IKEv2 的安全性分析：ML-KEM 附加密钥交换与最终认证

本报告的其他语言版本：English。

draft-ietf-ipsecme-ikev2-mlkem-09 · ProVerif+ Agent 报告

文稿	Post-quantum Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2)（协议定义）; Internet Key Exchange Protocol Version 2 (IKEv2)（辅助）; Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2)（辅助）; Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)（辅助）
检查的性质	11 条：11 条成立，0 条不成立
发现	无

目录

1 协议和范围
2 发现
3 检查过的性质
4 本次分析的局限
附录 A：逐条性质的解读
附录 C：主张和证明器的答案
附录 D：分析是怎么跑的

1 协议和范围

这些文稿描述了在 IKEv2 中把 ML-KEM 作为第二个密钥交换加入的情形：两个对等方，一个发起方和一个响应方，先执行 IKE_SA_INIT，然后执行一次携带 ML-KEM 公钥和密文的 IKE_INTERMEDIATE 交换，最后执行 IKE_AUTH。发起方持有自己的签名密钥，响应方持有自己的签名密钥；响应方还持有它应答的那次交换所用的 ML-KEM 解封装秘密。

每个会话开始时先协商一个经典 Diffie-Hellman 秘密和两个 nonce，并据此派生 IKE SA 密钥。随后发起方在受保护的 IKE_INTERMEDIATE 消息中发送一个 ML-KEM 封装公钥，响应方回送一个密文，双方重新派生密钥，使密钥也依赖 ML-KEM 共享秘密。接着 IKE_AUTH 让每一方对自己的第一条消息、对方的 nonce 和身份，以及一个覆盖所有 IKE_INTERMEDIATE 消息的值进行签名，因此双方在交换结束时都确信自己是在本次运行中与所指名的对等方通信。

参与方：

- **发起方**：发起 IKE SA。持有：长期签名密钥。
- **响应方**：应答并执行封装。持有：长期签名密钥、ML-KEM 解封装秘密。

图 1 展示了文稿所规定的交换过程。

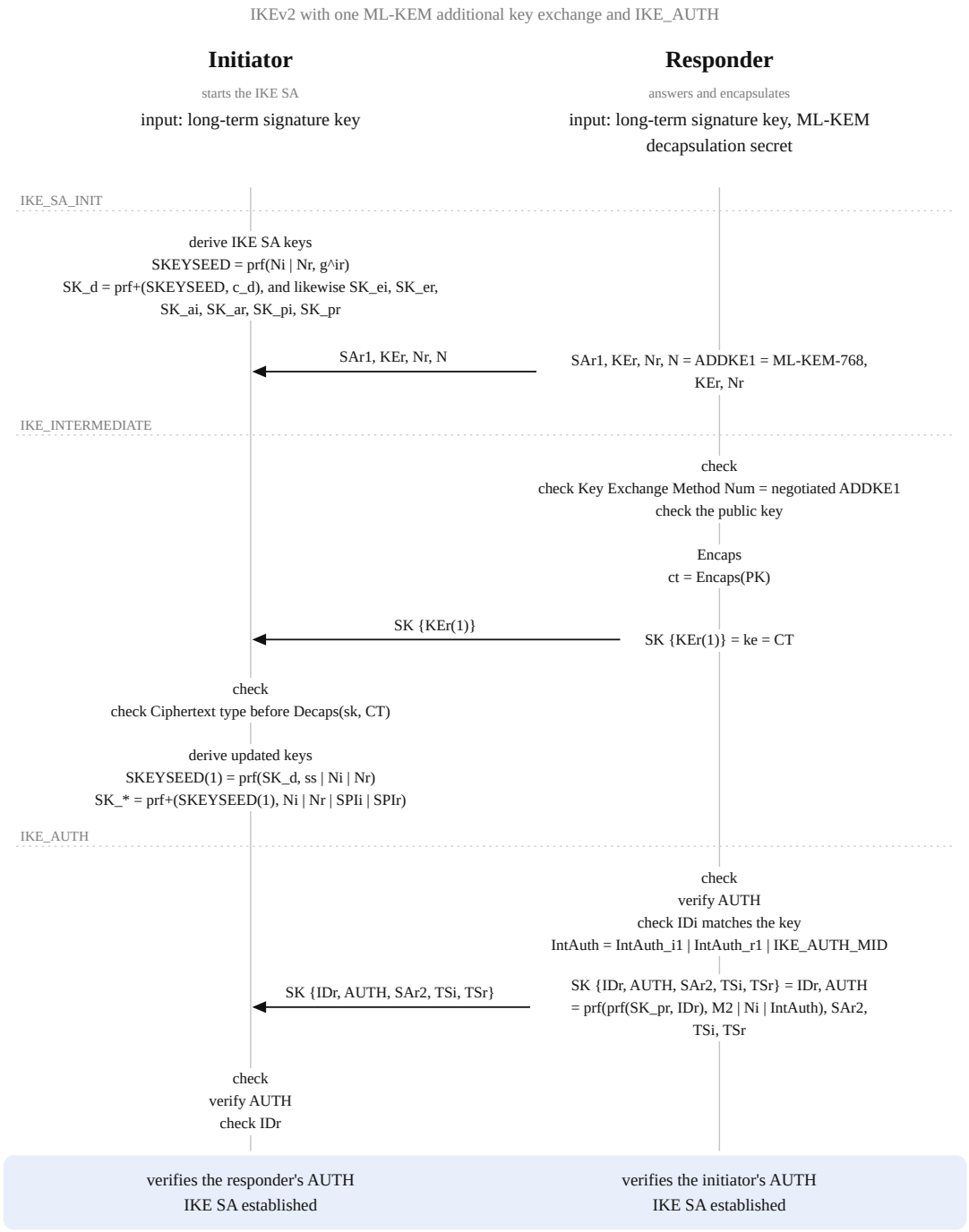


图 1. 文稿所规定的协议。

分析的范围见附录 D：分析了什么、略去了什么，以及它依据的文稿章节。

2 发现

没有发现。 分析没有发现文稿尚未陈述或尚未排除的任何问题。第 3 节的表给出了每条性质的结果。

在分析范围内，协议提供了它应当提供的保证，分析也没有发现文稿尚未陈述的任何问题。双方都确信对方的身份、双方的 nonce、SPI 以及 ML-KEM 公钥和密文，并且每一次接受都对应着对等方的一次不同运行。IKE SA 密钥对网络攻击者保持保密，即使单独丢失经典 Diffie-Hellman 秘密或单独丢失 ML-KEM 秘密它们仍然安全，并且在之后双方长期签名密钥都泄露时仍然安全。文稿自身陈述的已知弱点没有被转化为

发现：降级需要算法协商，而本范围将其固定排除在外；经典交换被攻破后的暴露则被证明会在 IKE_AUTH 中被发现。所有答案都来自一个用抽象共享秘密替代 Diffie-Hellman 的模型；Tamarin+ Agent 会建模代数，可以解决 Diffie-Hellman 方面的问题。

3 检查过的性质

每一行是一条提交给 ProVerif 的性质。结果是 ProVerif 在分析者的协议模型上给出的答案；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
A03	**对等方与附加KE的一致性。** 若响应方（或发起方）在 IKE_AUTH 完成后接受 IKE SA，则存在一个对端真实运行，其角色、双方意图身份、Ni、Nr、SPI 以及 IKE_INTERMEDIATE 中协商的附加 KE 方法与共享秘密一致。	无	成立	中	是
A04	**不会重放到第二次接受。** 每次一方接受 IKE SA 都对应一个不同的对端真实运行；同一 IKE_SA_INIT/IKE_INTERMEDIATE/IKE_AUTH 消息序列不能被重放产生第二次接受。	无	成立	中	是
A08	**附加KE绑定到协商。** IKE_INTERMEDIATE 中接受的附加 KE 方法、顺序与共享秘密对应 IKE_SA_INIT 中协商的 ADDKE 变换，并绑定到同一 IKE SA 的 SPI、nonce 与 AUTH。	无	成立	中	是
K01	**IKE SA密钥保密性。** 攻击者不能推导 IKE SA 的 SKEYSEED、SK_d、SK_ei/SK_er、SK_ai/SK_ar、SK_pi/SK_pr（含附加 KE 更新后的各代），也不能推导双方长期认证密钥。	无	成立	中	是
C01	**IKE SA密钥的前向保密。** 在 IKE SA 完成并擦除临时秘密之后，泄露双方长期认证密钥不能使攻击者获得此前会话的 SKEYSEED 或 SK。	双方长期认证密钥 (会话完成后)	成立	中	是
R05	**不会降级到不含ML-KEM的KE。** 攻击者不能使双方接受一个不含 ML-KEM 的 KE 提议，当双方策略要求 ML-KEM 时；接受的配置满足最低策略。	无	成立	低	是
C08	**会话密钥在一次KE被攻破后仍安全。** 在传统 (EC)DH 共享秘密或 ML-KEM 共享秘密之一被攻击者获得时，IKE SA 会话密钥仍对攻击者保密。	传统 (EC)DH 共享秘密 g^ir 或 ML-KEM 共享秘密 ss (KE 完成后、会话密钥派生后)	成立	中	是
K01.8	**IKE SA密钥保密性，用户问题。** 攻击者不能推导 IKE SA 的 SKEYSEED 与各 SK（含附加 KE 更新后的各代）。	无	成立	中	是
A03.9	**IKE SA接受时的一致绑定。** 每次一方接受 IKE SA 时，双方对身份、Ni、Nr、SPI、附加 KE 结果与 AUTH 一致。	无	成立	中	是
U01	**对IKE_INTERMEDIATE的篡改会被发现。** 攻击者删除、替换或篡改 IKE_INTERMEDIATE 附加 KE 时，双方不会在未察觉的情况下接受 IKE SA；接受的附加 KE 对应协商结果且被 AUTH 覆盖。	无	成立	中	是
X01	**ML-KEM密钥对与密文的新鲜性。** 同一对等方的任意两个 IKE SA 都不使用相同的 ML-KEM 封装公钥或相同的 ML-KEM 密文：发起方为每次 ML-KEM 密钥交换生成新的密钥对，响应方生成新的密文，且不复用任何随机数。	无	成立	低	是

文稿写明而起草的清单里没有、由分析者补充的目标（见附录 D）：X01.

提出的问题，以及分析者的回答：

问题	回答	依据
Q1: IKE SA 密钥保密	是。IKE SA 密钥在 ML-KEM 交换前后都对网络攻击者保密；即使攻击者在会话后单独获得经典 Diffie-Hellman 秘密、单独获得 ML-KEM 共享秘密，以及获得双方长期签名密钥，它们仍然安全。	K01, K01.8, C08, C01
Q2: 双方 KE 结果、身份与最终 AUTH 的一致绑定	是。每次接受都对应着对等方的一次真实运行，其身份、Ni、Nr、SPI、ML-KEM 公钥和密文都相同，并且 AUTH 签名覆盖了 nonce、身份以及 IKE_INTERMEDIATE 的内容。	A03, A03.9, A08, A04
Q3: 附加 KE 的删除/替换/协商篡改是否被检测	删除或替换 IKE_INTERMEDIATE 密钥交换数据不会导致未被察觉的接受：接受的密文始终是响应方发送并签名覆盖的那一个，即使攻击者已经攻破经典 Diffie-Hellman 交换、能够读取和伪造该消息也是如此。	U01, A08, A03

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了什么或未能给出什么，其中密码学被视为理想的，完全不涉及实现。

本次分析不覆盖的内容，按分析者的陈述：

- 不建模算法协商：ML-KEM 参数集以及附加密钥交换是否存在都是固定的，因此草案描述的降级攻击在此无法展现。
- Diffie-Hellman 被替换为抽象的交换性共享秘密，因此没有证明关于指数代数的任何内容；经典交换被攻破的攻击者通过把该会话的 g^ir 交给它来建模。
- ML-KEM 是理想的密钥封装机制：不建模解封装失败、隐式拒绝，也不建模草案第 2.2 节中的畸形密钥或密文检查。
- 子 SA 密钥材料、CREATE_CHILD_SA、IKE_FOLLOWUP_KE、重密钥以及无子 SA 的 IKE SA 不在范围内，也不建模。
- 不建模消息 ID、重叠请求的窗口以及 IKE 分片；重放性质依赖新的 nonce 和身份，而非消息 ID 规则。
- 不询问可用性：响应方在认证前的 DoS 暴露、大量 IKE_INTERMEDIATE 交换的开销以及重组限制均未覆盖。
- 不建模身份机密性、NAT 穿越、EAP 以及基于口令的认证。
- 擦除只作为阶段边界建模：一次运行的所有内容都在泄露释放之前结束，因此对于获得仍在运行的会话的临时秘密的攻击者，什么也没有说明。

宿主记录的内容：

- C01、R05、C08、U01 的答案依赖于模型简化的一个操作（附录 D）。
- 没带对照查询的证明（附录 C）：A03: a03_i, A03: a03_r, A04: a04_r, A04: a04_i, A08: a08, K01: k01_final, K01: k01_secret, K01: k01_ltk, R05: r05, K01.8: k01_final, K01.8: k01_secret, A03.9: a03_i, A03.9: a03_r, U01: a08, U01: u01_dh, X01: x01_pki, X01: x01_ct。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，以及什么能解决它们，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、能否照现在的样子使用，以及它有多大价值。

A03: 对等方与附加KE的一致性

若响应方（或发起方）在 IKE_AUTH 完成后接受 IKE SA，则存在一个对端真实运行，其角色、双方意图身份、Ni、Nr、SPI 以及 IKE_INTERMEDIATE 中协商的附加 KE 方法与共享秘密一致。

双方在交换结束时都知道自己与哪个对等方通信，以及该次运行使用了哪些 nonce、SPI、ML-KEM 公钥和密文；每次接受都对应着另一方的一次完整运行，因此网络上的攻击者无法让一方接受另一方从未使用过的值。

- Result: Holds；是否回答所问：是；可用但有保留
- 价值 中：组合流程的一项核心认证保证，已对任意数量的会话证明，但基于理想化原语，且 Diffie-Hellman 被抽象化。
- 文稿中已说明：是。文稿说明的位置：s0371、s0376、s0559、s0568
- 依据：Diffie-Hellman 是抽象的交换性共享秘密，而非群代数。；算法协商由范围固定。；签名是理想的：没有密钥替换，没有证书处理。；模型中的会话名是新鲜的，因此匹配基于身份、nonce 和密钥交换数据，而非 IKE SPI。

A03.9: IKE SA接受时的一致绑定

每次一方接受 IKE SA 时，双方对身份、Ni、Nr、SPI、附加 KE 结果与 AUTH 一致。

当以用户的问题表述时，同样的共识成立：在每次接受时，双方在两个方向上对身份、两个 nonce、SPI、附加密钥交换结果和 AUTH 值都一致。

- Result: Holds；是否回答所问：是；可用但有保留
- 价值 中：确认了加入 IKE_INTERMEDIATE 后 IKE_AUTH 本应提供的绑定，但它与 A03 是同一个证明。
- 文稿中已说明：是。文稿说明的位置：s0371、s0559
- 依据：与 A03 相同的简化：理想签名、抽象的 Diffie-Hellman、固定的算法套件。

A04: 不会重放到第二次接受

每次一方接受 IKE SA 都对应一个不同的对端真实运行；同一 IKE_SA_INIT/IKE_INTERMEDIATE/IKE_AUTH 消息序列不能被重放产生第二次接受。

一段录制的 IKE_SA_INIT、IKE_INTERMEDIATE 和 IKE_AUTH 序列不能被重放以在响应方产生第二次接受，一次响应方运行也不能被发起方计数两次：该对应关系在两个方向上都是单射的。

- Result: Holds；是否回答所问：是；可用但有保留
- 价值 中：文稿通过 Message ID 规则要求的一项性质，这里被证明仅由密码学绑定即可推出；这值得了解，但它并非文稿所依赖的机制。
- 文稿中已说明：是。文稿说明的位置：s0549、s0371
- 依据：Message ID 规则未被建模；单射性来自新鲜 nonce 与身份以及对其的签名。；重传和重叠窗口未被建模。

A08: 附加KE绑定到协商

IKE_INTERMEDIATE 中接受的附加 KE 方法、顺序与共享秘密对应 IKE_SA_INIT 中协商的 ADDKE 变换，并绑定到同一 IKE SA 的 SPI、nonce 与 AUTH。

发起方接受的 ML-KEM 密文正是响应方产生的那个，接受的方法也正是协商的方法，因此附加密钥交换不能被替换或重新绑定到另一次运行。该绑定来自对 IKE_INTERMEDIATE 内容以及由身份派生密钥的 AUTH 签名。

- Result: Holds；是否回答所问：是；可用但有保留
- 价值 中：表明 RFC9242 的 IntAuth 机制确实将附加密钥交换绑入认证，这正是草案设计的要点。
- 文稿中已说明：是。文稿说明的位置：s0621、s0623、s0559、s0568
- 依据：协商在模型中是常量，因此答案覆盖的是绑定，而非方法的选择。；ML-KEM 是理想的：密文与共享秘密通过一个未解释的函数相关联。

K01: IKE SA密钥保密性

攻击者不能推导 IKE SA 的 SKEYSEED、SK_d、SK_ei/SK_er、SK_ai/SK_ar、SK_pi/SK_pr（含附加 KE 更新后的各代），也不能推导双方长期认证密钥。

两代密钥的 IKE SA 密钥以及长期签名密钥都保持在网络攻击者掌握之外：它无法从所见内容推导出 SKEYSEED、方向密钥或 AUTH 密钥。

- Result: Holds；是否回答所问：是；可用但有保留
- 价值 中：组合流程的一项核心保证，但 IKEv2 的读者不会怀疑它，而且这里它是在理想化原语下成立的。
- 文稿中已说明：是。文稿说明的位置：s0363、s0623、s0625
- 依据：Diffie-Hellman 是抽象的，因此保密性的经典部分是被假设的，而非从群推导出来的。；KEM 是理想的，PRF 是随机函数；未证明任何具体原语的强度。

K01.8: IKE SA密钥保密性，用户问题

攻击者不能推导 IKE SA 的 SKEYSEED 与各 SK（含附加 KE 更新后的各代）。

对于用户关于密钥保密性的问题，答案与 K01 相同：SKEYSEED 以及两代的每一个派生密钥，在 ML-KEM 交换前后都保持在网络攻击者掌握之外。

- Result: Holds；是否回答所问：是；可用但有保留
- 价值 中：它直接回答了用户的第一个问题，保留与 K01 相同的注意事项。
- 文稿中已说明：是。文稿说明的位置：s0363、s0626
- 依据：与 K01 相同的简化。

C01: IKE SA密钥的前向保密

在 IKE SA 完成并擦除临时秘密之后，泄露双方长期认证密钥不能使攻击者获得此前会话的 SKEYSEED 或 SK。

会话完成后，即使攻击者获得双方的长期签名密钥，仍无法恢复该会话的密钥。对照运行——其中会话密钥本身被交出——表明该性质可以失败，因此证明并非空洞。

- Result: Holds；是否回答所问：是；可用但有保留
- 价值 中：再现了文稿作为要求所述的前向保密，适用于任意数量的会话，前提正是临时秘密被擦除。
- 文稿中已说明：是。文稿说明的位置：rfc7296:2446、rfc7296:2454、s0411

- 依据：擦除被建模为阶段边界：在泄露被释放之前，该运行的临时秘密已消失，这符合文稿的要求但文稿未将其形式化。；Diffie-Hellman 是抽象的，因此经典组件的前向保密依赖于该抽象。

C08: 会话密钥在一次KE被攻破后仍安全

在传统 (EC)DH 共享秘密或 ML-KEM 共享秘密之一被攻击者获得时，IKE SA 会话密钥仍对攻击者保密。

一个被接受的 IKE SA 所携带的密钥，攻击者无法仅从经典共享秘密算出，也无法仅从 ML-KEM 共享秘密算出：派生过程混合了两者。同时交出两个组件确实会破坏它，正如对照所示。

- Result: Holds；是否回答所问：是；可用但有保留
- 价值 中：这正是该扩展存在的理由所在的性质，已在两个单组件攻破下展示；由于 Diffie-Hellman 的代数未被建模，Tamarin+ Agent 才是能解决那一侧的工具。
- 文稿中已说明：是。文稿说明的位置：rfc9370:910、rfc9370:925、s0029、s0583
- 依据：Diffie-Hellman 是抽象的：经典攻破的攻击者被给予会话的 g^ir 而非指数。；KEM 是理想的，因此攻破 ML-KEM 的攻击者被建模为把 ss 交给它。；每个攻击者只保护一次运行：攻破在整个运行中一次性选定。

R05: 不会降级到不含ML-KEM的KE

攻击者不能使双方接受一个不含 ML-KEM 的 KE 提议，当双方策略要求 ML-KEM 时；接受的配置满足最低策略。

在此模型中双方接受的每个 IKE SA 都是 ML-KEM 混合的：被接受的公钥正是 IKE_INTERMEDIATE 中携带的那个，且方法被绑入 AUTH。草案描述的降级未被展现，因为模型按范围要求固定了算法套件，因此该性质是针对固定套件回答的，而非针对协商。

- Result: Holds；是否回答所问：部分；可用但有保留
- 价值 低：它确认了被接受的交换是混合的，这由固定范围推出；它没有回答降级问题，而文稿本身将该问题列为已知问题。
- 文稿中已说明：是。文稿说明的位置：main:369、s0030、s0031
- 依据：算法协商完全未被建模：不存在攻击者可将双方引向的替代提议。；要求 ML-KEM 的策略是固定范围，而非被建模的检查。
- 未决：当双方也支持仅经典序列时，主动攻击者能否强制一个不含 ML-KEM 的提议。
- 下一步：对带有两个提议的 SA 载荷协商建模，或复用草案引用的分析，以展现降级。

U01: 对IKE_INTERMEDIATE的篡改会被发现

攻击者删除、替换或篡改 IKE_INTERMEDIATE 附加 KE 时，双方不会在未察觉的情况下接受 IKE SA；接受的附加 KE 对应协商结果且被 AUTH 覆盖。

删除、替换或修改 IKE_INTERMEDIATE 密钥交换数据不会导致未被察觉的接受：被接受的 IKE SA 总是携带响应方发送并签名的密文。即使攻击者拥有经典 Diffie-Hellman 秘密、因而能读取并伪造这些消息，这也成立，因为替换会在 IKE_AUTH 中暴露。

- Result: Holds；是否回答所问：是；可用但有保留
- 价值 中：它将 RFC9242 的陈述——对 IKE_INTERMEDIATE 的伪造会在 IKE_AUTH 中显现——机械化，且针对的正是文稿所指名的攻击者。
- 文稿中已说明：是。文稿说明的位置：rfc9242:463、rfc9242:501、s0559、s0568
- 依据：拥有 g^ir 的攻击者被建模为把该秘密交给它；它得不到签名密钥，这是草案所指名的条件。；删除仅在会话丢失消息便永不完成的意义上被建模；模型中没有失败答案。；Diffie-Hellman 是抽象的。

X01: ML-KEM密钥对与密文的新鲜性

No two IKE SAs of one peer use the same ML-KEM encapsulation key or the same ML-KEM ciphertext: the initiator generates a fresh keypair and the responder a fresh ciphertext for each ML-KEM key exchange, and no randomness is reused.

Each IKE SA uses its own ML-KEM encapsulation key and its own ciphertext; no two sessions share either, as the draft requires, so neither peer reuses the randomness of a key exchange.

- 结果：Holds；是否回答了所问：是；可在有保留的情况下使用
- 价值低：它检查的是草稿用一句话陈述的规则；真正有趣的部分，即两个种子的独立性，不在模型中。
- 文稿中有无陈述：是。文稿中的位置：main:334，s0023
- 依据：新鲜性是每次运行中的一个新名称；ProVerif 覆盖任意数量的会话。；ML-KEM 种子与 Diffie-Hellman 种子的独立性（草稿第 3 节同样要求）未被建模：不存在共享种子。

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，以及各攻击和分析者对每个攻击的判定。

目标	级别	界	查询	对照	攻击	主张
A03	proved		a03_i			2 proved
A04	proved		a04_r			2 proved
A08	proved		a08			1 proved
K01	proved		k01_final			3 proved
C01	proved		c01	checked		1 proved
R05	proved		r05			2 proved
C08	proved		c08_dh	checked		2 proved
K01.8	proved		k01_final			2 proved
A03.9	proved		a03_i			2 proved
U01	proved		a08			2 proved
X01	proved		x01_pki			2 proved

逐条主张，按分析者对每条主张的措辞；每条的答案是证明器给出的：

目标	主张	攻击者	回答	查询	对照
A03	如果发起方接受该 IKE SA，则响应方确实完成了同一次运行：身份、Ni、Nr、IKE_INTERMEDIATE 的 ML-KEM 密文和公钥一致。	network	proved	a03_i	无
A03	如果响应方接受该 IKE SA，则发起方确实在其 AUTH 签名下发送了相同的身份、Ni、Nr、附加 KE 共享秘密和密文，以及 ML-KEM 公钥。	network	proved	a03_r	无
A04	每次响应方接受都对应一次不同的发起方运行：IKE_SA_INIT/IKE_INTERMEDIATE/IKE_AUTH 序列不能被重放成第二次接受。	network	proved	a04_r	无
A04	每次发起方接受都对应一次不同的响应方运行。	network	proved	a04_i	无
A08	发起方在 IKE_INTERMEDIATE 中接受的 ML-KEM 密文，就是响应方在 KEr(1) 中实际发送、并由 AUTH 覆盖的那个密文；附加 KE 方法是协商确定的常量，KE 数据绑定到 SPI 和 nonce。	network	proved	a08	无
K01	两代密钥的 SKEYSEED、SK_d、SK_ai/SK_ar、SK_ei/SK_er 和 SK_pi/SK_pr 对网络攻击者保持秘密。	network	proved	k01_final	无
K01	第一代 SKEYSEED 和 IKE_SA_INIT 密钥对网络攻击者保持秘密。	network	proved	k01_secret	无
K01	双方对端的长期认证私钥不能被攻击者推导出来。	network	proved	k01_ltk	无
C01	会话完成后，获得双方长期签名密钥的攻击者无法恢复该会话的 SKEYSEED 或 SK。	ltk_leak	proved	c01	checked
R05	被接受的 IKE SA 总是来自一次 ML-KEM 附加密钥交换：发起方接受的公钥是在 IKE_INTERMEDIATE 中收到的，ML-KEM 方法是以明文携带并绑定进 AUTH 的那个。	network	proved	r05	无
R05	即使经典 (EC)DH 被攻破，也不能让双方接受一个不是 ML-KEM 混合的 IKE SA。	dh_break	proved	r05	无
C08	获得经典 (EC)DH 共享秘密 g^ir 的攻击者无法推导出已建立 IKE SA 的最终 SKEYSEED 或 SK。	dh_break	proved	c08_dh	checked

目标	主张	攻击者	回答	查询	对照
C08	获得 ML-KEM 共享秘密 ss 的攻击者无法推导出已建立 IKE SA 的最终 SKEYSEED 或 SK。	`kem_break`	proved	c08_kem	checked
K01.8	两代密钥的 SKEYSEED 和所有 SK 对网络攻击者保持秘密。	`network`	proved	k01_final	无
K01.8	初始代密钥（SKEYSEED、SK_d 和各方向密钥）对网络攻击者保持秘密。	`network`	proved	k01_secret	无
A03.9	如果发起方接受，则响应方完成了相同的绑定：身份、Ni、Nr、ML-KEM 密文和公钥一致。	`network`	proved	a03_i	无
A03.9	如果响应方接受，则发起方在其 AUTH 签名下发送了相同的身份、Ni、Nr、共享秘密和密文。	`network`	proved	a03_r	无
U01	修改或替换 IKE_INTERMEDIATE 密文会被发现：被接受的 IKE SA 总是携带响应方发送并签名的那个密文。	`network`	proved	a08	无
U01	即使攻击者拥有经典 g^ir（因而能读取并伪造 IKE_INTERMEDIATE 消息），被接受的 IKE SA 仍然携带响应方发送的密文；替换会在 IKE_AUTH 中被发现。	`dh_break`	proved	u01_dh	无
X01	没有两个 IKE SA 使用相同的 ML-KEM 封装密钥（发起方的 KEi(1)）。	`network`	proved	x01_pki	无
X01	没有两个 IKE SA 使用相同的 ML-KEM 密文（响应方的 KEr(1)）；响应方不复用其随机性。	`network`	proved	x01_ct	无

附录 D：分析是怎么跑的

LLM 分析者从文稿构建协议模型，并把每条性质交给 ProVerif；第 3 节的每个结果都是证明器给出的答案。

ProVerif+ Agent 会话 session-20261114T184054，2026-11-14。状态：已完成。模型：deepseek-v4-1-flash-261017。步数：64，证明器 132 秒，实际耗时 20 分钟，成本 0.251 美元。

上下文：宿主从对话中移除了过时部分 2 次，共 557996 个字符（较早的推理，以及显示模型在其最近一次更改之前状态的内容）。轨迹文件保留了全部内容。

ProVerif：运行了 108 个证明，99 个已判定，9 个无答案，114 秒，记录了 32 个答案。

分析了什么

协议	IKEv2：ML-KEM 附加密钥交换与最终认证
版本	draft-ietf-ipsecme-ikev2-mlkem-09
分析范围	固定一种 ML-KEM 参数集、一次 IKE_INTERMEDIATE 附加 KE 与 IKE_AUTH；固定认证方法，暂不做 Child SA 重协商及通用多轮 KE。
不在范围内	多个 RFC 的组合流程，建模成本高于单服务；身份认证方法、密钥泄露场景与 PQ 抽象必须固定。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	658 个带编号的原文单元（222590 字节），来自下列各节。本报告中诸如 s0001 的引用就是这些原文单元之一

分析所依据的文稿各节：

文稿	章节	标题
main	2	ML-KEM in IKEv2
main	2.1	Key Exchange Payload
main	2.2	Recipient Tests
main	3	Security Considerations
rfc7296	1	Introduction
rfc7296	1.1	Usage Scenarios
rfc7296	1.1.1	Security Gateway to Security Gateway in Tunnel Mode
rfc7296	1.1.2	Endpoint-to-Endpoint Transport Mode
rfc7296	1.1.3	Endpoint to Security Gateway in Tunnel Mode
rfc7296	1.1.4	Other Scenarios
rfc7296	1.2	The Initial Exchanges
rfc7296	1.3	The CREATE_CHILD_SA Exchange
rfc7296	1.3.1	Creating New Child SAs with the CREATE_CHILD_SA Exchange
rfc7296	1.3.2	Rekeying IKE SAs with the CREATE_CHILD_SA Exchange
rfc7296	1.3.3	Rekeying Child SAs with the CREATE_CHILD_SA Exchange
rfc7296	1.4	The INFORMATIONAL Exchange
rfc7296	1.4.1	Deleting an SA with INFORMATIONAL Exchanges

文稿	章节	标题
rfc7296	1.5	Informational Messages outside of an IKE SA
rfc7296	1.6	Requirements Terminology
rfc7296	1.7	Significant Differences between RFC 4306 and RFC 5996
rfc7296	1.8	Differences between RFC 5996 and This Document
rfc7296	2	IKE Protocol Details and Variations
rfc7296	2.1	Use of Retransmission Timers
rfc7296	2.2	Use of Sequence Numbers for Message ID
rfc7296	2.3	Window Size for Overlapping Requests
rfc7296	2.4	State Synchronization and Connection Timeouts
rfc7296	2.5	Version Numbers and Forward Compatibility
rfc7296	2.6	IKE SA SPIs and Cookies
rfc7296	2.6.1	Interaction of COOKIE and INVALID_KE_PAYLOAD
rfc7296	2.7	Cryptographic Algorithm Negotiation
rfc7296	2.8	Rekeying
rfc7296	2.8.1	Simultaneous Child SA Rekeying
rfc7296	2.8.2	Simultaneous IKE SA Rekeying
rfc7296	2.8.3	Rekeying the IKE SA versus Reauthentication
rfc7296	2.9	Traffic Selector Negotiation
rfc7296	2.9.1	Traffic Selectors Violating Own Policy
rfc7296	2.9.2	Traffic Selectors in Rekeying
rfc7296	2.10	Nonces
rfc7296	2.11	Address and Port Agility
rfc7296	2.12	Reuse of Diffie-Hellman Exponentials
rfc7296	2.13	Generating Keying Material
rfc7296	2.14	Generating Keying Material for the IKE SA
rfc7296	2.15	Authentication of the IKE SA
rfc7296	2.16	Extensible Authentication Protocol Methods
rfc7296	2.17	Generating Keying Material for Child SAs
rfc7296	2.18	Rekeying IKE SAs Using a CREATE_CHILD_SA Exchange
rfc7296	2.19	Requesting an Internal Address on a Remote Network
rfc7296	2.20	Requesting the Peer's Version
rfc7296	2.21	Error Handling
rfc7296	2.21.1	Error Handling in IKE_SA_INIT
rfc7296	2.21.2	Error Handling in IKE_AUTH
rfc7296	2.21.3	Error Handling after IKE SA is Authenticated
rfc7296	2.21.4	Error Handling Outside IKE SA
rfc7296	2.22	IPComp
rfc7296	2.23	NAT Traversal

文稿	章节	标题
rfc7296	2.23.1	Transport Mode NAT Traversal
rfc7296	2.24	Explicit Congestion Notification (ECN)
rfc7296	2.25	Exchange Collisions
rfc7296	2.25.1	Collisions while Rekeying or Closing Child SAs
rfc7296	2.25.2	Collisions while Rekeying or Closing IKE SAs
rfc9242	3	Intermediate Exchange Details
rfc9242	3.1	Support for Intermediate Exchange Negotiation
rfc9242	3.2	Using Intermediate Exchange
rfc9242	3.3	The IKE_INTERMEDIATE Exchange Protection and Authentication
rfc9242	3.3.1	Protection of IKE_INTERMEDIATE Messages
rfc9242	3.3.2	Authentication of IKE_INTERMEDIATE Exchanges
rfc9242	3.4	Error Handling in the IKE_INTERMEDIATE Exchange
rfc9370	2	Multiple Key Exchanges
rfc9370	2.1	Design Overview
rfc9370	2.2	Protocol Details
rfc9370	2.2.1	IKE_SA_INIT Round: Negotiation
rfc9370	2.2.2	IKE_INTERMEDIATE Round: Additional Key Exchanges
rfc9370	2.2.3	IKE_AUTH Exchange
rfc9370	2.2.4	CREATE_CHILD_SA Exchange
rfc9370	2.2.5	Interaction with IKEv2 Extensions
rfc9370	2.2.5.1	Interaction with Childless IKE SA

协议的目的，按原文步骤在文稿中的定位：固定一种 ML-KEM 参数集、一次 IKE_INTERMEDIATE 附加 KE 与 IKE_AUTH；固定认证方法，暂不做 Child SA 重协商及通用多轮 KE。

对照文稿定性质

在写出任何查询之前，分析者先把草拟的性质清单与文稿本身对协议目的的陈述作了对照。名称、性质所涉及的内容以及文稿的陈述都是分析者的解读；所列位置在文稿中确实存在。

ID	简称	对象	文稿怎么说	出处
A03	对等方与附加KE的一致性	响应方与发起方各自确信对方的身份、Ni 与 Nr、SPI 以及附加 KE 方法和共享秘密 SK(1)，依据是 AUTH 载荷和 IntAuth 块。	RFC7296 2.15 定义了每个对等方签名的签名字节（自己的第一条消息、对等方的 nonce、对等方的 ID）；RFC9242 3.3.2 增加了对 IKE_INTERMEDIATE 消息的 IntAuth；RFC9370 2.2.2 把 SK(1) 放入 SKEYSEED(1)。	s0371, s037 s0559, s056 s0623, s062

ID	简称	对象	文稿怎么说	出处
A04	不会重放到第二次接受	每一次接受 IKE SA 都对应着对等方一次不同的真实运行；同一组 IKE_SA_INIT/IKE_INTERMEDIATE/IKE_AUTH 序列不能被重放以产生第二次接受。	RFC7296 2.2 和 RFC9242 3.2 要求 IKE_INTERMEDIATE 使用 Message ID 1,2,...，IKE_AUTH 使用下一个值，并要求验证这些值；该运行绑定到新鲜的 Ni/Nr 和 AUTH。	s0212, s054 s0567
A08	附加KE绑定到协商	在 IKE_INTERMEDIATE 中被接受的附加 KE 方法、其位置和共享秘密 SK(1)，与 IKE_SA_INIT 中协商的 ADDKE 转换相对应，并绑定到同一组 IKE SA SPI、nonce 和 AUTH。	RFC9370 2.2.2 要求 KE method 字段与第 n 个协商的附加交换相匹配，并把 SK(n)、Ni 和 Nr 放入 SKEYSEED(n)；RFC9242 3.3.2 把 IKE_INTERMEDIATE 的内容放入 AUTH。	s0602, s062 s0623, s055 s0568
K01	IKE SA密钥保密性	两代密钥的 SKEYSEED、SK_d、SK_ei/SK_er、SK_ai/SK_ar 和 SK_pi/SK_pr，以及长期认证密钥，都不被攻击者获知。	RFC7296 2.14 从 SKEYSEED 派生所有 IKE SA 密钥，RFC9370 2.2.2 在每次附加密钥交换之后从 SKEYSEED(n) 重新派生它们；这些密钥保护后续交换。	s0363, s036 s0623, s062 s0555
C01	IKE SA密钥的前向保密	已完成会话的 SKEYSEED 和 SK 对在会话之后获得双方长期认证密钥的攻击者保持秘密，临时秘密已被擦除。	RFC7296 2.12 指出，前向保密意味着连接关闭且其密钥被遗忘后，拥有全部长期密钥的攻击者无法重建会话密钥，并要求每个端点遗忘可重新计算它们的信息。	rfc7296:244 rfc7296:245 s0347, s041
R05	不会降级到不含ML-KEM的KE	本地策略要求 ML-KEM 时对等方所接受的 KE 方法；攻击者必须不能使对等方最终确定在包含 ML-KEM 的密钥交换序列上。	RFC9370 和草案指出，破坏传统 (EC)DH 的主动在途攻击者可强制使用最弱公共密钥交换，并建议拒绝不含 ML-KEM 的提案。	s0030, s003 s0032
C08	会话密钥在一次KE被攻破后仍安全	已建立 IKE SA 的 SKEYSEED 和 SK，面对获得两个密钥交换组件之一（经典 g^ir 或 ML-KEM 共享秘密 ss）的攻击者。	RFC9370 4 指出，量子攻击者可能获知经典密钥交换得到的值，而来自后量子算法的其他 SK(x) 值可确保最终 SKEYSEED 不被攻破；草案称该混合派生为 IND-CPA，但未证明 IND-CCA2。	rfc9370:910 rfc9370:925 s0029, s056 s0583
K01.8	IKE SA密钥保密性，用户问题	两代密钥的 SKEYSEED 和每个 SK 都不被网络攻击者获知。	与 K01 相同的条款：RFC7296 2.14 和 RFC9370 2.2.2。	s0363, s036 s0623, s062
A03.9	IKE SA接受时的一致绑定	每次接受时双方在身份、Ni、Nr、SPI、附加 KE 结果和 AUTH 值上一致。	与 A03 相同的条款：RFC7296 2.15 的签名字节与 RFC9242 3.3.2 的 IntAuth 块。	s0371, s037 s0559, s056

ID	简称	对象	文稿怎么说	出处
U01	对IKE_INTERMEDIATE的篡改会被发现	删除、替换或修改 IKE_INTERMEDIATE 的 KE 数据不得导致未被发现的接受；被接受的附加 KE 是协商的那个，并被 AUTH/IntAuth 覆盖。	RFC9242 5 指出 IKE_INTERMEDIATE 数据在 IKE_AUTH 完成前未被认证，伪造会在 IKE_AUTH 中变得明显；RFC9242 3.3.2 把内容绑定到 AUTH。	rfc9242:463 rfc9242:501 s0559, s056 s0602, s062
X01	ML-KEM密钥对与密文的新鲜性	发起方在 KEi(1) 中发送的 ML-KEM 公钥和响应方在 KEr(1) 中发送的密文，跨越所有会话。	草案要求为每次 ML-KEM 密钥交换生成临时密钥对和密文，并禁止响应方在生成 KEM 密文时重用随机性。	main:334, s0023

分析者依据文稿补充的性质：X01.

文稿里的安全表述，逐段去向

宿主把文稿里说明协议保护什么、防什么的章节逐段列出，共 54 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 16 段，没选 38 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:320-321	没有陈述目标	它只说明 RFC9242 和 RFC9370 的安全考虑适用；这些段落在此单独解读。
P02	main:323-338	X01, K01	
P03 至 P06	main:340-358	X01	
P07	main:360-361	没有陈述目标	它指向 KEM 的实现指南，没有陈述本协议的任何性质。
P08	main:363-367	C08	
P09	main:369-383	R05, `dh_break`	
P10 至 P11	main:385-400	R05	
P12 至 P13	main:404-408	没有陈述目标	Internet-Draft 的页面附属内容，没有正文。
P14	main:411-429	不在范围内	它讨论无子 SA 的 IKE SA、CREATE_CHILD_SA 重密钥和 IKE_FOLLOWUP_KE；任务只固定一次 IKE_INTERMEDIATE 附加交换，不涉及 Child SA 重密钥。
P15	rfc7296:6478-6488	不在范围内	它陈述基础 IKEv2 中身份保护的限制（发起方先表明身份，冒充的响应方可以探测它）。任务固定了被建模参与方的公开身份，不涉及身份机密性。
P16	rfc7296:6490-6494	不在范围内	EAP 认证；任务固定了认证方法，而该方法不是 EAP。
P17	rfc7296:6496-6500	不在范围内	不产生新指数运算的重复 CREATE_CHILD_SA 重密钥；Child SA 重密钥不在任务范围内。
P18	rfc7296:6502-6514	证明器问不了	Diffie-Hellman 群的强度，这是原语和指数长度的性质，不是消息流的性质。
P19	rfc7296:6516-6519	证明器问不了	同一主题：群本身的强度。
P20	rfc7296:6525-6527	没有陈述目标	一段说明 IKE 鼓励定义更多群的备注；没有必须成立或可以被攻击的内容。

段落	出处	定为	不选的原因
P21	rfc7296:6529-6530	C01	
P22	rfc7296:6532-6538	证明器问不了	实现抵抗未认证对端 DoS 的稳健性，这是可用性，不能作为迹性质来问。
P23	rfc7296:6540-6542	证明器问不了	协商出的 PRF 的最小输出长度，这是原语的强度。
P24	rfc7296:6544-6549	证明器问不了	随机数发生器的质量，这是符号模型不表示的原语假设。
P25	rfc7296:6551-6556	不在范围内	它禁止协商 ENCR_NULL 和 NONE 完整性；任务固定了算法套件，不建模加密或完整性变换的协商。
P26	rfc7296:6558-6563	不在范围内	由口令导出的预共享密钥；任务固定了数字签名认证，不建模基于口令的认证。
P27 至 P28	rfc7296:6565-6580	不在范围内	NAT_DETECTION 通知泄露的信息；NAT 穿越未建模。
P29	rfc7296:6582-6606	不在范围内	不生成密钥的 EAP 方法；EAP 不是被建模的认证方法。
P30	rfc7296:6608-6612	不在范围内	对 EAP 部署的要求；EAP 未建模。
P31	rfc7296:6614-6619	证明器问不了	长消息导致重组缓冲区耗尽，这是可用性性质。
P32 至 P33	rfc7296:6621-6633	不在范围内	准入控制、信任锚和对端授权数据库：本地策略配置，在被建模的交换之外。
P34 至 P41	rfc7296:6637-6696	不在范围内	Child SA 的流量选择器授权；流量选择器和 Child SA 创建都不在建模范围内。
P42	rfc9242:463-470	U01, A03	
P43	rfc9242:472-477	证明器问不了	大量大型 IKE_INTERMEDIATE 交换造成的 DoS，这是可用性性质。
P44	rfc9242:479-499	证明器问不了	同一 DoS 主题：在 IKE_AUTH 之前中止的恶意发起方以及交换数量的上限。
P45	rfc9242:501-514	U01, C08, `dh_break`	
P46	rfc9370:883-891	C08, K01, `dh_break`	
P47	rfc9370:893-908	证明器问不了	Grover 算法与对称密钥长度，这是原语的强度。
P48	rfc9370:910-916	C08, `dh_break`	
P49	rfc9370:918-923	C08	
P50	rfc9370:925-932	C08, C01, `dh_break`	
P51	rfc9370:934-942	证明器问不了	它说明认证步骤仍是经典的，这是签名原语抵抗量子计算机的强度；符号模型假设签名不可伪造，只能通过交出密钥来回答，而那样会使其他所有答案失效。
P52	rfc9370:944-954	没有陈述目标	关于后量子真实性紧迫性的理由说明；没有陈述本协议的任何性质。
P53	rfc9370:956-961	证明器问不了	发起方被认证之前 DoS 敏感性增加，这是可用性性质。
P54	rfc9370:963-980	不在范围内	无子 SA 的 IKE SA 和 IKE_FOLLOWUP_KE 备选方案；重密钥和后续交换不在任务范围内。

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 31 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 5 项，没设的 26 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	参与方	按定义全部失守	受控的发起方知道自己的长期密钥和自己的会话密钥，因此其会话的每条机密性性质按构造即失效；文稿在此不要求在失陷参与方下成立任何机密性性质。
S02	响应方	参与方	按定义全部失守	响应方同理：控制它的人知道它自己的密钥和会话秘密。
S03	主动中间人	参与方	攻击者得不到更多	主动在路径上的攻击者就是网络攻击者本身；除网络之外它不持有任何东西。
S04	IKE SA 身份绑定	值	攻击者得不到更多	身份绑定是握手中携带的公开协议状态；持有它并不能给网络攻击者带来它没有的东西。
S05	Ni、Nr、SPIi、SPIr	值	攻击者得不到更多	Ni、Nr 和 SPI 以明文发送。
S06	附加 KE 方法与共享秘密 SK	值	`kem_break`	
S07	AUTH 载荷	值	攻击者得不到更多	AUTH 载荷在线上传输；在理想签名下它不泄露任何信息。
S08	Message ID	值	攻击者得不到更多	Message ID 在每个报头中都是明文。
S09	Ni、Nr	值	攻击者得不到更多	Ni 和 Nr 以明文发送。
S10	AUTH	值	攻击者得不到更多	同 S07：AUTH 载荷是传输的。
S11	ADDKE 变换类型与 ID	值	攻击者得不到更多	ADDKE 变换类型与 ID 在 SA 载荷中以明文协商。
S12	KE 方法字段	值	攻击者得不到更多	KE 方法字段在 KE 载荷中以明文传输。
S13	SPIi、SPIr	值	攻击者得不到更多	SPI 是每个 IKE 报头的首字段。
S14	SKEYSEED	值	按定义全部失守	持有 SKEYSEED 就是持有会话密钥；关于它的每条机密性性质按定义即失效，文稿也不要求在它之下成立任何性质。
S15	SK_d	值	按定义全部失守	SK_d 同理，所有后续密钥都由它导出。
S16	SK_ei/SK_er	值	按定义全部失守	SK_ei 和 SK_er 同理。
S17	SK_ai/SK_ar	值	按定义全部失守	SK_ai 和 SK_ar 同理。
S18	SK_pi/SK_pr	值	按定义全部失守	SK_pi 和 SK_pr 同理。
S19	长期认证密钥	值	`ltk_leak`	
S20	历史 SKEYSEED 与 SK	值	按定义全部失守	在攻击者已持有历史会话密钥的情况下追问前向保密，按定义即失效。
S21	SA 提议与选择的 KE 方法	值	攻击者得不到更多	SA 提议与选择以明文携带；网络攻击者可以修改它们，但 RFC7296 和 RFC9370 将它们绑定进 AUTH，这正是 R05 所要求的。
S22	策略配置	值	攻击者得不到更多	本地策略选择不是秘密，给不了攻击者任何它尚未在网络尝试的东西。
S23	SKEYSEED 与 SK	值	按定义全部失守	同 S14 至 S18。
S24	g^ir	值	`dh_break`	
S25	ML-KEM ss	值	`kem_break`	
S26	身份	值	攻击者得不到更多	对端身份是公开名称。
S27	Ni、Nr、SPI	值	攻击者得不到更多	Nonce 和 SPI 是公开的。
S28	附加 KE 结果	值	`kem_break`	

ID	参与方或值	类别	攻击者条件	不设的原因
S29	ADDKE 协商结果	值	攻击者得不到更多	协商出的变换列表以明文携带。
S30	IKE_INTERMEDIATE KE 数据	值	攻击者得不到更多	ML-KEM 公钥和密文按设计就是公开的；它们导出的共享秘密由 S25 覆盖。
S31	AUTH/IntAuth	值	攻击者得不到更多	AUTH 和 IntAuth 值在线上传输。

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”是为该性质设定的攻击者，在其下证明器让某个主张悬而未决，或没有记录任何内容；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：可读取、丢弃、修改和发送消息，不持有任何一方的秘密		
`dh_break`	某会话的经典 (EC)DH 临时共享秘密 g^ir，如同拥有密码学相关量子计算机的攻击者在 IKE_SA_INIT 交换进行期间破坏该交换时所获得的那样	草案指出，拥有 CRQC 的主动在途攻击者可在协商进行期间破解传统 (EC)DH 临时交换；RFC9370 指出，量子攻击者可能获知经典密钥交换所得到的值。	main:369, rfc9370:910, s0030, s0583
`kem_break`	某会话的 ML-KEM 共享秘密 ss，如同破坏后量子密钥交换的攻击者所获得的那样	RFC9370 以现有或未来后量子算法可能被攻破为由，论证了多次密钥交换的必要性；草案仅将混合派生称为 IND-CPA。	rfc9370:883, main:363, s0029, s0583
`ltk_leak`	双方长期认证（签名）私钥，在会话完成且其临时秘密已被擦除之后获得	RFC7296 2.12 陈述了前向保密目标：针对在连接关闭后获取两端点全部长期密钥的攻击者；RFC9370 4 指出认证步骤仍为经典。	rfc7296:2446, rfc9370:934

ID	`network`	`dh_break`	`kem_break`	`ltk_leak`
A03	成立			
A04	成立			
A08	成立			
K01	成立			
C01				成立
R05	成立	成立		
C08		成立	成立	
K01.8	成立			
A03.9	成立			
U01	成立	成立		
X01	成立			

原文和目标

Source: 658 units, 222590 bytes, frozen in source-delivery-01.json. Targets: 8 approved (A03, A04, A08, K01, C01, R05, C08, U01); the questions asked: 3. The list of targets was approved as drafted, beforehand, with --approve-targets.

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

- approve_package: 批准源文包 protocol-8fc5b1f5e64e7786ee00259b5460

本步骤自报：1 次请求（1 次失败），0.000 USD，输入 94170 token，输出 4420 token，耗时 29 秒。

关于证明器和模型的说明

- C01：在 ProVerif 中作答，分析者为该目标命名 dh_algebra
- R05：在 ProVerif 中作答，分析者为该目标命名 dh_algebra
- C08：在 ProVerif 中作答，分析者为该目标命名 dh_algebra
- U01：在 ProVerif 中作答，分析者为该目标命名 dh_algebra

简化代数（xor、dh_algebra、other_algebra）的 ProVerif 模型给予攻击者的能力少于真实运算：其中的证明是针对更弱攻击者的证明，其中的攻击仍是攻击。省略对会变化的值（changing_state）的检查的 ProVerif 模型让各方接受更多：其中的证明成立，其中的攻击可能不过是缺失的检查。Tamarin+ Agent 按原样对这些建模。

分析者为各目标命名的内容：

步骤	目标	特征	理由
59	C08, C01, U01, R05	dh_algebra, many_sessions	经典密钥交换未用 Diffie-Hellman 代数建模：IKE_SA_INIT 交换的共享秘密是两个指数的抽象可交换函数，因此攻击者获得的能力少于真实协议；dh_break 攻击者的建模方式是在运行结束后把该会话的 g^ir 交给攻击者，而非让它计算指数。因此，混合性质和降级性质的答案建立在这一简化之上，按原样建模 DH 代数的 Tamarin+ Agent 可以裁定它们。
59	A03, A03.9, A04, A08, K01, K01.8, X01	plain_primitives, many_sessions	这些目标仅使用哈希、PRF/KDF、签名、对称加密以及作为理想原语的 ML-KEM 抽象，且 ProVerif 在一次运行中覆盖任意数量的会话，因此不涉及界。算法套件的协商由任务范围固定，未建模。

分析者的结束说明

十一个目标，全部由 ProVerif 在单一流程模型（IKE_SA_INIT、一次 IKE_INTERMEDIATE ML-KEM 交换、IKE_AUTH）上作答，另加一个来自安全考虑的补充目标。

已确立（对任意数量的会话、针对网络攻击者）：双方就身份、Ni、Nr、ML-KEM 公钥和密文达成一致，且附加密钥交换通过 IntAuth 绑定进 AUTH；每次接受都对应其对端的一次不同运行（单射，双向）；两代 IKE SA 密钥和长期签名密钥保持秘密；被接受的密文始终是响应方自己的，因此对 IKE_INTERMEDIATE 的替换或修改会被发现；每个 ML-KEM 密钥和密文仅使用一次；被接受的 IKE SA 始终是 ML-KEM 混合的那一个。分别针对被破坏的经典交换（dh_break）和被破坏的 ML-KEM（kem_break），最终会话密钥和 SKEYSEED 均无法获得，并有对照查询：同时交出两个分量时密钥即失守。针对稍后双方长期签名密钥泄露（ltk_leak），已完成的会话保持其密钥，并有对照查询：交出会话密钥时即失败。

无发现：每个结果都是文稿所要求或陈述的内容，因此未报告任何新内容。文稿所指出的两个弱点被重现为限制而非发现：降级到非 ML-KEM 序列需要算法协商，而范围已将其固定排除（因此 R05 仅对固定套件作答），而 IKE_INTERMEDIATE 暴露给持有 g^ir 的攻击者，正是 u01_dh 所表明的在 IKE_AUTH 中被发现的情形。

阻碍更多的因素：模型用抽象可交换共享秘密替代 Diffie-Hellman，用理想 KEM 替代 ML-KEM，因此混合性质和降级性质建立在简化之上；按原样建模 DH 代数的 Tamarin+ Agent 可以裁定 Diffie-Hellman 一侧。十七个证明在无对照变体的情况下被记录；报告的对照结构显示了哪些。说明见 notes.md。