IKEv2 ML-DSA 认证的安全性分析

本报告的其他语言版本：English。

draft-ietf-ipsecme-ikev2-pqc-auth-12 · ProVerif+ Agent 报告

文稿	Signature Authentication in the Internet Key Exchange Version 2 (IKEv2) using PQC （协议定义）; Internet Key Exchange Protocol Version 2 (IKEv2) （辅助）; Signature Authentication in the Internet Key Exchange Version 2 (IKEv2) （辅助）
检查的性质	13 条：12 条成立，1 条不成立（1 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

该草案为 IKEv2 初始交换增加了后量子认证。发起方和响应方执行 IKE_SA_INIT，在其中协商 SA、交换 Diffie-Hellman 共享值和 nonce，并通告各自支持的签名哈希算法。每一方持有一个 ML-DSA-65 签名密钥，以及对方证书的信任锚。在 IKE_AUTH 中，每一方对一段数据进行签名，该数据由它收到的首轮报文、对方的 nonce 以及自身身份的 PRF 构成，并把签名连同自身身份放入经过加密和完整性保护的载荷中发送。

交换结束时，每一方都确信：对端持有其已接受证书中所指明的密钥；对端的签名覆盖了两个 nonce 和两条 IKE_SA_INIT 报文；双方共享相同的 IKE SA 密钥。会话密钥对网络上的任何人都保密，即使攻击者事后同时获得两个签名密钥，该密钥仍然保密。

参与方：

- **发起方**：提议 SA，先签名。持有：ML-DSA-65 签名密钥；响应方的信任锚；自身身份 IDi。
- **响应方**：选择 SA，应答。持有：ML-DSA-65 签名密钥；发起方的信任锚；自身身份 IDr。

图 1 展示了文稿所规定的交换流程。

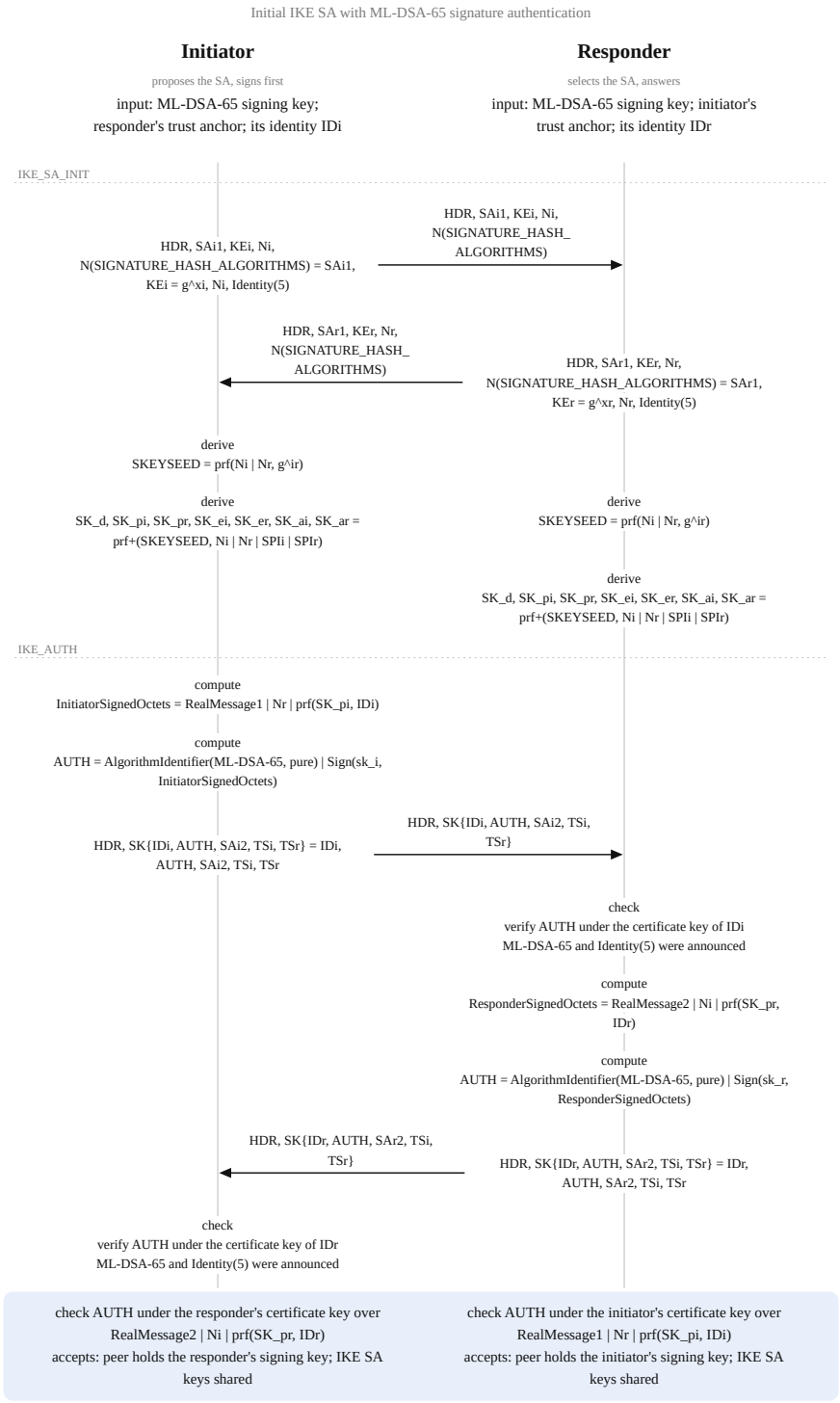


图 1. 所规定的协议。

分析范围见附录 D：分析了什么、省略了什么，以及依据的是文稿的哪些章节。

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问题。第 3 节的表格给出了每条性质的结果。

无发现：所考察的每项保证在模型中均成立，两处不成立都是文稿自身已写明的情形。相互 ML-DSA-65 认证、身份与两个 nonce 及两条 IKE_SA_INIT 报文的绑定、单次使用一致性，以及在要求 PQC 的部署中拒绝传统签名，这些在任意数量的会话中都成立，面对能够伪造所有传统签名的攻击者时也成立。两处已知弱

点被复现：当发起方被接受为 Diffie-Hellman 对端时，在路径上的攻击者可以从 IKE_AUTH 中读到发起方的身份；而允许回退的部署会被传统签名伪造者直接冒充。大多数答案依赖于一个将 Diffie-Hellman 理想化为其单一法则的模型，因此前向保密和会话密钥的结果是在该理想化下成立的，若要按原样定论，需要具备 DH 代数的证明器。全部十三个目标都有答案，每个证明都带有会失败的对照查询。

3 检查过的性质

每一行是一条提交给 ProVerif 的性质。结果是 ProVerif 对分析者所建协议模型的回答；价值以及文稿是否已写明该结果，是分析者的判断，理由见附录 A。

ID	性质	假定的泄露	结果	价值	文稿是否已写
A02	**对端身份认证。** 每当发起方（或响应方）在 IKE_AUTH 中接受对端身份时，对端必须存在一次以本方身份为通信对象的真实运行。	无	成立	中	是
A03	**AUTH 载荷的会话绑定。** 每当一方接受时，存在匹配的对端运行，且双方对相互身份、Ni、Nr 以及首轮 IKE_SA_INIT 报文内容一致。	无	成立	中	是
A04	**AUTH 不可跨会话重放。** 每次本方接受都对应一次不同的对端真实运行（单射匹配），同一对端运行不能被多次接受。	无	成立	中	是
A08	**签名算法绑定。** 接受方所接受的签名算法与哈希算法，必须来自对端真实提议且被 AUTH 覆盖的能力信号，并与实际验证签名所用算法一致。	无	成立	中	是
R05	**不可降级至传统 AUTH。** 在要求 PQC 签名认证的部署中，接受方不会接受回退到传统签名认证的会话。	无	成立	中	是
K01	**IKE SA 与签名密钥保密性。** 攻击者不能推导出 IKE SA 的会话密钥（SKEYSEED 及其派生密钥）或任一方的 ML-DSA 长期签名私钥。	无	成立	低	是
C01	**IKE SA 密钥前向保密。** 会话完成并擦除后，泄露双方长期签名私钥不能使攻击者得到该会话的 IKE SA 密钥。	双方长期 ML-DSA 签名私钥 (会话完成后)	成立	中	是
C02	**自身密钥泄露不导致冒充。** 接受方自己的 ML-DSA 签名私钥泄露后，在本方仍诚实执行的前提下，攻击者不能冒充未泄露的对端使本方接受。	接受方的 ML-DSA 签名私钥 (会话建立前泄露)	成立	低	否
C08	**传统签名被攻破时 PQC 认证仍有效。** 在传统签名原语被攻破（攻击者可伪造传统签名）而 ML-DSA 签名仍安全时，强制 PQC 认证的会话中身份认证与算法绑定仍成立。	传统签名算法的签名私钥 (会话建立前)	成立	中	是
A03.10	**AUTH 绑定身份与 nonce。** 每当一方接受时，存在匹配的对端运行，且双方对相互身份、Ni、Nr 与首轮报文内容一致。	无	成立	中	是
A08.11	**能力信号篡改可被检测。** 接受方所接受的签名算法与哈希算法，必须来自对端真实提议且被 AUTH 覆盖的能力信号，并与实际验证签名所用算法一致。	无	成立	中	不确定

ID	性质	假定的泄露	结果	价值	文稿是否已写
C02.12	**自身密钥泄露不破坏对端身份。** 接受方自己的 ML-DSA 签名私钥泄露后，在本方仍诚实执行的前提下，攻击者不能冒充未泄露的对端使本方接受；同时存在正常会话作为正例。	接受方的 ML-DSA 签名私钥 (会话建立前泄露)	成立	低	否
X01	**IDi 与 IDr 的身份保护。** 仅观察并修改网络的攻击者始终无法获知 IKE_AUTH 交换中 ID 载荷的内容，因此无法判断发起方声称的是哪个身份，也无法判断响应方使用的是哪个身份。	无	攻击成立（文稿已写明）	中	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.

所提出的问题及分析者的回答：

问题	回答	依据
Q1: AUTH 对身份、nonce、首轮报文的绑定	是：AUTH 载荷在发起方到响应方和响应方到发起方两个方向上，都绑定了两个身份、两个 nonce 和两条 IKE_SA_INIT 报文，适用于任意数量的会话，在传统签名可被伪造时也成立。	A03, A03.10, A02, A04
Q2: 算法能力信号被修改时成功会话是否仍按实际签名验证	是，但有一点需要注意：SIGNATURE_HASH_ALGORITHMS 和 SUPPORTED_AUTH_METHODS 通知位于被签名的数据之内，因此修改它们会破坏认证，要求 PQC 的部署也绝不会接受传统 AUTH；但 Authentication Data 内部的 AlgorithmIdentifier 本身不在签名覆盖之下，所以接收方对验证算法的选择依赖于一个攻击者可修改的字段，其唯一保护是：在错误算法下验证会失败。	A08, A08.11, R05, C08
Q3: PQ 签名密钥泄露对身份认证的影响及正例控制	本方签名密钥泄露不会让攻击者冒充未被攻破的另一个对端来使接受方接受，且正例控制表明同一配置能完成正常会话；另外，在会话之后获得两个签名密钥的攻击者不会学到该会话的任何密钥材料。	C02, C02.12, C01

4 本次分析的局限

这里的结果是协议模型上的结果：它说明所规定的报文和检查提供了或未能提供什么，其中密码学被视为理想原语，不涉及任何实现。

正如分析者所述，本次分析不覆盖以下内容：

- Diffie-Hellman 被理想化为其单一法则 g^xy = g^yx；模型中没有表示针对该交换的代数攻击，也没有关于 DH 秘密的量子假设。Tamarin+ Agent 对 DH 按其原样建模，可以定论前向保密相关问题。
- 证书和信任锚被视为给定：每个角色都收到对端的公钥以及该公钥所属的身份，因此不分析证书链验证。
- IKE_AUTH 内部的 Child SA 协商（SAi2、TSi、TSr）及其之后的一切，包括 CREATE_CHILD_SA 和 INFORMATIONAL 交换，都在模型之外，EAP 和密钥更新同样如此。
- 不建模消息 ID、重叠请求窗口、重传和分片；新鲜性论证由 nonce 承担。
- IKE_AUTH 载荷使用理想化的加密和 MAC 保护，因此不分析 AEAD nonce 重用以及 SK_e 和 SK_a 密钥调度的细节。
- 传统签名被建模为一种不会被攻破的策略选择，其密钥由攻击者持有；不分析针对特定遗留算法的攻击。
- 模型中不验证首轮 Diffie-Hellman 共享值，因为文稿没有要求；身份保护攻击依赖这一点，而验证对端共享值的一方可以阻止该攻击。

- 只建模两个对端之间的初始交换。涉及安全网关、端点、NAT 穿越以及 RFC 7296 第 5.1 节中 PAD/流量选择器授权的场景不在覆盖范围内。

每条性质还有哪些未决之处，以及什么能定论它，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、解读依据是什么、能否按原样使用，以及它的价值如何。

A02: 对端身份认证

每当发起方（或响应方）在 IKE_AUTH 中接受对端身份时，对端必须存在一次以本方身份为通信对象的真实运行。

双方通过 ML-DSA-65 签名相互认证，任何一方都不会在没有对端匹配运行的情况下接受对端身份。该结果对于能够伪造所有传统签名的攻击者也成立。

- 结果：成立；是否回答了所问：是；可用但有注意事项
- 价值 中：这是草案的一项核心保证，但无人质疑过它；其价值在于它现在是机械化的，并且对于传统签名能抵御 CRQC 攻击者。
- 文稿中是否陈述：是。文稿中的位置：s0103、s0387
- 依据：假设证书和信任锚存在：每个角色都获得对端的公钥以及该公钥所属的身份，并且不检查证书链。；模型包含一对诚实对端；查询按名称提及该对端。；该模型中的攻击者知道所有传统签名密钥，因此该证明针对的是比仅网络攻击更强的攻击者。

A03: AUTH 载荷的会话绑定

每当一方接受时，存在匹配的对端运行，且双方对相互身份、Ni、Nr 以及首轮 IKE_SA_INIT 报文内容一致。

签名确实绑定了草案所称绑定的内容：双方身份、双方 nonce 以及两条 IKE_SA_INIT 报文。在任一方向上被修改的报文都会破坏 AUTH，会话在该检查处停止。

- 结果：成立；是否回答了所问：是；可用但有注意事项
- 价值 中：在证明器中确认了草案以散文论述的性质。
- 文稿中是否陈述：是。文稿中的位置：s0387、s0389、s0391
- 依据：被签名的块按草案描述建模；长度、SPI 和分片细节被省略。；响应方一侧以发起方的运行事件来陈述，因为响应方在发起方之前接受。；攻击者被赋予所有传统签名密钥。

A04: AUTH 不可跨会话重放

每次本方接受都对应一次不同的对端真实运行（单射匹配），同一对端运行不能被多次接受。

接受一个会话不能被计为两次：每次接受都映射到一次不同的对端运行，因此录制的 AUTH 不能被重放到第二个会话中。这就是草案的 nonce 论证，以机械化方式展示。

- 结果：成立；是否回答了所问：是；可用但有注意事项
- 价值 中：草案以散文陈述了它；模型对任意数量的会话展示了它。
- 文稿中是否陈述：是。文稿中的位置：s0012、s0045、s0387
- 依据：未对消息标识符和消息 ID 窗口建模；此处只有 nonce 使每个会话唯一。；消息 3 和 4 中的子 SA 创建是不透明常量。

A08: 签名算法绑定

接受方所接受的签名算法与哈希算法，必须来自对端真实提议且被 AUTH 覆盖的能力信号，并与实际验证签名所用算法一致。

在要求 ML-DSA-65 的部署中，任何会话都不会以传统签名被接受，并且接收方使用的算法和哈希来自对端自己的消息，而 AUTH 覆盖了这些消息。因此修改 SIGNATURE_HASH_ALGORITHMS 通知只会破坏交换。

- 结果：成立；是否回答了所问：是；可用但有注意事项
- 价值 中：回答了草案的意图，但有一个注意事项：载荷中的算法标识符不被任何签名覆盖。
- 文稿中是否陈述：是。文稿中的位置：s0019、s0020、s0044、s0557
- 依据：算法是不同的符号构造器；真实签名方案上的算法混淆不在模型范围内。；严格配置是对响应方策略的一项检查；宽松配置是同一参与方的第二个实例。；对于 ML-DSA，只对 Identity 哈希建模；传统算法只是另一个单一选择。
- 未决：Authentication Data 内的 AlgorithmIdentifier 本身不在签名之下，因此从载荷中选择验证算法的接收方信任了一个攻击者可修改的字段；符号模型只能表明在重新标记的算法下验证会失败。

R05: 不可降级至传统 AUTH

在要求 PQC 签名认证的部署中，接受方不会接受回退到传统签名认证的会话。

在要求 PQC 认证且无回退的情况下，能够伪造传统签名的攻击者一无所获：不会以传统 AUTH 建立任何会话。当允许回退时，同一攻击者立即成功，这就是草案描述的攻击。

- 结果：成立；是否回答了所问：是；可用但有注意事项
- 价值 中：草案的建议作为一项检查得到确认，其警告在对照查询中被复现。
- 文稿中是否陈述：是。文稿中的位置：s0044
- 依据：策略是接受方中的一项检查，正如草案对部署的要求；操作员如何配置它未被分析。；只对两种配置建模：要求 PQC，以及允许回退。

K01: IKE SA 与签名密钥保密性

攻击者不能推导出 IKE SA 的会话密钥（SKEYSEED 及其派生密钥）或任一方的 ML-DSA 长期签名私钥。

在运行期间，已认证会话的 IKE SA 密钥材料以及任一 ML-DSA 签名密钥都不会到达攻击者。会话密钥保密性仅对完成认证的会话声称，对照查询表明，对于 AUTH 尚未检查的会话，如果攻击者自己应答了 IKE_SA_INIT，则该会话的种子为攻击者所知。

- 结果：成立；是否回答了所问：是；可用但有注意事项
- 价值 低：由理想化的 DH 和从未发送的密钥推出；真正的问题需要 DH 代数和一个量子假设。
- 文稿中是否陈述：是。文稿中的位置：s0379、s0382
- 依据：Diffie-Hellman 被理想化为其单一法则，因此不表示交换上的任何代数攻击。；会话密钥事件仅在 AUTH 检查之后发出，因此半开交换不计为会话。
- 未决：会话密钥的保密性依赖于对端的 Diffie-Hellman 共享值；模型将 DH 理想化为 g^xy = g^yx，对交换的量子安全性未作说明。

C01: IKE SA 密钥前向保密

会话完成并擦除后，泄露双方长期签名私钥不能使攻击者得到该会话的 IKE SA 密钥。

在会话之后获得双方 ML-DSA 签名密钥的攻击者得不到该会话的任何密钥材料：会话密钥来自临时交换和 nonce，而非签名密钥。对照查询表明泄露本身是有效的。

- 结果：成立；是否回答了所问：是；可用但有注意事项
- 价值 中：这是模型中的一项核心保证；其分量取决于 DH 理想化，而范围确定了这一点。
- 文稿中是否陈述：是。文稿中的位置：s0379、s0381、s0363
- 依据：Diffie-Hellman 被理想化，且临时指数从未输出，这正是原文所假设的。；泄露发生在后续阶段，在建模运行的所有交换结束之后。；DH 交换的抗量子性既未被声称也未被分析。
- 未决：如果 DH 代数允许比交换律更多的东西，答案是否仍然成立，而这正是真正的前向保密论证必须所在之处。

C02: 自身密钥泄露不导致冒充

接受方自己的 ML-DSA 签名私钥泄露后，在本方仍诚实执行的前提下，攻击者不能冒充未泄露的对端使本方接受。

泄露的自身签名密钥不会让攻击者冒充另一个诚实对端：在被攻破方的接受仍然意味着另一对端运行了匹配的会话。因此密钥泄露冒充是不可能的，这正是用自己的密钥签署对端 nonce 所承诺的。

- 结果：成立；是否回答了所问：是；可用
- 价值 低：草案没有对密钥泄露冒充提出任何要求；该结果直接来自签名构造，因此陈述起来代价低，但不会让任何人惊讶。
- 文稿中是否陈述：否。所依据的原文：s0387、s0103
- 依据：被攻破方是与 A02/A03 所用对端不同的一对诚实对端，因此泄露不会与普通认证的答案混淆。；对端身份和密钥由配置提供给本方，因此证书有效性被假设。；只把接受方的签名密钥交给攻击者；其 Diffie-Hellman 指数保持秘密。

C02.12: 自身密钥泄露不破坏对端身份

接受方自己的 ML-DSA 签名私钥泄露后，在本方仍诚实执行的前提下，攻击者不能冒充未泄露的对端使本方接受；同时存在正常会话作为正例。

与密钥泄露主张相同的结论，同时表明正常会话在同一配置中可达，因此该证明不是关于一个不可能出现的情形。

- 结果：成立；是否回答了所问：是；可用
- 价值 低：这是对前一个主张的对照查询，而非其自身的结果。
- 文稿中是否陈述：否。所依据的原文：s0387、s0103
- 依据：正例对照是一个可达会话，而非关于任意会话的证明。

C08: 传统签名被攻破时 PQC 认证仍有效

在传统签名原语被攻破（攻击者可伪造传统签名）而 ML-DSA 签名仍安全时，强制 PQC 认证的会话中身份认证与算法绑定仍成立。

在攻击者掌握所有传统签名密钥的情况下，要求 ML-DSA-65 的部署中的会话仍然仅由 ML-DSA-65 进行认证，且对端身份仍然被绑定。被攻破的旧算法只影响允许回退的部署，而草案说攻击正是在那里奏效。

- 结果：成立；是否回答了所问：是；可用但有保留
- 价值中：在草案自身的攻击模型下确认了草案自身给出的补救措施：将第 9 节的论证机械化。

- 文稿中有明确表述：是。出处：s0044、s0038
- 依据：通过直接向攻击者提供传统签名密钥来建模伪造传统签名的能力，这正是草案的假设。；ML-DSA-65 是不可攻破的符号签名；未分析其计算安全性。

A03.10：AUTH 绑定身份与 nonce

每当一方接受时，存在匹配的对端运行，且双方对相互身份、Ni、Nr 与首轮报文内容一致。

AUTH 载荷绑定身份、两个 nonce 以及两条 IKE_SA_INIT 报文，因此问题 Q1 的这一部分答案为是。

- 结果：成立；是否回答了所问：是；可用但有保留
- 价值中：回答了所问问题；实质内容与 A03 相同。
- 文稿中有明确表述：是。出处：s0387、s0389、s0391
- 依据：与 A03 相同：签名块按草案定义建模，未包含 SPI 与分片细节。

A08.11：能力信号篡改可被检测

接受方所接受的签名算法与哈希算法，必须来自对端真实提议且被 AUTH 覆盖的能力信号，并与实际验证签名所用算法一致。

修改能力通知不会产生一个使用非真实通告并验证的算法被接受的会话：通知位于签名数据之内，且要求 PQC 的部署只接受 ML-DSA-65。

- 结果：成立；是否回答了所问：是；可用但有保留
- 价值中：肯定地回答了问题 Q2；文稿称通知受 AUTH 保护，但未提及 AUTH 载荷本身的算法标识字段，因此可能重要的部分仍未确定。
- 文稿中有明确表述：不明确。依据的原文：rfc7296:489、s0019、s0020、s0044
- 依据：与 A08 相同：算法标识是不同的符号构造子，因此无法表示跨算法混淆。
- 未决：攻击者能否重新标记 AUTH 载荷内的 AlgorithmIdentifier，并让签名在所命名的算法下验证通过：这是关于签名方案的问题，超出模型范围。

X01: IDi 与 IDr 的身份保护

仅观察和修改网络的攻击者永远不会获知 IKE_AUTH 交换的 ID 载荷内容，因此无法分辨发起方声称了哪个身份，或响应方使用了哪个身份。

该主张不成立：路径上的攻击者从 IKE_AUTH 请求中读出发起方的身份。它用 g 的 Diffie-Hellman 份额应答 IKE_SA_INIT，使共享秘密成为发起方自身的公开值，从而导出加密密钥并解密该请求。该轨迹中未完成 AUTH，这正是 RFC 7296 所述的保留条件。

- 结果：攻击成立（文稿中有明确表述）；是否回答了所问：是；可用但有保留
- 价值中：复现了一个已知后果，但机制现已明确：问题在于未经验证的 Diffie-Hellman 份额，而非 ML-DSA 认证的弱点。
- 文稿中有明确表述：是。出处：rfc7296:489、s0084、s0379、s0381
- 依据：该攻击需要退化份额 g 被接受；验证对端 Diffie-Hellman 公开值的一方可阻止它，而模型没有此类检查，因为文稿未要求。；身份被视为各方持有的名称，而非攻击者已知的名称。；未建模 EAP 或后续交换，且在建模运行中发起方身份未以其他方式暴露。

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、是否检查了对照查询，以及各攻击及分析者对每项攻击的判定。

目标	级别	界	查询	对照	攻击	主张
A02	proved		a02_i	checked		4 proved
A03	proved		a03_i	checked		3 proved
A04	proved		a04_i	checked		3 proved
A08	proved		a08_notrad	checked		4 proved
R05	proved		a08_notrad	checked		2 proved
K01	proved		k01_sess	checked		3 proved
C01	proved		c01	checked		1 proved
C02	proved		c02_r	checked		2 proved
C08	proved		a08_notrad	checked		2 proved
A03.10	proved		a03_i	checked		2 proved
A08.11	proved		a08_notrad	checked		3 proved
C02.12	proved		c02_r	checked		2 proved
X01	none				x01 (holds_in_source)	1 attack

逐条主张，按分析者对每条主张的措辞；每条的答案来自证明器：

目标	主张	攻击者	回答	查询	对照
A02	发起方一侧：只要发起方接受了对端 id_b 的身份，某个由 id_b 运行的响应方就已经接受 id_a 为对端（在对端身份上满足非单射一致）；攻击者仅拥有网络	`network`	proved	a02_i	checked
A02	响应方一侧：只要响应方接受了 id_a 为其对端，发起方就曾以该响应方为对端、并以相同的 Ni、Nr 和 IKE_SA_INIT 请求运行过一次会话（响应方先于发起方接受，因此运行事件即为匹配事件）	`network`	proved	a02_r	checked
A02	发起方一侧，所有传统签名密钥都落入攻击者手中：对端身份仍仅由 ML-DSA-65 认证	`crqc_traditional`	proved	a02_i	checked
A02	响应方一侧，所有传统签名密钥都落入攻击者手中：对端身份和第一轮消息仍仅由 ML-DSA-65 认证	`crqc_traditional`	proved	a02_r	checked
A03	发起方一侧：响应方的接受与发起方在双方身份、Ni、Nr 以及 IKE_SA_INIT 请求和响应的内容上一致，因此 AUTH 覆盖了对端的 nonce 和第一轮消息	`network`	proved	a03_i	checked
A03	响应方一侧：发起方的运行与响应方的接受在对端身份、Ni、Nr 和 IKE_SA_INIT 请求内容上一致	`network`	proved	a02_r	checked
A03	发起方一侧，传统签名可被伪造：对端 nonce、身份以及两条 IKE_SA_INIT 消息仍由 ML-DSA-65 AUTH 绑定	`crqc_traditional`	proved	a03_i	checked

目标	主张	攻击者	回答	查询	对照
A04	发起方一侧：响应方的每次接受都对应一次不同的响应方接受（单射一致），因此记录的 AUTH 不会被重复计数	`network`	proved	a04_i	checked
A04	响应方一侧：发起方的每次接受都对应一次不同的发起方运行（单射一致）	`network`	proved	a04_r	checked
A04	发起方一侧，传统签名可被伪造：没有记录的 AUTH 被接受两次，每次接受都映射到一次不同的对端接受	`crqc_traditional`	proved	a04_i	checked
A08	部署要求 PQC 认证的响应方，从不接受用传统签名算法生成的 AUTH，无论 AUTH 载荷携带什么算法标识符	`network`	proved	a08_notrad	checked
A08	接受方使用的算法和哈希是对端真实、受 AUTH 覆盖的信号：对端自身的运行携带了验证 AUTH 时所用的同一些 IKE_SA_INIT 消息，因此被修改的通知无法通过认证	`network`	proved	a03_i	checked
A08	传统签名可被伪造时，要求 PQC 的部署仍只接受 ML-DSA-65 AUTH，因此算法标识符的任何降级都不被接受	`crqc_traditional`	proved	a08_notrad	checked
A08	即使传统签名可被伪造，算法信号仍是对端真实的，因为 AUTH 覆盖了两条 IKE_SA_INIT 消息	`crqc_traditional`	proved	a03_i	checked
R05	在要求 ML-DSA 认证并禁止回退的部署中，任何会话都不会以传统签名认证被接受，因此攻击者无法强制降级	`network`	proved	a08_notrad	checked
R05	无降级：当网络中存在具备 CRQC 能力的伪造者时，要求 PQC 的部署不会建立任何以传统签名认证的会话	`crqc_traditional`	proved	a08_notrad	checked
K01	响应方的 ML-DSA 签名密钥在运行期间从不为攻击者所知	`network`	proved	k01_ltk2	checked
K01	已认证会话的 IKE SA 密钥材料（SKEYSEED 及七个派生密钥）在运行期间从不为攻击者所知	`network`	proved	k01_sess	checked
K01	发起方的 ML-DSA 签名密钥在运行期间从不为攻击者所知	`network`	proved	k01_ltk	checked
C01	已建立会话的任何 IKE SA 密钥材料都不会到达在交换之后获得两个 ML-DSA 长期签名密钥的攻击者手中（SKEYSEED 由临时 DH 秘密和 nonce 派生，而非由签名密钥派生）	`ltk_after_session`	proved	c01	checked
C02	若接受方自身的 ML-DSA 签名密钥在会话之前就为攻击者所知，该方仍只在对端运行过匹配会话时才接受对端身份，因此攻击者无法向它冒充未受攻陷的对端	`own_ltk`	proved	c02_r	checked
C02	同一主张的较弱解读：在自身签名密钥公开的情况下，接受方的每次接受仍蕴含对端曾以它为对端运行过某次会话	`own_ltk`	proved	c02_dn	checked
C08	所有传统签名密钥都为攻击者所知时，要求 PQC 认证的部署仍从不接受传统 AUTH，因此被攻破的遗留算法没有可乘之机	`crqc_traditional`	proved	a08_notrad	checked
C08	传统签名可被伪造时，ML-DSA-65 仍在响应方一侧认证对端身份	`crqc_traditional`	proved	a02_r	checked

目标	主张	攻击者	回答	查询	对照
A03.10	AUTH 绑定了对端身份、双方 nonce 和 IKE_SA_INIT 消息：响应方的接受与发起方的会话在所有这些方面一致（问题 Q1）	`network`	proved	a03_i	checked
A03.10	传统签名可被伪造时，AUTH 仍绑定身份和 nonce（问题 Q1）	`crqc_traditional`	proved	a03_i	checked
A08.11	被修改的能力信号不成立：响应方仅在签名后的 IKE_SA_INIT 请求所宣告的 Identity 哈希与所验证的 ML-DSA-65 标识符一致时才接受对端的 AUTH（问题 Q2）	`network`	proved	a08_notrad	checked
A08.11	对端的算法信号是真实的，且要求 PQC 的部署只接受 ML-DSA-65，即使传统签名可被伪造（问题 Q2）	`crqc_traditional`	proved	a08_notrad	checked
A08.11	被接受的算法和哈希来自对端自身的、受 AUTH 覆盖的 IKE_SA_INIT 消息（问题 Q2）	`network`	proved	a03_i	checked
C02.12	与第一条相同的主张，把正常会话作为正面对照：泄漏下的接受并非空洞，双方之间的会话可达	`own_ltk`	proved	c02_r	checked
C02.12	同一主张的较弱解读（任意对端运行，不限于 nonce 相同的那次），并以可达会话作为正面对照（问题 Q3）	`own_ltk`	proved	c02_dn	checked
X01	发起方在 IKE_AUTH 请求中放入的 IDi 值对在路径上的攻击者并非隐藏：攻击者可在任何 AUTH 验证之前读到它	`network`	attack (holds_in_source)	x01	

附录 D：分析是怎么跑的

LLM 分析者依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-20261114T222941，2026-11-14。状态：已完成。模型：deepseek-v4-1-flash-261017。步数：40，证明器 27 s，实际耗时 14 min，费用 0.126 USD。

ProVerif：运行 108 个证明，108 个已判定，0 个无答案，21 s，记录 38 个回答。

分析了什么

协议	IKEv2 ML-DSA authentication
版本	draft-ietf-ipsecme-ikev2-pqc-auth-12
分析范围	固定 ML-DSA-65、RFC7427 Digital Signature AUTH 与初始 IKE SA，完整 SignedOctets、身份及算法选择；DH 理想化，不凭签名升级声称 DH 会话密钥抗量子；不含 EAP/rekey。
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	573 个编号原文单元（187263 字节），来自下文所列各节。本报告中形如 s0001 的引用就是其中一个原文单元

分析所依据的文稿章节：

文稿	章节	标题
main	3	IKEv2 中 PQC 认证的通用框架
main	3.1	指定 PQC 签名算法
main	3.2	签名的生成与验证
main	3.2.1	在 IKEv2 中处理 PQC 签名
main	3.3	通告所支持密钥对类型的机制
main	4	在 IKEv2 中指定 ML-DSA
main	6	ML-DSA 与 SLH-DSA 的使用
main	9	安全考量
rfc7296	1	引言
rfc7296	1.1	使用场景
rfc7296	1.1.1	隧道模式下安全网关到安全网关
rfc7296	1.1.2	端到端传输模式
rfc7296	1.1.3	隧道模式下端点到安全网关
rfc7296	1.1.4	其他场景
rfc7296	1.2	初始交换
rfc7296	1.3	CREATE_CHILD_SA 交换
rfc7296	1.3.1	使用 CREATE_CHILD_SA 交换创建新的子 SA
rfc7296	1.3.2	使用 CREATE_CHILD_SA 交换为 IKE SA 重新生成密钥

文稿	章节	标题
rfc7296	1.3.3	使用 CREATE_CHILD_SA 交换为子 SA 重新生成密钥
rfc7296	1.4	INFORMATIONAL 交换
rfc7296	1.4.1	使用 INFORMATIONAL 交换删除 SA
rfc7296	1.5	IKE SA 之外的信息性消息
rfc7296	1.6	需求术语
rfc7296	1.7	RFC 4306 与 RFC 5996 之间的重要差异
rfc7296	1.8	RFC 5996 与本文档之间的差异
rfc7296	2	IKE 协议细节与变体
rfc7296	2.1	重传定时器的使用
rfc7296	2.2	消息 ID 序列号的使用
rfc7296	2.3	重叠请求的窗口大小
rfc7296	2.4	状态同步与连接超时
rfc7296	2.5	版本号与前向兼容性
rfc7296	2.6	IKE SA SPI 与 Cookie
rfc7296	2.6.1	COOKIE 与 INVALID_KE_PAYLOAD 的交互
rfc7296	2.7	密码算法协商
rfc7296	2.8	重新生成密钥
rfc7296	2.8.1	子 SA 的同时重新生成密钥
rfc7296	2.8.2	IKE SA 的同时重新生成密钥
rfc7296	2.8.3	IKE SA 的重新生成密钥与重新认证
rfc7296	2.9	流量选择器协商
rfc7296	2.9.1	违反自身策略的流量选择器
rfc7296	2.9.2	重新生成密钥过程中的流量选择器
rfc7296	2.10	Nonce
rfc7296	2.11	地址与端口灵活性
rfc7296	2.12	Diffie-Hellman 指数的重用
rfc7296	2.13	生成密钥材料
rfc7296	2.14	为 IKE SA 生成密钥材料
rfc7296	2.15	IKE SA 的认证
rfc7296	2.16	可扩展认证协议方法
rfc7296	2.17	为子 SA 生成密钥材料
rfc7296	2.18	使用 CREATE_CHILD_SA 交换为 IKE SA 重新生成密钥
rfc7296	2.19	请求远程网络上的内部地址
rfc7296	2.20	请求对端版本
rfc7296	2.21	错误处理
rfc7296	2.21.1	IKE_SA_INIT 中的错误处理

文稿	章节	标题
rfc7296	2.21.2	IKE_AUTH 中的错误处理
rfc7296	2.21.3	IKE SA 认证完成后的错误处理
rfc7296	2.21.4	IKE SA 之外的错误处理
rfc7296	2.22	IPComp
rfc7296	2.23	NAT 穿越
rfc7296	2.23.1	传输模式 NAT 穿越
rfc7296	2.24	显式拥塞通知（ECN）
rfc7296	2.25	交换碰撞
rfc7296	2.25.1	重新生成密钥或关闭子 SA 时的碰撞
rfc7296	2.25.2	重新生成密钥或关闭 IKE SA 时的碰撞
rfc7427	3	认证载荷

源文中的步骤在文稿中定位到的协议用途：固定 ML-DSA-65、RFC7427 Digital Signature AUTH 与初始 IKE SA，完整 SignedOctets、身份及算法选择；DH 理想化，不凭签名升级声称 DH 会话密钥抗量子；不含 EAP/rekey。

对照文稿定性质

在撰写查询之前，分析者将草拟的性质清单与文稿本身所声明的协议用途逐项对照。性质的名称、性质涉及的内容以及文稿的说法均属分析者的解读；所列位置在文稿中确实存在。

ID	简称	对象	文稿怎么说	出处
A02	对端身份认证	发起方确信自己认证的对端就是它想要通信的响应方。响应方同样确信对端是发起方。	每一方都在 IDi/IDr 中声明自己的身份，并用 AUTH 载荷证明自己掌握对应密钥。双方必须验证所有签名和 MAC（RFC 7296 第 1.2 节和第 2.15 节）。	s0002, s0055, s0103, s0387
A03	AUTH 载荷的会话绑定	双方，关于对端身份、双方的 nonce Ni 和 Nr，以及两个 IKE_SA_INIT 消息的内容——这些都在签名覆盖之下。	SignedOctets 包含 RealMessage1 或 RealMessage2、另一方的 nonce 以及 prf(SK_p, ID')。RFC 7296 第 2.15 节指出，每一方对另一方的 nonce 进行签名至关重要。	s0012, s0045, s0103, s0387, s0389, s0391
A04	AUTH 不可跨会话重放	双方，关于一次接受可以归因于多少次对端运行：一次对端运行不能被另一方计算两次。	由于 nonce 被包含在内，签名数据在每个会话中都是唯一的，因此录制的 AUTH 不能在另一个会话中再次呈现（草案第 9 节；RFC 7296 第 2.15 节）。	s0012, s0045, s0387
A08	签名算法绑定	接受方，关于它用于验证 AUTH 的签名和哈希算法：该算法必须是对方确实通告过的、且被 AUTH 覆盖的算法，并且必须是实际用于验证的算法。	SIGNATURE_HASH_ALGORITHMS 和 SUPPORTED_AUTH_METHODS 通知受 AUTH 载荷保护。Authentication Data 内部的 AlgorithmIdentifier 选择算法（RFC 7427 第 3 节；草案第 9 节）。	s0019, s0020, s0044, s0557, s0566
R05	不可降级至传统 AUTH	接受方，关于会话的认证方法：在要求 PQC 签名认证的部署中，不得使用传统签名算法建立任何会话。	当 PQC 认证为强制要求时，实现不得回退到传统算法。要求保护的部署必须强制要求 PQC 认证，且不得允许回退（草案第 9 节）。	s0044

ID	简称	对象	文稿怎么说	出处
K01	IKE SA 与签名密钥保密性	双方，关于 IKE SA 密钥材料（SKEYSEED、SK_d、SK_e*、SK_a*、SK_p*）以及它们的 ML-DSA 长期签名密钥：攻击者无法推导出其中任何一个。	SKEYSEED = prf(Ni | Nr, g^ir) 以及派生出的七个密钥（RFC 7296 第 2.14 节）。ML-DSA 私钥从不离开签名方。	s0379, s0382, s0387
C01	IKE SA 密钥前向保密	一个已完成的 IKE SA，关于攻击者后来同时获取两个长期 ML-DSA 签名密钥的情形：会话密钥材料仍然保密。	会话密钥由临时 DH 交换和 nonce 派生，而不由签名密钥派生。RFC 7296 第 5 节假定 DH 指数在使用后被擦除。	s0379, s0381, s0382, s0363
C02	自身密钥泄露不导致冒充	接受方，关于其对端身份，当其自身的 ML-DSA 长期签名密钥已经泄露时。	AUTH 是签名方用自己的长期密钥对包含另一方 nonce 的数据所作的签名（RFC 7296 第 2.15 节）。草案没有单独讨论密钥泄露冒充。	s0387, s0103, s0044
C08	传统签名被攻破时 PQC 认证仍有效	接受方，关于其对端身份和实际使用的算法，当传统签名可以被伪造但 ML-DSA 未被攻破时。	第 9 节：能够伪造传统签名的攻击者可以冒充支持传统认证的对端，并且可以通过修改通知来降级。强制要求 PQC 认证可以消除该攻击。	s0044, s0038, s0049
A03.10	AUTH 绑定身份与 nonce	双方，关于对端所接受的 nonce、身份和第一轮消息内容（用户问题 Q1）。	用户问题 Q1。RFC 7296 第 2.15 节根据 RealMessage1/2、对端的 nonce 和 prf(SK_p, ID') 定义了 InitiatorSignedOctets 和 ResponderSignedOctets。	s0387, s0389, s0391, s0103
A08.11	能力信号篡改可被检测	接受方，关于会话中使用的算法和哈希选择，当通知载荷被修改时（用户问题 Q2）。	用户问题 Q2。这些通知被 AUTH 覆盖，要求 Identity 哈希的 PQC 算法不得与未通告该算法的对端一起使用（草案第 3.2.1 节和第 9 节）。	s0019, s0020, s0044, s0557
C02.12	自身密钥泄露不破坏对端身份	接受方，关于其对端身份，当其自身的 ML-DSA 签名密钥已经泄露时，并以一次正常会话作为阳性对照（用户问题 Q3）。	用户问题 Q3。构造与 C02 相同，并在正常流程上设置了明确的阳性对照。	s0387, s0103, s0044
X01	IDi 与 IDr 的身份保护	发起方，关于其自身在 IKE_AUTH 请求中携带的身份值 IDi，以及响应方的 IDr，针对路径上的攻击者。	RFC 7296 第 1.2 节：IKE_AUTH 消息是加密的，因此身份对窃听者隐藏。然而，无法完成 IKE_AUTH 的路径上攻击者仍然可以看到发起方的身份（RFC 7296 第 5 节，P09）。	s0084, s0097, s0102

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 53 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 12 段，没选 41 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:595-610	R05, A08, `crqc_traditional`	

段落	出处	定为	不选的原因
P02	main:612-620	A03, A04	
P03	main:622-631	证明器问不了	NIST 安全类别：原语的强度。
P04	main:636-636	没有陈述目标	页脚和页眉。
P05	main:640-640	没有陈述目标	草案的页面页眉。
P06	main:643-649	证明器问不了	ML-DSA 参数集的设计强度。
P07	main:651-653	证明器问不了	RFC 9881 的侧信道和不可否认性性质：不是迹性质。
P08	main:655-662	证明器问不了	原语的签名次数限制；SLH-DSA 不在固定的 ML-DSA-65 范围内。
P09	rfc7296:6478-6488	X01, `network`	
P10	rfc7296:6490-6494	不在范围内	EAP 认证；任务排除了 EAP。
P11	rfc7296:6496-6500	不在范围内	用 CREATE_CHILD_SA 重新生成密钥；范围内只有初始 IKE SA。
P12	rfc7296:6502-6514	证明器问不了	Diffie-Hellman 群的强度；模型把 DH 理想化了。
P13	rfc7296:6516-6519	证明器问不了	同一条 Diffie-Hellman 群强度讨论。
P14	rfc7296:6525-6527	证明器问不了	DH 强度讨论的延续（分页）。
P15	rfc7296:6529-6530	C01	
P16	rfc7296:6532-6538	证明器问不了	拒绝服务：可用性，不是迹性质。
P17	rfc7296:6540-6542	证明器问不了	PRF 输出长度和算法强度。
P18	rfc7296:6544-6549	证明器问不了	随机数生成器的质量。
P19	rfc7296:6551-6556	不在范围内	任务固定了 IKE SA 的加密和完整性算法；只分析签名算法的选择。
P20	rfc7296:6558-6563	不在范围内	预共享密钥认证；任务固定了签名认证。
P21	rfc7296:6565-6572	不在范围内	NAT 检测和地址隐藏：NAT 穿越不在所建模的交换之内。
P22	rfc7296:6578-6580	不在范围内	NAT 检测段落的延续（分页）。
P23	rfc7296:6582-6606	不在范围内	不生成密钥的 EAP 方法；EAP 被排除。
P24	rfc7296:6608-6612	不在范围内	对 EAP 部署的要求。
P25	rfc7296:6614-6619	证明器问不了	重组缓冲区耗尽：可用性。
P26 至 P27	rfc7296:6621-6633	A02	

段落	出处	定为	不选的原因
P28	rfc7296:6637-6643	不在范围内	Child SA 的流量选择器授权；Child SA 不在所建模的交换之内。
P29 至 P35	rfc7296:6645-6696	不在范围内	流量选择器授权。
P36	rfc7427:398-400	证明器问不了	选择合适的哈希函数：原语的强度。
P37 至 P38	rfc7427:402-417	A08	
P39 至 P40	rfc7427:419-429	A08, A03	
P41	rfc7427:431-435	证明器问不了	降级到极弱密码：原语的强度。
P42	rfc7427:437-439	证明器问不了	MD5 不在哈希注册表中。
P43	rfc7427:441-444	证明器问不了	RSASSA-PKCS1-v1_5 和填充方法的弱点：原语的强度，而且任务固定了 ML-DSA-65。
P44	rfc7427:446-449	证明器问不了	DSA 与 SHA-1 的限制：原语的强度。
P45	rfc9593:446-450	没有陈述目标	指向 RFC 7296 的安全考虑，那里已逐段覆盖。
P46	rfc9593:452-459	R05, `network`	
P47	rfc9593:461-465	R05, C08, `crqc_traditional`	
P48	rfc9881:573-574	没有陈述目标	指向 RFC 5280 的安全考虑，模型将其假定掉。
P49	rfc9881:576-579	证明器问不了	ML-DSA 的 SUF-CMA：原语的强度。
P50	rfc9881:581-590	证明器问不了	密钥生成的 PRNG 质量。
P51	rfc9881:592-604	证明器问不了	侧信道泄露和通过功耗分析恢复密钥。
P52	rfc9881:606-614	证明器问不了	确定性签名与随机化签名的取舍：本地选择，验证相同，模型正是这样反映的。
P53	rfc9881:616-627	证明器问不了	不可否认性需要争议模型，不是迹性质。

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	X01	
K03	强保密／秘密值不可区分性	K01	
K04	密钥用途、方向与会话分离	证明器问不了	符号密钥按构造就是不同的项，因此查询无法区分密钥重用与密钥分离。
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	K01, A03	
A06	显式密钥确认	不适用	初始交换没有显式的密钥确认消息。
A07	身份—凭据—密钥绑定	A02	

条目	目录里的性质	作为哪条性质检查	不检查的原因
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	没有业务操作或一次性令牌参与。
R04	消息接受顺序／窗口安全	不在范围内	Message-ID 窗口（RFC 7296 第 2.2 节和第 2.3 节）不在所建模的交换之内。
C03	已知密钥安全／泄露隔离	C01	
C04	临时秘密／部分状态泄露韧性	不在范围内	没有对临时或部分内存泄露建模。
C05	泄露后安全恢复（PCS）	不在范围内	任务排除了重新生成密钥和泄露后恢复。
C06	注册凭据泄露后的增强认证	不适用	不涉及注册记录或 PAKE 式认证。
C07	抗离线字典攻击	不适用	签名认证中不涉及低熵共享秘密。
Z01	授权执行正确性	不适用	没有受保护的操作或资源访问被授权。
Z02	委托权限不扩张	不适用	各方之间没有委托。
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被绑定。
Z04	撤销与过期生效	不适用	没有权限的撤销或过期。
Z05	跨租户／跨服务安全隔离	不适用	没有多租户或跨服务隔离。
S01	加密 nonce 唯一性	证明器问不了	SK{} 封装被理想化了；AEAD nonce 重用对符号证明器不可见。
S02	重传／密钥重安装安全	不在范围内	重传和密钥重安装属于 CREATE_CHILD_SA 和 INFORMATIONAL，任务将其排除。
S03	抗回滚与状态单调性	不在范围内	安全状态回滚涉及重新生成密钥和已存储的 SA。
S04	跨阶段安全上下文一致性	不在范围内	跨阶段上下文混淆需要重新生成密钥、漫游或恢复，这些都被排除。
S05	终止与旧状态失效	不在范围内	拆除和去认证被排除。
P01	身份匿名性	不适用	对端身份是已知的证书名字；只声称对窃听者的身份保护，而这正是新增的目标。
P02	会话不可关联性	不适用	没有临时身份或假名使会话不可关联。
P03	用户／凭据存在性隐藏	不适用	没有查询用户或凭据目录。
V01	条件性进展／错误恢复	证明器问不了	进展和错误恢复是活性性质。
V02	无非预期死锁	证明器问不了	无死锁是活性性质。
V03	受限资源滥用／抗放大	不在范围内	资源滥用和抗拥塞 cookie 不在所建模的认证之内。

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 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 4 项，没设的 23 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	`own_ltk`	
S02	响应方	参与方	`own_ltk`	

ID	参与方或值	类别	攻击者条件	不设的原因
S03	路径攻击者	参与方	攻击者得不到更多	它就是网络上的攻击者本身；不对它询问任何性质。
S04	接受方	参与方	`own_ltk`	
S05	未泄露对端	参与方	攻击者得不到更多	这个对端的密钥按密钥泄露目标的假设保持秘密；如果攻击者持有该密钥，那它就是这个对端本身，它完成的一个会话就是一次真实运行。
S06	攻击者	参与方	攻击者得不到更多	攻击者本身。
S07	对端身份	值	攻击者得不到更多	身份是任何一方都能查到的证书名称；知道它们并不影响认证问题仍可询问。
S08	身份	值	攻击者得不到更多	身份是任何一方都能查到的证书名称；关于它们的保密问题属于附加的身份保护目标，针对网络攻击者询问。
S09	Ni	值	攻击者得不到更多	身份是任何一方都能查到的证书名称；关于它们的保密问题属于附加的身份保护目标，针对网络攻击者询问。
S10	Nr	值	攻击者得不到更多	身份是任何一方都能查到的证书名称；关于它们的保密问题属于附加的身份保护目标，针对网络攻击者询问。
S11	IKE_SA_INIT 报文	值	攻击者得不到更多	身份是任何一方都能查到的证书名称；关于它们的保密问题属于附加的身份保护目标，针对网络攻击者询问。
S12	签名	值	攻击者得不到更多	身份是任何一方都能查到的证书名称；关于它们的保密问题属于附加的身份保护目标，针对网络攻击者询问。
S13	SIGNATURE_HASH_ALGORITHMS 通知	值	攻击者得不到更多	通知、AlgorithmIdentifier 以及它们所隐含的选择都是对端公开宣告的值；持有它们并不比网络多得到什么，网络本来就能看到 IKE_SA_INIT 通知。
S14	SUPPORTED_AUTH_METHODS 通知	值	攻击者得不到更多	通知、AlgorithmIdentifier 以及它们所隐含的选择都是对端公开宣告的值；持有它们并不比网络多得到什么，网络本来就能看到 IKE_SA_INIT 通知。
S15	AlgorithmIdentifier	值	攻击者得不到更多	通知、AlgorithmIdentifier 以及它们所隐含的选择都是对端公开宣告的值；持有它们并不比网络多得到什么，网络本来就能看到 IKE_SA_INIT 通知。
S16	认证方法选择	值	攻击者得不到更多	通知、AlgorithmIdentifier 以及它们所隐含的选择都是对端公开宣告的值；持有它们并不比网络多得到什么，网络本来就能看到 IKE_SA_INIT 通知。
S17	签名算法选择	值	攻击者得不到更多	通知、AlgorithmIdentifier 以及它们所隐含的选择都是对端公开宣告的值；持有它们并不比网络多得到什么，网络本来就能看到 IKE_SA_INIT 通知。
S18	SKEYSEED	值	按定义全部失守	一旦 SKEYSEED 已知，该 IKE SA 的保密性按定义即告失守，因此没有目标会在这一假设下询问会话性质。

ID	参与方或值	类别	攻击者条件	不设的原因
S19	SK_d	值	按定义全部失守	一旦 SKEYSEED 已知，该 IKE SA 的保密性按定义即告失守，因此没有目标会在这一假设下询问会话性质。
S20	SK_ei/SK_er	值	按定义全部失守	一旦 SKEYSEED 已知，该 IKE SA 的保密性按定义即告失守，因此没有目标会在这一假设下询问会话性质。
S21	SK_ai/SK_ar	值	按定义全部失守	一旦 SKEYSEED 已知，该 IKE SA 的保密性按定义即告失守，因此没有目标会在这一假设下询问会话性质。
S22	SK_pi/SK_pr	值	按定义全部失守	一旦 SKEYSEED 已知，该 IKE SA 的保密性按定义即告失守，因此没有目标会在这一假设下询问会话性质。
S23	ML-DSA 签名私钥	值	`own_ltk`, `ltk_after_session`	
S24	IKE SA 会话密钥	值	按定义全部失守	与 SKEYSEED 相同：这些密钥正是保密目标所保护的对象。
S25	对端身份认证	值	攻击者得不到更多	这些是目标所询问的性质，而不是某一方单独持有的值。
S26	身份认证	值	攻击者得不到更多	这些是目标所询问的性质，而不是某一方单独持有的值。
S27	算法绑定	值	攻击者得不到更多	这些是目标所询问的性质，而不是某一方单独持有的值。

每条性质在各攻击者条件下的答案

这些攻击者由分析者在写查询之前设定；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下对该性质给出的答案；“无答案”是为该性质设定、但证明器未作结论或没有记录任何内容的攻击者；空单元格是分析者没有为该性质设定的攻击者。

攻击者	持有什么	依据	出处
`network`	仅限网络：它能读取、丢弃、修改和发送报文，但不持有任何一方的秘密		
`crqc_traditional`	双方所有传统（后量子之前）签名私钥，因此它可以随意用传统签名算法生成 AUTH 载荷；它没有 ML-DSA 私钥。	草案假设存在具备 CRQC 能力的攻击者，能够伪造传统签名（第 9 节），并且 PQC 签名认证可能按部署策略可选。	s0044, s0045, s0049
`own_ltk`	接受对端身份的一方所持有的 ML-DSA 长期签名私钥，在会话开始前获得；对端的 ML-DSA 密钥保持秘密。	密钥泄露冒充：RFC 7296 第 2.15 节规定 AUTH 是用签名者自己的密钥对包含对方 nonce 的数据所作的签名，因此问题在于泄露自己的密钥是否能让攻击者冒充另一个未被泄露的对端。	s0387, s0389, s0391, s0103
`ltk_after_session`	双方的 ML-DSA 长期签名私钥，在 IKE SA 建立并擦除其密钥材料之后获得。	IKE SA 密钥来自临时 Diffie-Hellman 交换和 nonce（RFC 7296 第 2.14 节），并假设指数在使用后即被擦除（第 5 节）；草案没有声称 DH 会话密钥具备抗量子能力。	s0379, s0381, s0382, s0363

ID	`network`	`crqc_traditional`	`own_ltk`	`ltk_after_session`
A02	成立	成立		

ID	network	crqc_traditional	own_ltk	ltk_after_session
A03	成立	成立		
A04	成立	成立		
A08	成立	成立		
R05	成立	成立		
K01	成立			
C01				成立
C02			成立	
C08		成立		
A03.10	成立	成立		
A08.11	成立	成立		
C02.12			成立	
X01	不成立			

原文和目标

Source: 573 units, 187263 bytes, frozen in source-delivery-01.json. Targets: 9 approved (A02, A03, A04, A08, R05, K01, C01, C02, C08); the questions asked: 3. The list of targets was approved as drafted, beforehand, with --approve-targets.

宿主按其既定默认值（任务 `decisions: auto`）作出的决定，供你核对：

- approve_package: 批准源文包 protocol-c2cbd1d4b40623958b6c0349162f

这一步自身的报告：1 次请求（1 次失败），0.000 USD，输入 81276 token，输出 4413 token，26 秒。

关于证明器和模型的说明

分析者为目标命名的内容：

step	targets	features	reason
33	A02, A03, A03.10, A04, A08, A08.11, C01, C02, C02.12, C08, K01, R05, X01	plain_primitives, many_sessions	所有答案都依赖于把 ML-DSA-65 视为不可伪造的签名、一个 PRF、一个 MAC 和理想化加密，并把 Diffie-Hellman 化简为其唯一法则 g^(xy)=g^(yx)（模型没有超出这一点的 DH 代数，因此除了身份保护攻击中出现的 g 的退化份额之外，不表示任何 DH 攻击）。各角色被复制，因此认证、保密和前向保密的答案都适用于任意数量的会话和任意数量的对端，并且只跟踪两个固定的会话密钥值。没有建模计数器或序列号，因此没有目标依赖于会变化的值。

分析者的结束说明

该模型可以运行（正常流程已验证），并且全部十三个目标都有记录的答案。每条答案都配有一个对照查询，前提是存在变体。在 model.pv 上通过证明确立的结论如下：双向 ML-DSA-65 认证（A02）；两个身份、两个 nonce 以及两条 IKE_SA_INIT 消息的绑定（A03、A03.10）；单射一致性，因此已记录的 AUTH 不会被重复计数（A04）；在要求 PQC 的部署中只使用单一算法，且算法/哈希信号来自受 AUTH 保护的消息（A08、A08.11）；不回退到传统 AUTH（R05）；以及当所有传统签名密钥都落入攻击者手中时仍保持相同的保证（C08）。以下性质同样成立：运行期间的会话密钥与签名密钥保密性（K01）；已建立的 IKE SA 密钥的前向保密，即使攻击者后来同时获得两个签名密钥（C01）；以及对自身签名密钥已泄露一方所发起的

密钥泄露冒充的抵抗能力（C02、C02.12）。以下结果已被复现，并与文稿中的陈述一致：发起方的身份可被自行应答 IKE_SA_INIT 的路径攻击者读取（X01，RFC 7296 §1.2/§5）；允许回退的部署会被传统签名伪造者直接冒充（R05 的对照查询，draft §9）。无发现：没有确立任何文稿尚未说明的内容。阻碍更强结果的因素：Diffie-Hellman 被理想化为 g^xy = g^yx，因此前向保密和会话密钥的答案仅在该理想化下成立；而身份泄露背后的退化份额机制，正是模型确实展示出的那一个 DH 产物。证书验证、消息 ID、分片、Child SA 流量选择器、EAP 和重新密钥均不在模型范围内。Tamarin+ Agent 按 DH 的原样建模，将按照规范所陈述的方式解决前向保密问题。