Review TLS 混合完整转录的安全性分析

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	12 条：8 条成立，4 条不成立（4 个攻击）
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

该协议是采用混合组 X25519MLKEM768 的 TLS 1.3 握手：客户端与服务器协商出一个临时混合秘密，服务器用证书完成自我认证。客户端持有一个 ML-KEM-768 密钥对、一个 X25519 临时标量和一个 ClientHello 随机数；服务器持有其长期签名密钥，并选取一个新的 ML-KEM 封装、一个新的 X25519 标量和一个 ServerHello 随机数。

客户端的 key_exchange 是封装密钥后接 X25519 份额，服务器回应一个 ML-KEM 密文后接其 X25519 份额，双方把两个分量的共享秘密拼接成 TLS 1.3 密钥调度所消费的值。由于只有公开份额进入转录哈希，每条握手消息都被绑定：服务器通过其 Certificate 对转录签名，两条 Finished 消息确认两端从同一混合秘密派生出相同的握手密钥。

参与方：

- **Client**：发起方，不持有客户端证书。持有：服务器证书（验证密钥），受信任。
- **Server**：用证书认证。持有：签名密钥和证书。

图 1 展示了文稿所规定的交换过程。

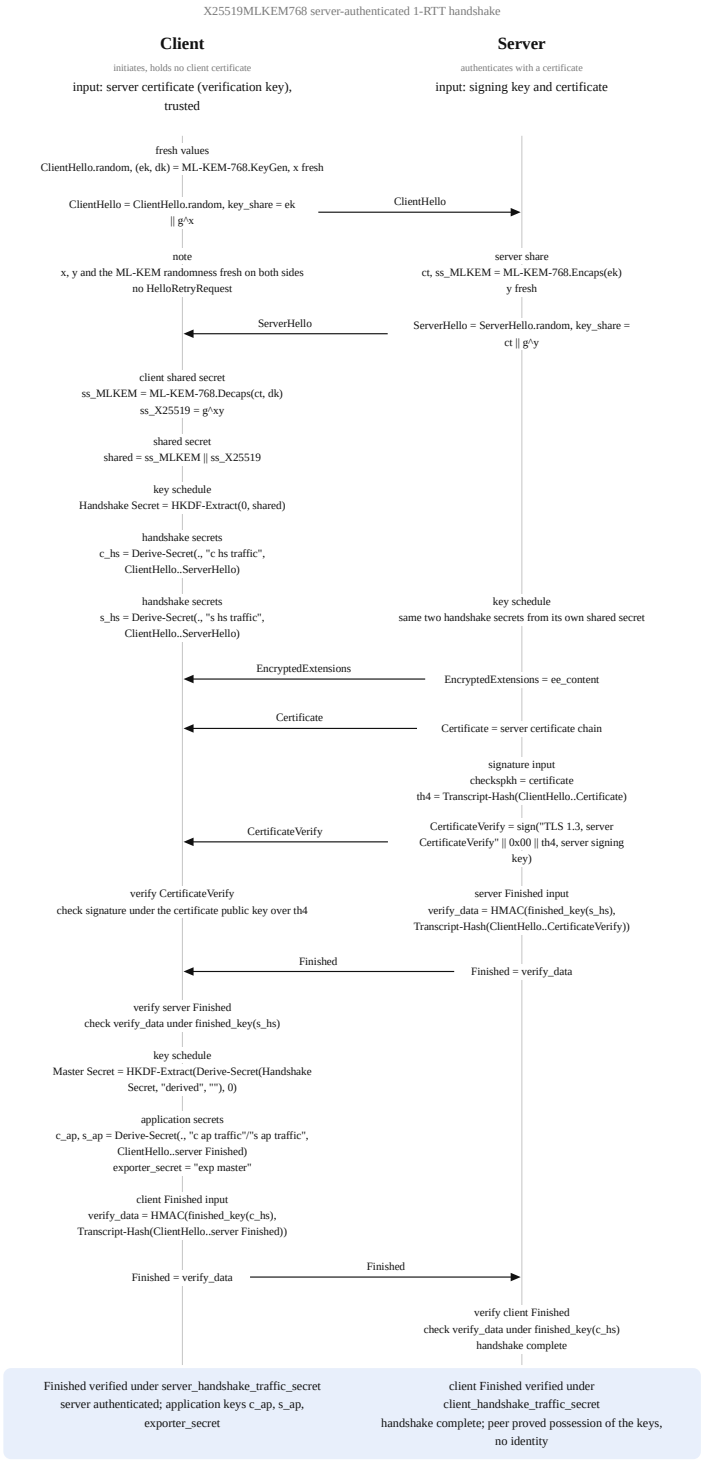


图 1. 文稿所规定的协议。

分析的范围见附录 D：分析了什么、遗漏了什么，以及它依据的文稿章节。

2 发现

没有发现。 分析没有发现文稿尚未写明或尚未排除的任何问题。第 3 节的表格给出了每条性质的结果。

在已分析的范围内——一次 1-RTT 握手、服务器认证、X25519MLKEM768、无 HRR、无 PSK、无 0-RTT——协议提供了该配置文件所期望的东西。共检查了十二个目标；十一个已有答案，第十二个是方法检查，已满足。没有发现新的弱点：这里复现的每个否定结果都是文稿已经写明的结果，因此本报告没有发

现。这些保证是在一个模型上的证明，该模型使用理想签名、理想 KDF 和哈希，并将 X25519 归约为 g^xy = g^yx 这一规律，因此它们在这些假设下成立；Tamarin+ Agent 保留指数和 KEM 的原样，是能去掉第二个假设的工具。值得读者注意的一个行为是：此模式下的服务器无法区分诚实客户端和攻击者自己运行的客户端会话，RFC 9846 已写明这一点，模型也复现了它。

3 检查过的性质

每一行是一条提交给 ProVerif 的性质。结果是 ProVerif 在分析者所建协议模型上给出的答案；价值和文稿是否已写明该结果都是分析者的判断，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	**服务器向客户端认证。** 每当客户端完成握手并接受服务器身份，就存在一次服务器真实运行，且该运行意图的对端身份就是该客户端。	无	成立	中	是
A03	**会话密钥协商。** 每当一方完成握手，就存在对端的一次匹配运行，双方对身份、协商组、混合共享秘密及由它派生的握手/应用流量密钥一致。	无	攻击成立（文稿已写明）	中	是
A04	**接受唯一性。** 每次客户端或服务器成功接受都对应一次不同的对端真实运行，同一对端运行不能被两次接受匹配。	无	攻击成立（文稿已写明）	中	是
A06	**Finished 密钥确认。** 在确认接受点，验证方要求对端对本次会话同一密钥真实导出并发送匹配的 Finished 确认。	无	攻击成立（文稿已写明）	中	是
A08	**转录与角色绑定。** 接受的协商组、角色与 transcript 对应获批的对端提议和当前会话上下文，CertificateVerify 与 Finished 覆盖完整消息序列。	无	成立	中	是
K01	**会话密钥保密性。** 攻击者不能推导服务器长期签名私钥、握手流量密钥、应用流量密钥与 exporter 秘密。	无	成立	中	是
C01	**长期密钥泄露下的前向保密。** 会话完成并擦除临时状态之后泄露服务器长期签名私钥，攻击者仍不能得到此前会话的握手或应用流量密钥。	服务器长期签名私钥 (会话完成并擦除临时秘密之后)	成立	中	是
C04	**单一组件失效下的混合主张。** 泄露 X25519 临时私钥或 ML-KEM 解封装私钥之一时，攻击者仍不能得到应用流量密钥；每个泄露组合单独记录。	X25519 临时私钥或 ML-KEM-768 解封装私钥（单分量） (会话期间或之后)	成立	中	是
K04	**派生密钥分离。** 客户端/服务器方向、握手/应用数据用途以及不同会话的密钥互不相同，派生上下文绑定正确。	无	成立	低	是
A08.10	**CertificateVerify 绑定完整转录。** CertificateVerify 与 Finished 覆盖完整握手消息序列并绑定发送方角色，接受方不会把其他序列或其他角色的证据当作本次有效。	无	成立	中	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
C04.11	**单一组件失效，密钥仍保密。** 泄露 X25519 临时私钥或 ML-KEM 解封装私钥之一时，攻击者仍不能得到应用流量密钥。	X25519 临时私钥或 ML-KEM-768 解封装私钥（单分量） (会话期间或之后)	成立	中	是
Q3	**基线模型上的攻击。** 要求攻击轨迹在保留规范检查的基线模型中复现。	无	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）。

所提的问题及分析者的回答：

问题	回答	依据
Q1: CertificateVerify/Finished 对完整消息序列与角色绑定	客户端一侧：客户端接受的 CertificateVerify 在服务器上下文串下覆盖从 ClientHello 到 Certificate 的消息，Finished 值由此链式衔接，因此二者都不能被移到另一序列，也不能被另一个角色重用。服务器无法对其对端作出同样的论断，因为此模式下客户端未被认证，可能是攻击者驱动的会话。	A08, A08.10, A02, A06
Q2: 应用流量密钥保密与单个 KEM/DH 分量泄露区分	只恢复 X25519 标量、或只知道 ML-KEM 解封装密钥时，应用流量密钥仍然保密；两者都知道时就失去保密。这正是混合主张，报告中对每个方向分别给出答案。	C04, C04.11, K01
Q3: 每个攻击须复现到未移除规范检查的基线模型	所有报告的轨迹都来自同一个基线模型，该模型保留证书检查、签名验证和两项 Finished 检查；协议未认证的一方唯一的接受行为是服务器接受攻击者自己客户端会话发来的 Finished，RFC 9846 附录 F.1 已写明这一点。	Q3, A03, A06

4 本次分析的局限

这里的结果是协议模型上的结果：它说明规定的消息和检查给出或不给出什么，其中密码学被视为理想，对实现不作任何断言。

据分析者所述，本分析不覆盖以下内容：

- 不同会话的会话密钥之间未证明互不相同；只检查了一个会话内部的密钥分离。
- 套件的 AEAD、记录层、nonce 处理和 KeyUpdate 机制未建模。
- X25519 是仅遵守 g^xy = g^yx 这一条规律的幂运算；没有建模其他代数性质，也没有建模量子攻击者。C04 的单分量主张在该抽象下成立。
- ML-KEM 用封装函数和解封装析构函数表示；RFC 10024 第 4.2 节的封装密钥检查和密文长度检查未建模。
- 证书链验证、吊销和签名算法检查不在范围内；证书按值比较。
- 一方的失陷只建模为所列三种泄露：X25519 标量、ML-KEM 解封装密钥、握手后的服务器签名密钥。
- HRR、PSK、0-RTT、恢复和客户端证书被范围排除，因此本文对它们不作任何断言。

宿主记录的内容：

- A02、A03、A04、A06、A08、K01、C01、C04、K04、A08.10、C04.11 的答案依赖于模型所做的简化（附录 D）。
- 没带对照查询的证明（附录 C）：A02: a02, A03: a02, A04: a04c, A06: a06s, A08: a08, K04: k04_dir, K04: k04_pur, A08.10: a08。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。

每条性质还有哪些未决之处、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，不是证明器的答案：这些答案对协议意味着什么、解读依据什么、能否按原样使用，以及它有多大价值。

A02: 服务器向客户端认证

每当客户端完成握手并接受服务器身份，就存在一次服务器真实运行，且该运行意图的对端身份就是该客户端。

每当客户端完成握手，就存在一个运行了同一会话的服务器：它签署了同一转录，并在该会话的握手密钥下发送了 Finished。网络攻击者无法让客户端接受一个没有服务器运行过的会话，也无法把服务器的飞行消息移到另一个客户端会话中。

- 结果：成立；回答了所问：是；可带保留使用
- 价值中：这是一条在无界会话上证明的中心认证保证，但模型理想化了签名并限制了 Diffie-Hellman 代数。
- 文稿已写明：是。文稿中的位置：rfc9846:6490
- 依据：X25519 是仅遵守 g^xy = g^yx 的幂运算；Finished 检查是应用该规律之处，会话由经 Certificate 的转录哈希命名，其中只使用公开值；证书检查建模为证书值上的相等；链验证不在范围内；哈希、KDF 和签名均为理想

A03: 会话密钥协商

每当一方完成握手，就存在对端的一次匹配运行，双方对身份、协商组、混合共享秘密及由它派生的握手/应用流量密钥一致。

对于客户端完成的会话，两端持有相同的握手密钥和相同的混合共享秘密：客户端接受的服务器 Finished 就是该密钥下对该转录的 MAC。对于服务器侧，无法对对端得出任何结论，因为此模式下只有服务器经过认证：服务器会接受来自任何客户端会话的 Finished，包括攻击者自己运行的会话。

- 结果：攻击成立（文稿中有述）；是否回答了所问：部分；可在有保留条件的情况下使用
- 价值中：正面的一半是有用的保证；负面的一半是协议声明的行为，因此结果是在精确条件下的机械性确认。
- 文稿中有述：是。文稿中的位置：rfc9846:6486
- 依据：对密钥值的协商一致是通过 Finished 检查读取的，而不是通过密钥项的直接相等，ProVerif 在此无法表述后者；X25519 代数限于 g^xy = g^yx；客户端在模型中没有凭证，因此服务器没有可用于认证它的东西
- 未决：将密钥值本身的一致作为独立查询

A04: 接受唯一性

每次客户端或服务器成功接受都对应一次不同的对端真实运行，同一对端运行不能被两次接受匹配。

每次客户端接受都匹配一次不同的服务器运行，因此同一个服务器飞行不能被重放为两次接受。服务器接受不匹配诚实客户端的某次不同运行：攻击者可以用服务器打开自己的客户端会话，这是一次真实的客户端运行，因此没有诚实会话被重用。

- 结果：攻击成立（文稿中有述）；是否回答了所问：部分；可在有保留条件的情况下使用

- 价值中：会话密钥的唯一性在客户端侧得到确认，服务器侧有记录的缺口得到复现。
- 文稿中有述：是。文稿中的位置：rfc9846:6486
- 依据：会话标识符是经由 Certificate 的转录哈希，因此运行的不同即该哈希的不同；一次运行中会话无界；新鲜性来自 ClientHello 随机数和两个临时共享

A06: Finished 密钥确认

在确认接受点，验证方要求对端对本次会话同一密钥真实导出并发送匹配的 Finished 确认。

客户端只有在服务器 Finished 是由同一混合共享秘密和同一转录派生的握手流量密钥下的 MAC 时才接受它，因此它确认的是密钥，而不仅仅是转录。服务器以同样的方式验证其客户端 Finished，但无法分辨是哪一方计算了它。

- 结果：攻击成立（文稿中有述）；是否回答了所问：部分；可在有保留条件的情况下使用
- 价值中：确认了客户端侧的密钥确认，并给出了服务器侧的精确边界。
- 文稿中有述：是。文稿中的位置：rfc9846:6435
- 依据：MAC 理想化：攻击者没有握手密钥就无法伪造 Finished；服务器侧被表述为密钥确认，而非对端的认证

A08: 转录与角色绑定

接受的协商组、角色与 transcript 对应获批的对端提议和当前会话上下文，CertificateVerify 与 Finished 覆盖完整消息序列。

客户端接受的 CertificateVerify 是服务器经由 Certificate 对转录产生的，因此组、两个共享、EncryptedExtensions 和证书在签名之前就已绑定。来自另一会话或客户端角色的签名不能被移入本会话。

- 结果：成立；是否回答了所问：是；可在有保留条件的情况下使用
- 价值中：在理想签名下证明了 RFC 10024 安全论证所依赖的转录绑定。
- 文稿中有述：是。文稿中的位置：rfc9846:6413, rfc9846:6420
- 依据：签名是理想的且不可伪造；上下文字符串区分服务器和客户端角色；客户端角色未建模

A08.10: CertificateVerify 绑定完整转录

CertificateVerify 与 Finished 覆盖完整握手消息序列并绑定发送方角色，接受方不会把其他序列或其他角色的证据当作本次有效。

直接回答该问题：CertificateVerify 覆盖 ClientHello、ServerHello、EncryptedExtensions 和 Certificate，其上下文字符串指明签名角色；每个 Finished 覆盖该转录加上其之前的消息。这两条消息都不能被移到另一序列，也不能被另一角色重用。

- 结果：成立；是否回答了所问：是；可在有保留条件的情况下使用
- 价值中：所要求的完整序列和角色绑定检查得到肯定回答，HRR 路径按范围排除。
- 文稿中有述：是。文稿中的位置：rfc9846:6413
- 依据：无 HRR，因此转录的 message_hash 替换从不适用；无客户端证书，因此只出现服务器上下文字符串

K01: 会话密钥保密性

攻击者不能推导服务器长期签名私钥、握手流量密钥、应用流量密钥与 exporter 秘密。

服务器签名密钥、客户端和服务器握手流量秘密、客户端和服务器应用流量秘密以及 exporter 秘密，都不能被仅有网络的攻击者推导。每个对照查询确认该查询可以失败：一旦会话的两个临时组件都被公布，同一密钥就会泄露。

- 结果：成立；是否回答了所问：是；可用
- 价值中：在有对照查询的情况下，对无界会话上的保密目标给出了清晰的陈述；DH 代数的简化在此对攻击者没有帮助。
- 文稿中有述：是。文稿中的位置：rfc9846:6483
- 依据：AEAD 和 KDF 是理想的；保密性是对秘密本身提出的，而不是对由它们派生的流量密钥；客户端密钥仅针对服务器也运行过的会话查询

C01: 长期密钥泄露下的前向保密

会话完成并擦除临时状态之后泄露服务器长期签名私钥，攻击者仍不能得到此前会话的握手或应用流量密钥。

一旦握手完成且临时状态已消失，公布服务器的长期签名密钥并不会给出服务器所运行会话的应用流量秘密：那些只依赖于每会话的混合秘密。对照查询表明，一旦会话的两个临时组件都被公布，同一查询就会失败。

- 结果：成立；是否回答了所问：是；可在有保留条件的情况下使用
- 价值中：相对于长期密钥的前向保密是该配置的核心主张，并显示为仅依赖于临时组件保持秘密。
- 文稿中有述：是。文稿中的位置：rfc9846:6504
- 依据：泄露发生在握手之后；模型没有擦除失败，因此假设临时秘密不被保留；X25519 代数限于 g^xy = g^yx；模型无法说明临时标量能抵抗量子攻击者

C04: 单一组件失效下的混合主张

泄露 X25519 临时私钥或 ML-KEM 解封装私钥之一时，攻击者仍不能得到应用流量密钥；每个泄露组合单独记录。

恢复一个会话的 X25519 标量，如同拥有量子计算机的被动观察者所能做到的，只要 ML-KEM 解封装密钥保持秘密，应用流量秘密就仍然保密：拼接秘密中的 ML-KEM 组件仍然未知。仅知道 ML-KEM 解封装密钥是对称的情形：X25519 组件仍然提供保护。公布两个组件会破坏该会话，如对照查询所示。

- 结果：成立；是否回答了所问：是；可在有保留条件的情况下使用
- 价值中：这正是混合配置存在的性质，按组件得到确认；组合器本身的密码学仍是一个假设。
- 文稿中有述：是。文稿中的位置：main:299, rfc9954:550
- 依据：混合秘密是进入 HKDF 的两个组件秘密的拼接；RFC 9954 的对偶 PRF 论证未建模，只对 KDF 做了理想化；ML-KEM 是基于析构函数的封装，因此除非解封装密钥已知，ML-KEM 共享秘密是保密的；X25519 标量作为值公布，代表量子攻击者的恢复

C04.11: 单一组件失效，密钥仍保密

泄露 X25519 临时私钥或 ML-KEM 解封装私钥之一时，攻击者仍不能得到应用流量密钥。

直接回答该问题：只破坏两个临时组件之一时，该会话的应用流量密钥不可推导；两个都被破坏时则可推导。两个方向由不同查询回答，因此报告显示了哪个组件承载保证。

- 结果：成立；是否回答了所问：是；可在有保留条件的情况下使用
- 价值中：逐组件直接回答了该配置为之规定的实际问题。

- 文稿中有述：是。文稿中的位置：rfc9954:550
- 依据：理想的 KDF 和 MAC；定长秘密的拼接在模型中是单射的；不对量子攻击者破坏组合器本身作任何主张

K04: 派生密钥分离

客户端/服务器方向、握手/应用数据用途以及不同会话的密钥互不相同，派生上下文绑定正确。

一个会话的客户端和服务器应用流量秘密是不同的值，exporter 秘密不同于应用秘密，因为每个都用自己的标签从主秘密派生。因此，一个方向或一个用途的密钥永远不会被用作另一个。

- Result: Holds；对所问的回答：是；有保留地可用
- Value low：直接来自密钥调度中的标签规则；值得作为一项检查记录，而不是作为结果。
- 文稿中有说明：是。文稿中的位置：rfc9846:6495
- 依据：标签是常量，KDF 是理想的，因此不同标签产生不同输出；未覆盖：两个不同会话的机密之间的差异性，以及由某个机密派生出的流量密钥

Q3: 基线模型上的攻击

要求攻击轨迹在保留规范检查的基线模型中复现。

分析报告的每条轨迹都来自同一个模型，该模型保留了证书相等性检查、CertificateVerify 签名验证和两处 Finished 验证。为该目标记录的轨迹是：服务器接受来自攻击者所驱动客户端会话的 Finished；在所有检查都在位的情况下它可达，并且这正是 RFC 9846 附录 F.1 针对单向认证连接所述的行为。

- Result: Attack holds（文稿中有说明）；对所问的回答：是；可用
- Value low：这是分析的一项要求，而不是文稿的陈述；它的回答是该要求已满足，且它所指出的唯一一条轨迹就是文稿记录的那条。
- 文稿中有说明：是。文稿中的位置：rfc9846:6486
- 依据：该模型就是基线：没有任何分支移除检查；该模型上存在完整握手，这正是所检查的内容

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，以及带有分析者对每条攻击的判定的攻击。

目标	级别	界	查询	对照	攻击	主张
A02	proved		a02			1 proved
A03	proved		a02		a06c (holds_in_source)	1 proved, 1 attack
A04	proved		a04c		a04s (holds_in_source)	1 proved, 1 attack
A06	proved		a06s		a06c (holds_in_source)	1 proved, 1 attack
A08	proved		a08			1 proved
K01	proved		k01_ssk	checked		6 proved
C01	proved		c01	checked		1 proved
C04	proved		c04_x	checked		2 proved
K04	proved		k04_dir			2 proved
A08.10	proved		a08			1 proved
C04.11	proved		c04_x	checked		2 proved
Q3	reachable		run		a06c (holds_in_source)	2 reachable, 1 attack

逐条主张，按分析者对每条主张的措辞；对每条主张的回答来自证明器：

目标	主张	攻击者	回答	查询	对照
A02	每当客户端完成握手，就存在一个针对同一 transcript 的服务器运行：它在该同一消息序列上发送了 Certificate、CertificateVerify 和一个服务器 Finished。	network	proved	a02	none
A03	客户端只接受服务器运行过的 transcript；由于它检查的服务器 Finished 是在其自身握手流量密钥下的 MAC，两端持有相同的握手密钥和相同的混合共享机密。	network	proved	a02	none
A03	每当服务器完成握手，它所接受的对端都是同一会话的一次客户端运行。	network	attack (holds_in_source)	a06c	
A04	每次客户端接受都对应一次不同的服务器运行。	network	proved	a04c	none
A04	每次服务器接受都对应同一会话的一次不同的客户端运行。	network	attack (holds_in_source)	a04s	
A06	仅当服务器 Finished 是由同一混合共享机密和同一 transcript 派生出的服务器握手流量密钥下的 MAC 时，客户端才接受它。	network	proved	a06s	none
A06	仅当客户端 Finished 是在它所派生出的客户端握手流量密钥下的 MAC 时，服务器才接受它。	network	attack (holds_in_source)	a06c	

目标	主张	攻击者	回答	查询	对照
A08	客户端接受的每个 CertificateVerify 都由服务器针对经过 Certificate 的 transcript 生成，其中包括协商的群、共享值以及链中携带的身份信息。	`network`	proved	a08	none
K01	网络攻击者无法推导出服务器长期签名私钥。	`network`	proved	k01_ssk	checked
K01	网络攻击者无法推导出某个会话的客户端应用流量机密。	`network`	proved	k01_cap	checked
K01	网络攻击者无法推导出某个会话的服务器应用流量机密。	`network`	proved	k01_sap	checked
K01	网络攻击者无法推导出某个会话的客户端握手流量机密。	`network`	proved	k01_chs	checked
K01	网络攻击者无法推导出某个会话的服务器握手流量机密。	`network`	proved	k01_shs	checked
K01	网络攻击者无法推导出某个会话的 exporter 机密。	`network`	proved	k01_exp	checked
C01	在服务器长期签名密钥被泄露且临时状态被擦除后，真实服务器所运行会话的应用流量机密仍保持机密。	`server_sig_key_after_session`	proved	c01	checked
C04	在会话的 X25519 标量被恢复而 ML-KEM 解封装密钥仍保密的情况下，该会话的应用流量机密仍保持机密。	`x25519_scalar_crqc`	proved	c04_x	checked
C04	在客户端的 ML-KEM-768 解封装密钥已知而 X25519 标量仍保密的情况下，该会话的应用流量机密仍保持机密。	`mlkem_decaps_key`	proved	c04_k	checked
K04	同一会话的客户端和服务器应用流量机密不同。	`network`	proved	k04_dir	none
K04	某个会话的 exporter 机密与其客户端应用流量机密不同，每个密钥都用各自的标签从主机密派生。	`network`	proved	k04_pur	none
A08.10	CertificateVerify 覆盖 ClientHello、ServerHello、EncryptedExtensions、Certificate 的整个序列，并通过其上下文串绑定服务器角色；随后 Finished 值又覆盖该内容加上签名，因此二者都不能被移到另一个会话，也不能被另一角色使用。	`network`	proved	a08	none
C04.11	仅 X25519 临时标量被恢复时，该会话的应用流量密钥仍保持机密。	`x25519_scalar_crqc`	proved	c04_x	checked
C04.11	仅 ML-KEM-768 解封装密钥已知时，该会话的应用流量密钥仍保持机密。	`mlkem_decaps_key`	proved	c04_k	checked
Q3	所报告的每次攻击都是基线模型的一条轨迹，该模型保留了证书相等性检查、CertificateVerify 签名验证和两处 Finished 检查，因此没有为得到它而移除任何检查。		reachable	run	
Q3	所报告的每条攻击轨迹都是基线模型的一条轨迹，该模型保留了证书相等性检查、CertificateVerify 签名验证和两处 Finished 检查，因此没有移除规范的任何检查。	`network`	reachable	run	

目标	主张	攻击者	回答	查询	对照
Q3	分析所报告的轨迹在基线模型上可达，该模型保留了证书相等性检查、CertificateVerify 签名验证和两处 Finished 检查：没有为得到它而移除任何规范检查。	`network`	attack (holds_in_source)	a06c	

附录 D：分析是怎么跑的

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

ProVerif+ Agent 会话 session-20261114T233005，2026-11-14。状态：已完成。模型：deepseek-v4-1-flash-261017。步数：58，证明器 109 秒，实际耗时 15 分钟，成本 0.207 USD。

上下文：宿主从对话中移除了陈旧部分 1 次，共 227894 个字符（较早的推理，以及显示模型在最近一次变更之前的内容）。轨迹文件保留了一切。

ProVerif：运行了 152 次证明，148 次得出结论，4 次无答案，91 秒，记录了 25 个答案。

分析了什么

协议	Review TLS hybrid full transcript
版本	rfc10024
分析范围	首轮 hello-only transcript 简化的独立修正模型：固定 X25519MLKEM768 服务器认证 1-RTT，所有 handshake 消息进入相应 transcript，CertificateVerify、server/client Finished、握手消息 AEAD 和 application/exporter secrets 按基线分层，不能以公开证书/Finished 替代密钥控制。排除 HRR/PSK/0-RTT。
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	549 numbered passages (144873 bytes) from the sections listed below. A reference such as s0001 in this report is one of these passages

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	共享密钥
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	共享密钥计算
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

文稿	章节	标题
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	握手后的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 绑定值
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	New Session Ticket 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	更新流量密钥

文稿	章节	标题
rfc9846	7.3	流量密钥计算
rfc9846	7.4	非对称共享密钥计算
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

协议目的，即源文步骤在文稿中定位到的内容：首轮 hello-only transcript 简化的独立修正模型：固定 X25519MLKEM768 服务器认证 1-RTT，所有 handshake 消息进入相应 transcript，CertificateVerify、server/client Finished、握手消息 AEAD 和 application/exporter secrets 按基线分层，不能以公开证书/Finished 替代密钥控制。排除 HRR/PSK/0-RTT。

对照文稿定性质

在编写任何查询之前，分析者先把起草的性质清单对照文稿本身对协议目的的表述逐项核对。名称、性质所针对的对象以及文稿的说法都出自分析者的解读；所列的出处确实存在于文稿中。

ID	简称	对象	文稿怎么说	出处
A02	服务器向客户端认证	客户端确信它接受的服务器确实在客户端所见的转录上运行了握手。	RFC 9846 将对等方认证列为握手目标：客户端对的对等方身份视图应反映服务器的身份，基于签名的模式通过握手转录上的签名来认证服务器。	rfc9846:6490, rfc9846:6537, s0409, s0435
A03	会话密钥协商	两个端点从同一混合共享密钥导出相同的会话密钥和相同的协商参数。	RFC 9846 把建立相同的会话密钥以及会话密钥的保密性列为主动网络攻击者不得破坏的目标。	rfc9846:6478, rfc9846:6483, s0015, s0491
A04	接受唯一性	客户端与服务器的不同握手产生不同的接受，每次接受对应一个对等方运行。	RFC 9846 陈述了会话密钥的唯一性：任意两次不同的握手都应产生不同且不相关的会话密钥。	rfc9846:6495, s0435, s0491
A06	Finished 密钥确认	验证方要求在本会话所导出的握手密钥下校验 Finished MAC。	RFC 9846 指出 Finished 消息对于提供握手及所计算密钥的认证至关重要，接收方必须校验其内容。	rfc9846:6435, rfc9846:6436, s0435, s0445
A08	转录与角色绑定	协商组、各方角色以及整个消息序列都被绑定进 CertificateVerify 和 Finished。	RFC 10024 指出安全性分析关键依赖 TLS 1.3 消息转录；RFC 9846 定义了覆盖每条握手消息的转录哈希以及角色上下文字符串。	main:270, rfc9846:6413, rfc9846:6420, s0063, s0068, s0420
K01	会话密钥保密性	服务器的长期签名密钥、握手流量密钥、应用流量密钥以及导出器密钥，均不为网络攻击者所知。	RFC 9846 陈述了会话密钥的保密性：共享会话密钥应仅为通信双方所知，攻击者不得知晓。	rfc9846:6483, rfc9846:6511, s0491, s0511, s0546
C01	长期密钥泄露下的前向保密	真实服务器运行过的会话，在服务器长期签名密钥被泄露且临时状态已擦除之后。	RFC 9846 陈述了相对于长期密钥的前向保密：只要临时材料被擦除，握手后泄露签名密钥不会危及会话密钥。	rfc9846:6504, s0504, s0511, s0521
C04	单一组件失效下的混合主张	某会话的 X25519 组件被攻破、或其 ML-KEM 解封装密钥被攻破时的应用流量密钥，每次只攻破一个。	RFC 9954 指出，只要至少一个组件密钥交换算法未被攻破，混合共享密钥就是安全的；RFC 10024 指出了 CRQC 恢复 X25519 标量以及封装随机数暴露的情形。	rfc9954:550, main:299, main:282, s0025, s0051, s0511

ID	简称	对象	文稿怎么说	出处
K04	派生密钥分离	同一会话的客户端密钥与服务器密钥，以及同一方的应用密钥、握手密钥和导出器密钥，彼此不同。	RFC 9846 指出一次握手产生的各个会话密钥应当不同且相互独立，并用各自的标签和方向导出每个密钥。	rfc9846:6495, rfc9846:6497, s0511, s0528
A08.10	CertificateVerify 绑定完整转录	同一种绑定，按用户的问题来解读：CertificateVerify 和 Finished 是否覆盖完整序列以及发送方的角色。	覆盖 ClientHello 至认证消息的转录哈希，以及分别用于服务器和客户端的 CertificateVerify 上下文字符串。	rfc9846:6413, rfc9846:6445, s0063, s0360, s0445
C04.11	单一组件失效，密钥仍保密	同一种单一组件泄露，按用户的问题来解读：仅当一个 KEM 或 DH 组件被攻破时，应用流量密钥仍保持保密。	混合构造的目的在于，只要至少一个组件算法未被攻破，最终会话密钥就是安全的。	rfc9954:550, rfc9954:117, s0015, s0051
Q3	基线模型上的攻击	分析方法：所报告的攻击都在一个保留了规范所要求检查的模型上复现。	任务说明指出，每条攻击轨迹仅在明确假设下成立，并且必须能在保留规范检查的基线模型中复现；这是对分析的要求，而不是协议性质。	s0019

分析者没有补充性质：起草的清单已覆盖文稿写明的目标。

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 13 段，没选 7 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	A08, A08.10, A03	
P02	main:273-276	证明器问不了	关于抗侧信道实现的指引；实现的强度不是迹性质。
P03	main:278-280	A03	
P04	main:282-287	C04, `mlkem_decaps_key`	
P05	main:289-297	C04, `mlkem_decaps_key`	
P06	main:299-306	C04, C04.11, `x25519_scalar_crqc`	
P07	main:308-310	C04.11, `x25519_scalar_crqc`, `mlkem_decaps_key`	
P08	rfc7748:783-793	证明器问不了	curve25519 的安全强度属于原语强度，不是迹性质。
P09	rfc7748:802-808	证明器问不了	同上：curve448 的原语强度。
P10	rfc7748:810-818	A03, `network`	
P11	rfc7748:820-825	A08, `network`	
P12	rfc7748:827-837	不在范围内	曲线实现之间可观察的差异属于实现指纹问题，不在所建模的握手范围内。
P13	rfc9846:4676-4677	A02, A03, A04, A06, A08, A08.10, K01, K04, C01, `network`, `server_sig_key_after_session`	
P14	rfc9954:550-558	C04, C04.11, `x25519_scalar_crqc`, `mlkem_decaps_key`	

段落	出处	定为	不选的原因
P15	rfc9954:560-569	证明器问不了	KEM 的 IND-CCA2 安全性以及公钥重用下的安全性属于计算假设，不是迹性质。
P16	rfc9954:571-574	A03	
P17	rfc9954:576-582	证明器问不了	变长秘密的时序侧信道无法查询。
P18	rfc9954:584-586	证明器问不了	KDF 所用哈希的抗碰撞性属于计算假设。
P19	rfc9954:588-592	A03	
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 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	K01	
K03	强保密／秘密值不可区分性	K01	
D01	消息完整性与数据来源真实性	A08, A06	
A01	对端曾参与性（Aliveness）	A02, A03	
A05	隐式密钥认证	A03, K01	
A07	身份—凭据—密钥绑定	A08	
R01	认证／挑战新鲜性	A04	
R02	消息级抗重放	不在范围内	未对记录层重放窗口建模；本任务只覆盖握手。
R03	业务操作至多一次	不适用	该协议不承载业务操作。
R04	消息接受顺序／窗口安全	不在范围内	接受窗口和顺序属于记录层机制，不在所建模的握手范围内。
R05	抗降级／安全策略保持	不在范围内	本任务固定 X25519MLKEM768 组，并排除 HRR、PSK 和 0-RTT，因此模型中没有协商备选方案。
C02	抗密钥泄露冒充（KCI）	不适用	范围仅限服务器端的证书认证；客户端不持有长期凭据，因此不存在其凭据被盗后可冒充另一方的对端。
C03	已知密钥安全／泄露隔离	C04	
C05	泄露后安全恢复（PCS）	不在范围内	未对恢复、PSK 或密钥更新建模。
C06	注册凭据泄露后的增强认证	不适用	该协议中不存在口令或注册记录。
C07	抗离线字典攻击	不适用	不使用低熵秘密。
C08	指定原语失效下的目标保持	C04, C04.11	
Z01	授权执行正确性	不适用	握手不包含任何授权层。
Z02	委托权限不扩张	不适用	无委托。
Z03	授权与身份／会话／操作绑定	不适用	无授权令牌。
Z04	撤销与过期生效	不适用	无撤销或过期。
Z05	跨租户／跨服务安全隔离	不适用	无租户或共享节点。
S01	加密 nonce 唯一性	不在范围内	未对记录层的 AEAD nonce 管理建模。

条目	目录里的性质	作为哪条性质检查	不检查的原因
S02	重传／密钥重安装安全	不在范围内	密钥重安装和重传处理不在所建模的 1-RTT 握手范围内。
S03	抗回滚与状态单调性	不在范围内	在此范围内，握手不保存对回滚敏感的版本或计数器状态。
S04	跨阶段安全上下文一致性	不适用	该协议只有单一的握手上下文，没有恢复、迁移或注册阶段。
S05	终止与旧状态失效	不在范围内	未对连接拆除建模。
P01	身份匿名性	不适用	服务器身份是公开的，客户端未经认证，因此不存在匿名性目标。
P02	会话不可关联性	不适用	不交换客户端身份或票据，因此各次运行无法通过身份关联。
P03	用户／凭据存在性隐藏	不适用	不存在用户或凭据查找。
V01	条件性进展／错误恢复	证明器问不了	条件下的进展不是可以向 ProVerif 查询的迹性质。
V02	无非预期死锁	证明器问不了	无死锁无法查询。
V03	受限资源滥用／抗放大	证明器问不了	除计数事件之外的资源消耗无法查询。

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 21 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 2 项，没设的 19 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	客户端只控制自己的临时秘密，而任何攻击者本来就能在网络上自行运行一个客户端会话；其他会话的性质不会因此改变。
S02	服务器	参与方	`server_sig_key_after_session`	
S03	服务器身份	值	攻击者得不到更多	服务器证书及其公钥都是公开的。
S04	客户端身份	值	攻击者得不到更多	客户端在此模式下未经认证，协议中也没有它的身份值。
S05	X25519MLKEM768 混合共享秘密	值	按定义全部失守	该会话的每个密钥都是混合共享秘密的函数；一旦攻击者持有它，就没有任何文稿要求其保密。
S06	握手流量密钥	值	按定义全部失守	该会话的所有握手密钥和应用密钥都派生自握手流量秘密。
S07	应用流量密钥	值	按定义全部失守	按定义，持有某会话的应用流量密钥即失去该会话的保密性。
S08	协商参数	值	攻击者得不到更多	协商参数在握手中传输，是公开的。
S09	握手 transcript	值	攻击者得不到更多	transcript 由网络攻击者能看到的报文构成。
S10	随机数	值	攻击者得不到更多	hello 随机数是公开的；从生成器取出的临时秘密由两个分量泄露攻击者另行覆盖。
S11	会话密钥	值	按定义全部失守	按定义，持有会话密钥即失去该会话。
S12	Finished 验证数据	值	攻击者得不到更多	Finished 验证数据是派生密钥下的 MAC；持有它不会给出任何密钥。
S13	协商组 X25519MLKEM768	值	攻击者得不到更多	组标识是公开且固定的。
S14	transcript 哈希	值	攻击者得不到更多	transcript 哈希可由公开报文计算。

ID	参与方或值	类别	攻击者条件	不设的原因
S15	角色上下文串	值	攻击者得不到更多	上下文串是公开常量。
S16	服务器长期签名私钥	值	`server_sig_key_after_session`	
S17	exporter 秘密	值	按定义全部失守	exporter 秘密与流量密钥派生自同一主秘密；按定义，持有它即失去该会话的 exporter 输出。
S18	历史会话握手流量密钥	值	按定义全部失守	按定义，持有某会话的握手流量密钥即失去该会话；其他会话使用新的临时秘密。
S19	历史会话应用流量密钥	值	按定义全部失守	按定义，持有某会话的应用流量密钥即失去该会话。
S20	混合共享秘密	值	按定义全部失守	对使用它的会话而言，与 S05 是同一个值。
S21	CertificateVerify 签名	值	攻击者得不到更多	CertificateVerify 签名在握手中发送；它是长期密钥下的签名，不是密钥。

每条性质在各攻击者条件下的答案

攻击者由分析者设定，且在编写查询之前就已设定；每个答案都记录在其中一个攻击者之下。单元格是证明器在该攻击者下对该性质给出的答案；“无答案”是该性质下证明器未对某项主张作出判定、或未记录任何内容的那个攻击者；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、修改和发送报文，不持有任何一方的秘密。		
`x25519_scalar_crqc`	某已完成会话（客户端和服务器）的 X25519 临时私钥标量，由密码学相关量子计算机在会话结束后恢复；ML-KEM 解封装密钥保持秘密。	文稿警告：具备 CRQC 的被动观察者可以从公开份额中恢复 ECDH 临时标量。	main:299
`mlkem_decaps_key`	客户端持有的 ML-KEM-768 解封装密钥（因而也掌握封装随机数 m 和该会话的 ML-KEM 共享秘密）；X25519 标量保持秘密。	文稿指出客户端在解封装过程中会精确恢复 m，并且通过 m 泄露的 RNG 输出构成额外的暴露。	main:282, main:289
`server_sig_key_after_session`	服务器长期签名私钥，在握手完成且临时状态被擦除之后取得。	RFC 9846 规定了对长期密钥的前向保密：握手后泄露签名密钥不得危及会话密钥。	rfc9846:6504

ID	`network`	`x25519_scalar_crqc`	`mlkem_decaps_key`	`server_sig_key_after_session`
A02	成立			
A03	不成立			
A04	不成立			
A06	不成立			
A08	成立			
K01	成立			
C01				成立
C04		成立	成立	
K04	成立			
A08.10	成立			

ID	network	x25519_scalar_crqc	mlkem_decaps_key	server_sig_key_after_session
C04.11		成立	成立	
Q3	不成立			

原文和目标

Source: 549 units, 144873 bytes, frozen in source-delivery-01.json. Targets: 9 approved (A02, A03, A04, A06, A08, K01, C01, C04, K04); the questions asked: 3. The list of targets was approved as drafted, beforehand, with --approve-targets.

宿主按其文档所述默认值（任务 `decisions: auto`）所做的决定，供你核对：

- approve_package: 批准源文包 protocol-9ed9cece2ceac30bf32cd9a216a4

本步骤的自述：1 请求（1 失败），0.000 USD，67700 tokens 输入、4653 输出，27 s。

关于证明器和模型的说明

- A02：在 ProVerif 中作答，分析者为该目标指定 dh_algebra
- A03：在 ProVerif 中作答，分析者为该目标指定 dh_algebra
- A04：在 ProVerif 中作答，分析者为该目标指定 dh_algebra
- A06：在 ProVerif 中作答，分析者为该目标指定 dh_algebra
- A08：在 ProVerif 中作答，分析者为该目标指定 dh_algebra
- K01：在 ProVerif 中作答，分析者为该目标指定 dh_algebra
- C01：在 ProVerif 中作答，分析者为该目标指定 dh_algebra
- C04：在 ProVerif 中作答，分析者为该目标指定 dh_algebra
- K04：在 ProVerif 中作答，分析者为该目标指定 dh_algebra
- A08.10：在 ProVerif 中作答，分析者为该目标指定 dh_algebra
- C04.11：在 ProVerif 中作答，分析者为该目标指定 dh_algebra

对代数做了简化的 ProVerif 模型（xor、dh_algebra、other_algebra）给攻击者的能力比真实运算更少：在那里得到证明，就是针对更弱攻击者的证明；在那里出现攻击，就是攻击。省略了对会变化的值所做检查的 ProVerif 模型（changing_state）则让各方接受更多：在那里得到证明就成立，在那里出现攻击可能只是缺少了这项检查。Tamarin+ Agent 按原样对这些建模。

分析者为各目标指定的内容：

step	targets	features	reason
44	A02, A03, A04, A06, A08, A08.10, K01, C01, C04, C04.11, K04	plain_primitives, dh_algebra, many_sessions	哈希、MAC、HKDF 式派生、无 AEAD 的密钥编排以及证书签名都建模为理想原语。X25519 用指数运算建模，只采用单一规律 g^xy = g^yx，不附加其他代数性质；ProVerif 在检查 Finished 或签名时会应用该规律，因此对密钥项的协商一致只能通过会话记录标识符体现，而组件泄露的结论依赖这一简化。所有性质都在同一次运行中、针对任意数量的客户端和服务器会话提问，客户端密钥和服务器签名密钥只在握手之后泄露。

分析者的结语

针对这十二个目标，在 model.pv 上记录了二十四条答案。已证明：服务器对客户端的认证及其区分性（A02、A04）；通过 Finished 检查就会话记录和握手密钥达成一致（A03 第一条主张）；客户端侧的密钥确认（A06 第一条主张）；CertificateVerify 的会话记录与角色绑定（A08、A08.10）；签名密钥、两个握手流量

密钥和两个应用流量密钥以及导出密钥的保密性（K01，六条主张，各带对照查询）；服务器签名密钥泄露后的前向保密（C01，带对照查询）；混合主张在两个方向上逐组件验证（C04、C04.11，带对照查询）；按方向和用途的密钥分离（K04）。已证伪并记录为文稿所述内容：在这种仅服务器模式下，服务器无法区分诚实客户端和攻击者自己运行的客户端会话（A03、A04 和 A06 的第二条主张；RFC 9846 附录 F.1），并在保留全部检查的基线模型上复现。未发现文稿未述的弱点，因此本报告没有发现。这些证明依赖于理想的签名、KDF 和哈希，以及把 X25519 归约为 g^xy = g^yx；范围不包含任何跨步骤变化的值，因此没有有界模型，也没有状态审查。Tamarin+ Agent 保留指数和 KEM 的原样，正是它能消除单组件主张所受代数限制的原因。