PQ EAP-AKA prime 完整认证的安全性分析

本报告的其他语言版本：English。

draft-ietf-emu-pqc-eapaka-05 · ProVerif+ Agent 报告

文稿	Post-Quantum Key Encapsulation Mechanisms (PQ KEMs) in EAP-AKA prime （协议定义）; Improved Extensible Authentication Protocol Method for 3GPP Mobile Network Authentication and Key Agreement (EAP-AKA') （辅助）; Forward Secrecy Extension to the Improved Extensible Authentication Protocol Method for Authentication and Key Agreement (EAP-AKA' FS) （辅助）
检查的性质	15 条：11 条成立，4 条不成立（8 个攻击）
发现	无；另在附录 B 复现已知结论： 2

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 B：复现的已知结论
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

PQ EAP-AKA' 在 EAP-AKA' FS 之上加入了 ML-KEM 密钥封装。peer 及其 USIM 通过从运营商后端获取的 AKA 向量向 EAP 服务器认证，peer 则把共享秘密封装到服务器的 ML-KEM 公钥上。

交换以一个隐私友好的身份开始，随后是一个列出前向保密密钥派生函数的 AKA'-Challenge，接着是 peer 请求使用 ML-KEM，再是一个携带 ML-KEM 公钥的重复 Challenge，最后是 peer 带有 AT_RES 和 KEM 密文的响应。双方最终都得到 AKA 的 CK 和 IK 加上 KEM 共享秘密，并由此派生 MK_PQ_SHARED_SECRET、MSK 和 EMSK。

各方：

- **Peer / USIM**：带有 USIM 的 EAP peer。持有：K、身份、网络名。
- **EAP 服务器**：其背后是受信任的 AD。持有：K、网络名。
- **AD**：认证后端。持有：运营商密钥、用户数据。

图 1 展示了文稿所规定的交换流程。

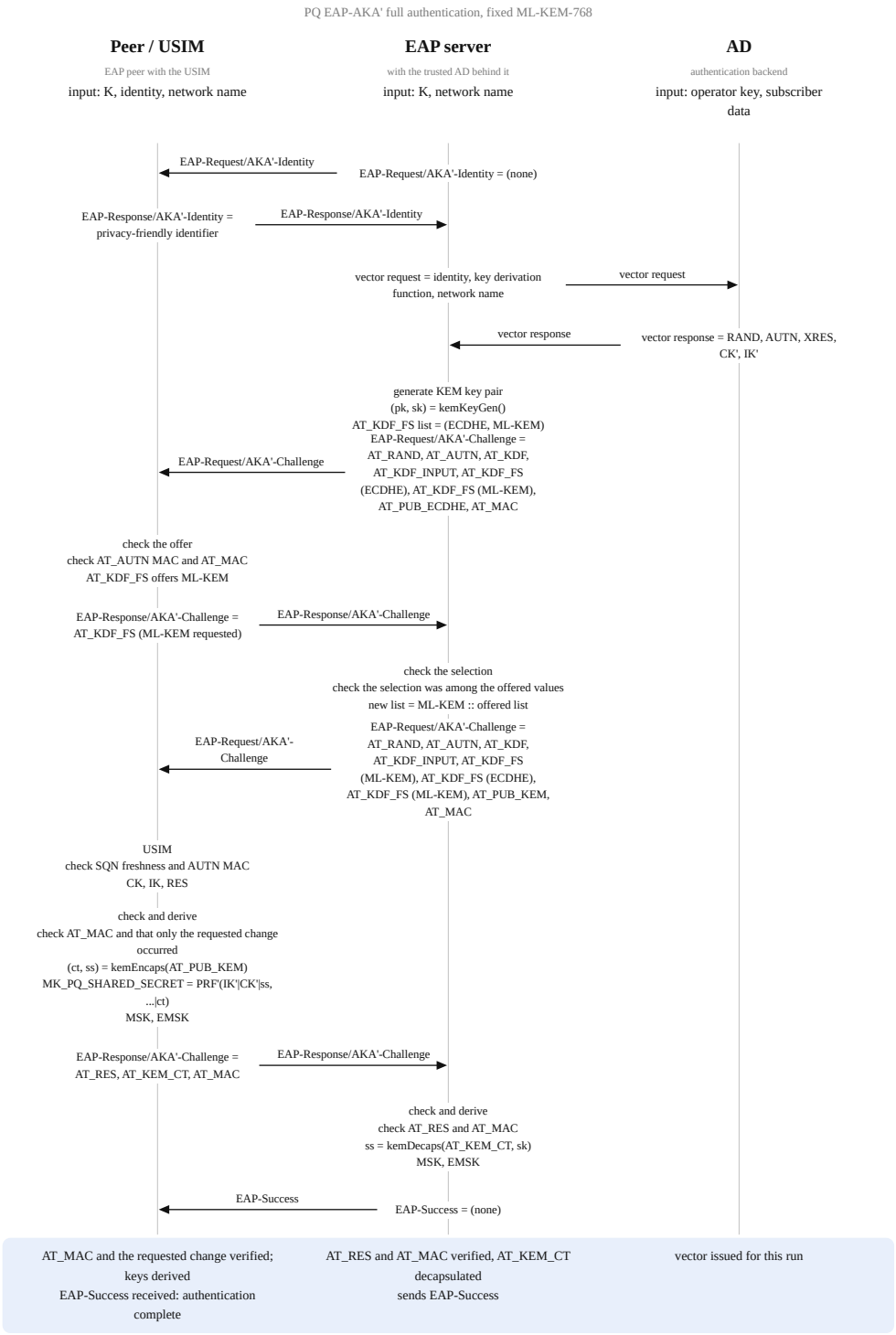


图 1. 文稿规定的协议。

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已排除的内容。性质不成立之处，文稿本身已知悉：附录 B 复现了 2 个此类结果。

在建模范围内，协议提供了它应当提供的保证：peer 与 EAP 服务器相互认证，会话密钥保持保密，ML-KEM 交换对事后获得 AKA 长期密钥的攻击者提供了前向保密。没有新结果：分析复现的两个弱点——未受保护的 EAP-Success 以及持有长期密钥即可实施的冒充——文稿中均已写明。重放保护依赖 AKA 序列号，模型仅在将其展开到两步之后才进行检查。分片以及 AT_CHECKCODE 的身份保护未建模，因此对它们不作任何主张。其余结果是在理想化 KEM 以及未解释的 AKA 和 PRF 函数之上的证明。

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；价值和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
A03	**对等方与EAP服务器的双向认证。** 每当 peer 接受一次完整认证，应存在一个服务器运行，双方身份一致，且双方导出的 MSK/EMSK 与协商的 ML-KEM 参数一致；服务器成功时同样对应 peer 的真实运行。	无	攻击成立（文稿已写明）	中	是
A04	**挑战交换的重放保护。** peer 的每次成功接受对应不同的服务器 Challenge 运行；服务器每次成功对应不同的 peer 响应运行，旧消息重放不能产生新的成功。	无	成立	中	是
K01	**会话密钥的保密性与前向保密。** 攻击者不能导出 MSK、EMSK、MK_PQ_SHARED_SECRET；在 AKA 长期密钥泄露后，先前记录的交换仍不能导出 MK_PQ_SHARED_SECRET。	AKA 长期密钥 (会话完成后泄露)	成立	中	是
C01	**已完成会话的前向保密。** 会话完成后泄露 AKA 长期密钥，攻击者仍不能导出该历史会话的 MSK/EMSK/MK_PQ_SHARED_SECRET。	AKA 长期密钥 (会话完成后泄露)	成立	中	是
R05	**强制PQ KEM抵抗降级。** 在双方或任一方本地策略强制要求 PQ KEM 时，攻击者不能使认证在未协商 ML-KEM 的情况下成功。	AKA 长期密钥 (协商期间泄露)	成立	中	是
A08	**AT_MAC绑定KDF列表、身份和RAND。** peer 接受的 ML-KEM 参数、网络名、身份与挑战值对应服务器实际提议并经 AT_MAC 保护的值。	无	攻击成立（文稿已写明）	中	是
D01	**AT_MAC保护消息的完整性。** peer 与 server 接受的每个受 AT_MAC 保护的消息（含分片重组后的属性）对应允许发送方的真实发送，载荷与上下文字段一致。	无	成立	低	是
R02	**消息实例至多被接受一次。** 同一分片消息实例在单次认证中至多被接受一次，重复分片或乱序分片导致中止而非重复处理。	无	成立	低	是
R01	**当前运行的AUTN与KEM值。** peer 接受的 AUTN 与 KEM 值对应当前运行，旧 AUTN 或旧 KEM 值不能被接受为新认证。	无	在界内成立（变化值展开到 2 步）	中	是
A06	**对等方与服务器之间的密钥确认。** peer 与 server 在确认点有协议证据表明对端已导出同一会话密钥。	无	攻击成立（文稿已写明）	中	是
K01.11	**MSK保密性与对等方-服务器一致性。** 攻击者不能导出 MSK；peer 与 server 对 MSK 达成一致。	无	成立	中	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
A08.12	**已接受挑战值的AT_MAC绑定。** peer 接受的 AT_KDF_FS 列表、身份、网络名与挑战值对应服务器实际提议并经 AT_MAC 保护的值。	无	攻击成立（文稿已写明）	中	是
R05.13	**强制PQ策略下无降级。** 在强制 PQ 配置下，攻击者不能通过重放或降级使认证在未协商 ML-KEM 的情况下成功。	AKA 长期密钥 (协商期间泄露)	成立	中	是
X01	**密钥与密文及KEM密钥的绑定。** 当 peer 与 server 以相同的 MK_PQ_SHARED_SECRET 完成时，他们对所使用的密文 AT_KEM_CT 和 KEM 公钥 AT_PUB_KEM 达成一致，以对抗网络上的攻击者	无	成立	低	是
X02	**未来会话的前向保密。** 在 AKA 长期密钥泄露之后，持有该密钥的攻击者无法导出真实 peer 与真实 server 完成的后续会话的 MK_PQ_SHARED_SECRET	USIM 与运营商共享的 AKA 长期密钥 K（以及任意 RAND 对应的 CK' 和 IK'）；在早先一次认证运行之后获得，并用于攻击先前记录的运行和后续运行	成立	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, X02.

提出的问题及分析者的回答：

问题	回答	依据
Q1: MSK 保密和 peer/server 密钥一致	MSK 对网络攻击者保持保密，peer 与 server 派生出相同的 MK_PQ_SHARED_SECRET 和 MSK；但 peer 始终无法确认 server 持有该密钥。	K01.11, K01, A06
Q2: AT_KDF_FS 列表及身份/网络名/挑战绑定	对网络攻击者而言，peer 接受的 AT_KDF_FS 列表、身份、网络名、RAND 和 AT_PUB_KEM 是服务器经 AT_MAC 保护的值，但对持有 AKA 长期密钥的攻击者则不成立。	A08.12, A08
Q3: 重放与降级策略在强制 PQ 配置下的行为	在策略强制要求 PQ KEM 时，一旦启用 SQN 比较，记录的挑战即被拒绝，且即使持有长期密钥，重放或降级都不能使任一方在未协商 ML-KEM 的情况下完成。	A04, R01, R05.13

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提供了或未能提供什么，其中密码学被视为理想的，完全不涉及实现。

分析者指出，本分析未覆盖的内容：

- ML-KEM 被理想化为对新鲜共享秘密的公钥封装；AKA f1/f2、PRF' 和 AT_MAC 被当作未解释的单向函数。不作任何计算或量子意义上的主张。
- SQN 新鲜性比较仅在 bounded.pv 中建模，签发方与 peer 展开到两步；AKA 接受窗口、SQN 回绕以及用 AUTS 进行的重新同步未建模。

- 分片（AT_FRAGMENT 排序、总长度、跨包 AT_MAC、重复与乱序分片）未建模；对分片属性不作任何主张。
- AT_CHECKCODE 和身份交换未建模；身份仅通过 K_aut 和 MK_PQ_SHARED_SECRET 绑定。
- 快速重认证、仅 ECDHE 的回退路径、无策略降级路径、通道绑定以及下层或隐私性质不在范围内。
- 仅建模一个运营商密钥和一个 peer 身份；不诚实的服务网络、多个身份以及真实的接受窗口被省略。

宿主记录的内容：

- A04、R02、R01 的回答依赖于模型所做的一处简化（附录 D）。

每条性质尚存哪些开放问题、以及怎样才能解决，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、能否直接采用、以及价值几何。

A03: 对等方与EAP服务器的双向认证

每当 peer 接受一次完整认证，应存在一个服务器运行，双方身份一致，且双方导出的 MSK/EMSK 与协商的 ML-KEM 参数一致；服务器成功时同样对应 peer 的真实运行。

在网络攻击者面前，peer 只有在服务器确实发送了最终挑战时才接受它，服务器也只有在 peer 以相同值和密钥发送响应时才接受它。peer 的完成未与服务器绑定：EAP-Success 未受保护，因此 peer 可能在服务器并未完成的情况下认为其已完成。持有 AKA 长期密钥的攻击者可以冒充任一方，正如文稿所述。

- 结果：攻击成立（文稿中已说明）；回答所问：部分；可用但有保留
- 价值 中：它机械地展示了双向认证中哪部分成立、哪部分不成立，但两处失败都已在文稿中说明。
- 文稿中已说明：是。文稿中说明的位置：rfc4187:3772、rfc9678:1005
- 依据：ML-KEM 被理想化为对全新共享密钥的公钥封装；AKA 函数、PRF' 和 AT_MAC 被视为未解释的单向函数；模型中的会话在长期密钥泄露之前或之后运行，从不同时发生；身份交换与 AT_CHECKCODE 未建模
- 待解决：部署中是否使用 AT_RESULT_IND，这会改变对等方的完成主张
- 下一步：若已知某部署使用 AT_RESULT_IND，则对其建模。

A04: 挑战交换的重放保护

peer 的每次成功接受对应不同的服务器 Challenge 运行；服务器每次成功对应不同的 peer 响应运行，旧消息重放不能产生新的成功。

有了序列号比较，录制的挑战会被拒绝，录制的响应也无法产生第二次服务器成功，因为服务器的 RAND 每次运行都是新的。没有比较时，重放的挑战会被接受，这正是展开模型能够回答该目标的原因。

- 结果：成立；回答所问：是；可用但有保留
- 价值 中：它确认了文稿提出的重放主张，代价是需要两步展开且没有窗口模型。
- 文稿中已说明：是。文稿中说明的位置：rfc9048:1183、rfc4187:3707
- 依据：peer 的 SQN 状态在 bounded.pv 中展开为两步；AKA 接受窗口、SQN 回绕和重新同步未建模；bounded.pv 中的服务器阶段发送挑战时不检查响应
- 待解决：更长的展开以及真实的接受窗口
- 下一步：用按实际方式对计数器建模的工具检查窗口和重新同步。

K01: 会话密钥的保密性与前向保密

攻击者不能导出 MSK、EMSK、MK_PQ_SHARED_SECRET；在 AKA 长期密钥泄露后，先前记录的交换仍不能导出 MK_PQ_SHARED_SECRET。

网络攻击者无法从交换中导出 MSK 和 EMSK，运行结束后才获得 AKA 长期密钥的攻击者仍然无法导出 MK_PQ_SHARED_SECRET，因为这需要 KEM 共享密钥。对照查询显示泄露确实有效：仅由长期密钥导出的值（如 K_aut）会被恢复。

- 结果：成立；回答所问：是；可用但有保留
- 价值 中：对核心保密性与前向保密主张的清晰证明，受理想化 KEM 的限制。
- 文稿中已说明：是。文稿中说明的位置：main:1131、rfc9678:929
- 依据：KEM 已理想化；不作计算性或量子主张；AKA 与 PRF' 是未解释函数；攻击者只在运行结束后获得长期密钥
- 待解决：ML-KEM-768 本身的计算安全性
- 下一步：对符号证明器而言无需下一步；计算性主张属于该算法。

C01: 已完成会话的前向保密

会话完成后泄露 AKA 长期密钥，攻击者仍不能导出该历史会话的 MSK/EMSK/MK_PQ_SHARED_SECRET。

已完成运行的 MK_PQ_SHARED_SECRET 及其 MSK 和 EMSK 对之后获得 AKA 长期密钥的攻击者仍然不可及：KEM 共享密钥被封装到会话随后丢弃的密钥对。这成立仅因为服务器为该会话使用全新的 KEM 密钥对，正如安全考虑所要求的那样。

- 结果：成立；回答所问：是；可用但有保留
- 价值 中：机械地复现了文稿的前向保密主张，并明确指出了新密钥对条件。
- 文稿中已说明：是。文稿中说明的位置：rfc9678:929
- 依据：模型中每次运行一个 KEM 密钥对，如 s0158 所建议；KEM 已理想化；长期密钥只在运行结束后揭示
- 待解决：若部署复用 KEM 密钥对会发生什么
- 下一步：对密钥对复用建模，以表明此时前向保密会丢失，正如 s0158 所暗示的那样。

R05: 强制PQ KEM抵抗降级

在双方或任一方本地策略强制要求 PQ KEM 时，攻击者不能使认证在未协商 ML-KEM 的情况下成功。

当 peer 要求 ML-KEM 时，它会拒绝不含 ML-KEM 的提议，而服务器只有在 peer 选择了 ML-KEM 之后才完成；即使攻击者持有长期密钥，这一点也成立。因此保护来自策略检查，与文稿所述完全一致。

- 结果：成立；回答所问：是；可用但有保留
- 价值 中：它把保护明确归于文稿建议的策略检查，但没有对无策略降级路径建模。
- 文稿中已说明：是。文稿中说明的位置：s0153、s0159
- 依据：模型中策略固定为 required；peer 的检查被建模为要求包含 ML-KEM 和 ECDHE 的规范提议；无策略时回退到 EAP-AKA' 或仅 ECDHE 未建模
- 待解决：无策略回退路径与仅 ECDHE 部署
- 下一步：加入关闭策略的回退分支，以复现文稿所述的降级。

A08: AT_MAC绑定KDF列表、身份和RAND

peer 接受的 ML-KEM 参数、网络名、身份与挑战值对应服务器实际提议并经 AT_MAC 保护的值。

peer 接受的列表、身份、RAND、网络名和 AT_PUB_KEM 是网络攻击者下服务器受 AT_MAC 保护的值。持有长期密钥的攻击者可以伪造它们，文稿就 ML-KEM 提议说明了这一点。

- 结果：攻击成立（文稿中已说明）；回答所问：部分；可用但有保留
- 价值 中：展示了绑定及其确切限制，两者都已在文稿中说明。

- 文稿中已说明：是。文稿中说明的位置：rfc9678:989、rfc9678:1005
- 依据：网络名在双方都是固定常量；身份交换未建模；身份通过 K_aut 和 MK_PQ 绑定；KDF 列表是固定的 ML-KEM-768 提议
- 待解决：使用身份交换时通过 AT_CHECKCODE 进行的身份绑定
- 下一步：若分片身份消息在范围内，则对 AT_CHECKCODE 建模。

D01: AT_MAC保护消息的完整性

peer 与 server 接受的每个受 AT_MAC 保护的消息（含分片重组后的属性）对应允许发送方的真实发送，载荷与上下文字段一致。

对于承载在单个 EAP 包中的消息，每个被接受的受 AT_MAC 保护的挑战和响应都对应另一方的真实发送且内容相同。该目标还提到分片属性，而分片未建模，因此不对其作任何主张。

- 结果：成立；回答所问：部分；可用但有保留
- 价值 低：非分片部分直接源于 AT_MAC；目标强调的分片部分不在模型中。
- 文稿中已说明：是。文稿中说明的位置：rfc9048:1175
- 依据：AT_FRAGMENT 的顺序、总长度和跨包 AT_MAC 未建模；AT_MAC 被建模为对消息字段的单个项
- 待解决：重组后分片属性的完整性
- 下一步：对 AT_FRAGMENT 建模，包括步进确认和覆盖所有分片的 MAC。

R02: 消息实例至多被接受一次

同一分片消息实例在单次认证中至多被接受一次，重复分片或乱序分片导致中止而非重复处理。

在一个认证中，挑战或响应实例至多被接受一次：peer 的序列号排除了重复，服务器的新鲜 RAND 在其一侧排除了重复。重复或乱序的 AT_FRAGMENT 处理未建模。

- 结果：成立；回答所问：部分；可用但有保留
- 价值 低：消息层面的主张成立；目标同时提出的分片层面主张未经验证。
- 文稿中已说明：是。文稿中说明的位置：s0014、s0060
- 依据：peer 的 SQN 状态两步展开；分片未建模
- 待解决：重复和乱序分片
- 下一步：对分片序列及其确认建模。

R01: 当前运行的AUTN与KEM值

peer 接受的 AUTN 与 KEM 值对应当前运行，旧 AUTN 或旧 KEM 值不能被接受为新认证。

旧 AUTN 不会被接受为新认证：peer 保留已接受的序列号并拒绝不大于该值的值，因此录制的挑战会被拒绝。旧 KEM 公钥也无法插入，因为 AT_MAC 将其绑定到 RAND 和身份。

- 结果：在界内成立（变化值展开为 2 步）；回答所问：是；可用但有保留
- 价值 中：在比较存在的情况下，通过较短的展开确认了新鲜性主张。
- 文稿中已说明：是。文稿中说明的位置：rfc4187:3707
- 依据：SQN 状态的两步展开；接受窗口未建模
- 待解决：更长的展开和真实窗口
- 下一步：用以窗口对计数器作整数建模的工具进行检查。

A06: 对等方与服务器之间的密钥确认

peer 与 server 在确认点有协议证据表明对端已导出同一会话密钥。

服务器获得了 peer 已完成的证据：AT_RES 和 AT_MAC 绑定了 peer 的响应和密文。peer 没有获得服务器已完成的证据，因为它唯一的信号是 EAP-Success，而攻击者可以发送该消息。文稿同时指出了缺失的密钥确认和未受保护的成功包。

- Result：攻击成立（文稿中已说明）；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：对已知缺口的具体复现，并给出了确切条件（最后的 EAP-Success）。
- 文稿中已说明：是。文稿中的位置：rfc4187:3766, rfc9048:1402
- 依据：AT_RESULT_IND 未建模；AT_MAC 用未解释的 MAC 函数建模
- 未决：部署中是否使用 AT_RESULT_IND
- 下一步：对 AT_RESULT_IND 建模，并重新提出对等方方向的主张。

K01.11：MSK保密性与对等方-服务器一致性

攻击者不能导出 MSK；peer 与 server 对 MSK 达成一致。

网络攻击者无法导出 MSK，服务器接受的响应携带的 MK_PQ_SHARED_SECRET 与对等方的相同，因此双方导出相同的 MSK。这是一个密钥协商结果，并不是向对等方确认服务器持有该密钥。

- Result：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：在理想化 KEM 上以证明回答了用户的第一个问题。
- 文稿中已说明：是。文稿中的位置：s0091, s0107
- 依据：KEM 已理想化；一致性通过已接受消息所携带的值来体现
- 未决：向对等方确认该一致性
- 下一步：见 A08。

A08.12：已接受挑战值的AT_MAC绑定

peer 接受的 AT_KDF_FS 列表、身份、网络名与挑战值对应服务器实际提议并经 AT_MAC 保护的值。

在网络攻击者下，已接受的 AT_KDF_FS 列表、身份、网络名和挑战值就是服务器的受保护值。如文稿所述，它们无法抵御持有长期密钥的攻击者。

- Result：攻击成立（文稿中已说明）；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：就用户的第二个问题而言，内容与 A08 相同。
- 文稿中已说明：是。文稿中的位置：rfc9678:989
- 依据：网络名在两侧固定；提议是固定的 ML-KEM-768 列表
- 未决：通过身份交换实现的身份绑定
- 下一步：见 A08。

R05.13：强制PQ策略下无降级

在强制 PQ 配置下，攻击者不能通过重放或降级使认证在未协商 ML-KEM 的情况下成功。

在策略要求使用 PQ KEM 的情况下，即使是持有长期密钥的攻击者，重放或降级也无法让对等方或服务器在没有 ML-KEM 的情况下完成。若无该策略，文稿称 ML-KEM 提议可以被移除，而本模型并未覆盖这一情况。

- Result：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：就强制配置回答了用户的第三个问题。
- 文稿中已说明：是。文稿中的位置：s0153, s0159
- 依据：策略固定为必需；未建模无策略的回退路径
- 未决：无策略配置
- 下一步：加入回退分支，以复现文稿所述的降级。

X01: 密钥与密文及KEM密钥的绑定

当 peer 与 server 以相同的 MK_PQ_SHARED_SECRET 完成时，在网络攻击者面前，它们对所使用密文 AT_KEM_CT 和 KEM 公钥 AT_PUB_KEM 达成一致

当 peer 与 server 以相同的 MK_PQ_SHARED_SECRET 完成时，它们使用了相同的密文和相同的 KEM 公钥。这是将二者都纳入派生、且封装具有单射性的符号性推论。

- Result：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 低：它只是重述了派生的结构；计算性绑定主张需要计算模型。
- 文稿中已说明：是。文稿中的位置：main:1144
- 依据：KEM 是符号封装；该绑定是结构性的，而非计算性的
- 未决：计算性 MAL-BIND-K-CT/PK
- 下一步：对符号证明器而言无需处理。

X02: 未来会话的前向保密

在 AKA 长期密钥泄露之后，持有该密钥的攻击者无法导出真实 peer 与真实 server 完成的后续会话的 MK_PQ_SHARED_SECRET

长期密钥泄露后，持有该密钥的攻击者无法获知真实 peer 与真实 server 都完成的后续会话的 MK_PQ_SHARED_SECRET，因为共享秘密被封装到新的服务器密钥。亲自扮演其中一方的攻击者确实会获知该会话的密钥，这一点文稿也有说明。

- Result：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：在文稿给出的限定条件下，确认了未来会话的前向保密陈述。
- 文稿中已说明：是。文稿中的位置：rfc9678:935
- 依据：会话密钥对每次运行都是新的；KEM 已理想化；该主张针对双方真实参与者都完成的会话
- 未决：泄露后扮演某一方的攻击者
- 下一步：无需处理；该情形即文稿所述的冒充。

附录 B：复现的已知结论

若某条性质如文稿所述本就不成立，或被文稿搁置，则不算发现。以下即属此类：分析在模型上复现了它，并给出了确切条件。

B.1 伪造的 EAP-Success 使对等方误以为失败的运行成功

类型	协议规范本身的弱点
文稿出处	rfc4187:3772, rfc4187:3766
价值	中
涉及的性质	A03, A06 （见第 3 节）
依据	ProVerif attack query `a03_peer_fin`

发生了什么。 对等方判断服务器已完成的唯一信号是最后的 EAP-Success，而它既不带 AT_MAC，也没有重放保护。对等方发出响应后，网络上的攻击者发送 EAP-Success；对等方导出密钥并报告成功，而服务器从未收到该响应。密钥本身仍保密，因此损失的是关于服务器的错误认知，而非密钥泄露。

攻击者需要什么。 攻击者位于 peer 与 server 之间的网络路径上，能够丢弃对等方的响应，随后发送 EAP-Success。不需要任何密钥。

攻击者能得到什么。 对等方以为服务器已对它完成认证，并开始使用服务器从未接受的会话密钥。访问本来就会被拒绝，但对等方可能基于一个并不存在的运行采取行动，其状态也可能与服务器失去同步。

拟议修改。 为此方法要求受保护的结果指示 AT_RESULT_IND：服务器在 EAP-Success 之前，发送以 K_aut 为密钥、受完整性保护的成功指示，携带 RAND 和导出的 MK_PQ_SHARED_SECRET；对等方只有在验证该指示之后才接受 EAP-Success 并报告完成。已在模型上核查：加入该修改后，伪造成功的攻击不再存在，正常流程仍然存在，其余所有已记录的答案保持不变。

用 ProVerif 复核。 该修改被放入模型的一个副本中：服务器在 EAP-Success 之前，发送以 K_aut 为密钥、受完整性保护的成功指示（AT_RESULT_IND），携带 RAND 和 MK_PQ_SHARED_SECRET；对等方只有在验证该指示之后才接受 EAP-Success 并报告完成。在修改后的模型上，ProVerif 证明了 `a03_peer_fin`：该攻击在那里不再可能。协议的正常流程仍能被找到。其余 32 个已记录的答案保持不变。这是对模型的初步核查：它表明该修改在那里消除了这一攻击，并不表明它不会引入其他问题。修改后的模型：`records/fixes/0079-fix-succ-ind.pv`。

B.2 AKA 长期密钥使攻击者可以冒充任一方

类型	协议规范本身的弱点
文稿出处	rfc9678:1005, main:1131
价值	中
涉及的性质	A03, A08, A08.12 （见第 3 节）
依据	ProVerif attack queries `a03_peer_chal_ltk`, `a03_server_resp_ltk`, `a08_chal1_ltk`

发生了什么。 持有 AKA 长期密钥的攻击者可以针对任意 RAND 计算 AUTN MAC 和 AT_MAC，从而向对等方伪造 Challenge；它也能计算 AT_RES 和 AT_MAC，在没有对等方的情况下与服务器完成交换。在伪造的运行中，攻击者使用自己的 KEM 公钥，因此也获知会话密钥。

攻击者需要什么。 攻击者持有长期密钥 K（从而对任意 RAND 可得到 CK' 和 IK'），并位于其所攻击运行的路径上。

攻击者能得到什么。 在该次运行中，可以完全冒充网络面对对等方，或冒充对等方面对服务器，且会话密钥为攻击者所知。真实双方完成的此前和此后运行仍受保护，前向保密的结果表明了这一点。

拟议修改。 无。本协议的任何消息、校验或派生修改都无法消除它：长期密钥就是 AKA 凭据，AUTN 和 AT_MAC 按其定义即由它计算得出。唯一可用的缓解是要求 PQ KEM 的本地策略，已作为 R05 提出，因此未测试任何协议修改。

附录 C：主张和证明器的答案

证明器对每个目标的记录：达到的等级、达到该等级的查询、是否检查了对照查询，以及各攻击及分析者对其的判定。

目标	级别	界	查询	对照	攻击	主张
A03	proved		a03_peer_chal	checked	a03_peer_fin (holds_in_source); a03_peer_chal_ltk (holds_in_source); a03_server_resp_ltk (holds_in_source)	2 proved, 3 attack
A04	proved		a04_server_inj	checked	a04_peer_inj (model_artifact)	1 proved, 1 bounded, 1 attack
K01	proved		k01_msk	checked		3 proved
C01	proved		k01_kp	checked		1 proved
R05	proved		r05_peer	checked		3 proved
A08	proved		a08_chal1	checked	a08_chal1_ltk (holds_in_source); a03_peer_chal_ltk (holds_in_source)	2 proved, 2 attack
D01	proved		a03_server_resp	checked		3 proved
R02	proved		a04_server_inj	checked		1 proved, 1 bounded
R01	bounded	变化的值展开到 2 步	a04_peer_inj	checked	a04_peer_inj (model_artifact)	1 bounded, 1 attack
A06	proved		a03_server_resp	checked	a03_peer_fin (holds_in_source)	1 proved, 1 attack
K01.11	proved		k01_msk	checked		2 proved
A08.12	proved		a08_chal1	checked	a08_chal1_ltk (holds_in_source); a03_peer_chal_ltk (holds_in_source)	2 proved, 2 attack
R05.13	proved		r05_peer	checked		4 proved
X01	proved		a03_server_resp	checked		1 proved
X02	proved		k01_future	checked		1 proved

逐条主张，按分析者对每条主张的措辞；每条的回答来自证明器：

目标	主张	攻击者	回答	查询	对照
A03	对端完成（EAP-Success）意味着服务器完成，且 MK_PQ_SHARED_SECRET 相同（攻击者在网络上）。	`network`	attack (holds_in_source)	a03_peer_fin	
A03	在持有 AKA 长期密钥的攻击者下，对端接受的挑战对应一次服务器发送，且取值相同。	`ltk_holder`	attack (holds_in_source)	a03_peer_chal_ltk（a03_peer_chal 的对照）	
A03	在持有 AKA 长期密钥的攻击者下，服务器完成对应一次真实的、取值相同的对端响应。	`ltk_holder`	attack (holds_in_source)	a03_server_resp_ltk（a03_server_resp 的对照）	

目标	主张	攻击者	回答	查询	对照
A03	对端只在服务器发送携带相同身份、RAND、AT_KDF_FS 列表和 AT_PUB_KEM 时接受挑战（攻击者在网络上）。	network	proved	a03_peer_chal	checked
A03	服务器只在一次具有相同 AT_RES、AT_KEM_CT、AT_PUB_KEM 和 MK_PQ_SHARED_SECRET 的对端运行下接受响应（攻击者在网络上）。	network	proved	a03_server_resp	checked
A04	对端不会两次接受同一个挑战实例（攻击者在网络上）。	network	attack (model_artifact)	a04_peer_inj	
A04	对端不会两次接受同一个挑战实例：对端保留已接受的 SQN，并拒绝不大于它的值（攻击者在网络上）。	network	bounded（变化的值展开到 2 步）	a04_peer_inj	checked
A04	服务器不会两次接受同一个响应实例；每个服务器成功对应一次不同的对端响应（攻击者在网络上）。	network	proved	a04_server_inj	checked
K01	攻击者无法从一次已完成的运行推导出 MSK。	network	proved	k01_msk	checked
K01	即使 AKA 长期密钥泄漏，攻击者也无法从记录的交换中推导出一次已完成运行的 MK_PQ_SHARED_SECRET。	ltk_after_session	proved	k01_kp	checked
K01	攻击者无法从一次已完成的运行推导出 EMSK。	network	proved	k01_emsk	checked
C01	在 AKA 长期密钥泄漏后，一次已完成运行的 MK_PQ_SHARED_SECRET 以及 MSK/EMSK 仍保持机密。	ltk_after_session	proved	k01_kp	checked
R05	对端只有在已协商出 ML-KEM 值之后才接受挑战。	network	proved	r05_peer	checked
R05	服务器只有在对端选定了 ML-KEM 值之后才完成。	ltk_holder	proved	r05_server	checked
R05	在持有长期密钥的攻击者下，不存在未协商 ML-KEM 却认证成功的运行。	ltk_holder	proved	r05_peer	checked
A08	在持有长期密钥的攻击者下，对端接受的列表、身份和 RAND 是一次 AT_MAC 下的服务器发送。	ltk_holder	attack (holds_in_source)	a08_chal1_ltk（a08_chal1 的对照）	
A08	在持有长期密钥的攻击者下，对端接受的列表、身份、RAND 和 AT_PUB_KEM 是一次 AT_MAC 下的服务器发送。	ltk_holder	attack (holds_in_source)	a03_peer_chal_ltk（a03_peer_chal 的对照）	
A08	对端接受的 AT_KDF_FS 列表、身份和 RAND 是服务器的 AT_MAC 保护值。	network	proved	a08_chal1	checked
A08	对端接受的 AT_KDF_FS 列表、身份、RAND 和 AT_PUB_KEM 是服务器的 AT_MAC 保护值。	network	proved	a03_peer_chal	checked
D01	对端或服务器接受的每一条 AT_MAC 保护的挑战和响应，都对应另一方一次内容相同的真实发送（分片属性未建模）。	network	proved	a03_server_resp	checked
D01	对端接受的每一条 AT_MAC 保护的挑战，都对应一次内容相同的真实服务器发送。	network	proved	a08_chal1	checked

目标	主张	攻击者	回答	查询	对照
D01	对端接受的每一条 AT_MAC 保护的最终挑战，都对应一次内容相同的真实服务器发送。	network	proved	a03_peer_chal	checked
R02	在一次认证中，一个挑战实例至多被接受一次；重复传输会被拒绝（攻击者在网络上）。	network	bounded（变化的值展开到 2 步）	a04_peer_inj	checked
R02	服务器至多接受一次同一个响应实例。	network	proved	a04_server_inj	checked
R01	旧 AUTN 不会被当作新的认证接受：对端保留最后接受的 SQN，并拒绝不大于它的值。	network	bounded（变化的值展开到 2 步）	a04_peer_inj	checked
R01	旧 AUTN 或旧 KEM 值不会被当作新的认证接受。	network	attack (model_artifact)	a04_peer_inj	
A06	对端有协议证据表明服务器完成了该运行并推导出相同的密钥。	network	attack (holds_in_source)	a03_peer_fin	
A06	服务器有协议证据表明对端推导出相同的 MK_PQ_SHARED_SECRET：AT_RES 和 AT_MAC 绑定了对端的响应。	network	proved	a03_server_resp	checked
K01.11	攻击者无法推导出 MSK，且对端与服务器就该运行的 MK_PQ_SHARED_SECRET 达成一致。	network	proved	k01_msk	checked
K01.11	服务器接受的 AT_RES、AT_KEM_CT、AT_PUB_KEM 和 MK_PQ_SHARED_SECRET 就是对端的（密钥协商）。	network	proved	a03_server_resp	checked
A08.12	在持有长期密钥的攻击者下，接受的列表和挑战值是服务器的 AT_MAC 保护值。	ltk_holder	attack (holds_in_source)	a08_chal1_ltk（a08_chal1 的对照）	
A08.12	在持有长期密钥的攻击者下，接受的列表和 AT_PUB_KEM 是服务器的 AT_MAC 保护值。	ltk_holder	attack (holds_in_source)	a03_peer_chal_ltk（a03_peer_chal 的对照）	
A08.12	接受的 AT_KDF_FS 列表、身份、网络名称和挑战值是服务器的 AT_MAC 保护值。	network	proved	a08_chal1	checked
A08.12	接受的 AT_KDF_FS 列表、身份和挑战值（含 AT_PUB_KEM）是服务器的 AT_MAC 保护值。	network	proved	a03_peer_chal	checked
R05.13	在强制 PQ KEM 策略下，对端只有在 ML-KEM 已协商后才接受挑战。	network	proved	r05_peer	checked
R05.13	在强制 PQ KEM 策略下，服务器只有在 ML-KEM 已协商后才完成。	network	proved	r05_server	checked
R05.13	在持有长期密钥的攻击者和强制 PQ KEM 策略下，重放和降级都不能让对端在没有 ML-KEM 的情况下接受。	ltk_holder	proved	r05_peer	checked
R05.13	在持有长期密钥的攻击者和强制 PQ KEM 策略下，重放和降级都不能让服务器在没有 ML-KEM 的情况下完成。	ltk_holder	proved	r05_server	checked

目标	主张	攻击者	回答	查询	对照
X01	当对端和服务器以相同的 MK_PQ_SHARED_SECRET 完成时，它们对 AT_KEM_CT 和 AT_PUB_KEM 的取值一致。	`network`	proved	a03_server_resp	checked
X02	长期密钥泄漏后，持有该密钥的攻击者无法推导出真实对端和真实服务器都完成的后续会话的 MK_PQ_SHARED_SECRET。	`ltk_after_session`	proved	k01_future	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，并将每条性质交给 ProVerif；第 3 节中的每个结果都是证明器的回答。

ProVerif+ Agent 会话 session-20261114T214415，2026-11-14。状态：已完成。模型：deepseek-v4-1-flash-261017。步数：81，证明器 29 秒，实际耗时 17 分钟，成本 0.205 USD。

背景：宿主从对话中删除了过时部分 1 次，共 396579 个字符（先前的推理，以及模型在最近一次修改前看到的内容）。轨迹文件保留全部内容。

ProVerif：运行了 108 个证明，107 个已判定，1 个无答案，12 秒，记录了 66 个答案。

分析了什么

协议	PQ EAP-AKA prime full authentication
版本	draft-ietf-emu-pqc-eapaka-05
分析范围	固定 ML-KEM-768、一次完整非重认证流程与新鲜 AKA vector；AKA 算法和 KEM 理想化，可信 AAA 与运营商密钥为假设。模型包含 AT_MAC、KDF 列表检查、AUTN freshness、成功条件；分片的顺序/总长/MAC 必须抽象保留或明确未覆盖，不能凭无分片模型证明分片安全。
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	348 个编号原文单元（82641 字节），来自下列章节。本报告中的 s0001 这样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	6	PQ KEM Enhancements by Design
main	7	Message Fragmentation and Reassembly
main	7.1	Fragmentation Attribute
main	7.2	Fragmentation Procedure
main	7.3	Correlating Fragments and Acknowledgments
main	7.4	Reassembly
main	7.5	Fragment Ordering and Flow Control
main	7.6	Applicability
main	8	Protocol Construction
main	8.1	Protocol Call Flow
main	8.2	Key Steps in protocol construction
main	9	Extensions to EAP-AKA' FS
main	9.1	AT_PUB_KEM
main	9.2	AT_KEM_CT
main	9.3	AT_KDF_FS

文稿	章节	标题
main	10	Capability Negotiation
main	12	Security Considerations
main	12.1	Selecting ML-KEM Variants
rfc9048	3	EAP-AKA'
rfc9048	3.1	AT_KDF_INPUT
rfc9048	3.2	AT_KDF
rfc9048	3.3	Key Derivation
rfc9048	3.4	Hash Functions
rfc9048	3.4.1	PRF'
rfc9048	3.4.2	AT_MAC
rfc9048	3.4.3	AT_CHECKCODE
rfc9048	3.5	Summary of Attributes for EAP-AKA'
rfc9678	6	Extensions to EAP-AKA'
rfc9678	6.1	AT_PUB_ECDHE
rfc9678	6.2	AT_KDF_FS
rfc9678	6.3	Forward Secrecy Key Derivation Functions
rfc9678	6.4	ECDHE Groups
rfc9678	6.5	Message Processing
rfc9678	6.5.1	EAP-Request/AKA'-Identity
rfc9678	6.5.2	EAP-Response/AKA'-Identity
rfc9678	6.5.3	EAP-Request/AKA'-Challenge
rfc9678	6.5.4	EAP-Response/AKA'-Challenge
rfc9678	6.5.5	EAP-Request/AKA'-Reauthentication
rfc9678	6.5.6	EAP-Response/AKA'-Reauthentication
rfc9678	6.5.7	EAP-Response/AKA'-Synchronization-Failure
rfc9678	6.5.8	EAP-Response/AKA'-Authentication-Reject
rfc9678	6.5.9	EAP-Response/AKA'-Client-Error
rfc9678	6.5.10	EAP-Request/AKA'-Notification
rfc9678	6.5.11	EAP-Response/AKA'-Notification

源文步骤在文稿中定位的协议目的：固定 ML-KEM-768、一次完整非重认证流程与新鲜 AKA vector；AKA 算法和 KEM 理想化，可信 AAA 与运营商密钥为假设。模型包含 AT_MAC、KDF 列表检查、AUTN freshness、成功条件；分片的顺序/总长/MAC 必须抽象保留或明确未覆盖，不能凭无分片模型证明分片安全。

对照文稿定性质

在编写查询之前，分析者将草拟的性质清单与文稿自身对协议目的的表述进行对照。名称、性质所涉及的对象以及文稿的说法都是分析者的解读；所引用的位置确实存在于文稿中。

ID	简称	对象	文稿怎么说	出处
A03	对等方与EAP服务器的双向认证	对等方确信自己在与其归属运营商的 EAP 服务器通信，服务器确信对等方的身份；双方为协商的 ML-KEM 运行导出相同的 MSK/EMSK	rfc9048 第 7 节声称 EAP-AKA' 具有双向认证；流程中对等方验证 AT_AUTN/AT_MAC，服务器检查 AT_RES/AT_MAC，两者都通过才算成功（s0088、s0091）	rfc9048:1170, s0088, s0091
A04	挑战交换的重放保护	对等方每次接受都对应一次新鲜的服务器挑战运行，服务器每次成功都对应一次新鲜的对等方响应；旧消息不能产生新的成功	rfc9048 第 7 节作出重放保护主张；rfc4187 第 12.6 节说完整认证的重放保护来自 RAND 和 AUTN	rfc9048:1183, rfc4187:3707, s0091
K01	会话密钥的保密性与前向保密	MSK、EMSK 和 MK_PQ_SHARED_SECRET 对网络攻击者保密，并且在攻击者在运行后获得 AKA 长期密钥的情况下也保密	s0091：仅泄露 AKA 长期密钥不足以让攻击者从先前录制的交换中导出 MK_PQ_SHARED_SECRET；s0107 给出了推导过程	s0091, s0107
C01	已完成会话的前向保密	已完成运行的 MK_PQ_SHARED_SECRET 和 MSK/EMSK 对之后获得 AKA 长期密钥的攻击者保密	rfc9678 第 7 节：录制了认证运行并在之后获得 AKA 长期密钥的人无法重建会话密钥；s0091 对 MK_PQ_SHARED_SECRET 有相同表述	rfc9678:929, s0091, s0158
R05	强制PQ KEM抵抗降级	当对等方或服务器要求 PQ KEM 时，若未协商出 ML-KEM 值，任何认证都不能完成	s0153：要求 PQ KEM 的服务器或对等方若找不到 PQ KEM，必须视同认证失败；s0159：需要防护移除提议的部署必须通过本地策略要求 PQ KEM	s0153, s0159
A08	AT_MAC绑定KDF列表、身份和RAND	对等方接受的 AT_KDF_FS 列表、身份、网络名称、RAND/AUTN 和 AT_PUB_KEM 就是服务器在 AT_MAC 下发送的值	s0159：AT_MAC 保护 AT_KDF_FS 提议和对等方的选择；rfc9678 第 6.2 节：对等方必须检查所请求的变更（且仅有该变更）已发生（s0289）	rfc9678:989, s0159, s0289, s0152
D01	AT_MAC保护消息的完整性	对等方或服务器接受的每条受 AT_MAC 保护的消息都对应允许的发送方以相同内容进行的真实发送	rfc9048 第 7 节对 EAP 数据包作出完整性保护主张；s0061/s0062 说分片消息的 AT_MAC 覆盖所有分片，且数据仅在 AT_MAC 验证后才被处理	rfc9048:1175, s0061, s0062
R02	消息实例至多被接受一次	一次认证中，挑战或响应实例至多被接受一次；重复或重排的传输会中止，而不是被处理两次	s0014 和 s0042（一次分片交换，锁步），s0047 和 s0056（重传复用 Identifier），s0060（顺序不一致会中止交换）	s0014, s0042, s0047, s0056, s0060
R01	当前运行的AUTN与KEM值	对等方接受的 AUTN 和 AT_PUB_KEM 属于当前运行；旧的 AUTN 或旧的 KEM 值不会被当作新的认证接受	s0099（USIM 验证 AUTN），s0125/s0141（每次运行生成新鲜值），rfc4187 第 12.6 节（完整认证的重放保护来自 RAND 和 AUTN）	rfc4187:3707, s0085, s0099, s0125, s0141
A06	对等方与服务器之间的密钥确认	双方在各自的确认点都有协议证据表明对方导出了相同的会话密钥	rfc9048 第 7 节指出 AKA 本可从密钥确认中受益；AT_RES/AT_MAC 为服务器提供关于对等方的证据，而对等方唯一的完成信号是 EAP-Success，rfc4187 第 12.6 节说它不受完整性保护	rfc9048:1402, rfc4187:3724, s0091

ID	简称	对象	文稿怎么说	出处
K01.11	MSK保密性与对等方-服务器一致性	MSK 对网络攻击者保密，且对等方与服务器为一次运行导出相同的 MSK（用户问题 Q1）	用户问题 Q1；s0107 从 MK_PQ_SHARED_SECRET 定义 MSK，s0091 说密钥基于 CK、IK 和 PQ KEM 共享秘密	s0107, s0091
A08.12	已接受挑战值的AT_MAC绑定	已接受的 AT_KDF_FS 列表、身份、网络名称和挑战值都是服务器受 AT_MAC 保护的值（用户问题 Q2）	用户问题 Q2；s0289 和 s0159	s0289, s0159, s0186
R05.13	强制PQ策略下无降级	在策略要求 PQ KEM 的情况下，重放和降级都不能使认证在缺少 ML-KEM 时成功（用户问题 Q3）	用户问题 Q3；s0153、s0159	s0153, s0159, s0289
X01	密钥与密文及KEM密钥的绑定	MK_PQ_SHARED_SECRET、AT_KEM_CT、AT_PUB_KEM	s0161：PRF' 将共享秘密绑定到密文（MAL-BIND-K-CT），ML-KEM 将其绑定到公钥（MAL-BIND-K-PK）	main:1144
X02	未来会话的前向保密	后续会话的 MSK、EMSK、MK_PQ_SHARED_SECRET	rfc9678 第 7 节：即使长期密钥已泄露，只要攻击者未成为运行的主动参与方，所有未来会话仍提供前向保密	rfc9678:935

分析者依据文稿补充的性质：X01、X02。

文稿里的安全表述，逐段去向

宿主把文稿里说明协议保护什么、防什么的章节逐段列出，共 260 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 90 段，没选 170 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	main:1121-1123	证明器问不了	随机数生成器的质量属于实现层面的性质，而非迹性质
P002	main:1125-1129	C01, K01, `ltk_after_session`	
P003	main:1131-1136	A08, R05, `ltk_holder`	
P004	main:1138-1142	证明器问不了	本地配置的最大重组长度以及它所约束的 DoS 代价属于资源问题，超出迹模型的范围
P005	main:1144-1149	X01	
P006 至 P007	main:1158-1162	没有陈述目标	版面附属内容
P008	main:1167-1171	证明器问不了	IND-CCA2 安全性和参数集的选择属于计算性主张
P009 至 P010	rfc3748:2182-2190	没有陈述目标	关于 EAP 威胁模型的一般性陈述
P011 至 P012	rfc3748:2194-2203	`network`	
P013	rfc3748:2205-2206	不在范围内	发现用户身份涉及身份交换和隐私友好标识符，而本流程将其作为固定值携带
P014	rfc3748:2208-2208	D01, A08	

段落	出处	定为	不选的原因
P015	rfc3748:2210-2213	A04, A06	
P016	rfc3748:2215-2216	没有陈述目标	该协议不使用口令短语，因此不存在字典攻击
P017	rfc3748:2218-2219	A03	
P018	rfc3748:2221-2222	R05	
P019	rfc3748:2224-2225	K01	
P020	rfc3748:2233-2234	不在范围内	EAP 会话之后使用的密码套件不在所建模的流程之内
P021	rfc3748:2236-2238	R05	
P022	rfc3748:2240-2244	A08	
P023	rfc3748:2246-2252	没有陈述目标	关于攻击可能是远程的观察；只给出了网络攻击者
P024 至 P025	rfc3748:2256-2261	没有陈述目标	要求各方法声明其主张
P026	rfc3748:2263-2271	A03, A04, D01, K01	
P027	rfc3748:2273-2276	证明器问不了	以比特计的密钥强度属于计算性估计
P028	rfc3748:2286-2294	证明器问不了	以比特计的密钥强度的定义
P029	rfc3748:2296-2299	证明器问不了	关于密钥强度定义的说明
P030	rfc3748:2301-2308	证明器问不了	密钥强度对算法的依赖
P031	rfc3748:2310-2313	K01	
P032	rfc3748:2315-2317	没有陈述目标	要求各方法说明其不作哪些主张
P033	rfc3748:2321-2322	没有陈述目标	主张术语的介绍
P034	rfc3748:2324-2328	A08, R05	
P035	rfc3748:2339-2344	A03	
P036	rfc3748:2346-2351	D01	
P037	rfc3748:2353-2355	A04, R01, R02	
P038 至 P039	rfc3748:2357-2368	K01	

段落	出处	定为	不选的原因
P040	rfc3748:2370-2374	证明器问不了	以比特计的密钥强度
P041	rfc3748:2376-2383	没有陈述目标	不使用口令或其他低熵秘密
P042	rfc3748:2392-2396	不在范围内	快速重认证不属于所建模的完整认证
P043	rfc3748:2398-2405	不在范围内	密码绑定是隧道化 EAP 方法的性质，而非 EAP-AKA' 本身的性质
P044	rfc3748:2407-2411	C01	
P045	rfc3748:2413-2417	R02, D01	
P046	rfc3748:2419-2423	不在范围内	与下层标识符的信道绑定不属于所建模的流程
P047	rfc3748:2425-2427	没有陈述目标	说明主张列表并非穷尽
P048	rfc3748:2431-2434	不在范围内	身份交换能否省略涉及身份交换，而非挑战交换
P049	rfc3748:2436-2439	不在范围内	身份中 realm 部分的转发未被建模
P050	rfc3748:2445-2449	A08	
P051	rfc3748:2451-2455	没有陈述目标	建议使用已认证的身份进行访问决策
P052	rfc3748:2459-2461	不在范围内	通过 EAP 隧道的中间人不在所建模的方法之内
P053 至 P054	rfc3748:2463-2481	不在范围内	EAP 方法序列以及通过隧道的恶意认证者不在所建模的方法之内
P055 至 P059	rfc3748:2483-2502	没有陈述目标	针对隧道化部署的缓解措施，而非本协议的性质
P060	rfc3748:2506-2508	D01	
P061	rfc3748:2510-2514	A04, R02	
P062 至 P064	rfc3748:2516-2531	D01	
P065	rfc3748:2533-2536	不在范围内	Identity、Notification 和 Nak 消息的覆盖未被建模（AT_CHECKCODE 为可选，且不在所建模的流程中）
P066	rfc3748:2538-2542	不在范围内	隧道保护不在所建模的方法之内
P067 至 P068	rfc3748:2551-2562	D01	
P069	rfc3748:2564-2567	A08, R02	
P070 至 P072	rfc3748:2571-2587	没有陈述目标	AKA 中不使用口令或口令短语

段落	出处	定为	不选的原因
P073 至 P075	rfc3748:2591-2611	A03	
P076 至 P077	rfc3748:2615-2629	R05	
P078 至 P079	rfc3748:2633-2643	没有陈述目标	关于下层的实现说明
P080	rfc3748:2645-2651	不在范围内	实现的的重试计数器，而非协议消息
P081	rfc3748:2659-2665	K01	
P082	rfc3748:2667-2671	不在范围内	其他协议对 MSK/EMSK 的使用不在本方法之内
P083	rfc3748:2673-2677	不在范围内	AAA-Key 派生不在本方法之内
P084	rfc3748:2679-2682	K01	
P085 至 P086	rfc3748:2684-2693	不在范围内	密钥材料的导出和介质无关性，而非本流程的迹性质
P087	rfc3748:2695-2699	R05	
P088 至 P089	rfc3748:2701-2713	证明器问不了	以比特计的有效密钥强度
P090 至 P091	rfc3748:2715-2729	K01	
P092	rfc3748:2731-2735	不在范围内	关于 EMSK 使用方式的规则不在所建模的流程之内
P093	rfc3748:2737-2740	不在范围内	密钥生命周期处理不在所建模的流程之内
P094 至 P095	rfc3748:2742-2752	没有陈述目标	关于如何设计密钥派生的建议，非本协议的性质
P096 至 P099	rfc3748:2765-2789	不在范围内	EAP 会话之后的密码套件和数据保护不在所建模的流程之内
P100 至 P105	rfc3748:2793-2828	不在范围内	链路层指示（PPP、IEEE 802.1X、802.11）不在所建模的方法之内
P106 至 P107	rfc3748:2832-2842	没有陈述目标	关于认证者与后端服务器分工的描述；模型假定 AD 可信
P108	rfc3748:2844-2847	A03	
P109	rfc3748:2849-2855	不在范围内	AAA 协议的逐包保护不在所建模的方法之内
P110 至 P112	rfc3748:2857-2880	不在范围内	EAP 之后的安全关联和 AAA-Key 传输不在所建模的流程之内
P113 至 P115	rfc3748:2884-2898	没有陈述目标	未定义明文口令认证
P116 至 P122	rfc3748:2902-2945	不在范围内	与 NAS 标识符的信道绑定不在所建模的流程之内

段落	出处	定为	不选的原因
P123 至 P124	rfc3748:2949-2963	A06	
P125	rfc3748:2965-2969	没有陈述目标	关于针对恶意认证者不要求受保护的结果指示的陈述
P126	rfc3748:2975-2983	A06	
P127	rfc3748:2985-2989	不在范围内	空闲超时和资源释放属于资源问题
P128	rfc3748:2991-2997	A06	
P129 至 P132	rfc3748:2999-3030	没有陈述目标	关于如何发送结果指示的指导
P133 至 P134	rfc3748:3032-3046	A06	
P135	rfc3748:3048-3056	没有陈述目标	关于 EAP-TLS 的示例
P136	rfc4187:3594-3597	没有陈述目标	EAP-AKA 安全考虑的引言
P137 至 P138	rfc4187:3608-3629	不在范围内	EAP-AKA 中的身份保护依赖假名和身份交换，而所建模的流程将其作为固定值携带
P139 至 P140	rfc4187:3633-3641	A03	
P141	rfc4187:3643-3646	不在范围内	与认证者的信道绑定不在所建模的方法之内
P142	rfc4187:3650-3659	证明器问不了	淹没认证中心属于资源问题
P143	rfc4187:3663-3664	证明器问不了	以比特计的有效密钥强度
P144	rfc4187:3666-3672	K01	
P145	rfc4187:3676-3680	没有陈述目标	AKA 不是口令协议，因此字典攻击不适用
P146	rfc4187:3684-3689	D01, A04	
P147	rfc4187:3691-3694	D01	
P148	rfc4187:3696-3701	K01	
P149	rfc4187:3707-3713	A04, R01	
P150	rfc4187:3715-3719	不在范围内	快速重认证未被建模
P151	rfc4187:3721-3722	A08	
P152 至 P154	rfc4187:3724-3740	A06	

段落	出处	定为	不选的原因
P155 至 P157	rfc4187:3744-3757	R05	
P158 至 P159	rfc4187:3761-3777	A06	
P160 至 P161	rfc4187:3781-3799	不在范围内	通过隧道协议的中间人攻击不在所建模的方法之内
P162	rfc4187:3808-3811	证明器问不了	随机数生成器的质量
P163	rfc9048:1131-1136	没有陈述目标	EAP-AKA' 性质的介绍
P164	rfc9048:1138-1139	没有陈述目标	性质列表的范围陈述
P165	rfc9048:1141-1152	A08, R05	
P166	rfc9048:1154-1160	不在范围内	从 EAP-AKA' 降级到 EAP-AKA 属于 EAP 方法的选择，不在本方法的协商之内
P167	rfc9048:1162-1168	没有陈述目标	对未来扩展的展望
P168	rfc9048:1170-1173	A03	
P169	rfc9048:1175-1181	D01	
P170	rfc9048:1183-1186	A04, R01, R02	
P171 至 P173	rfc9048:1188-1206	K01	
P174	rfc9048:1208-1210	K01, C01	
P175	rfc9048:1212-1213	没有陈述目标	PRF 构造的描述
P176	rfc9048:1215-1216	证明器问不了	以比特计的密钥强度
P177	rfc9048:1218-1221	没有陈述目标	不使用口令
P178	rfc9048:1223-1228	证明器问不了	以比特计的密钥强度
P179 至 P181	rfc9048:1230-1247	不在范围内	快速重连不属于所建模的完整认证
P182 至 P183	rfc9048:1249-1260	C01	
P184 至 P197	rfc9048:1264-1344	不在范围内	身份隐私依赖 SUCI 或假名以及身份交换，而所建模的流程将其作为固定标识符携带
P198	rfc9048:1348-1351	没有陈述目标	关于未发现针对原始信任模型的攻击的陈述
P199	rfc9048:1353-1356	没有陈述目标	关于攻击需要不同信任模型的陈述

段落	出处	定为	不选的原因
P200 至 P201	rfc9048:1358-1380	不在范围内	服务网络误用密钥的内部攻击不在所建模的信任假设（可信 AAA 和运营商）之内
P202	rfc9048:1382-1391	没有陈述目标	运营商之间的流量隧道，非本方法的性质
P203	rfc9048:1393-1400	证明器问不了	耗尽序列号空间属于资源问题
P204	rfc9048:1402-1404	不在范围内	不带会话密钥的 AKA 和 HTTP Digest AKAv1 不在本流程之内
P205	rfc9048:1406-1411	A06	
P206	rfc9048:1413-1418	没有陈述目标	关于长期密钥泄露的报告；攻击者以 ltk_after_session 录入
P207	rfc9048:1420-1433	不在范围内	基于重同步的订户检测不在所建模的完整认证之内
P208	rfc9048:1435-1442	不在范围内	SQN 重同步和密钥流重用不在所建模的流程之内
P209	rfc9048:1444-1448	不在范围内	寻呼协议攻击不在 AKA 之内
P210 至 P211	rfc9048:1452-1458	没有陈述目标	关于普遍监控的一般性考虑
P212 至 P213	rfc9048:1460-1472	没有陈述目标	密钥材料的运行保护
P214	rfc9048:1474-1482	C01, `ltk_after_session`	
P215 至 P216	rfc9048:1486-1515	A08	
P217	rfc9048:1517-1526	A08, `ltk_holder`	
P218	rfc9048:1528-1537	没有陈述目标	如何为接入网分配名称
P219	rfc9678:868-870	没有陈述目标	本节的范围陈述
P220	rfc9678:872-882	没有陈述目标	关于密钥泄露风险的描述
P221	rfc9678:884-888	没有陈述目标	关于缺失前向保密后果的描述
P222 至 P223	rfc9678:890-894	没有陈述目标	对已记录流量和未来流量的后果
P224	rfc9678:896-898	没有陈述目标	路径上攻击的列举
P225 至 P226	rfc9678:900-924	没有陈述目标	建议强制要求前向保密
P227	rfc9678:926-933	C01, K01, `ltk_after_session`	
P228	rfc9678:935-937	X02, `ltk_after_session`	
P229	rfc9678:939-943	A03, A08, `ltk_holder`	
P230	rfc9678:945-954	没有陈述目标	关于重新运行交换以保护另一方向的描述

段落	出处	定为	不选的原因
P231 至 P233	rfc9678:958-973	没有陈述目标	关于销毁临时密钥和密钥传输的部署指导
P234	rfc9678:977-978	没有陈述目标	本节的范围陈述
P235 至 P236	rfc9678:980-986	A08, R05	
P237 至 P238	rfc9678:988-1003	A08, R05, `ltk_holder`	
P239 至 P240	rfc9678:1005-1025	R05	
P241 至 P242	rfc9678:1027-1046	K01, C01, `ltk_after_session`	
P243 至 P249	rfc9678:1050-1096	证明器问不了	拒绝服务和计算代价属于资源问题
P250	rfc9678:1100-1102	不在范围内	身份隐私依赖隐私友好身份机制，不在所建模的流程之内
P251 至 P252	rfc9678:1106-1115	不在范围内	流量分析和跟踪属于隐私性质，不在所建模的流程之内
P253 至 P255	rfc9678:1119-1136	不在范围内	AT_ENCR 内重认证假名的隐私不在所建模的流程之内
P256 至 P258	rfc9678:1140-1161	证明器问不了	量子计算假设
P259	rfc9678:1163-1170	证明器问不了	对称算法的抗量子性
P260	rfc9678:1172-1184	证明器问不了	量子威胁对前向保密的影响

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 12 条，没检查 20 条。“文稿没有提到”不能作为不检查的原因。

条目	目录里的性质	作为哪条性质检查	不检查的原因
K02	载荷与端到端保密性	不在范围内	使用 MSK 的协议的端到端载荷保密性不在本方法的范围内
K03	强保密／秘密值不可区分性	不在范围内	本方法的主张是密钥派生和密钥的保密性，而不是允许值的不可区分性；rfc3748 第 7.2.1 节并未主张这一点
K04	密钥用途、方向与会话分离	K01	
A01	对端曾参与性（Aliveness）	A03	
A02	弱一致性认证	A03	
A05	隐式密钥认证	A03, K01	
A07	身份—凭据—密钥绑定	A08	
R03	业务操作至多一次	不适用	EAP-AKA' 不执行任何可计费或改变状态的业务操作
R04	消息接受顺序／窗口安全	R02	
C02	抗密钥泄露冒充（KCI）	A08	

条目	目录里的性质	作为哪条性质检查	不检查的原因
C03	已知密钥安全／泄露隔离	C01	
C04	临时秘密／部分状态泄露韧性	C01	
C05	泄露后安全恢复（PCS）	X02	
C06	注册凭据泄露后的增强认证	不适用	EAP-AKA' 中不存在注册记录或注册秘密
C07	抗离线字典攻击	不适用	AKA 使用长期密钥而非口令；rfc4187 第 12.5 节说明 EAP-AKA 不易受字典攻击
C08	指定原语失效下的目标保持	证明器问不了	原语失效属于计算假设
Z01	授权执行正确性	不适用	EAP-AKA' 不携带授权令牌、委托、撤销或租户模型
Z02	委托权限不扩张	不适用	EAP-AKA' 不携带授权令牌、委托、撤销或租户模型
Z03	授权与身份／会话／操作绑定	不适用	EAP-AKA' 不携带授权令牌、委托、撤销或租户模型
Z04	撤销与过期生效	不适用	EAP-AKA' 不携带授权令牌、委托、撤销或租户模型
Z05	跨租户／跨服务安全隔离	不适用	EAP-AKA' 不携带授权令牌、委托、撤销或租户模型
S01	加密 nonce 唯一性	不适用	建模流程中不使用基于 nonce 的加密原语
S02	重传／密钥重安装安全	R02	
S03	抗回滚与状态单调性	R01	
S04	跨阶段安全上下文一致性	不在范围内	重新认证和重连阶段不在所建模的完整认证范围内
S05	终止与旧状态失效	不适用	所建模的流程以 EAP-Success 结束，没有拆除状态
P01	身份匿名性	不在范围内	身份隐私取决于 SUCI 或假名方案以及身份交换，而所建模的流程将其作为固定标识符携带
P02	会话不可关联性	不在范围内	不可关联性取决于所建模流程之外的假名生成
P03	用户／凭据存在性隐藏	不在范围内	隐藏用户是否存在涉及身份交换，不在所建模流程的范围内
V01	条件性进展／错误恢复	证明器问不了	进展性、无死锁和资源消耗不是 ProVerif 能判定的迹性质
V02	无非预期死锁	证明器问不了	进展性、无死锁和资源消耗不是 ProVerif 能判定的迹性质
V03	受限资源滥用／抗放大	证明器问不了	进展性、无死锁和资源消耗不是 ProVerif 能判定的迹性质

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 24 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 8 项，没设的 16 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	peer	参与方	`ltk_holder`	
S02	EAP server	参与方	`ltk_holder`	
S03	USIM	参与方	`ltk_after_session`	
S04	AD	参与方	`ltk_holder`	
S05	MSK	值	按定义全部失守	MSK 正是 K01 要防止攻击者获取的值；对于 MSK 已丢失的会话，不再主张其他性质
S06	EMSK	值	按定义全部失守	EMSK 是 K01 的保护值；其丢失后不再要求其他性质

ID	参与方或值	类别	攻击者条件	不设的原因
S07	MK_PQ_SHARED_SECRET	值	按定义全部失守	持有 MK_PQ_SHARED_SECRET 恰恰是 K01 所禁止的；在此条件下没有性质能成立
S08	K_aut	值	`ltk_holder`	
S09	K_encr	值	`ltk_holder`	
S10	K_re	值	`ltk_holder`	
S11	KEM 共享秘密 ss	值	按定义全部失守	持有某一会话的 ss 按定义就泄露了该会话的 MK_PQ_SHARED_SECRET；在此条件下不再要求其他性质
S12	AT_KDF_FS 列表	值	攻击者得不到更多	AT_KDF_FS 列表以明文携带
S13	AT_PUB_KEM	值	攻击者得不到更多	AT_PUB_KEM 是以明文发送的公钥
S14	AT_KEM_CT	值	攻击者得不到更多	AT_KEM_CT 以明文发送，在没有 sk 的情况下不泄露关于 ss 的任何信息
S15	AT_MAC	值	攻击者得不到更多	AT_MAC 值是公开的，且与具体会话相关
S16	AT_RES	值	攻击者得不到更多	AT_RES 是仅对其自身 RAND 有效的 AKA 响应值；其重放由重放主张覆盖
S17	AKA 长期密钥	值	`ltk_after_session`, `ltk_holder`	
S18	协商的 ML-KEM 参数	值	攻击者得不到更多	协商的 ML-KEM 参数是公开的
S19	AT_KDF_INPUT 网络名	值	攻击者得不到更多	网络名是按设计以明文发送的
S20	Identity	值	攻击者得不到更多	身份以明文携带；标识符的隐私不在所建模流程的范围内
S21	AT_RAND/AT_AUTN	值	攻击者得不到更多	RAND 和 AUTN 是公开值；旧的 AUTN 由 R01 覆盖
S22	AT_FRAGMENT 分片	值	攻击者得不到更多	分片是公开数据；其顺序和完整性由 R02 和 D01 要求
S23	EAP Identifier	值	攻击者得不到更多	EAP Identifier 是公开的八位组字段
S24	AUTN	值	攻击者得不到更多	AUTN 是公开的；旧 AUTN 的重放是新鲜性主张 R01

每条性质在各攻击者条件下的答案

攻击者是分析者在编写查询之前设定的；每个答案都是在其中某一个攻击者条件下记录的。单元格是证明器在该攻击者条件下对该性质的答案；“无答案”指为该性质设定了一个攻击者条件，但在该条件下证明器让某个主张处于未决状态，或者没有记录任何内容；空单元格指分析者没有为该性质设定该攻击者条件。

攻击者	持有什么	依据	出处
`network`	仅网络：它能读取、丢弃、修改和发送消息，不持有任何一方的秘密		
`ltk_after_session`	USIM 与运营商共享的 AKA 长期密钥 K（以及随之而来的任意 RAND 对应的 CK' 和 IK'）；在一次较早的认证运行之后获得，并用于针对已记录的较早运行和较晚的运行	s0091：仅泄露 AKA 长期密钥并不足以从已记录的交换中推导出 MK_PQ_SHARED_SECRET；s0158 指出跨会话复用密钥对会破坏前向保密；rfc9678 第 7 节讨论了获得长期密钥的攻击者	rfc9678:935, s0091, s0158
`ltk_holder`	认证之前或认证期间由路径上的主动攻击者持有的 AKA 长期密钥 K	s0159：持有长期密钥的攻击者仍可移除 ML-KEM 提议；rfc9678 第 7 节指出持有长期密钥的攻击者可以冒充任何一方，且必须位于路径上	rfc9678:1005, s0159

ID	network	ltk_after_session	ltk_holder
A03	不成立		不成立
A04	成立		
K01	成立	成立	
C01		成立	
R05	成立		成立
A08	成立		不成立
D01	成立		
R02	成立		
R01	成立		
A06	不成立		
K01.11	成立		
A08.12	成立		不成立
R05.13	成立		成立
X01	成立		
X02		成立	

原文和目标

来源：348 个原文单元，82641 字节，冻结于 source-delivery-01.json。 目标：已批准 10 个（A03, A04, K01, C01, R05, A08, D01, R02, R01, A06）；提出的问题：3 个。 目标清单已按草案事先获批，使用的是 --approve-targets。

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

- approve_package: 批准源文包 protocol-92a4b07b3f694b3fa7e5a5e8b766

本步骤自报：1 次请求（1 次失败），0.000 USD，输入 47699 个 token，输出 4814 个，27 秒。

关于证明器和模型的说明

- A04：在 ProVerif 中作答，分析者为该目标指定了 changing_state
- R02：在 ProVerif 中作答，分析者为该目标指定了 changing_state
- R01：在 ProVerif 中作答，分析者为该目标指定了 changing_state

对代数（xor、dh_algebra、other_algebra）做简化的 ProVerif 模型给攻击者的能力弱于真实运算：在该模型中证明成立，就是针对较弱攻击者的证明；在该模型中发现攻击，就是真实的攻击。省略对变化值（changing_state）检查的 ProVerif 模型让参与方接受更多：在该模型中证明成立，就是成立；在该模型中发现攻击，可能只是缺少了那项检查。Tamarin+ 对这些如实地建模。

以步数计的界是 bounded.pv 上的答案：这是分析者的第二个 ProVerif 模型，其中持有变化值的一方在保留其检查的前提下展开到该步数。该模型做的事少于协议本身，因此性质仅在这些步数内成立，不会更远；在该模型中发现的攻击就是攻击。步数是分析者的陈述。

分析者的状态审查

这一部分是分析者本人对原文的解读，不是证明器的答案。ProVerif 在“shown by ProVerif”一栏给出“yes”，表示 ProVerif 在展开模型中找到了包含这些步骤的迹，因此这些步骤是可能的；这些步骤是否破坏了某个目标，只由答案表中的“attack”一项说明，至于它们还付出了什么代价，则是分析者的解读。“nothing found”只说明查看了哪些模式，并不证明任何事情。

值	由谁保存	何时改变	何时检查	引用
AUTN 中的 SQN（USIM 用来判断新鲜性并进行比较的序列号）	对端背后的 USIM；归属网络（AD）在认证向量中生成该值	对端/USIM 接受一次认证后，用被接受的 SQN 替换已存储的值	当对端处理最终的 EAP-Request/AKA'-Challenge 并用 USIM 验证 AT_AUTN 时	s0085、s0099、s0088

模式	结果	目标	由 ProVerif 展示	步骤
replay	nothing found			在比较已到位的情况下，录制的挑战会被对端链的第二步拒绝：ProVerif 验证了没有任何挑战实例会被接受两次。没有比较时（对照 a04_peer_ctl），重放可以通过，因此该性质依赖这项检查。
repeat_one_time_action	nothing found			每次接受都会把保存的 SQN 推进到刚被接受的值，因此同一个向量无法被安装两次；排除重放的那项检查同样排除了这种情况。
desynchronisation	nothing found			攻击者可以先投递较晚的向量、再投递较早的向量，这会使对端存储的值变大，导致较早的向量失败；但攻击者不会因此获得任何密钥或认证结果，归属网络也总能签发新向量。使用 AUTS 的重新同步不在建模流程之内。
update_before_check	nothing found			在展开后的对端中，保存的值只有在 AT_MAC、列表、AUTN 和 SQN 检查全部通过后才会交给下一步；一旦失败，该步骤结束，值保持不变。
no_rollback_on_failure	nothing found			被拒绝的消息不会改变保存的 SQN；模型中不存在失败路径会推进或重置它。
race_between_sessions	nothing found			展开后的对端按顺序只保存一个值，因此 bounded.pv 中无法安排两个并发认证；同一个 USIM 的两个会话能否在存储的 SQN 上产生竞争，需要由能按真实方式对计数器建模的工具来处理（Tamarin+ Agent）。
distinguishable_failure	nothing found			模型中所有对端失败都是静默的：不发送任何答案，交换随即停止，因此失败答案不会告诉攻击者对端保存的是哪个值。
wrap_or_window	nothing found			展开后的 SQN 取三个连续值，不会回绕；AKA 接受窗口在此未建模（需由 Tamarin+ Agent 处理）。

分析者为目标所命名的内容：

步骤	目标	特征	原因
48	A04、R01、R02	changing_state	重放和至多一次主张依赖于 USIM 保存并与收到的 AUTN 比较的 AKA 序列号（s0085、s0099）：只有当 SQN 大于保存的值时，对端才接受挑战。model.pv 省略了这项比较；bounded.pv 将签发方和对端展开到两步，并保留了这项比较。
48	A03、A06、K01、K01.11、C01、X01、X02	plain_primitives	ML-KEM 被理想化为公钥封装：对端在 AT_PUB_KEM 下加密一个新的共享秘密，只有服务器能解封装；AKA 函数 f1/f2、PRF' 派生和 AT_MAC 都是未解释的单向函数。除此之外没有使用任何代数定律，因此证明只在这种理想化下成立，而对这种理想化发现的攻击就是对协议的攻击。

分析者的结束语

在 model.pv 中建模了 PQ EAP-AKA' 完整认证（固定 ML-KEM-768、一个 AKA 向量、可信 AD），并另有 bounded.pv，其中将 AKA 序列号展开到两步并带有新鲜性比较。正常流程存在；为各目标设定的攻击者下，全部 15 个目标都有答案，每个证明都配有失败的对照。

已确立：在网络攻击者下对端/服务器一致；MSK/EMSK 保密性，以及后续 AKA 长期密钥泄露后 MK_PQ 的前向保密；双方真实参与的后续会话的前向保密；MK_PQ 与密文和 KEM 公钥的密钥绑定；在要求 PQ 策略时，即使拥有长期密钥，没有 ML-KEM 也无法完成；一旦 SQN 比较到位，没有挑战会被接受两次（有界，两步，去掉比较的对照被证伪）；服务器侧的单射一致。

不成立且在文稿中已说明（此处复述，并非新发现）：对端的完成依赖于未受保护的 EAP-Success，持有 AKA 长期密钥的攻击者可以冒充任一方并伪造 ML-KEM 提议。第一项有经过检查的补救措施：增加一个受完整性保护的成功指示（AT_RESULT_IND），用 K_aut 作为密钥，可以消除该攻击，保留正常流程，并且不改变其他任何答案。

阻碍其余部分：分片和 AT_CHECKCODE 未建模，因此 D01 和 R02 仅对单包消息给出答案；SQN 接受窗口、回绕以及两个会话在存储值上的竞争不在两步展开范围内，需由 Tamarin+ Agent 处理；KEM 和 AKA/PRF 函数是理想化的，因此不作出任何计算性或量子主张。