LAKE PQ 签名方法 0 的安全性分析 0

本报告的其他语言版本：English。

draft-ietf-lake-pqsuites-02 · ProVerif+ Agent 报告

文稿	Quantum-Resistant Cipher Suites for LAKE（协议定义）；Ephemeral Diffie-Hellman Over COSE (EDHOC)（辅助）
检查的性质	16 条：14 条成立，2 条不成立（3 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

LAKE 是一种轻量级认证密钥交换协议；本文稿为它注册后量子密码套件。RFC 9528 的方法 0 得以保留，临时 Diffie-Hellman 交换被替换为 ML-KEM：封装密钥作为 G_X 在 message_1 中传输，KEM 密文作为 G_Y 在 message_2 中传输，共享密钥 K 送入密钥调度。双方都用 ML-DSA 签名进行认证，各自持有凭据（ID_CRED_I、CRED_I 和 ID_CRED_R、CRED_R）及其长期签名密钥；公钥事先已知。

该交换共四条消息：发起方发送 message_1，携带其新的封装密钥和 C_I；响应方回复 KEM 密文以及受保护的（C_R、ID_CRED_R、Signature_or_MAC_2）；发起方回复受保护的（ID_CRED_I、Signature_or_MAC_3）；响应方用 message_4 确认。每个 transcript 哈希和派生密钥都来自 KEM 秘密和所交换的消息。

交换结束时，发起方知道：持有一个身份、且其密钥验证了 Signature_or_MAC_2 的响应方运行了本次会话并算出了相同的 PRK_out。响应方对发起方也知道同样的事。双方都持有 PRK_out，应用密钥由它导出。

参与方：

- **发起方 I**：签名方法 0，每个会话一对 ML-KEM 密钥。持有：ID_CRED_I、CRED_I、I 的 ML-DSA 私钥、R 的公钥。
- **响应方 R**：签名方法 0。持有：ID_CRED_R、CRED_R、R 的 ML-DSA 私钥、I 的公钥。

图 1 展示了文稿所规定的交换。

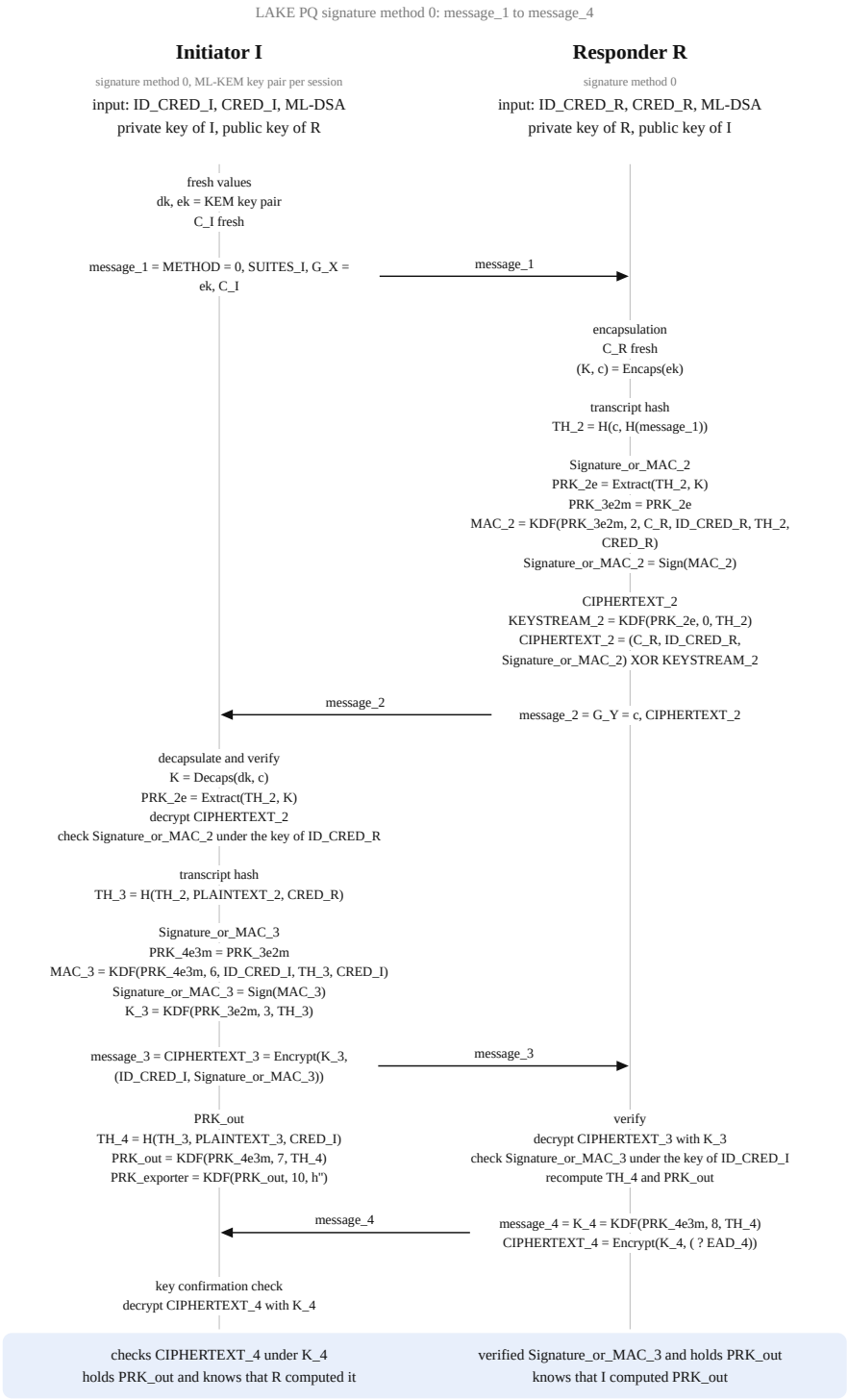


图 1. 文稿所规定的协议。

分析的范围见附录 D：分析了什么、省略了什么，以及它依据的文稿章节。

2 发现

没有发现。 分析没有发现文稿未曾写明或已排除的内容。第 3 节的表格给出了每条性质的结果。

在建模范围内，该密码套件提供了文稿声称它提供的东西：没有发现新的弱点。双向的相互认证、会话一致性、重放保护、密钥确认、会话密钥保密性、密钥分离、长期密钥泄露后的前向保密，以及凭据、标识符和密码套件的绑定，都针对网络上的攻击者进行了验证，其中大多数都带有对照查询——在该对照中，

保护性检查被去掉或该值被泄露，而性质不成立。找到的两个攻击正是文稿写明的那两个：泄露的 KEM 解封装密钥会暴露该会话的密钥，别无其他；主动攻击者能获知响应方的凭据标识符。有两条主张只得到部分回答：身份保护无法以其不可区分形式得出结论，密钥泄露冒充仅在会话之后已知密钥的情况下进行了测试。这些结果依赖于理想化的 ML-KEM、ML-DSA、哈希和 KDF，依赖于每个参与方只支持一个套件的单一密码套件，并且不涉及错误消息、EAD 字段或跨运行的可链接性。

3 检查过的性质

每一行是一条提交给 ProVerif 的性质。结果是 ProVerif 对分析者的协议模型的回答；价值和文稿是否已写明该结果属于分析者的判断，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	**方法 0 中的双向认证。** 每当发起方（或响应方）在完成签名验证后接受本次会话，就存在一个以本方为对端身份真实运行的响应方（或发起方）会话。	无	成立	中	是
A03	**双方会话匹配。** 每次一方接受会话时，都存在一个匹配的对端运行，双方对角色、身份、连接标识 C_I/C_R、凭据 CRED_I/CRED_R、transcript 哈希 TH_2/TH_3 与所选密码套件一致。	无	成立	中	是
A04	**无对端运行重放。** 每次一方接受会话都对应一个不同的对端运行，同一对端运行不能被两次接受为两个不同会话。	无	成立	中	是
A06	**来自消息 4 的密钥确认。** 发起方接受 message_4（或受导出密钥保护的应用消息）时，响应方已导出同一 PRK_out 并发出匹配的确认。	无	成立	中	是
K01	**会话密钥保密性。** 攻击者不能导出 KEM 共享密钥 K、PRK_out、PRK_exporter 或由导出接口得到的应用密钥。	无	成立	中	是
K04	**派生密钥间的密钥分离。** 不同 info_label、不同方向（K_3 与 K_4）以及不同会话派生的密钥互不相同；同一 (exporter_label, context) 不被用于两个不同用途。	无	成立	中	是
A08	**转录与凭证绑定。** 接受方接受的连接标识、凭据标识、transcript 哈希与密码套件，与对端实际发送并在签名中覆盖的值一致，且套件选择符合 SUITES_I 顺序规则。	无	成立	中	是
R05	**无密码套件降级。** 响应方接受的套件是发起方 SUITES_I 中按偏好顺序第一个双方都支持的套件；伪造的错误消息不能使发起方改变偏好顺序或省略更优套件。	无	成立	低	是
C01	**已完成会话的前向保密。** 会话完成之后泄露双方的长期签名私钥，攻击者仍不能导出此前会话的 KEM 共享密钥、PRK_out 或应用密钥。	发起方与响应方的长期签名私钥 (会话完成并擦除临时 KEM 私钥之后)	成立	中	是
C04	**临时 KEM 密钥泄露边界。** 泄露发起方某次会话的 KEM 解封装私钥 dk 后，检查该会话的 KEM 共享密钥与 PRK_out 是否随之暴露，以及其他会话的密钥是否仍保密。	发起方本次会话的 KEM 解封装私钥 dk (会话进行中或完成之后)	攻击成立（文稿已写明）	低	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
A03.11	**方向与转录一致性。** 每次一方接受会话时，都存在匹配的对端运行，双方对身份、连接标识、transcript 哈希与方向一致；message_2 的签名只对响应方方向有效，message_3 的签名只对发起方方向有效。	无	成立	中	是
K01.12	**新鲜 KEM 密钥与导出器保密性。** 每次会话使用新生成的 KEM 密钥对，攻击者不能导出 PRK_out、PRK_exporter 或由导出接口得到的应用密钥。	无	成立	中	是
A08.13	**凭证与标识符绑定。** 接受方接受的凭据、连接标识与密码套件，与对端实际发送并在签名与 transcript 哈希中覆盖的值一致。	无	成立	中	是
X01	**发起者身份保护。** 以响应方身份参与的攻击者无法分辨两个发起方凭据（ID_CRED_I、CRED_I）中哪一个参与了发起方发送 message_3 的会话	无	成立	中	是
X02	**仅对被动攻击者的响应者标识符保护。** 仅进行观察的攻击者无法分辨两个响应方凭据中哪一个参与了会话，但用自己的 message_1 应答的攻击者能获知响应方的凭据标识符	无	攻击成立（文稿已写明）	低	是
X03	**长期密钥泄露下的 KCI 保护。** 持有发起方长期签名密钥的攻击者无法使发起方接受一个响应方从未运行的会话	双方的长期 ML-DSA 签名私钥，在某个会话完成之后获知	成立	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, X03.

所提的问题，以及分析者的回答：

问题	回答	依据
Q1: 双方身份认证和不同消息方向的签名绑定	两个方向都成立，且各自绑定到自己的消息：接受 message_2 迫使存在一个响应方运行，接受 message_3 迫使存在一个发起方运行，二者具有相同的 C_I、C_R 和身份，一个方向的签名不能用于另一个方向。发起方去掉签名检查的对照会接受伪造的 message_2 并因此不成立。	A02, A03.11, A03
Q2: 临时 KEM key 每会话新鲜与 exporter 保密	在模型中每个会话都使用新的 KEM 密钥对，K、PRK_out、PRK_exporter 和由导出器派生的应用密钥对网络上的攻击者保持保密，并配有对照查询——在对照中泄露的解封装密钥使同一查询不成立。	K01.12, K01, C04
Q3: 凭据/connection identifiers/cipher suite 的 transcript 绑定	凭据标识符、连接标识符和 transcript 哈希都绑定到对端的签名和 transcript 哈希，因此一方只接受对端运行签过名的值；密码套件也以同样方式被覆盖，但模型固定了一个已选套件，且没有 SUITES_I 协商或错误消息，所以顺序规则未被检查。	A08.13, A08, R05

4 本次分析的局限

这里的结果是协议模型上的结果：它说明所规定的消息和检查给出或不给出什么，密码学被视为理想的，而完全不涉及实现。

如分析者所述，本次分析不覆盖的内容：

- ML-KEM、ML-DSA、各哈希、KDF、message_2 的流密码以及 message_3 和 message_4 的 AEAD 都是理想原语：没有证明任何计算性陈述，尤其没有证明后量子安全性。
- 只对一套选定算法集的单一密码套件建模；SUITES_I 是固定的两元素列表，每个参与方只支持所选套件，且错误消息未建模，因此伪造错误后不得重排 SUITES_I 的规则未被检查。
- EAD_1 到 EAD_4、连接标识符更新、RFC 9528 附录 H 的密钥更新以及传输层的消息去重都在模型之外。
- 泄露的长期密钥只在所询问的会话之后交给攻击者；因此会话期间的密钥泄露冒充只得到部分覆盖（X03）。
- 身份保护是作为关于凭据标识符的保密性问题提出的，而不是作为两个候选身份之间的不可区分性；非干扰形式未由 ProVerif 证明。
- 通过明文连接标识符 C_I 和 C_R 实现的跨运行可链接性（RFC 9528 9.5 已指出）未建模。
- 侧信道、时序、资源耗尽以及任何需要计量付出而非事件的内容都不覆盖。

宿主记录的内容：

- 没带对照查询的证明（附录 C）：K04: sep_m3, K04: sep_m4, K04: sep_prk, R05: suite_agree, A08.13: suite_agree。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，以及什么能解决它，见附录 A。

附录 A：逐条性质的解读

这是分析者本人对证明器给出的答案的解读，而不是证明器的回答：这些答案对协议意味着什么、解读建立在什么之上、能否按原样使用，以及它有多大价值。

A02: 方法 0 中的双向认证

每当发起方（或响应方）在完成签名验证后接受本次会话，就存在一个以本方为对端身份真实运行的响应方（或发起方）会话。

两个方向的认证都成立。接受 message_2 的发起方背后有一个响应方运行，具有相同的 C_I、C_R 和相同身份；接受 message_3 的响应方背后有一个发起方运行。承载这一点的是签名检查：一旦发起方省略该检查，伪造的 message_2 就会被接受，该性质随之不成立。

- 结果：成立；回答了所问：是；可带保留地使用
- 价值 中：这是对一项核心保证的证明，但该保证是文稿已经主张的那一项，且建立在理想化原语之上。
- 文稿中有述：是。文稿何处有述：s0036、s0002
- 依据：ML-KEM 与 ML-DSA 是理想的：没有攻击者能从密文计算出封装的秘密，也不能伪造签名。；泄露的长期密钥只在一次会话之后才交给攻击者，因此会话期间的密钥泄露冒充不在覆盖范围内。；单一密码套件，且无凭据吊销。

A03: 双方会话匹配

每次一方接受会话时，都存在一个匹配的对端运行，双方对角色、身份、连接标识 C_I/C_R、凭据 CRED_I/CRED_R、transcript 哈希 TH_2/TH_3 与所选密码套件一致。

被接受会话的双方在连接标识、签名所用凭据以及所哈希的 transcript 上一致。发起方的接受指明了其密钥验证了 Signature_or_MAC_2 的响应方身份，响应方的接受则指明了其密钥验证了 Signature_or_MAC_3 的发起方身份。

- 结果：成立；回答了所问：是；可带保留地使用
- 价值 中：匹配会话的一致性是在一个强概念下证明的，其中包含身份，但这是 RFC 已经陈述的性质。
- 文稿中有述：是。文稿何处有述：s0190、s0223
- 依据：凭据是公开的，并按消息中携带的标识查找；在模型中，凭据不会被错误绑定到另一个密钥。；理想化的签名、KEM、哈希与 KDF。

A04: 无对端运行重放

每次一方接受会话都对应一个不同的对端运行，同一对端运行不能被两次接受为两个不同会话。

没有录制的流程会被接受两次。重放的 message_2 会失败，因为密钥流来自该会话自身的临时 KEM 秘密；重放的 message_3 会失败，因为响应方的密钥 K_3 与 transcript 属于同一次运行。两种协议的注入形式均已证明。

- 结果：成立；回答了所问：是；可带保留地使用
- 价值 中：它以确切条件确认了 RFC 9528 9.1 关于重放与跨会话注入的主张。
- 文稿中有述：是。文稿何处有述：s0022、s0189、s0222

- 依据：发起方按草案要求为每次会话生成新的 KEM 密钥对。；传输层去重未被建模，此处也不需要，因为各会话的密钥不同。；理想化原语。

A06: 来自消息 4 的密钥确认

发起方接受 message_4（或受导出密钥保护的应用消息）时，响应方已导出同一 PRK_out 并发出匹配的确认。

接受 message_4 意味着响应方导出了相同的 PRK_out，并在 K_4 下生成了 CIPHERTEXT_4，因此发起方获得了密钥确认。若发起方变体接受任意 message_4，该性质即被破坏，可见承载该性质的是这一检查。

- 结果：成立；回答了所问：是；可带保留地使用
- 价值 中：密钥确认是一项已陈述的保证；本结果补充了 message_4 检查的确切作用。
- 文稿中有述：是。文稿何处有述：s0281、s0266
- 依据：K_4 与 AEAD 是理想的，因此有效的 CIPHERTEXT_4 只能来自持有 PRK_out 的一方。；message_4 在协议中是可选的；模型总是发送它。；EAD_4 是常量。

K01: 会话密钥保密性

攻击者不能导出 KEM 共享密钥 K、PRK_out、PRK_exporter 或由导出接口得到的应用密钥。

对仅掌握网络的攻击者而言，KEM 共享秘密、PRK_out、PRK_exporter 以及通过导出接口派生的应用密钥始终保密。KEM 秘密只有在对方签名验证之后才计为会话秘密，也正是此时它成为真实会话的密钥。

- 结果：成立；回答了所问：是；可带保留地使用
- 价值 中：这是对新密码套件的保密性与密钥安全性的证明，建立在理想化原语之上。
- 文稿中有述：是。文稿何处有述：s0019、s0123、s0127
- 依据：KEM 是理想的：封装的秘密只能通过解封装获得。；KDF 若被攻破则不会被发现。；强制会话中止的攻击者确实会得知其封装所针对的秘密，但该会话永远不会被接受。

K04: 派生密钥间的密钥分离

不同 info_label、不同方向（K_3 与 K_4）以及不同会话派生的密钥互不相同；同一 (exporter_label, context) 不被用于两个不同用途。

在不同 info_label 下派生的密钥相互独立：攻击者即使持有某会话的 KEYSTREAM_2 以及 K_3，也得不到该会话的 K_4 或 PRK_out，尽管它能读取 PLAINTEXT_2。这正是图 6 所依赖的标签分离。

- 结果：成立；回答了所问：是；可带保留地使用
- 价值 中：它确认了 RFC 陈述的派生纪律，并明确指出 message-2 密钥流是最薄弱的部分。
- 文稿中有述：是。文稿何处有述：s0123
- 依据：KDF 是理想的，且标签是互不相同的常量；KMAC256 输出分离若存在真实弱点则不会显现。；该泄露是会话之后的揭示，而非会话期间的攻破。

A08: 转录与凭证绑定

接受方接受的连接标识、凭据标识、transcript 哈希与密码套件，与对端实际发送并在签名中覆盖的值一致，且套件选择符合 SUITES_I 顺序规则。

一方只会接受其密钥签署了对端 MAC 的那个凭据标识，而该 MAC 覆盖了本方持有的 transcript，因此凭据、标识与 transcript 哈希被绑定在一起。在传输途中改动其中任何一项都会使检查失败，而不会绑定错误的凭据。

- 结果：成立；回答了所问：是；可带保留地使用
- 价值 中：身份错误绑定防护正是 RFC 9528 9.1 所主张的；本证明明确了被覆盖的字段。
- 文稿中有述：是。文稿何处有述：s0190、s0223、s0239
- 依据：凭据是公开的，且假定标识到密钥的查找是明确的。；理想化的签名与 KDF。

R05: 无密码套件降级

响应方接受的套件是发起方 SUITES_I 中按偏好顺序第一个双方都支持的套件；伪造的错误消息不能使发起方改变偏好顺序或省略更优套件。

在所选定的单一套件内，套件携带于 message_1 中并由 TH_2 覆盖，被接受会话的双方使用同一套件，因此被修改的 SUITES_I 只会导致会话失败，而不会导致更弱的套件。协商本身——包括套件数组以及可能被伪造的错误消息——不在模型范围内。

- 结果：成立；回答了所问：部分；可带保留地使用
- 价值 低：绑定部分可由 transcript 哈希在结构上推出；而让降级防护真正有意义的那部分并未分析。
- 文稿中有述：是。文稿何处有述：s0167、s0169、s0075
- 依据：每个参与方只有一个密码套件和一个受支持的套件。；无错误消息、无 SUITES_R、无重试。
- 未决：SUITES_I 的排序以及带 SUITES_R 的伪造错误消息的处理未被建模。；模型中每个参与方只支持一个套件，因此真正的降级无法表达。

C01: 已完成会话的前向保密

会话完成之后泄露双方的长期签名私钥，攻击者仍不能导出此前会话的 KEM 共享密钥、PRK_out 或应用密钥。

双方长期签名密钥泄露之后，已完成会话的 KEM 共享秘密、PRK_out 与 PRK_exporter 仍保持保密。前向保密成立，因为会话密钥来自临时 KEM 秘密而非长期密钥；在让某会话的解封装密钥泄露的对照中，同样的查询会失败。

- 结果：成立；回答了所问：是；可带保留地使用
- 价值 中：前向保密正是草案“先存储、后解密”论证所依赖的；本证明确认了其结构性原因。
- 文稿中有述：是。文稿何处有述：s0086、s0048
- 依据：密钥只在会话之后才被泄露，这正是前向保密所问的问题。；假定临时私钥已被擦除；解封装密钥也泄露的会话属于 C04。；理想化 KEM：ML-KEM 若被攻破，本结论也随之不成立。

C04: 临时 KEM 密钥泄露边界

泄露发起方某次会话的 KEM 解封装私钥 dk 后，检查该会话的 KEM 共享密钥与 PRK_out 是否随之暴露，以及其他会话的密钥是否仍保密。

一次会话的解封装密钥泄露会给出该会话的 KEM 秘密，再结合线路上的消息，还会给出其 PRK_out：攻击者解封装、读取 PLAINTEXT_2 并重新计算 TH_4。它不会给出其他会话的任何信息，因为每次会话都有自己全新的密钥对，其他会话的 PRK_out 仍保持保密。

- 结果：攻击成立（文稿中已说明）；回答了所问：是；可用

- 价值低：两半都来自 K = Decaps(dk, c) 和新鲜密钥要求；价值在于精确地确定边界。
- 文稿中已说明：是。文稿中的位置：s0018、s0022、s0123
- 依据：泄露是按会话发生的，且发生在会话之后，正如新鲜密钥要求所暗示的；在该主张中，攻击者并未同时获得长期密钥。

A03.11: 方向与转录一致性

每次一方接受会话时，都存在匹配的对端运行，双方对身份、连接标识、transcript 哈希与方向一致；message_2 的签名只对响应方方向有效，message_3 的签名只对发起方方向有效。

每次接受都对应一个具有相同身份、标识符和 transcript 的对端运行，且每个签名都在各自方向的上下文中计算，因此 message_2 的签名不能用作 message_3 的签名。

- 结果：Holds；回答了所问：是；可用但有保留
- 价值中：它直接回答了方向绑定的问题，正是它使两个签名不可转移。
- 文稿中已说明：是。文稿中的位置：s0190、s0223、s0231
- 依据：理想化签名和 KDF；每个角色一个套件和一份凭证。

K01.12: 新鲜 KEM 密钥与导出器保密性

每次会话使用新生成的 KEM 密钥对，攻击者不能导出 PRK_out、PRK_exporter 或由导出接口得到的应用密钥。

每次会话都使用新生成的 KEM 密钥对运行，得到的 K、PRK_out、PRK_exporter 和应用密钥对网络攻击者保持机密。导出器密钥仅通过 PRK_out 受到保护，因此其保密性就是 PRK_out 的保密性。

- 结果：Holds；回答了所问：是；可用但有保留
- 价值中：新鲜密钥要求是草案的 MUST；模型表明导出器链继承其保密性。
- 文稿中已说明：是。文稿中的位置：s0022、s0057、s0128
- 依据：新鲜性通过在每次会话内生成密钥对来建模；理想化 KEM 和 KDF。

A08.13: 凭证与标识符绑定

接受方接受的凭据、连接标识与密码套件，与对端实际发送并在签名与 transcript 哈希中覆盖的值一致。

一方接受的凭证、连接标识符和密码套件就是其对端使用并签名的那些：标识符位于 MAC 上下文和 transcript 哈希内，套件位于 message_1 内，因而位于 TH_2 内。已接受会话的双方使用同一套件。

- 结果：Holds；回答了所问：是；可用但有保留
- 价值中：它确认了模型所具有的字段的字段绑定，这正是实现者必须保持的。
- 文稿中已说明：是。文稿中的位置：s0190、s0223
- 依据：凭证和标识符从消息中携带的值无歧义地查找；只建模了一个套件。
- 未决：SUITES_I 的排序规则未分析（见 R05）。

X01: 发起者身份保护

an attacker taking part as a Responder cannot tell which of two initiator credentials (ID_CRED_I, CRED_I) took part in a session in which the Initiator sends message_3

以响应方身份参与的攻击者在会话期间不会获得发起者的凭证标识符：该标识符只在 CIPHERTEXT_3 内传输，其密钥需要 KEM 秘密，而发起者只有在响应方证明了其签名之后才发送 message_3。这就是 RFC 9528 9.1 针对主动攻击为发起者主张的身份保护。

- 结果：Holds；回答了所问：部分；可用但有保留
- 价值中：它复现了一项有文档记载的保证及其成立的理由，并说明了其中哪种形式尚未确定。
- 文稿中已说明：是。文稿中的位置：s0036
- 依据：该主张是标识符的保密性，而非两个候选身份之间的不可区分性；后者未被证明；理想化 KEM 和 AEAD。
- 未决：问题的不可区分性形式，即攻击者能否分辨使用了两个发起者凭证中的哪一个，无法确定：ProVerif 无法证明非干扰性，而它找到的一个推导使用了前向保密场景在运行结束时揭示的长期密钥，其中泄露的密钥会识别其持有者。

X02: 仅对被动攻击者的响应者标识符保护

an attacker who only observes cannot tell which of two responder credentials took part, but an attacker who answers with its own message_1 learns the responder's credential identifier

主动攻击者确实会获知响应者的凭证标识符，因此响应者的身份仅对被动攻击者受到保护。在协议中，攻击者只需发送自己的 message_1 并读取应答，因为它可以封装到自己的密钥对；在模型中，该路径和 message-2 密钥流泄露都以攻击者持有 ID_CRED_R 告终。

- 结果：攻击成立（文稿中已说明）；回答了所问：是；可用但有保留
- 价值低：它复现了 RFC 自己陈述的弱点；价值在于其原因是机械的。
- 文稿中已说明：是。文稿中的位置：s0036
- 依据：ProVerif 产生的轨迹通过泄露场景的密钥流揭示到达标识符；协议路径不需要泄露，且正是 RFC 所描述的路径；理想化 KEM。
- 未决：陈述的被动一半，即观察者无法分辨使用了哪个响应者凭证，未作为非干扰性问题确定。

X03: 长期密钥泄露下的 KCI 保护

an attacker holding the Initiator's long-term signature key cannot make the Initiator accept a session in which the Responder never ran

持有长期签名密钥的攻击者无法使发起者接受一个响应方从未运行的会话：接受仍然需要该发起者被给定的身份密钥下的签名，并对照新鲜的 C_R 和 TH_2 进行检查。这正是算法密钥泄露冒充保护所针对的方向，但模型只在运行之后才把密钥交给攻击者。

- 结果：Holds；回答了所问：部分；可用但有保留
- 价值低：该结果是对有文档记载的 KCI 主张的较弱解读；说明这一点比将其升级更有用。
- 文稿中已说明：是。文稿中的位置：s0084
- 依据：泄露发生在会话之后；每个角色一份凭证，理想化签名。
- 未决：在此模型中攻击者仅在会话之后才知道密钥，因此密钥有效期间的冒充未被测试；若模型从一开始就知道密钥，则会失去响应方侧认证目标，而一旦发起者的密钥公开，该目标按定义就已失去。

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，以及各项攻击及分析者对每项的判定。

目标	级别 界	查询	对照	攻击	主张
A02	proved	auth_i	checked		2 proved
A03	proved	auth_i	checked		2 proved
A04	proved	auth_i_inj	checked		2 proved
A06	proved	conf4	checked		1 proved
K01	proved	k_secret	checked		4 proved
K04	proved	sep_m3			3 proved
A08	proved	auth_i	checked		2 proved
R05	proved	suite_agree			1 proved
C01	proved	fs_prk	checked		3 proved
C04	proved	fs_prk	checked	dk_k (holds_in_source); dk_prk (holds_in_source)	1 proved, 2 attack
A03.11	proved	auth_i	checked		2 proved
K01.12	proved	k_secret	checked		2 proved
A08.13	proved	auth_r	1 of 2		2 proved
X01	proved	id_i_secret	checked		1 proved
X02	none			id_r_reveal (holds_in_source)	1 attack
X03	proved	auth_i	checked		1 proved

逐条主张，按分析者对每条主张的表述；对每条的回答是证明器的：

目标	主张	攻击者	回答	查询	对照
A02	如果发起方在验证 Signature_or_MAC_2 之后接受一个会话，那么曾有一个响应方会话使用相同的 C_I、C_R 和相同的响应方身份运行；网络上的攻击者除了这些消息之外不掌握任何东西。	`network`	proved	auth_i	checked
A02	如果响应方在验证 Signature_or_MAC_3 之后接受一个会话，那么曾有一个发起方会话使用相同的 C_I、C_R 和相同的发起方身份运行；网络上的攻击者除了这些消息之外不掌握任何东西。	`network`	proved	auth_r	checked
A03	发起方一侧：发起方接受的 C_R、ID_CRED_R 和 transcript 哈希，来自一个确实运行过的响应方会话，因为 Signature_or_MAC_2 是在包含这些内容的上下文上校验的。	`network`	proved	auth_i	checked
A03	响应方一侧：响应方接受的 C_I、C_R、ID_CRED_I 和 TH_3，属于一个确实运行过的发起方会话，因为 Signature_or_MAC_3 是在包含这些内容的上下文上校验的。	`network`	proved	auth_r	checked

目标	主张	攻击者	回答	查询	对照
A04	每个响应方运行至多被一个发起方接受：记录下来的 message_2 不能被重放到第二个发起方会话，也不存在一个接受对应两个响应方运行的情况。	`network`	proved	auth_i_inj	checked
A04	每个发起方运行至多被一个响应方接受：记录下来的 message_3 不能被重放进入第二个响应方会话。	`network`	proved	auth_r_inj	checked
A06	如果发起方接受了 message_4，那么曾有一个响应方会话派生出了相同的 PRK_out 并发送了匹配的确认；对 K_4 下 CIPHERTEXT_4 的校验正是使这一点成立的原因。	`network`	proved	conf4	checked
K01	双方接受的会话的 KEM 共享密钥 K（G_XY）不会到达网络上的攻击者。	`network`	proved	k_secret	checked
K01	已接受会话的 PRK_out 不会到达网络上的攻击者。	`network`	proved	prk_secret	checked
K01	已接受会话的 PRK_exporter 以及由 PRK_out 派生的应用密钥不会到达网络上的攻击者。	`network`	proved	exp_secret	checked
K01	通过 EDHOC_Exporter 从已接受会话的 PRK_out 派生的应用密钥不会到达网络上的攻击者。	`network`	proved	app_secret	checked
K04	持有某会话 KEYSTREAM_2 的攻击者无法获得该会话的 K_3，尽管它此后可以读取 PLAINTEXT_2。	`key_leak`	proved	sep_m3	none
K04	持有某会话 KEYSTREAM_2 和 K_3 的攻击者无法获得该会话的 K_4。	`key_leak`	proved	sep_m4	none
K04	持有某会话 KEYSTREAM_2 和 K_3 的攻击者无法获得该会话的 PRK_out。	`key_leak`	proved	sep_prk	none
A08	发起方接受的凭证标识符（ID_CRED_R，以及为其取得的 CRED_R）就是其密钥签署了 MAC_2 的那一个，因此凭证不会被错误绑定到另一身份的密钥上。	`network`	proved	auth_i	checked
A08	响应方接受的凭证标识符（ID_CRED_I，以及为其取得的 CRED_I）就是其密钥签署了 MAC_3 的那一个，并且它使用的 transcript 哈希就是它所收到消息的哈希。	`network`	proved	auth_r	checked
R05	已接受会话的双方对所选 cipher suite 达成一致；携带 SUITES_I 的 message_1 被 TH_2 覆盖，因此一旦 suite 被改动，双方会话就会不一致，不会产生接受。	`network`	proved	suite_agree	none
C01	在会话之后获知两个长期 ML-DSA 签名密钥的攻击者，无法获得该会话的 PRK_out。	`ltk_leak`	proved	fs_prk	checked
C01	在会话之后获知两个长期签名密钥的攻击者，无法获得该会话的 PRK_exporter 或应用密钥。	`ltk_leak`	proved	fs_exp	checked
C01	获知两个长期签名密钥的攻击者无法获得已接受会话的 KEM 共享密钥 K。	`ltk_leak`	proved	fs_k	checked
C04	泄露某个发起方会话的临时解封装密钥 dk 会暴露该会话的 KEM 共享密钥 K，并随之暴露整个会话密钥链。	`kem_dk_leak`	attack (holds_in_source)	dk_k（k_secret 的对照）	
C04	泄露某个会话的 dk 会暴露该会话的 PRK_out：攻击者进行解封装，用 KEYSTREAM_2 读取 PLAINTEXT_2，并重新计算 TH_4 和 PRK_out。	`kem_dk_leak`	attack (holds_in_source)	dk_prk（prk_secret 的对照）	
C04	除 dk 泄露的那个会话之外，其他会话的密钥仍然保密：持有一个会话 dk 的攻击者无法获得任何其他已接受会话的 PRK_out。	`kem_dk_leak`	proved	fs_prk	checked

目标	主张	攻击者	回答	查询	对照
A03.11	发起方接受的标识符、凭证和 transcript 哈希与某个响应方运行相匹配，因此双方处于同一会话。	`network`	proved	auth_i	checked
A03.11	方向性：响应方的接受绑定到发起方自己的 message_3，因为 MAC_3 是在包含 ID_CRED_I、TH_3 和 CRED_I 的上下文上签名的；一个方向的签名不能用于另一个方向。	`network`	proved	auth_r	checked
K01.12	每个会话都使用新生成的 KEM 密钥对，因此会话的 K 和 PRK_out 对网络攻击者保密。	`network`	proved	k_secret	checked
K01.12	已接受会话的 PRK_out、PRK_exporter 以及由 exporter 派生的应用密钥对网络攻击者保持保密。	`network`	proved	prk_secret	checked
A08.13	一方接受的凭证，就是其密钥对该方所持有的 transcript 签署了其对端 MAC 的那一个，因此凭证、标识符和 transcript 被绑定在一起。	`network`	proved	auth_r	checked
A08.13	一方接受的 cipher suite 就是 message_1 中携带并被 TH_2 覆盖的那一个，且已接受会话的双方使用同一 suite。	`network`	proved	suite_agree	none
X01	以响应方身份参与的攻击者在会话过程中无法获得发起方的凭证标识符：该标识符只在 CIPHERTEXT_3 内传输，而读取它需要 K_3，且发起方只有在验证响应方签名之后才发送 message_3。	`network`	proved	id_i_secret	checked
X02	以响应方身份参与的攻击者会获知响应方的凭证标识符：它可以对自己构造的 message_1 进行封装，并从解密得到的 PLAINTEXT_2 中读取 ID_CRED_R。	`network`	attack (holds_in_source)	id_r_reveal（id_i_secret 的对照）	
X03	持有长期签名密钥的攻击者无法使发起方接受一个响应方一侧从未运行过的会话：发起方用其所获身份对应的密钥校验 Signature_or_MAC_2，而它持有的密钥无法针对新的 C_R 和 TH_2 生成该签名。	`ltk_leak`	proved	auth_i	checked

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-20261114T231222，2026-11-14。状态：已完成。模型：deepseek-v4-1-flash-261017。步数：48，证明器 76 秒，总耗时 17 分钟，费用 0.161 美元。

ProVerif：运行 73 次证明，67 次判定，6 次无答案，56 秒，记录 43 个回答。

分析了什么

协议	LAKE PQ signature method 0
版本	draft-ietf-lake-pqsuites-02
分析范围	明确选择 method 0 双向签名及草案 6.4 注册的 ML-KEM/ML-DSA cipher suite；m1 中临时 KEM 公钥、m2 中 ct、m3 和可选 m4，完整 transcript/credential/context 及 key derivation。不是 authkem 草案，无需修正那份文稿的五消息歧义；预置可信公钥，算法理想化。
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	281 个编号原文单元（41464 字节），取自下文列出的各节。本报告中形如 s0001 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	2	采用抗量子算法的 LAKE
main	3	在密钥交换中使用 KEM
main	4	安全考虑
main	4.1	经典 LAKE 安全性质
main	4.2	后量子安全
main	4.2.1	先存储后解密
main	4.2.2	PQ/T 混合
main	4.2.3	侧信道考虑
main	6.4	LAKE 密码套件注册表
rfc9528	4	密钥派生
rfc9528	4.1	用于 EDHOC 消息处理的密钥
rfc9528	4.1.1	EDHOC_Extract
rfc9528	4.1.1.1	PRK_2e
rfc9528	4.1.1.2	PRK_3e2m
rfc9528	4.1.1.3	PRK_4e3m
rfc9528	4.1.2	EDHOC_Expand 与 EDHOC_KDF
rfc9528	4.1.3	PRK_out

文稿	章节	标题
rfc9528	4.2	用于 EDHOC 应用的密钥
rfc9528	4.2.1	EDHOC_Exporter
rfc9528	5	消息格式与处理
rfc9528	5.1	EDHOC 消息处理概要
rfc9528	5.2	EDHOC 消息 1
rfc9528	5.2.1	消息 1 的格式
rfc9528	5.2.2	发起方构造消息 1
rfc9528	5.2.3	响应方处理消息 1
rfc9528	5.3	EDHOC 消息 2
rfc9528	5.3.1	消息 2 的格式
rfc9528	5.3.2	响应方构造消息 2
rfc9528	5.3.3	发起方处理消息 2
rfc9528	5.4	EDHOC 消息 3
rfc9528	5.4.1	消息 3 的格式
rfc9528	5.4.2	发起方构造消息 3
rfc9528	5.4.3	响应方处理消息 3
rfc9528	5.5	EDHOC 消息 4
rfc9528	5.5.1	消息 4 的格式
rfc9528	5.5.2	响应方构造消息 4
rfc9528	5.5.3	发起方处理消息 4

协议的目的，如源文步骤在文稿中所定位的那样：明确选择 method 0 双向签名及草案 6.4 注册的 ML-KEM/ML-DSA cipher suite；m1 中临时 KEM 公钥、m2 中 ct、m3 和可选 m4，完整 transcript/credential/context 及 key derivation。不是 authkem 草案，无需修正那份文稿的五消息歧义；预置可信公钥，算法理想化。

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与文稿本身对协议目的的说明做了对照。名称、每条性质所涉及的对象，以及文稿的表述，都是分析者的解读；所引用的位置在文稿中确实存在。

ID	简称	对象	文稿怎么说	出处
A02	方法 0 中的双向认证	每一方在验证对端签名后接受会话时，都确信对端的身份	main 4.1 指出这些套件为 Method 0 保留了 RFC 9528 第 9 节的性质，包括双向认证	main:368, rfc9528:2237
A03	双方会话匹配	双方对其完成的会话中的 C_I、C_R、CRED_I、CRED_R 以及转录哈希达成一致	RFC 9528 9.1 指出 EDHOC 提供带活性、一致性和对端感知的双向认证	rfc9528:2238

ID	简称	对象	文稿怎么说	出处
A04	无对端运行重放	每次接受都对应不同的对端会话；录制的流程不会被接受两次	RFC 9528 9.1 指出认证覆盖范围可防止来自另一会话的重放和注入；每个会话都需要新的 KEM 密钥对	rfc9528:2268
A06	来自消息 4 的密钥确认	发起方在接受 message_4 时确信响应方计算出了相同的 PRK_out	RFC 9528 5.5.3 指出验证 message_4 之后，发起方确信响应方已计算出 PRK_out	rfc9528:1913
K01	会话密钥保密性	K、PRK_out、PRK_exporter 以及应用密钥对网络攻击者保持保密	main 为 Method 0 主张保密性和密钥安全；RFC 9528 9.1 指出一个会话密钥不会危及其它会话密钥	main:369, rfc9528:2309
K04	派生密钥间的密钥分离	同一 PRK 下以不同 info_label 派生的密钥相互独立	图 6 用各自不同的 info_label 派生每个密钥；9.2 指出一部分不得削弱另一部分	rfc9528:2468, rfc9528:1354
A08	转录与凭证绑定	接受的凭证标识符、连接标识符、转录哈希和密码套件与对端所用并签名的内容一致	RFC 9528 9.1 指出把凭证纳入转录哈希可防止身份错误绑定	rfc9528:2241
R05	无密码套件降级	选定的密码套件无法被更改：双方只以发起方选定的套件完成	RFC 9528 9.1 指出 EDHOC 增加了防降级的协商；5.2.2 因伪造的错误消息而禁止重排 SUITES_I	rfc9528:2272, rfc9528:2268
C01	已完成会话的前向保密	已完成会话的会话密钥对日后获知两个长期签名密钥的攻击者保持保密	RFC 9528 9.1 指出认证私钥的泄露不会危及过去的会话密钥；4.1.1.1 指出临时共享秘密提供前向保密	rfc9528:2284, rfc9528:2299
C04	临时 KEM 密钥泄露边界	某一会话的 dk 泄露会给出该会话的 K 和 PRK_out，但不会给出其它会话的密钥	K = Decaps(dk, c)，且每个会话使用新的 KEM 密钥对；RFC 9528 9.1 指出共享秘密的泄露会危及由它派生的密钥	rfc9528:2306
A03.11	方向与转录一致性	每次接受都对应一次对端运行，二者身份、标识符和转录哈希相同；每个签名仅对其方向有效	RFC 9528 9.1：一致性和对端感知；5.3.2 和 5.4.2 在不同上下文中对 MAC_2 和 MAC_3 签名	rfc9528:2238
K01.12	新鲜 KEM 密钥与导出器保密性	每个会话都使用新的 KEM 密钥对和 PRK_out，PRK_out、PRK_exporter 以及应用密钥对网络攻击者保持保密	每个会话都需要新的 KEM 密钥对；9.1 指出 PRK_out 的泄露会危及用 EDHOC_Exporter 派生的一切	rfc9528:2310
A08.13	凭证与标识符绑定	一方接受的凭证、标识符和密码套件正是对端所使用的、并被转录哈希和签名所覆盖的那些	RFC 9528 9.1：把凭证纳入转录哈希可防止身份错误绑定	rfc9528:2241
X01	发起者身份保护	发起方的凭证标识符和凭证	RFC 9528 9.1 指出 EDHOC 提供发起方抵御主动攻击的身份保护；main 为 Method 0 列出了身份保护	rfc9528:2248, main:369

ID	简称	对象	文稿怎么说	出处
X02	仅对被动攻击者的响应者标识符保护	响应方的凭证标识符和凭证	RFC 9528 9.1 指出 EDHOC 提供响应方抵御被动攻击的身份保护，而主动攻击者可以通过发送自己的 message_1 获取凭证标识符	rfc9528:2246, rfc9528:2249
X03	长期密钥泄露下的 KCI 保护	当发起方的长期密钥被知晓时，响应方对发起方的真实性	RFC 9528 9.1（Key Compromise Impersonation）指出经签名认证的 EDHOC 提供防护，抵御可访问长期密钥的攻击者	rfc9528:2366

分析者依据文稿补充的性质：X01, X02, X03.

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 124 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 19 段，没选 105 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
P001 至 P003	draft-ietf-jose-pqc-kem:550-571	不在范围内	COSE PQ-KEM 约定草案，不是本交换
P004	main:355-359	没有陈述目标	动机
P005	main:363-370	A02, K01, X01, X02	
P006	main:372-378	证明器问不了	基于原语安全性的论证
P007	main:382-388	证明器问不了	算法安全性引用
P008	main:390-393	证明器问不了	随机预言机模型，计算性
P009	main:395-399	证明器问不了	量子攻击者模型
P010	main:404-404	没有陈述目标	页脚
P011	main:408-408	证明器问不了	Q1 模型中的未来工作
P012	main:411-418	没有陈述目标	页眉
P013	main:420-422	证明器问不了	NIST 类别
P014	main:424-427	证明器问不了	原像抗性
P015	main:431-433	C01	
P016	main:437-443	证明器问不了	混合套件组合
P017	main:445-446	没有陈述目标	未来注册
P018	main:450-454	证明器问不了	侧信道
P019	main:456-458	证明器问不了	实现要求
P020	main:462-462	没有陈述目标	页脚
P021	main:466-466	没有陈述目标	页眉
P022	main:469-475	A04, C04, K01.12	
P023	main:479-480	X01, X02	

段落	出处	定为	不选的原因
P024 至 P027	rfc5116:913-940	不在范围内	AEAD 算法规范
P028 至 P030	rfc8392:500-521	不在范围内	CWT 规范
P031 至 P032	rfc8742:257-268	不在范围内	CWT 声明注册表
P033 至 P046	rfc8949:2406-2533	不在范围内	CBOR 编码
P047 至 P060	rfc9052:2388-2467	不在范围内	COSE 层
P061 至 P069	rfc9360:440-505	不在范围内	CWT/COSE 配置
P070	rfc9528:2231-2235	没有陈述目标	引用已发表的分析
P071	rfc9528:2237-2244	A02, A03, A06, A08, C01, A03.11	
P072	rfc9528:2246-2255	X01, X02, `network`	
P073	rfc9528:2257-2263	A02, A08	
P074	rfc9528:2265-2269	A04, A08.13	
P075	rfc9528:2271-2278	R05, A03	
P076	rfc9528:2280-2290	C01	
P077	rfc9528:2292-2297	没有陈述目标	关于凭据类型的建议
P078	rfc9528:2299-2311	C01, C04	
P079	rfc9528:2313-2323	证明器问不了	比特安全性
P080	rfc9528:2325-2337	证明器问不了	MAC 强度求和
P081	rfc9528:2339-2348	A02, A06, K01	
P082	rfc9528:2350-2354	不在范围内	EAD_1 和 EAD_2
P083	rfc9528:2356-2364	不在范围内	EAD_3 和 EAD_4
P084	rfc9528:2366-2375	C01, C04, X03	
P085	rfc9528:2377-2382	证明器问不了	抵赖
P086	rfc9528:2384-2386	没有陈述目标	引用分析
P087	rfc9528:2390-2396	没有陈述目标	实现要求
P088	rfc9528:2398-2407	A04, C04, K01.12	
P089	rfc9528:2409-2421	X02	
P090	rfc9528:2423-2429	没有陈述目标	曲线密钥验证，此处未使用
P091	rfc9528:2431-2441	没有陈述目标	密钥重用建议
P092	rfc9528:2443-2456	A02, X01	
P093	rfc9528:2458-2470	K04	
P094	rfc9528:2474-2479	证明器问不了	密钥长度协调
P095	rfc9528:2481-2494	证明器问不了	算法要求
P096 至 P098	rfc9528:2498-2528	证明器问不了	后量子考量
P099	rfc9528:2532-2544	X02	
P100	rfc9528:2546-2558	不在范围内	通过明文连接标识符关联；无关联性模型
P101	rfc9528:2562-2572	不在范围内	威胁模型与追踪

段落	出处	定为	不选的原因
P102	rfc9528:2574-2582	不在范围内	长度侧信道
P103 至 P104	rfc9528:2586-2609	证明器问不了	拒绝服务
P105 至 P117	rfc9528:2613-2745	没有陈述目标	实现指导
P118 至 P119	rfc9964:283-290	不在范围内	ML-DSA COSE 配置
P120	rfc9964:294-299	C01, `ltk_leak`	
P121	rfc9964:303-309	不在范围内	HashML-DSA 理由
P122 至 P123	rfc9964:313-327	没有陈述目标	密钥验证要求
P124	rfc9964:331-335	不在范围内	密钥参数编码

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 11 条，没检查 21 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	不适用	无载荷；协议只建立密钥
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	A03, A08	
A01	对端曾参与性（Aliveness）	A02	
A05	隐式密钥认证	A03, A08	
A07	身份—凭据—密钥绑定	A08.13	
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	无业务操作
R04	消息接受顺序／窗口安全	不适用	无窗口或顺序规则
C02	抗密钥泄露冒充（KCI）	X03	
C03	已知密钥安全／泄露隔离	K04, C04	
C05	泄露后安全恢复（PCS）	不适用	建模流程中没有棘轮或密钥更新
C06	注册凭据泄露后的增强认证	不适用	无口令记录
C07	抗离线字典攻击	不适用	无低熵秘密
C08	指定原语失效下的目标保持	不适用	已注册套件在原语失效下不作任何主张
Z01	授权执行正确性	不适用	无授权
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	无令牌
Z04	撤销与过期生效	不适用	无撤销
Z05	跨租户／跨服务安全隔离	不适用	无租户
S01	加密 nonce 唯一性	不适用	每会话密钥仅用于一条消息
S02	重传／密钥重安装安全	不适用	无密钥安装

条目	目录里的性质	作为哪条性质检查	不检查的原因
S03	抗回滚与状态单调性	不适用	无状态可回滚
S04	跨阶段安全上下文一致性	不适用	单一握手阶段
S05	终止与旧状态失效	A04	
P01	身份匿名性	X01, X02	
P02	会话不可关联性	不在范围内	RFC 9528 9.5 指出可通过明文连接标识符关联；未构建关联性模型
P03	用户／凭据存在性隐藏	不适用	无可枚举的目录
V01	条件性进展／错误恢复	证明器问不了	活性
V02	无非预期死锁	证明器问不了	活性
V03	受限资源滥用／抗放大	证明器问不了	资源耗尽

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 28 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 14 项，没设的 14 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	发起方 I	参与方	`ltk_leak`, `kem_dk_leak`	
S02	响应方 R	参与方	`ltk_leak`	
S03	攻击者	参与方	攻击者得不到更多	这就是攻击者本身；网络攻击者始终被假定存在
S04	对端身份的真实性	值	`ltk_leak`	
S05	连接标识 C_I、C_R	值	攻击者得不到更多	在线上是公开的
S06	凭据 CRED_I、CRED_R	值	攻击者得不到更多	凭据是公开的
S07	transcript 哈希 TH_2、TH_3	值	攻击者得不到更多	中间哈希，没有 prk_2e 就无法得到密钥
S08	所选密码套件	值	攻击者得不到更多	在 message_1 中以明文发送
S09	会话唯一性	值	攻击者得不到更多	不是可持有的值；重放由 A04 覆盖
S10	临时 KEM 密钥对	值	`kem_dk_leak`	
S11	PRK_out	值	`kem_dk_leak`, `ltk_leak`, `key_leak`	
S12	K_4	值	`key_leak`	
S13	KEM 共享密钥 K	值	`kem_dk_leak`	
S14	PRK_exporter	值	`kem_dk_leak`, `ltk_leak`, `key_leak`	
S15	应用导出密钥	值	`kem_dk_leak`, `ltk_leak`	
S16	K_3	值	`key_leak`	
S17	KEYSTREAM_2	值	`key_leak`	
S18	导出密钥	值	`ltk_leak`, `kem_dk_leak`	
S19	C_I、C_R	值	攻击者得不到更多	在线上是公开的

ID	参与方或值	类别	攻击者条件	不设的原因
S20	ID_CRED_I、ID_CRED_R	值	攻击者得不到更多	标识符值；会话用了哪一个由两条身份目标查询
S21	CRED_I、CRED_R	值	攻击者得不到更多	凭据是公开的
S22	TH_2、TH_3、TH_4	值	攻击者得不到更多	中间哈希
S23	SUITES_I	值	攻击者得不到更多	以明文发送
S24	历史会话的 KEM 共享密钥 K	值	`ltk_leak`	
S25	其他会话的密钥	值	`kem_dk_leak`	
S26	身份	值	攻击者得不到更多	身份是公开的；会话用了哪一个由身份目标查询
S27	TH_2、TH_3	值	攻击者得不到更多	中间哈希
S28	方向	值	攻击者得不到更多	由承载签名的消息固定

每条性质在各攻击者条件下的答案

攻击者是分析者设定的，在写查询之前就已确定；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的答案；“无答案”是该性质下证明器未对某条主张作出判定或未记录任何内容时所对应的攻击者；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：读取、丢弃、修改和发送消息，不持有任何一方的秘密		
`ltk_leak`	双方的长期 ML-DSA 签名私钥，在会话完成后获知	RFC 9528 9.1 说明了私认证密钥泄露能带来什么、不能带来什么	rfc9528:2299
`kem_dk_leak`	某个发起方会话的 ML-KEM 解封装密钥，在该会话之后获知，外加网络	K = Decaps(dk, c)，且草案要求每个会话使用新的 KEM 密钥对，因此泄露的 dk 只属于一个会话	rfc9528:2306
`key_leak`	某个会话的 KEYSTREAM_2 和 K_3，在该会话之后获知，外加网络	图 6 在每个密钥各自的 info_label 下派生所有密钥，9.2 指出一部分不得降低另一部分	rfc9528:2468

ID	`network`	`ltk_leak`	`kem_dk_leak`	`key_leak`
A02	成立			
A03	成立			
A04	成立			
A06	成立			
K01	成立			
K04				成立
A08	成立			
R05	成立			
C01		成立		
C04			不成立	
A03.11	成立			
K01.12	成立			

ID	network	ltk_leak	kem_dk_leak	key_leak
A08.13	成立			
X01	成立			
X02	不成立			
X03		成立		

原文和目标

Source: 281 units, 41464 bytes, frozen in source-delivery-01.json. Targets: 10 approved (A02, A03, A04, A06, K01, K04, A08, R05, C01, C04); the questions asked: 3. The list of targets was approved as drafted, beforehand, with --approve-targets.

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

- approve_package: 批准源文包 protocol-3d24772d27239387d0704487813b

这一步的自我报告：1 requests (1 failed), 0.000 USD, 36304 tokens in and 5066 out, 31 s.

关于证明器和模型的说明

分析者为目标指定的名称：

step	targets	features	reason
42	A02, A03, A04, A06, K01, K04, A08, R05, C01, C04, A03.11, K01.12, A08.13, X01, X02, X03	plain_primitives, many_sessions	每个答案都依赖 ML-KEM 作为理想封装（用 dk 解封装恰好还原被封装的秘密）、ML-DSA 签名，以及哈希/KDF/流密码/AEAD 作为理想单向原语；除此之外不使用任何代数定律。所问性质覆盖两种角色的任意数量的会话。没有任何目标依赖在步骤之间会被替换的计数器、序列号或密钥，因此既没有有界展开，也没有 bounded.pv。

分析者的总结说明

在 ProVerif 中构建了 LAKE PQ 签名方法 0 的模型（用 ML-KEM 替代 RFC 9528 方法 0 的临时 DH，ML-DSA 签名，一个选定的 PQ 密码套件，message_1 到 message_4，包含完整会话记录和密钥调度）；正常流程存在，全部 16 个目标都有答案。

已确立（全部基于 model.pv，除非另有指明，攻击者位于网络上）：双向的相互认证（A02、A03、A03.11）及其单射形式，即 message_2 或 message_3 无法重放（A04），每项均配有去掉签名检查后失败的对照方；来自 message_4 的密钥确认（A06，配有去掉该检查的对照）；KEM 共享秘密、PRK_out、PRK_exporter 以及导出器派生的应用密钥的保密性（K01、K01.12）；密钥分离，即泄漏的 KEYSTREAM_2 和 K_3 既不能给出 K_4 也不能给出 PRK_out（K04，在持有这些密钥的攻击者条件下）；凭证、标识符和会话记录绑定（A08、A08.13）；前向保密，即会话之后两个长期签名密钥都泄漏也不会给出过去的会话密钥（C01，配有解封装密钥泄漏的对照）；以及 Initiator 的凭证标识符不会到达以 Responder 身份参与的攻击者（X01）。

发现了两个攻击，二者均已在文稿中说明，并作为 holds_in_source 提交：泄漏的 KEM 解封装密钥会暴露该会话的 K 和 PRK_out，但不涉及其他会话的任何内容（C04）；主动攻击者能获知 Responder 的凭证标识符，因此 Responder 的身份仅对被动攻击者受保护（X02）。没有超出文稿的发现。

部分完成：R05（密码套件降级）只针对所选套件的绑定给出了答案，因为 SUITES_I 协商和伪造的错误消息未建模；X03（密钥泄露冒充）的答案中，长期密钥仅在会话之后已知，因此密钥有效期间的冒充未被测试，身份保护问题也无法以其非干扰形式解决（ProVerif 无法证明它们；它给出的唯一推导使用已揭示的长期密钥，而这些密钥本质上会标识其持有者）。阻碍：一个在会话期间已知长期密钥的 Tamarin 模型可以解

决 X03，一个不含阶段 1 密钥揭示的模型可以解决身份不可区分性问题。所有答案都依赖理想化的 ML-KEM、ML-DSA、哈希和 KDF，以 `fit`（plain_primitives, many_sessions）记录；无需 bounded.pv，因为没有任何目标依赖在步骤之间会变化的值。