`network`	proved	hrr_bound	checked
R02	重复的 HRR 不会产生第二个被接受的运行：客户端完成单射地映射到服务器 HRR；攻击者仅拥有网络。	`network`	proved	hrr_inj	checked
R02	跨连接拼接的 HRR 不会被接受：客户端仅以其自身会话的 HRR 完成；攻击者仅拥有网络。	`network`	proved	hrr_bound	checked
C01	握手完成后，泄露服务器长期签名私钥不会揭示过去的会话共享秘密或握手/应用流量密钥；攻击者在网络之外拥有该签名密钥。	`server_sig_key_leak`	proved	fs	checked
C04	仅泄露 X25519 临时私钥标量不会揭示会话共享秘密或流量密钥；ML-KEM 仍然保护它们；攻击者在网络之外拥有该标量。	`x25519_sk_leak`	proved	x25519_hybrid	checked
C04	仅泄露 ML-KEM-768 解封装私钥不会揭示会话共享秘密或流量密钥；X25519 仍然保护它们；攻击者在网络之外拥有该密钥。	`mlkem_sk_leak`	proved	mlkem_hybrid	checked
C08	当 X25519 组件被攻破（攻击者获得 X25519 共享秘密）时，ML-KEM-768 仍然保护会话共享秘密和流量密钥；攻击者在网络之外拥有 X25519 共享秘密。	`x25519_broken`	proved	x25519_hybrid	checked
A08.11	被接受的 selected_group 是 X25519MLKEM768，与 CH1 提供的一致；攻击者仅拥有网络。	`network`	proved	group	checked
A08.11	transcript 被绑定：客户端仅以同一会话的 HRR 完成，因此 message_hash(CH1)、HRR 和 CH2 无法被替换；攻击者仅拥有网络。	`network`	proved	hrr_bound	checked
R02.12	重复的 HRR/CH 消息实例至多产生一个被接受的运行（对 HRR 的单射一致性）；攻击者仅拥有网络。	`network`	proved	hrr_inj	checked
R02.12	跨连接拼接的 HRR 不会被接受：客户端仅以绑定到其自身会话的 HRR 完成；攻击者仅拥有网络。	`network`	proved	hrr_bound	checked

目标	主张	攻击者	回答	查询	对照
A03.13	当客户端接受完成时，存在一个真实的服务器以匹配的身份和密钥共享运行（同一会话的服务器 Finished）；攻击者仅拥有网络。	`network`	proved	auth	checked
A03.13	双方派生出相同的应用流量密钥：无论客户端持有哪个应用密钥，服务器都派生出相同的密钥；攻击者仅拥有网络。	`network`	proved	appkey	checked
X01	完成的客户端只处理了唯一一个使用约定组的 HRR；在所建模的单次重试流程中，第二个 HRR 之后不会有完成；攻击者仅拥有网络。	`network`	proved	x01	checked
X02	接受的组/参数是 X25519MLKEM768，主动攻击者无法降级；攻击者仅拥有网络。	`network`	proved	group	checked
X02	客户端仅以匹配其自身会话的 HRR 完成，因此参数无法被攻击者选择的 HRR 替换；攻击者仅拥有网络。	`network`	proved	hrr_bound	checked
X03	攻击者无法分辨会话共享秘密取两个允许值中的哪一个（强保密性/不可区分性）；这不由符号 KEM 模型判定。	`network`	attack (model_artifact)	strong	

“攻击者分不清用的是两个值里的哪一个”这类性质，证明器从不直接判为不成立。它没有证出来，并给出了一条攻击者能把两个值分开的轨迹，攻击按这条轨迹记录：strong.

附录 D：分析是怎么跑的

分析者根据文稿构建协议模型，并将每个性质提交给 ProVerif；第 3 节中的每个结果都是证明器的回答。

ProVerif+ Agent 会话 session-20261115T080740，2026-11-15。状态：已完成。模型：deepseek-v4-1-flash-261017。步数：50，证明器 47 s，实际耗时 13 min，成本 0.118 USD。

ProVerif：运行了 109 次证明，107 次有判定，2 次无答案，31 s，记录了 48 个回答。

分析了什么

协议	TLS hybrid HelloRetryRequest profile
版本	rfc10024
分析范围	固定 X25519MLKEM768，单次 HelloRetryRequest 后完整服务器认证；保留 message_hash(CH1)、HRR、CH2 的 transcript 重构、cookie/selected_group 检查和第二次 HRR 拒绝。不将 HRR 过程当未认证的公钥替换成功。
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	541 numbered passages (142415 bytes) from the sections listed below. 本报告中的 s0001 之类的引用就是这些原文单元之一

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
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
rfc9846	4	握手协议
rfc9846	4.1	转录哈希
rfc9846	4.2	密钥交换消息
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

文稿	章节	标题
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 Binder
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	证书验证
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
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

文稿	章节	标题
rfc9846	7.5	导出器

源文包在文稿中定位到的协议目的：固定 X25519MLKEM768，单次 HelloRetryRequest 后完整服务器认证；保留 message_hash(CH1)、HRR、CH2 的 transcript 重构、cookie/selected_group 检查和第二次 HRR 拒绝。不将 HRR 过程当未认证的公钥替换成功。

对照文稿定性质

在写出查询之前，分析者把草拟的性质清单对照了文稿自身对协议目的的说明。名称、性质所关涉的内容以及文稿的说法都是分析者的解读；所列出处均存在于文稿中。

ID	简称	对象	文稿怎么说	出处
A03	HRR 后的服务器认证	客户端确信：若它在 HelloRetryRequest 之后完成握手，则确有一个真实服务器运行，其身份匹配、协商组为 X25519MLKEM768、密钥份额匹配且转录匹配。	RFC 9846 规定了 peer authentication：客户端对对端身份的看法应反映服务器的身份，且基于签名的模式在握手转录上认证服务器。	rfc9846:6490, s0345, s0401, s0427, s0437
A04	服务器运行不被双重接受	每一次客户端完成对应一次不同的真实服务器运行；一次服务器运行不能被接受两次（HRR/cookie/CH1 绑定）。	RFC 9846 要求 HRR/cookie 将重试的 ClientHello 绑定到 ClientHello1，并要求客户端在收到第二次 HRR 时中止；cookie 绑定 ClientHello1 的哈希。	s0080, s0126, s0167, s0168, s0247, s0251
A08	HRR 参数绑定到转录	客户端接受的 selected_group、密码套件、selected_version 和转录（message_hash(CH1)、HRR、CH2）与其 CH1 提议及 HRR 匹配，且不能被未认证的值替换。	RFC 9846 要求对照 supported_groups 和 key_share 检查 selected_group，保留 selected_version 和密码套件，并从 message_hash(CH1) 重构转录。	rfc9846:1074, s0057, s0058, s0126, s0131, s0133, s0247, s0251
K01	共享秘密与密钥的保密性	X25519MLKEM768 共享秘密、握手与应用流量密钥以及服务器长期签名私钥对网络攻击者保密。	RFC 9954 规定只要至少一个组件未被攻破，混合共享秘密就是安全的；RFC 9846 的密钥调度由其派生流量密钥。	rfc9954:550, s0015, s0044, s0045, s0522
K04	密钥分离与新鲜性	客户端与服务器的握手/应用流量秘密按方向和用途分离，不同会话不共享密钥。	RFC 9846 规定了会话密钥的唯一性：不同握手应产生不同且不相关的会话密钥，单个密钥应彼此不同且独立。	rfc9846:6495, s0503, s0522
R01	Cookie 绑定到当前 CH1	客户端接受的 HRR 及其 cookie 必须对应当前 ClientHello1；旧 HRR/cookie 不能作为本次运行的身份认证被接受。	RFC 9846 指出 cookie 使服务器能为无状态 HRR 绑定 ClientHello1 的哈希。	s0166, s0167, s0168
R02	HRR 或 ClientHello 不可重放	在一个连接内，给定的 HRR 或 ClientHello 实例至多被接受一次；跨连接拼接的 HRR 不能作为有效握手被接受。	RFC 9846 要求客户端在收到第二次 HRR 时中止，并禁止握手后复用 ClientHello；1-RTT 握手的重放受服务器 Random 限制。	s0080, s0087, s0126
C01	会话密钥的前向保密	握手完成后，服务器长期签名私钥的泄露不会暴露会话的握手或应用流量密钥。	RFC 9846 规定了相对于长期密钥的前向保密：只要临时材料被擦除，握手后签名密钥的失陷不会危及会话密钥。	rfc9846:6504, s0015, s0045

ID	简称	对象	文稿怎么说	出处
C04	单一坏组件下的混合安全	X25519 临时私钥份额或 ML-KEM 私钥份额的泄露，仍使会话共享秘密和流量密钥保持保密。	RFC 9954 规定只要至少一个组件的密钥交换算法未被攻破，混合秘密就是安全的。	rfc9954:550, s0015, s0019, s0041
C08	X25519 被攻破时 ML-KEM 提供保护	当 X25519 原语被攻破（攻击者获得 X25519 共享秘密）时，ML-KEM 组件仍保护会话共享秘密和流量密钥。	RFC 9954 规定只要至少一个组件未被攻破，混合秘密就保持安全；RFC 10024 将 X25519MLKEM768 固定为 ML-KEM 后接 X25519。	rfc9954:550, s0019, s0041, s0047
A08.11	selected_group 与转录绑定	客户端接受的 selected_group 与转录绑定到其 CH1 提议和 HRR 内容。	RFC 9846 要求客户端验证 selected_group 来自其 supported_groups 而非其 key_share，并用 message_hash(CH1) 重构转录。	rfc9846:1074, s0057, s0058, s0247, s0251
R02.12	HRR 或 ClientHello 的重放	重复的 HRR 或跨连接拼接的 HRR 不能作为有效握手被接受；消息实例至多被接受一次。	RFC 9846 要求收到第二次 HRR 时中止，并禁止握手后复用 ClientHello。	s0080, s0087, s0126
A03.13	服务器运行与应用密钥协商	当客户端接受完成时，确有一个真实服务器运行，其身份、组和密钥份额均匹配，且双方派生出相同的应用流量密钥。	RFC 9846 的 peer authentication 与认证消息：CertificateVerify 对转录签名，Finished 对其做 MAC；双方从共享秘密派生出相同的应用秘密。	rfc9846:6490, s0345, s0401, s0427, s0437, s0503
X01	第二次 HelloRetryRequest 后不完成	客户端及其正在建立的连接；第二次 HRR 是攻击者可能重放或拼接的消息。	RFC 9846 要求客户端在同一连接中收到第二次 HelloRetryRequest 时以 unexpected_message 中止。	s0126
X02	无降级的参数协商	客户端与服务器的密码参数，受保护以抵御主动网络攻击者。	RFC 9846 规定了降级保护：双方的密码参数应当相同，且与无攻击时相同。	rfc9846:6499
X03	会话共享秘密的强保密性	X25519MLKEM768 共享秘密及由其派生的流量密钥，对网络攻击者隐藏。	目录性质 K03（强保密/不可区分性）；该状态是证明器通过非干扰被要求达成的目标。	

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

宿主把文稿里说明协议保护什么、防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，或者为什么都不选。选了 3 段，没选 17 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	main:268-271	A03, A03.13, A08, A08.11, `network`	
P02	main:273-276	证明器问不了	面向实现者的侧信道指导；不是迹性质。
P03	main:278-280	证明器问不了	关于密码原语的定长假设，不是协议迹性质。
P04	main:282-287	证明器问不了	ML-KEM 封装随机性的性质，超出符号消息流范围。
P05	main:289-297	证明器问不了	针对不安全 RNG 的攻击；随机性质量超出符号模型范围。

段落	出处	定为	不选的原因
P06	main:299-306	C08, `x25519_broken`	
P07	main:308-310	证明器问不了	各组件之间与不安全 RNG 的交互；超出符号模型范围。
P08	rfc7748:783-793	证明器问不了	curve25519 的强度（约 128 位水平）；原语强度无法询问。
P09	rfc7748:802-808	证明器问不了	curve448 的强度取舍；原语强度无法询问。
P10	rfc7748:810-818	证明器问不了	贡献性行为／低阶点：符号 DH 定律 g^xy=g^yx 无法表示低阶点，因此全零共享秘密检查（main s0018）无法询问。
P11	rfc7748:820-825	没有陈述目标	面向设计者关于用公钥作标识符的建议；没有陈述协议目标。
P12	rfc7748:827-837	证明器问不了	实现层面的可区分性与时序；超出符号模型范围。
P13	rfc9846:4676-4677	没有陈述目标	指向附录 C、E、F；本身没有陈述任何目标。
P14	rfc9954:550-558	C04, C08, `x25519_broken`, `x25519_sk_leak`, `mlkem_sk_leak`	
P15	rfc9954:560-569	证明器问不了	要求 KEM 满足 IND-CCA2/FO；这是原语的性质，不是握手迹的性质。
P16	rfc9954:571-574	证明器问不了	关于密钥、密文和秘密值的定长假设。
P17	rfc9954:576-582	证明器问不了	变长时序侧信道；不是迹性质。
P18	rfc9954:584-586	证明器问不了	变长秘密值配合非抗碰撞哈希；属于密码学假设。
P19	rfc9954:588-592	没有陈述目标	设计指导：若非定长，则需要长度前缀；对本定长配置没有目标。
P20	rfc9954:594-597	证明器问不了	要求只使用定长共享秘密；这是对原语的假设。

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 32 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 13 条，没检查 19 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	任务建模的是握手；TLS 记录层载荷保密性未建模。
K03	强保密／秘密值不可区分性	X03	
D01	消息完整性与数据来源真实性	A03, A08	
A01	对端曾参与性（Aliveness）	A03, A03.13	
A02	弱一致性认证	A03	
A05	隐式密钥认证	A03, K01	
A06	显式密钥确认	A03.13	
A07	身份—凭据—密钥绑定	A03	
R03	业务操作至多一次	不适用	握手过程中没有业务操作、计费或一次性令牌。
R04	消息接受顺序／窗口安全	R02	
R05	抗降级／安全策略保持	X02	
C02	抗密钥泄露冒充（KCI）	不适用	本配置只认证服务器；客户端没有长期凭据，因此不存在客户端密钥泄露冒充目标。服务器密钥泄露即服务器身份本身，不是 KCI。

条目	目录里的性质	作为哪条性质检查	不检查的原因
C03	已知密钥安全／泄露隔离	K04	
C05	泄露后安全恢复（PCS）	不在范围内	主握手中没有棘轮或密钥更新；KeyUpdate（s0473）不在建模流程内。
C06	注册凭据泄露后的增强认证	不适用	没有 PAKE 或注册记录。
C07	抗离线字典攻击	不适用	没有口令或可猜测的秘密值。
Z01	授权执行正确性	不适用	握手中没有授权决策。
Z02	委托权限不扩张	不适用	没有委托或代理。
Z03	授权与身份／会话／操作绑定	不适用	没有授权令牌或服务会话。
Z04	撤销与过期生效	不适用	没有撤销或过期机制。
Z05	跨租户／跨服务安全隔离	不适用	没有租户或共享服务。
S01	加密 nonce 唯一性	不在范围内	AEAD nonce 属于记录层关注点；任务建模的是握手消息。
S02	重传／密钥重安装安全	R02	
S03	抗回滚与状态单调性	R02, X02	
S04	跨阶段安全上下文一致性	A08	
S05	终止与旧状态失效	不在范围内	建模的握手中没有拆除、去认证或注销。
P01	身份匿名性	不在范围内	身份保密性依赖记录层对 Certificate 消息的加密，而握手模型不包含这一层。
P02	会话不可关联性	不在范围内	会话不可关联性依赖未建模的记录层行为。
P03	用户／凭据存在性隐藏	不适用	没有登录、发现或注册查询。
V01	条件性进展／错误恢复	证明器问不了	无法对协议模型询问条件性进展／错误恢复（终止性）。
V02	无非预期死锁	证明器问不了	无法询问无死锁（终止性）。
V03	受限资源滥用／抗放大	证明器问不了	除事件计数外，无法询问资源开销与放大界。

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 27 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 12 项，没设的 15 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	客户端只持有自己的临时材料和没有长期凭据；网络攻击者本来就可以扮演客户端。
S02	服务器	参与方	`server_sig_key_leak`	
S03	服务器身份	值	攻击者得不到更多	服务器证书和身份是公开的。
S04	协商组与密钥份额	值	攻击者得不到更多	协商组和密钥份额在网络上传输。
S05	握手 transcript	值	攻击者得不到更多	握手 transcript 是公开的。
S06	HRR 与 CH1/CH2 的绑定	值	攻击者得不到更多	HRR/CH 绑定值是公开的。
S07	cookie	值	攻击者得不到更多	cookie 值以明文发送；只保护其完整性。
S08	selected_group	值	攻击者得不到更多	selected_group 是公开的。
S09	cipher suite	值	攻击者得不到更多	cipher suite 是公开的。

ID	参与方或值	类别	攻击者条件	不设的原因
S10	selected_version	值	攻击者得不到更多	selected_version 是公开的。
S11	transcript（message_hash(CH1)、HRR、CH2）	值	攻击者得不到更多	transcript 是公开的。
S12	X25519MLKEM768 共享秘密	值	one_session_key_leak	
S13	握手流量密钥	值	one_session_key_leak	
S14	应用流量密钥	值	one_session_key_leak	
S15	服务器长期签名私钥	值	server_sig_key_leak	
S16	client_handshake_traffic_secret	值	one_session_key_leak	
S17	server_handshake_traffic_secret	值	one_session_key_leak	
S18	client_application_traffic_secret	值	one_session_key_leak	
S19	server_application_traffic_secret	值	one_session_key_leak	
S20	CH1 哈希	值	攻击者得不到更多	Hash(ClientHello1) 是公开的。
S21	HRR	值	攻击者得不到更多	HRR 是公开的。
S22	CH1	值	攻击者得不到更多	ClientHello1 是公开的。
S23	CH2	值	攻击者得不到更多	ClientHello2 是公开的。
S24	历史会话握手/应用流量密钥	值	one_session_key_leak	
S25	流量密钥	值	one_session_key_leak	
S26	会话共享秘密	值	one_session_key_leak	
S27	transcript	值	攻击者得不到更多	transcript 是公开的。

每条性质在各攻击者条件下的答案

攻击者条件由分析者设定，在写查询之前就定好了；每个答案都记录在其中一个攻击者条件下。单元格是证明器在该攻击者条件下对该性质给出的答案；“无答案”是为该性质设定的一个攻击者条件，在该条件下证明器把某条主张留作未决，或者没有记录任何内容；空单元格是分析者没有为该性质设定的攻击者条件。

攻击者	持有什么	依据	出处
network	仅网络：读取、丢弃、修改和发送消息，不持有任何一方的秘密		
server_sig_key_leak	服务器的长期证书签名私钥，在握手完成后获得	RFC 9846 的前向保密是针对握手后长期签名密钥泄露而言的。	rfc9846:6504
x25519_sk_leak	某会话中客户端的 X25519 临时私有标量，以及对端的公开份额，但不含 ML-KEM 私钥	RFC 9846 的前向保密讨论指出，密钥份额对应的私钥必须擦除；RFC 9954 要求在一个组件未被攻破时仍保持安全。	rfc9954:550
mlkem_sk_leak	某会话中客户端的 ML-KEM-768 解封装私钥，但不含 X25519 私有标量	RFC 9954 混合性质：只要至少一个组件未被攻破就是安全的。	rfc9954:550
x25519_broken	该会话的 X25519 共享秘密（X25519 组件被攻破），而 ML-KEM 仍然安全	RFC 9954 混合性质：当一个组件失效时，拼接后的秘密仍必须保持安全；RFC 7748 指出 CRQC 可恢复 X25519 标量。	rfc9954:550, rfc7748:783
one_session_key_leak	某个已完成会话的共享秘密以及握手/应用流量密钥，在握手后从一方存储中读取	RFC 9846 规定不同握手之间的会话密钥唯一且无关，因此一个会话中泄露的密钥不得暴露另一个会话。	rfc9846:6495

ID	network	server_sig_key_leak	x25519_sk_leak	mlkem_sk_leak	x25519_broken	one_session_key_leak
A03	成立					
A04	成立					
A08	成立					
K01	成立					
K04	成立					成立
R01	成立					
R02	成立					
C01		成立				
C04			成立	成立		
C08					成立	
A08.11	成立					
R02.12	成立					
A03.13	成立					
X01	成立					
X02	成立					
X03	无答案					

原文和目标

Source: 541 units, 142415 bytes, frozen in source-delivery-01.json. Targets: 10 approved (A03, A04, A08, K01, K04, R01, R02, C01, C04, C08); the questions asked: 3. The list of targets was approved as drafted, beforehand, with --approve-targets.

宿主按其文档化的默认设置（任务 `decisions: auto`）做出的决定，供你核对：

- approve_package: 批准源文包 protocol-901b7b236d9f45b5e4ddfc180692

该步骤自报的结果：1 次请求（1 次失败），0.000 USD，输入 66836 个 token，输出 4526 个 token，耗时 28 s。

关于证明器和模型的说明

分析者为各目标指明的特征：

step	targets	features	reason
34	K01, C01, C04, C08, X03, A03, A03.13	plain_primitives	混合交换用 hash、MAC、KDF、签名以及一个符号化 KEM 加 Diffie-Hellman 来建模，Diffie-Hellman 只采用其单一法则 g^xy=g^yx；除此之外没有对 ML-KEM 或 X25519 的代数法则建模，因此保密性与前向保密的答案建立在这一朴素原语抽象之上。
34	A03, A04, A08, A08.11, R01, R02, R02.12, K01, K04, C01, C04, C08, X01, X02, A03.13	many_sessions	客户端、服务器和受损副本都被复制，因此认证、绑定、重放和密钥分离的答案对任意数量的会话和参与方都成立。

分析者的结束语

全部 16 个目标都有答案。其中 15 个在 model.pv 上得到证明，并配有对照查询，该对照查询会推翻一个更强或相反的变体：HRR 之后的服务器认证（A03、A03.13）、单射性一致且不会双重接受（A04）、HRR/selected_group/transcript 绑定（A08、A08.11、R01、R02、R02.12）、单次重试/不出现第二次 HRR 以及降级（X01、X02）、密钥保密性（K01）、在 network 和一次会话密钥泄漏下的密钥分离（K04）、在服务器签名密钥泄漏下的前向保密（C01），以及任一会话临时密钥泄漏或 X25519 被攻破下的混合性质（C04、C08）。X03（共享秘密的强保密性/不可区分性）无答案：符号化 KEM 只使用一个全局选定的秘密，使充当客户端的攻击者能够解封装并检验它，这属于 model_artifact；逐会话的强保密性检查则属于 Tamarin+ Agent 的范畴。没有新的发现：每一条得到证明的保证都在文稿中有所陈述（RFC 9846 的对端认证、唯一性、前向保密、降级；RFC 9954 的混合性质），文稿点名的每一次攻击在文稿给出的攻击者下都被排除。该分析是符号化的（KEM、仅带 g^xy=g^yx 的 DH、hash、MAC、签名），覆盖任意数量的会话，不覆盖记录层、原语强度、全零/小阶 X25519 检查、RNG 质量，也不覆盖固定单一群导致群/密码套件/版本绑定形同虚设这一点。没有出现改变状态的目标，因此不需要 bounded.pv，也不需要状态审查。