Hybrid 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-hybrid-pqc-eapaka-02 · ProVerif+ Agent 报告

文稿	Enhancing Security in EAP-AKA' with Hybrid Post-Quantum Cryptography（协议定义）；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	13 条：10 条成立，3 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

EAP-AKA' 完整认证，采用混合后量子密钥建立：对等方持有带 AKA 长期密钥 K 和一个身份的 USIM；EAP 服务器不持有自己的长期密钥，而是从归属 AAA 服务器（AD）为该用户获取新的 AKA 向量；随后对等方与服务器执行 EAP-AKA' 交换，其中 RFC 9678 的经典 ECDHE 群被固定的 ML-KEM-768 + X25519 混合方案取代。对等方先声明其身份，服务器发送来自该向量的挑战以及 AT_KDF_FS 提议，对等方选择混合值，服务器在 AT_PUB_HYBRID 中发送其混合公钥，同时附上所选择的值和原始列表，对等方以其封装和 AT_RES 回应。

交换结束后，服务器已校验 AT_RES 和 AT_MAC，并已解封装对等方的封装，因此它确信用户的身份以及与其共享的混合秘密；对等方已校验从其 USIM 得到的 AUTN 以及两个挑战上的 AT_MAC，因此它确信该挑战和混合公钥来自持有其身份有效 AKA 向量的一方。双方持有相同的 MK_HYBRID，并据此安装 MSK 和 EMSK；对等方关于服务器侧运行成功的唯一证据是未受保护的 EAP-Success。

各方：

- **对等方**：带 USIM 的 EAP 对等方。持有：K、身份、本地策略（hybrid required 可选）。
- **EAP 服务器**：服务网络的 EAP 服务器。持有：无长期密钥；每次运行从 AD 获取一个 AKA 向量。
- **AD**：归属 AAA 服务器，AKA 向量来源（受信任）。持有：K、SQN 计数器、网络名。

图 1 展示了文稿规定的交换流程。

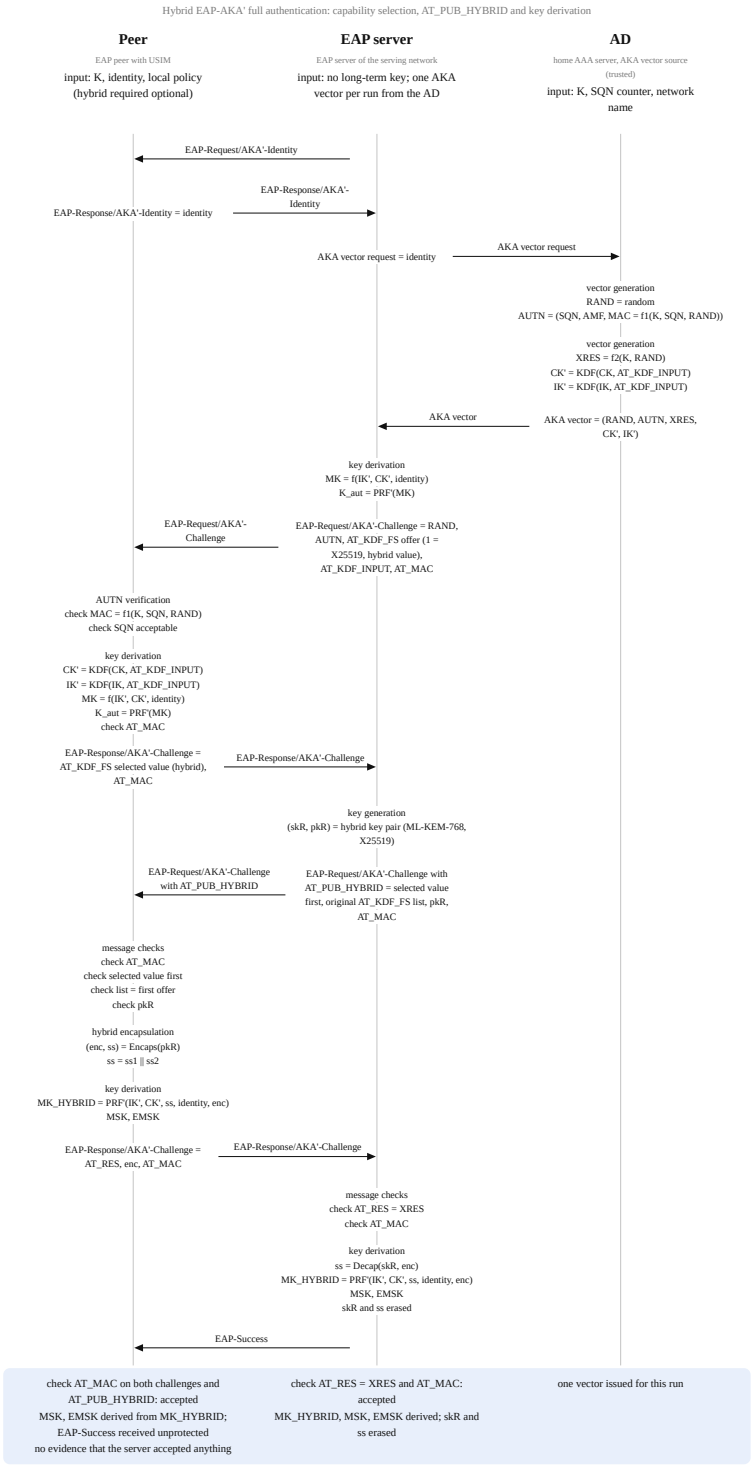


图 1. 文稿规定的协议。

分析范围见附录 D：分析了什么、省略了什么，以及它依据的文稿章节。

2 发现

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

在分析范围内，草案达到了其目标：要求 hybrid KEM 的对等方既不能被网络、也不能被持有有效向量的不诚实服务器推入仅经典的结果，且会话密钥在运行后 AKA 长期密钥丢失以及一个混合组件被攻破这两种情况下都能存活。挑战在两个方向上均满足一致性和密钥确认，且每个混合公钥只使用一次。唯一不成立的

性质是既有的已知问题：对等方派生密钥并在未受保护的 EAP-Success 上结束，因此它可能在服务器未接受任何内容时完成，RFC 4187 第 12.8 节已写明这一点。挑战的重放是首个模型省略 USIM 序列号所产生的伪影，一旦将该值与比较展开即被消除，因此没有新的发现。全部十三个目标都有答案；十二个基于理想化原语，一个（R01）基于两次运行的展开模型。

3 检查过的性质

每行是一条提交给 ProVerif 的性质。结果是 ProVerif 在分析者所建协议模型上的回答；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
A03	**对等方与服务器就完整流程达成一致。** 每当 peer 接受一次完整认证，就存在一个匹配的 server 运行，双方对 peer 身份、server 身份、所选 hybrid KEM 值、pkR/enc 与 MK_HYBRID 一致。	无	攻击成立（文稿已写明）	中	是
A04	**每个服务器接受都有其对等方运行。** 每次 server 成功接受都对应一个不同的 peer 运行，不存在两次接受映射到同一 peer 运行。	无	成立	中	否
A08	**AT_KDF_FS 列表绑定到真实提议。** peer 接受的 AT_KDF_FS 列表与所选 hybrid KEM 值必须对应服务器真实提议，且与首次列表只差所请求的改变；AT_MAC 覆盖该列表。	无	成立	中	否
K01	**会话密钥保持机密。** 攻击者不能推导出 MK_HYBRID、MSK、EMSK、K_re，除非其持有相应长期密钥或 ss。	无	成立	中	是
C01	**会话密钥的前向保密。** 会话完成后泄露长期密钥，攻击者仍不能推导该会话的 MSK/EMSK/MK_HYBRID。	长期密钥 IK'/CK'（会话完成后泄露）	成立	高	是
C08	**混合组合在一个组件被攻破时仍安全。** 在 X25519 分量或 ML-KEM 分量之一被攻破时，攻击者仍不能推导会话密钥 MSK/EMSK。	单个 hybrid KEM 分量（会话中或之后）	成立	高	否
R05	**本地混合策略防止降级。** 当本地策略要求 hybrid KEM 时，接受配置必须包含 hybrid KEM，攻击者不能通过移除或修改 AT_KDF_FS 使接受退化为仅经典 ECDHE。	无	成立	中	是
R01	**新鲜挑战，无重用证据。** peer 接受的认证证据必须来自本次挑战（新的 RAND/AUTN），旧证据不能被重用。	无	在界内成立（变化的值展开为 2 步）	中	否
A06	**双向密钥确认。** server 接受时，peer 已导出同一 K_aut 并发送正确 AT_MAC/AT_RES；peer 接受时，server 已导出同一 K_aut 并发送正确 AT_MAC。	无	成立	中	是
K01.10	**MK_HYBRID 或 ss 泄露后会话密钥仍安全。** 泄露 MK_HYBRID 或 ss 后，攻击者不能推导 MSK/EMSK。	MK_HYBRID 或 ss（派生后泄露）	攻击成立（文稿已写明）	低	是
R05.11	**修改的能力列表无法强制经典结果。** 在强制 hybrid 策略下，攻击者修改 AT_KDF_FS 列表不能使接受退化为仅经典 ECDHE。	无	成立	中	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
A03.12	**身份与新鲜挑战绑定。** peer 与 server 接受时，双方对身份、RAND/AUTN 新鲜挑战与成功结果一致。	无	攻击成立（文稿已写明）	中	是
X01	**每次交换使用新鲜混合 KEM 密钥对。** AT_PUB_HYBRID 的任何 pkR 值都不会用于两次认证交换：同一对等方的两个挑战绝不携带相同的 pkR。	无	成立	中	否

"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。

提出的问题，以及分析者的回答：

问题	回答	依据
Q1: 混合 MSK 分量泄露条件下保密	泄露 MK_HYBRID 会同时给出 MSK 和 EMSK，因为它们是 MK_HYBRID 的切片，所以交换过程中没有任何机制能阻止这一点；只泄露混合共享秘密则不会给出它们，因为 MK_HYBRID 还取用 AKA 运行中的 CK' 和 IK'。实际后果：把 MK_HYBRID 当作密钥材料本身来保护，并在运行后擦除 skR、ss 和封装秘密。	K01.10, C01, K01
Q2: 恶意修改能力列表不导致强制 hybrid 策略接受经典结果	否。修改或剥离 AT_KDF_FS 列表的攻击者无法让要求 hybrid KEM 的对等方接受仅经典的结果，因为回显的列表在 AT_MAC 之下返回，并与首次提议比较，且对等方要求混合值存在并被选择；网络攻击者和持有有效向量的不诚实服务器都不会成功。按策略允许回退的对等方确实会接受被剥离的提议，所以保护来自策略，而不是协商。	R05.11, R05, A08
Q3: peer/server 身份与新鲜认证挑战/成功绑定	当对等方接受时，它与服务器就 RAND/AUTN 挑战和混合公钥达成一致，且身份在双方同一次密钥派生中被绑定；因此身份与新鲜性这一半成立。对结果的一致不成立：对等方在未受保护的 EAP-Success 上结束，因此可能完成一次服务器从未接受的运行，所以对等方不得把自己侧的密钥派生当作服务器已接受的证据。	A03.12, A03, A06

4 本次分析的局限

这里的结果是协议模型上的结果：它说明规定的消息和检查在密码学视为理想的前提下给出或不给出什么，而不涉及任何实现。

正如分析者所述，本分析不覆盖的内容：

- 未对分片与重组（AT_FRAGMENT）和 AT_CHECKCODE 建模：消息按整体处理，因此没有涉及 MTU 限制，也没有涉及分片质询。
- 混合 KEM 是一个符号化封装，包含两个相互独立的组件：不作出任何计算性、IND-CCA 或后量子主张，因此 ML-KEM-768 和 X25519 的强度不在分析范围内。
- X25519 未被赋予其 Diffie-Hellman 代数性质；它是一个不透明的组件，因此需要关于经典部分进行代数推理的性质未被覆盖。
- 假定 AKA 向量是新鲜且可信的，而不含序列号的模型对质询没有新鲜性检查；展开模型只覆盖序列号为 1 和 2 的两次运行。
- 序列号接受规则、任何接受窗口以及 48 位回绕都不在这些文稿中；它们须来自 3GPP TS 33.102，并由 Tamarin+ Agent 以整数规则确定。
- 草案要求删除 skR、ss 及派生密钥，这一点未建模为擦除；前向保密结果假定删除确实发生，保留 skR 的情形未被覆盖。

- 同一用户的并发运行以及对保留值的竞争超出 ProVerif 能被询问的范围；展开的对等方按顺序执行其两次认证。
- 对等方的失败应答（Synchronization-Failure 对 Authentication-Reject）未被查询不可区分性；状态审查将其记录为候选发现，但没有模型查询。
- 身份请求、通知和重认证交换未建模；分析针对一次完整认证。
- 八个一致性及新鲜性证明（A03、A04、A08、A06 两个方向、A03.12、X01 以及展开的 R01）没有对照变体：本应失败的那个变体是网络攻击者同时持有 AKA 长期密钥并签署自己的质询，而本模型不包含这一情形。

宿主记录的内容：

- R01 的答案依赖于模型所做的一处简化（附录 D）。
- 没带对照查询的证明（附录 C）：A03: a03ch, A04: a04, A08: a08, R01: r01, A06: a06a, A06: a06b, A03.12: a03ch, X01: x01。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。

每条性质还留下什么未决，以及什么能解决它，见附录 A。

附录 A：逐条性质的解读

这是分析者自己对证明器答案的解读，不是证明器的答案：这些答案对协议意味着什么、解读依据什么、能否按现状使用，以及它有多大价值。

A03: 对等方与服务器就完整流程达成一致

每当 peer 接受一次完整认证，就存在一个匹配的 server 运行，双方对 peer 身份、server 身份、所选 hybrid KEM 值、pkR/enc 与 MK_HYBRID 一致。

接受混合质询响应的对等方只可能接受了服务器确实发送过的质询和 pkR，因为对回显列表和 pkR 的 AT_MAC 是用由 AKA 向量派生的密钥校验的。派生密钥上的一致性在相反方向不成立：对等方派生出 MK_HYBRID、MSK 和 EMSK 后，在一个未受保护的 EAP-Success 上结束，因此网络上的攻击者可以丢弃其响应，服务器则永远不会接受任何东西。对等方身份上的一致性由密钥派生本身承载，因为身份在双方都是 MK_HYBRID 的输入。

- 结果：攻击 成立（文稿中已陈述）；回答了所问：是；可在有保留的情况下使用
- 价值 中：正面的一半是草案所构建的保证，除符号化 KEM 之外，它成立所依赖的东西没有被任何简化触及；负面的一半是 EAP-AKA' 一直存在的弱点，文稿中已经陈述，此处为这一构造再现。
- 文稿中已陈述：是。文稿中的位置：rfc4187:3759, rfc4187:3766
- 依据：混合 KEM 是一个符号化封装，包含两个相互独立的组件；不作出任何计算性或后量子主张，因此一致性是关于符号项的一致性，而非关于真实密钥材料的一致性。；假定 AKA 向量是新鲜且可信的：AD 是诚实的，把每个向量交给一个服务器，且本模型未将对等方的 USIM 建模为拒绝过期质询。；未对分片与重组（AT_FRAGMENT、AT_CHECKCODE）建模；消息按整体处理。；服务器身份不作为任何消息中的项出现：对等方得到的保证是，某个持有其身份的有效向量的人发送了该质询。
- 未决：从未看到受保护成功指示的对等方是否应算作已完成运行，这是草案留给下层的策略问题。
- 下一步：协议主张无需进一步工作；关于受保护结果指示的部署问题超出协议证明器所能解决的范围。

A04: 每个服务器接受都有其对等方运行

每次 server 成功接受都对应一个不同的 peer 运行，不存在两次接受映射到同一 peer 运行。

每次服务器接受都对应一个不同的对等方运行：响应不能被重放以使服务器接受两次，因为服务器对自己收到的唯一回复的封装进行解封装，并为每个质询派生新的混合密钥对。这是仅针对网络的对等方响应上的单射一致性。

- 结果：成立；回答了所问：是；可在有保留的情况下使用
- 价值 中：这是交换的一项核心一致性性质，在符号化 KEM 抽象下得到证明；没有任何简化移除它所依赖的机制，即每个质询使用新的混合密钥对。我检索了草案和 RFC 9678，未找到关于 AT_RES 和 enc 的单射一致性陈述。
- 文稿中已陈述：否
- 依据：混合 KEM 解封装的建模使得只有针对该 pkR 所做的封装才能解封装；真实 KEM 的绑定性质是假定的，而非证明的。；服务器自身状态未建模为保留值，因此目标没有说明使用同一向量重试的服务器会怎样。
- 下一步：无。

A08: AT_KDF_FS 列表绑定到真实提议

peer 接受的 AT_KDF_FS 列表与所选 hybrid KEM 值必须对应服务器真实提议，且与首次列表只差所请求的改变；AT_MAC 覆盖该列表。

对等方接受的列表和混合值与服务器提议的完全一致，所选值被移到首位，因为对等方将回显与首次提议比较，并校验覆盖它的 AT_MAC。网络上的攻击者无法替换成不同的列表，也无法让对等方接受未曾提议的值。

- 结果：成立；回答了所问：是；可在有保留的情况下使用
- 价值 中：证明了使协商有意义的绑定，也是草案降级论述所依赖的绑定；它仅对不持有长期密钥的攻击者成立，而这正是草案声称的范围。
- 文稿中已陈述：否
- 依据：原文除“所选值在首位、其余按提议”之外，未将比较形式化；模型按草案指示遵循 RFC 9678 第 6.2 节。；提议列表建模为两个元素，X25519 在首位，然后是混合值；带扩展的更长列表未被覆盖。
- 下一步：无。

K01: 会话密钥保持机密

攻击者不能推导出 MK_HYBRID、MSK、EMSK、K_re，除非其持有相应长期密钥或 ss。

在运行期间，网络上的攻击者既学不到 MK_HYBRID，也学不到 MSK 和 EMSK；运行结束后丢失长期密钥也不会使其获得这些，因为混合共享秘密每次交换都是新鲜的，且从不出现在线路上。只有在 MK_HYBRID 本身被披露时这些密钥才会为人所知，而这正是草案的派生方式使其致命的泄露。

- 结果：成立；回答了所问：是；可在有保留的情况下使用
- 价值 中：会话密钥的机密性是草案的主要承诺，并且在文稿为其指出的两类攻击者下都成立；该证明针对理想化的 KEM 和 PRF。
- 文稿中已陈述：是。文稿中的位置：main:585
- 依据：PRF'、AKA 算法和 KEM 都是理想函数；该结果是关于构造的陈述，而非关于其强度的陈述。；长期密钥在运行后披露，而临时混合秘密不披露；草案自身关于保留 skR 的警告未建模。；在模型中 K_re 不能超出 MSK 被推导；关于 K_re 的主张与 MSK 依赖于同一步派生。
- 下一步：无。

C01: 会话密钥的前向保密

会话完成后泄露长期密钥，攻击者仍不能推导该会话的 MSK/EMSK/MK_HYBRID。

前向保密对混合构造成立：会话结束后，攻击者即使获得 AKA 长期密钥以及随之而来的 CK'、IK' 和 K_aut，也得不到该会话的 MK_HYBRID、MSK 或 EMSK，因为 KEM 秘密已经消失。这正是引入混合密钥建立所针对的性质，并且不受经典长期材料披露的影响。

- 结果：成立；所问是否有答案：是；可用但有保留
- 价值高：这是设计的核心保证，针对文稿点名的攻击者、会话结束后的长期密钥得到证明，且未做去除机制的简化，即每次交换都使用新的混合秘密；草稿之所以存在，原因正在于此。
- 文稿中是否陈述：是。文稿陈述位置：main:585
- 依据：按草稿要求，运行结束后混合私钥与共享秘密被擦除；若保留 skR 加上长期密钥即可得到会话密钥，如 main:585 所述。；前向保密仅对符号化 KEM 给出；对存储的会话记录加上未来破解 ML-KEM 或 X25519 的情形未作任何陈述。；AD 是诚实的，且每个向量只签发一次。
- 下一步：无。

C08: 混合组合在一个组件被攻破时仍安全

在 X25519 分量或 ML-KEM 分量之一被攻破时，攻击者仍不能推导会话密钥 MSK/EMSK。

一个混合组件被攻破不会破坏会话：攻击者持有该会话的 X25519 共享秘密，或持有 ML-KEM 分量的秘密，但不同时持有两者时，无法推导 MK_HYBRID、MSK 或 EMSK，因为组合秘密既需要两个分量，也需要 AKA 派生的 CK' 和 IK'。目标所依赖的是组合步骤，而不是各个 KEM 本身。

- 结果：成立；所问是否有答案：是；可用但有保留
- 价值高：混合组合的保证正是 ML-KEM 加 X25519 组合的全部意义所在，且针对目标点名的攻击者得到证明；保留在于，原语本身未做密码学建模。
- 文稿中是否陈述：否
- 依据：KEM 是符号化的：模型表明组合使用了两个分量和 AKA 材料，而不是表明 ML-KEM-768 或 X25519 能抵御真实攻击。；每次只攻破一个组件；泄露选择器是一种建模手段，使每条迹中恰好发生一次泄露。；草稿未定义组件被攻破的接口；这一解读是我们的，而正是这一性质使混合值得部署。
- 待解：在模型所假设的层面上，真实的 ML-KEM-768 或 X25519 被攻破是否可能，是一个计算问题，无法向证明器提出。
- 下一步：为组合给出计算论证，如同具体的混合 KEM 草稿所做的那样，将能解决符号模型之外的那部分。

R05: 本地混合策略防止降级

当本地策略要求 hybrid KEM 时，接受配置必须包含 hybrid KEM，攻击者不能通过移除或修改 AT_KDF_FS 使接受退化为仅经典 ECDHE。

按本地策略要求 hybrid KEM 的对端，绝不会在仅经典的配置上完成，即使攻击者从提议中剥离混合值，或持有有效 AKA 向量的不诚实服务器只提供带有效 AT_MAC 的 X25519。保护仅来自本地策略：在允许回退的情况下，对端确实会接受被剥离的提议，对照查询表明了这一点。

- 结果：成立；所问是否有答案：是；可用但有保留
- 价值中：这是草稿自身为其承认的降级所规定的缓解措施，针对文稿点名的两种攻击者都做了机械验证；它是在确认而非发现。
- 文稿中是否陈述：是。文稿陈述位置：main:593
- 依据：草稿将混合要求交由本地策略以 MAY 决定；模型按对端会话选择策略，两种配置都出现。；不诚实服务器被建模为获得有效向量并发送仅经典列表；它不尝试混合交换。；对端所做的比较按草稿和 RFC 9678 第 6.2 节的描述建模；列表更长或带扩展属性的部署不在覆盖范围内。
- 下一步：无。

R01: 新鲜挑战，无重用证据

peer 接受的认证证据必须来自本次挑战（新的 RAND/AUTN），旧证据不能被重用。

在不带新鲜性检查的模型上，录制的挑战被接受两次，这正是缺少序列号所允许的；在草稿所依赖的检查下，加上两个连续序列号的向量，对端不会两次接受同一挑战。因此重放不是草稿的缺陷，而是省略 USIM 序列号的后果；ProVerif 无法在任意会话数上完成的那一半，是在展开模型上完成的。

- 结果：在界内成立（变化值展开到 2 步）；所问是否有答案：是；可用但有保留
- 价值中：它让读者确切理解重放结果的含义，并给出有界证明：草稿对序列号的依赖在两次运行内是合理的；接受窗口的问题仍然未解。
- 文稿中是否陈述：否

- 依据：展开模型运行两次认证，序列号为 1 和 2，对端将接受的值交给下一次运行；运行之间的并发以及任何接受窗口的大小不在其中。；序列号接受规则本身在这些文稿中未作规定；模型遵循 AKA 规则，即只接受更大的值，草稿是假定而非陈述这一点。；不带检查的模型正是发现重放的那个模型；其攻击是模型产物，已记录在案。
- 待解：真实 USIM 中的接受窗口是否会让一个旧但足够新的向量通过，无法从这些文稿回答。
- 下一步：用 Tamarin+ Agent，将 3GPP 序列号规则写成整数约束，并增加运行次数，将能解决窗口与回绕问题。

A06: 双向密钥确认

server 接受时，peer 已导出同一 K_aut 并发送正确 AT_MAC/AT_RES；peer 接受时，server 已导出同一 K_aut 并发送正确 AT_MAC。

密钥确认在 AT_MAC 上双向成立：当服务器接受时，对端已导出相同的 K_aut 并发送了该响应；当对端接受挑战时，服务器已导出相同的 K_aut 并发送了该挑战。对端的保证止于挑战，因为响应之后的内容对它没有任何认证。

- 结果：成立；所问是否有答案：是；可用但有保留
- 价值中：确认两次 AT_MAC 检查给出了草稿所描述的相互保证，并清楚陈述了不对称性；它是对文稿所主张内容的证明。
- 文稿中是否陈述：是。文稿陈述位置：main:457
- 依据：AT_MAC 被建模为用 AKA 材料派生密钥对整条消息的 MAC；编码中各属性的确切覆盖范围取自草稿，未逐位核对。；身份请求与通知交换未建模。
- 下一步：无。

K01.10: MK_HYBRID 或 ss 泄露后会话密钥仍安全

泄露 MK_HYBRID 或 ss 后，攻击者不能推导 MSK/EMSK。

仅泄露混合共享秘密不会给出 MSK 或 EMSK，因为 MK_HYBRID 还需要来自 AKA 运行的 CK' 和 IK'。泄露 MK_HYBRID 则立即给出两者，这是定义使然：MSK 和 EMSK 是 MK_HYBRID 的切片，因此这一半由派生本身决定就是致命的，交换的任何改动都无济于事。

- 结果：攻击成立（文稿中已陈述）；所问是否有答案：是；可用
- 价值低：不成立的那一半是定义使然，成立的那一半由派生推出；它回答了用户的问题，但对协议没有说出任何意外之处。
- 文稿中是否陈述：是。文稿陈述位置：main:585
- 依据：MK_HYBRID、MSK 与 EMSK 之间的切片关系按草稿定义建模为私有派生。；两个组件的秘密被取为持有混合共享秘密的攻击者所会持有的内容；对端被建模为在运行后泄露它。
- 下一步：无。

R05.11: 修改的能力列表无法强制经典结果

在强制 hybrid 策略下，攻击者修改 AT_KDF_FS 列表不能使接受退化为仅经典 ECDHE。

修改 AT_KDF_FS 列表无法迫使要求 hybrid 的对端得到经典结果：回显的列表受 AT_MAC 保护并与首次提议比较，因此被改动的列表要么通不过检查，要么被拒绝。对持有有效 AKA 向量的不诚实服务器同样成立，因为该向量让它能计算 K_aut，但对端仍要求混合值存在且被选中。

- 结果：成立；所问是否有答案：是；可用但有保留

- 价值中：它直接回答了用户关于列表修改的问题，且覆盖两种攻击者，并表明保护来自 AT_MAC 加本地策略，而非来自 KEM。
- 文稿中是否陈述：是。文稿陈述位置：main:590
- 依据：按草稿所述，假定 AT_MAC 覆盖整个 AT_KDF_FS 列表和所选值；属性的编码未建模。；对端的策略在草稿中是 MAY；该性质是针对采用它的部署陈述的。
- 下一步：无。

A03.12: 身份与新鲜挑战绑定

peer 与 server 接受时，双方对身份、RAND/AUTN 新鲜挑战与成功结果一致。

当对端接受时，RAND/AUTN 挑战和它接受的混合公钥正是服务器所发送的，且身份在双方的同一次密钥派生中被绑定。结果一致并不反向成立：即使其响应被丢弃且服务器什么都没接受，对端也会在未受保护的 EAP-Success 上结束。

- 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 中：它把本次运行所保证的内容分成两半，第二半中记录了弱点；身份部分依赖的是关于派生的论证，而不是一个单独的查询。
- 文稿中已说明：是。文稿中的位置：rfc4187:3759
- 依据：关于身份的一致由双方根据身份派生 MK_HYBRID 来承载，而不是通过单独的比较；模型中没有服务器向对端声明身份的消息。；AKA 向量是新鲜的且受信任；序号检查不在本模型中。
- 下一步：无。

X01: 每次交换使用新鲜混合 KEM 密钥对

AT_PUB_HYBRID 的任何 pkR 值都不会用于两次认证交换：同一对端的两个挑战绝不会携带相同的 pkR。

没有混合公钥用于两次交换：每个携带 AT_PUB_HYBRID 的挑战都用新生成的密钥对来应答，因此同一对端的两个挑战绝不会携带相同的 pkR。这使得一次运行的封装在另一次运行中无法使用。

- 结果：成立；回答了所问：是；可用但有保留
- 价值 中：这是文稿中目标所要求的新鲜性保证，并且仅针对网络它成立；它是重放挑战必须破坏的两件事之一，因此值得单独陈述。
- 文稿中已说明：否
- 依据：密钥对的新鲜性通过在每次服务器运行内部生成密钥对来建模；如果在多次交换之间缓存密钥对，服务器就会破坏该性质，这种情况未被建模。；该性质针对产生消息的那次运行；重放的挑战不是第二次密钥对生成，这就是为什么承载重放的是 R01 而不是这个目标。
- 下一步：无。

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，以及每个攻击及分析者的判定。

目标	级别	界	查询	对照	攻击	主张
A03	proved		a03ch		a03keys (holds_in_source)	1 proved, 1 attack
A04	proved		a04			1 proved
A08	proved		a08			1 proved
K01	proved		c01	checked		2 proved
C01	proved		c01	checked		1 proved
C08	proved		c08	checked		1 proved
R05	proved		r05	checked		2 proved
R01	bounded	the changing value unrolled to 2 steps	r01		r01 (model_artifact)	1 bounded, 1 attack
A06	proved		a06a			2 proved
K01.10	proved		k0110b	checked	k0110a (holds_in_source)	1 proved, 1 attack
R05.11	proved		r05	checked		2 proved
A03.12	proved		a03ch		a03keys (holds_in_source)	1 proved, 1 attack
X01	proved		x01			1 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	对端接受挑战响应（AT_MAC 在 rand、autn 和回显列表、pkR 上有效）意味着 EAP 服务器针对同一 rand 和 pkR 发送了那条 ch2 消息；攻击者仅拥有网络。	`network`	proved	a03ch	none
A03	双方就 MK_HYBRID/MSK/EMSK 达成一致：一个派生了其密钥的对端运行，存在一个匹配的服务器运行，该运行接受了相同的 enc 并派生了相同的密钥；攻击者仅拥有网络。	`network`	attack (holds_in_source)	a03keys	
A04	服务器对 AKA'-Challenge 响应的每次成功接受都对应一个不同的对端运行：没有两次服务器接受共享同一个对端响应（对响应的一致性为单射）。	`network`	proved	a04	none
A08	对端接受的 AT_KDF_FS 列表和混合值就是服务器提供的那些（选中的值在前，其余与首次提供时相同），且处于对端验证过的 AT_MAC 之下；攻击者仅拥有网络。	`network`	proved	a08	none
K01	在会话结束后获得 AKA 长期密钥及其派生的一切（CK、IK、CK'、IK'、MK、K_aut）的攻击者，仍然无法派生该会话的 MK_HYBRID/MSK/EMSK；攻击者在运行后拥有长期密钥。	`ltk_after`	proved	c01	checked

目标	主张	攻击者	回答	查询	对照
K01	在运行本身期间（任何泄露之前），网络上的攻击者无法获知该会话的 MSK/EMSK；攻击者仅拥有网络。	`network`	proved	k01p0	checked
C01	当 AKA 长期密钥材料在会话之后被泄露时，已完成的会话仍保持 MSK/EMSK/MK_HYBRID 的机密性；攻击者在运行后拥有长期密钥。	`ltk_after`	proved	c01	checked
C08	当一个混合组件（X25519 共享秘密或 ML-KEM 组件）被攻破而另一个完好时，攻击者仍然无法派生 MK_HYBRID/MSK/EMSK；攻击者拥有该会话一个组件的共享秘密。	`one_component`	proved	c08	checked
R05	本地策略要求混合 KEM 的对端绝不会接受仅经典（仅 ECDHE）的配置，即使攻击者从 AT_KDF_FS 提供中移除了混合值；攻击者仅拥有网络。	`network`	proved	r05	checked
R05	本地策略要求混合 KEM 的对端绝不会接受由不诚实服务器提供的仅经典配置，即使该服务器持有有效的 AKA 向量并能签署任意 AT_KDF_FS 列表；攻击者是持有有效向量的不诚实 AAA/EAP 服务器。	`dishonest_server`	proved	r05	checked
R01	对端接受的证据来自新鲜的挑战：同一 RAND/AUTN 挑战不能被对端在两次不同的运行中接受；攻击者仅拥有网络。	`network`	attack (model_artifact)	r01	
R01	对端接受的证据来自新鲜的挑战：在 USIM 的序号检查到位、且 AD 先签发 SQN 1 再签发 SQN 2 的情况下，没有 RAND/AUTN 挑战会被对端在两次运行中接受；攻击者仅拥有网络。	`network`	bounded (the changing value unrolled to 2 steps)	r01	none
A06	当服务器接受（AT_RES 和 AT_MAC 有效）时，对端已经派生了相同的 K_aut 并发送了该响应；攻击者仅拥有网络。	`network`	proved	a06a	none
A06	当对端接受 AKA'-Challenge（AT_MAC 有效）时，服务器已经派生了相同的 K_aut 并发送了该挑战；攻击者仅拥有网络。	`network`	proved	a06b	none
K01.10	单独泄露混合共享秘密 ss（两个组件的秘密，而 IK'/CK' 仍保密）不会给出 MSK/EMSK；攻击者在运行后拥有该会话的 ss。	`mk_hybrid_reveal`	proved	k0110b	checked
K01.10	在该会话的 MK_HYBRID 被泄露之后，攻击者仍然无法派生 MSK/EMSK；攻击者在运行后拥有 MK_HYBRID。	`mk_hybrid_reveal`	attack (holds_in_source)	k0110a (the control of k0110b)	
R05.11	修改过的 AT_KDF_FS 列表无法使要求混合的对端接受仅经典的结果；攻击者仅拥有网络。	`network`	proved	r05	checked
R05.11	即使是不诚实服务器持有有效的 AKA 向量，也无法通过修改 AT_KDF_FS 列表使要求混合的对端接受仅经典的结果；攻击者是持有有效向量的不诚实服务器。	`dishonest_server`	proved	r05	checked
A03.12	当对端接受时，它接受的 RAND/AUTN 挑战和它收到的 pkR 就是 EAP 服务器发送的那些（关于新鲜挑战和混合密钥的一致）；攻击者仅拥有网络。	`network`	proved	a03ch	none
A03.12	当对端完成一次完整运行时，服务器已经接受了同一次运行，且双方对结果达成一致；攻击者仅拥有网络。	`network`	attack (holds_in_source)	a03keys	

目标	主张	攻击者	回答	查询	对照
X01	没有 pkR 用于两次认证交换：每个携带 AT_PUB_HYBRID 的挑战都使用新生成的混合密钥对（挑战与密钥对生成之间为单射对应）；攻击者仅拥有网络。	network	proved	x01	none

附录 D：分析是怎么跑的

一个 LLM 分析者从文稿构建协议模型，并把每个性质交给 ProVerif；第 3 节的每个结果都是证明器给出的答案。

ProVerif+ Agent 会话 session-20261114T214452，2026-11-14。状态：已完成。模型：deepseek-v4-1-flash-261017。步骤：45，证明器 58 秒，实际耗时 18 分钟，成本 0.194 美元。

上下文：会话从分析者的笔记重启了 1 次。轨迹文件保留了所有内容。

ProVerif：运行了 80 个证明，75 个已判定，5 个无答案，41 秒，记录了 21 个答案。

分析了什么

协议	Hybrid EAP-AKA prime full authentication
版本	draft-ietf-emu-hybrid-pqc-eapaka-02
分析范围	固定 ML-KEM-768+X25519 hybrid，先能力选择再发 AT_PUB_HYBRID；一次完整认证；可信 AAA/AKA vector 假设。支持稿固定库内 -05/-12/-04，明确原引用版本差异。包含协商列表回显、AT_MAC 与最终密钥绑定；不能将有限分片抽象推广为任意 MTU。
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	147 numbered passages (33631 bytes) from the sections listed below. A reference such as s0001 in this report is one of these passages

分析所依据的文稿章节如下：

文稿	章节	标题
main	5	Hybrid Enhancements by Design
main	6	Message Fragmentation and Reassembly
main	7	Capability Negotiation
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_HYBRID
main	10	Security Considerations
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

文稿	章节	标题
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到的协议目的：固定 ML-KEM-768+X25519 hybrid，先能力选择再发 AT_PUB_HYBRID；一次完整认证；可信 AAA/AKA vector 假设。支持稿固定库内 -05/-12/-04，明确原引用版本差异。包含协商列表回显、AT_MAC 与最终密钥绑定；不能将有限分片抽象推广为任意 MTU。

对照文稿定性质

在编写查询之前，分析者将草拟的性质列表与文稿本身对协议目的的说明进行了对照。名称、性质所涉及的对象以及文稿的说明都是分析者的解读；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
A03	对等方与服务器就完整流程达成一致	The peer and the EAP server agree, after a full hybrid authentication, on the peer identity, the KEM selection, pkR/enc and MK_HYBRID.	调用流程和关键步骤指出，服务器导出 ss = Decap(enc, skR) 并校验 AT_RES 和 AT_MAC，对等方验证 AT_MAC 和 AT_KDF_FS 列表；成功需要双方都正确。文稿没有说明对等方会得知服务器已接受。	s0028, s0031, s0035, s0036, s0038
A04	每个服务器接受都有其对等方运行	Every successful server acceptance corresponds to a distinct peer run; no two acceptances map to one peer run.	服务器必须为每次认证交换生成新的混合 KEM 密钥对，且密钥对不得重用（第 8.2 节）；响应会与该次交换的 XRES 和 AT_MAC 进行校验。	s0040, s0028, s0036
A08	AT_KDF_FS 列表绑定到真实提议	The list and hybrid KEM value the peer accepts are the ones the server really offered and selected, differing only by the requested change, and AT_MAC covers the list.	AT_MAC 保护 AT_KDF_FS 提议和对等方的选择，因为最终的 EAP-Request/AKA'-Challenge 同时携带所选值和原始列表（第 10 节）；RFC 9678 6.2 要求对等方检查只发生了所请求的变更。	main:582, s0057, s0015, s0018, s0028

ID	简称	对象	文稿怎么说	出处
K01	会话密钥保持机密	MK_HYBRID, MSK, EMSK and K_re are kept from the attacker unless it holds the long-term key or the hybrid shared secret.	MK_HYBRID = PRF'(IK'|CK'|ss, ...), MSK/EMSK/K_re 是它的切片；RFC 9048 7 指出，在 PRF 假设下，攻击者无法从其他密钥推导出这些密钥的任何非平凡信息。	rfc9048:1199, s0038, s0052
C01	会话密钥的前向保密	The MSK/EMSK/MK_HYBRID of a completed session stay secret when the AKA long-term key is disclosed after the session.	获得长期密钥的攻击者若不同时攻破混合 KEM，就无法推导出已记录交换的会话密钥（第 8.1 节）；RFC 9678 7 指出，获得所有 AKA 长期密钥的人无法在会话结束后重建用于保护该会话的密钥。	rfc9678:929, s0028, s0031, s0056
C08	混合组合在一个组件被攻破时仍安全	The session keys stay secret when one hybrid component (X25519 or ML-KEM) is broken and the other is intact.	混合密钥交换组合了多种算法，使得即使除一个组件算法外的所有组件都被攻破，安全性仍然成立（第 8 节）。	draft-irtf-cfrg-hybrid-kems:1031, s0021, s0052
R05	本地混合策略防止降级	A party that requires a hybrid KEM by local policy never completes on a classic-only (ECDHE-only) configuration when the adversary removes or modifies the AT_KDF_FS offer.	要求混合 KEM 的服务器如果发现对等方未选择混合 KEM，必须表现得如同认证失败；要求混合 KEM 的对等方如果发现没有混合值，必须表现得如同 AUTN 不正确（第 7 节）；需要防护能够移除提议的攻击者的部署，必须通过本地策略要求混合 KEM（第 10 节）。	main:585, s0019, s0057
R01	新鲜挑战，无重用证据	The evidence the peer accepts comes from a fresh challenge (new RAND/AUTN); evidence from an old exchange cannot be accepted again.	在完整认证中，EAP 交换的重放保护由底层 AKA 方案提供的 RAND 和 AUTN 实现，并且每次完整认证交换都使用不同的 K_aut。	rfc4187:3707, s0028, s0035
A06	双向密钥确认	When the server accepts, the peer had derived the same K_aut and sent a correct AT_MAC/AT_RES; when the peer accepts the challenge, the server had derived the same K_aut and sent a correct AT_MAC.	服务器仅在 AT_RES 有效时才导出密钥并验证 AT_MAC；对等方使用从 MK 导出的 K_aut 验证 AT_MAC；RFC 9048 7.2 记录 AKA 本可受益于额外的密钥确认。	rfc9048:1402, s0028, s0031
K01.10	MK_HYBRID 或 ss 泄露后会话密钥仍安全	After MK_HYBRID or the hybrid shared secret ss of a session is disclosed, the attacker still cannot derive that session's MSK/EMSK.	MSK 和 EMSK 是 MK_HYBRID 的切片，且 MK_HYBRID = PRF'(IK'|CK'|ss, ...)；文稿没有讨论泄露其中一个值会带来什么后果，这是用户提出的问题。	s0038, s0056
R05.11	修改的能力列表无法强制经典结果	Modifying the AT_KDF_FS list cannot make a hybrid-required peer or server accept a classic-only result.	双方都做出策略决定；可以通过本地策略要求混合 KEM（第 7 节、第 10 节）。	s0019, s0057

ID	简称	对象	文稿怎么说	出处
A03.12	身份与新鲜挑战绑定	When peer and server accept they agree on the identity, on the fresh RAND/AUTN challenge and on the outcome of the run.	对等方身份进入 MK 和 MK_HYBRID，AT_MAC 覆盖 RAND、AUTN 和列表，服务器校验 AT_RES 和 AT_MAC。	s0028, s0035, s0038
X01	每次交换使用新鲜混合 KEM 密钥对	The EAP server's hybrid KEM key pair (skR, pkR) and the pkR it sends in AT_PUB_HYBRID.	对于每次认证交换，服务器必须生成新的混合 KEM 密钥对；密钥对不得在认证交换之间重用（第 8.2 节）；草案的安全考虑指出，一个 KEM 密钥对应仅在一个 EAP 会话中使用。	draft-ietf-emu-pqc-eapaka:1126, s0040, s0033

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

宿主将文稿中说明协议保护什么、防范什么的章节逐段列出，共 405 段；分析者对每一段说明了去向：定为性质、定为攻击者条件，或者为什么两者都不选。选了 208 段，没选 197 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	draft-ietf-emu-pqc-eapaka:1121-1123	证明器问不了	对随机数生成器质量的要求，属于本原的性质。
P002	draft-ietf-emu-pqc-eapaka:1125-1129	C01	
P003	draft-ietf-emu-pqc-eapaka:1131-1136	A08, R05, `ltk_active`	
P004	draft-ietf-emu-pqc-eapaka:1138-1142	不在范围内	分片与属性总长度上限；模型整体携带属性，不对分片重组或其开销建模。
P005	draft-ietf-emu-pqc-eapaka:1144-1149	K01, A08	
P006 至 P007	draft-ietf-emu-pqc-eapaka:1158-1162	没有陈述目标	页眉与草案样板文字。
P008	draft-ietf-emu-pqc-eapaka:1167-1171	证明器问不了	ML-KEM 变体的安全级别，属于本原的性质。
P009 至 P021	draft-irtf-cfrg-concrete-hybrid-kems:485-530	证明器问不了	混合 KEM 构造本身的安全考虑（通用组合器、PRG、绑定目标）；这是本原的计算性质，不是 EAP 交换的性质。
P022 至 P023	draft-irtf-cfrg-hybrid-kems:1018-1027	证明器问不了	混合 KEM 构造本身的安全考虑（通用组合器、PRG、绑定目标）；这是本原的计算性质，不是 EAP 交换的性质。
P024 至 P026	draft-irtf-cfrg-hybrid-kems:1031-1046	C08	
P027 至 P040	draft-irtf-cfrg-hybrid-kems:1051-1140	证明器问不了	IND-CCA、密文第二原像抗性和强 Diffie-Hellman 都是对 KEM 组件的计算假设。

段落	出处	定为	不选的原因
P041 至 P046	draft-irtf-cfrg-hybrid-kems:1144-1181	A08, K01	
P047 至 P059	draft-irtf-cfrg-hybrid-kems:1185-1262	证明器问不了	KEM 构造的不可区分性与 PRG 要求；本原的性质。
P060 至 P062	draft-irtf-cfrg-hybrid-kems:1266-1278	C08	
P063 至 P073	draft-irtf-cfrg-hybrid-kems:1283-1316	证明器问不了	混合 KEM 的 IND-CCA 目标，属于本原的计算性质。
P074 至 P079	draft-irtf-cfrg-hybrid-kems:1320-1352	A08	
P080	draft-irtf-cfrg-hybrid-kems:1356-1357	没有陈述目标	说明混合 KEM 目标不是什么；对 EAP 交换没有要求。
P081 至 P147	draft-irtf-cfrg-hybrid-kems:1361-1810	证明器问不了	KEM 构造的绑定与 IND-CCA 目标的分析和引理，以及编码规则；关于本原的计算结果，符号模型不表示这些。
P148	main:564-567	证明器问不了	指向 KEM 草案的 IND-CCA 讨论；属于本原的性质。
P149	main:569-570	证明器问不了	ML-KEM 的安全级别与尺寸；属于本原的性质。
P150	main:578-578	证明器问不了	对随机数生成器的要求。
P151	main:582-582	C01	
P152	main:585-588	A08, R05, `ltk_active`	
P153	main:590-595	没有陈述目标	同一段的收尾句；没有额外要求。
P154 至 P155	rfc3748:2182-2190	没有陈述目标	说明 EAP 本身没有安全机制，并指向其他章节。
P156 至 P168	rfc3748:2194-2252	A03, A08, `network`	
P169 至 P192	rfc3748:2256-2427	A03, A06, A08, R01	
P193 至 P196	rfc3748:2431-2455	不在范围内	身份保护依赖假名或 SUCI，而建模的流程和选定的原文单元都没有包含这些。
P197 至 P204	rfc3748:2459-2502	A03	
P205 至 P214	rfc3748:2506-2567	A08, A06	
P215 至 P217	rfc3748:2571-2587	没有陈述目标	说明 AKA 不是口令协议，没有字典攻击暴露面；没有本协议的性质可问。

段落	出处	定为	不选的原因
P218 至 P220	rfc3748:2591-2611	不在范围内	下层对用户数据的保护，在 EAP 方法之外。
P221 至 P222	rfc3748:2615-2629	R05, A08	
P223 至 P225	rfc3748:2633-2651	没有陈述目标	关于实现怪癖的建议。
P226 至 P240	rfc3748:2659-2752	K01, C01	
P241 至 P244	rfc3748:2765-2789	证明器问不了	密码套件的强度，属于本原的性质。
P245 至 P250	rfc3748:2793-2828	不在范围内	下层行为。
P251 至 P257	rfc3748:2832-2880	R05, `dishonest_server`	
P258 至 P260	rfc3748:2884-2898	没有陈述目标	本协议中没有明文口令。
P261 至 P267	rfc3748:2902-2945	不在范围内	EAP-AKA' 不提供到认证者的信道绑定，且在建模流程之外。
P268 至 P280	rfc3748:2949-3056	A03	
P281	rfc4187:3594-3597	没有陈述目标	安全章节的引言；自身没有要求。
P282 至 P283	rfc4187:3608-3629	不在范围内	通过假名实现身份保护，在建模流程之外。
P284 至 P286	rfc4187:3633-3646	A03	
P287	rfc4187:3650-3659	证明器问不了	对认证中心的泛洪；属于资源消耗性质。
P288 至 P289	rfc4187:3663-3672	K01	
P290	rfc4187:3676-3680	没有陈述目标	说明对 128 位 AKA 密钥的暴力破解不可行；没有可对协议提出的问题。
P291 至 P299	rfc4187:3684-3740	R01, A08, A03	
P300 至 P302	rfc4187:3744-3757	R05, A08	

段落	出处	定为	不选的原因
P303 至 P304	rfc4187:3761-3777	A03	
P305 至 P306	rfc4187:3781-3799	不在范围内	通过隧道 EAP 实施的中间人攻击；隧道在建模流程之外。
P307	rfc4187:3808-3811	证明器问不了	随机数源的质量。
P308 至 P328	rfc9048:1131-1260	K01, C01, A08, R01	
P329 至 P342	rfc9048:1264-1344	不在范围内	通过 SUCI、假名和快速重认证名实现的标识符隐私，在建模流程之外。
P343 至 P354	rfc9048:1348-1448	A06, A03, `ltk_active`	
P355 至 P359	rfc9048:1452-1482	C01, `ltk_after`	
P360 至 P363	rfc9048:1486-1537	C01, `ltk_active`	
P364 至 P375	rfc9678:868-954	C01, `ltk_after`	
P376 至 P378	rfc9678:958-973	C01	
P379 至 P387	rfc9678:977-1046	A08, R05, C01, `ltk_active`	
P388 至 P394	rfc9678:1050-1096	证明器问不了	拒绝服务与公钥运算的开销；属于资源性质。
P395	rfc9678:1100-1102	不在范围内	对 Identity Response 的身份隐私要求，在建模流程之外。
P396 至 P397	rfc9678:1106-1115	不在范围内	未受保护的属性与流量分析；元数据和隐私在建模流程之外。
P398 至 P400	rfc9678:1119-1136	C01	
P401 至 P405	rfc9678:1140-1184	C08, C01, `one_component`, `ltk_active`	

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 16 条，没检查 17 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	EAP-AKA' 只派生密钥；它保护的载荷属于下层，任务未将其纳入。
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	K01	
D01	消息完整性与数据来源真实性	A08, A06	
A01	对端曾参与性（Aliveness）	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	A03	
R02	消息级抗重放	A04, R01	
R03	业务操作至多一次	不适用	该协议没有需要至多执行一次的业务操作。
R04	消息接受顺序／窗口安全	R01	
C02	抗密钥泄露冒充（KCI）	证明器问不了	在本模型中，每次泄露都发生在会话之后，因此无法表达在运行之前或运行期间持有长期密钥的攻击者；文稿本身就指出，这样的攻击者可以冒充任何一方。
C03	已知密钥安全／泄露隔离	K01	
C04	临时秘密／部分状态泄露韧性	C08	
C05	泄露后安全恢复（PCS）	证明器问不了	泄露后恢复需要一次在长期密钥泄露之后开始的运行；模型中的每次泄露都发生在会话之后，因此不存在更晚的运行。
C06	注册凭据泄露后的增强认证	不适用	没有注册流程，也没有多部分凭据；长期密钥由 USIM 和 AD 共享。
C07	抗离线字典攻击	不适用	AKA 长期密钥是 128 位随机密钥，不是可猜测的口令（RFC 4187 12.5）。
Z01	授权执行正确性	不适用	授权、委托、撤销和租户不属于 EAP 认证方法的一部分。
Z02	委托权限不扩张	不适用	授权、委托、撤销和租户不属于 EAP 认证方法的一部分。
Z03	授权与身份／会话／操作绑定	不适用	授权、委托、撤销和租户不属于 EAP 认证方法的一部分。
Z04	撤销与过期生效	不适用	授权、委托、撤销和租户不属于 EAP 认证方法的一部分。
Z05	跨租户／跨服务安全隔离	不适用	授权、委托、撤销和租户不属于 EAP 认证方法的一部分。
S01	加密 nonce 唯一性	A04	
S02	重传／密钥重安装安全	R01, A04	
S03	抗回滚与状态单调性	R01	
S04	跨阶段安全上下文一致性	A03	
S05	终止与旧状态失效	R01	
P01	身份匿名性	不在范围内	身份匿名性、不可关联性和存在性隐藏依赖 SUCI、假名和快速重认证身份，而建模的流程和选定的原文单元未将其纳入。
P02	会话不可关联性	不在范围内	身份匿名性、不可关联性和存在性隐藏依赖 SUCI、假名和快速重认证身份，而建模的流程和选定的原文单元未将其纳入。
P03	用户／凭据存在性隐藏	不在范围内	身份匿名性、不可关联性和存在性隐藏依赖 SUCI、假名和快速重认证身份，而建模的流程和选定的原文单元未将其纳入。
V01	条件性进展／错误恢复	证明器问不了	活性、无死锁和资源滥用超出了符号轨迹性质所能表达的范围。

条目	目录里的性质	作为哪条性质检查	不检查的原因
V02	无非预期死锁	证明器问不了	活性、无死锁和资源滥用超出了符号轨迹性质所能表达的范围。
V03	受限资源滥用／抗放大	证明器问不了	活性、无死锁和资源滥用超出了符号轨迹性质所能表达的范围。

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 19 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 3 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	攻击者得不到更多	受攻击者控制的 peer 只持有自己的 USIM 密钥和自己的会话密钥；对于服务器给出的保证，攻击者并不能比网络攻击者多得到什么。
S02	server	参与方	`dishonest_server`	
S03	USIM/AD	参与方	`ltk_active`, `ltk_after`	
S04	MK_HYBRID	值	按定义全部失守	把 MK_HYBRID 交给攻击者就等于交出会话密钥本身；K01 和 C01 所要求的保密性按定义即告失守，而文稿在这种失守下并未提出该要求。
S05	MSK	值	按定义全部失守	MSK、EMSK 和 K_re 就是会话密钥；持有它们会使保密性问题失去意义。
S06	EMSK	值	按定义全部失守	MSK、EMSK 和 K_re 就是会话密钥；持有它们会使保密性问题失去意义。
S07	K_re	值	按定义全部失守	MSK、EMSK 和 K_re 就是会话密钥；持有它们会使保密性问题失去意义。
S08	AT_MAC 覆盖的协商列表	值	攻击者得不到更多	受 MAC 覆盖的列表是公开字段；攻击者看到它并不会得到它本来就看不到的信息，而改动它会由 AT_MAC 发现。
S09	AT_RES	值	攻击者得不到更多	AT_RES、enc、pkR、AT_KDF_FS 列表、所选值、AT_MAC、RAND、AUTN 和 RES 都在链路上传输或是公开的；持有它们不会给网络攻击者增加任何东西。
S10	enc	值	攻击者得不到更多	AT_RES、enc、pkR、AT_KDF_FS 列表、所选值、AT_MAC、RAND、AUTN 和 RES 都在链路上传输或是公开的；持有它们不会给网络攻击者增加任何东西。
S11	pkR	值	攻击者得不到更多	AT_RES、enc、pkR、AT_KDF_FS 列表、所选值、AT_MAC、RAND、AUTN 和 RES 都在链路上传输或是公开的；持有它们不会给网络攻击者增加任何东西。
S12	AT_KDF_FS 列表	值	攻击者得不到更多	AT_RES、enc、pkR、AT_KDF_FS 列表、所选值、AT_MAC、RAND、AUTN 和 RES 都在链路上传输或是公开的；持有它们不会给网络攻击者增加任何东西。
S13	所选 hybrid KEM 值	值	攻击者得不到更多	AT_RES、enc、pkR、AT_KDF_FS 列表、所选值、AT_MAC、RAND、AUTN 和 RES 都在链路上传输或是公开的；持有它们不会给网络攻击者增加任何东西。
S14	AT_MAC	值	攻击者得不到更多	AT_RES、enc、pkR、AT_KDF_FS 列表、所选值、AT_MAC、RAND、AUTN 和 RES 都在链路上传输或是公开的；持有它们不会给网络攻击者增加任何东西。
S15	RAND	值	攻击者得不到更多	AT_RES、enc、pkR、AT_KDF_FS 列表、所选值、AT_MAC、RAND、AUTN 和 RES 都在链路上传输或是公开的；持有它们不会给网络攻击者增加任何东西。

ID	参与方或值	类别	攻击者条件	不设的原因
S16	AUTN	值	攻击者得不到更多	AT_RES、enc、pkR、AT_KDF_FS 列表、所选值、AT_MAC、RAND、AUTN 和 RES 都在链路上传输或是公开的；持有它们不会给网络攻击者增加任何东西。
S17	RES	值	攻击者得不到更多	AT_RES、enc、pkR、AT_KDF_FS 列表、所选值、AT_MAC、RAND、AUTN 和 RES 都在链路上传输或是公开的；持有它们不会给网络攻击者增加任何东西。
S18	K_aut	值	`ltk_active`	
S19	身份	值	攻击者得不到更多	peer 身份在 Identity 交换中传输，在建模的流程中是公开的。

每条性质在各攻击者条件下的答案

攻击者条件由分析者设定，在编写查询之前就已确定；每个答案都是在其中某一个条件下记录的。单元格是证明器在该攻击者条件下对该性质给出的答案；“无答案”是指该性质在某个攻击者条件下，证明器对某条主张未作判定，或没有记录任何结果；空单元格是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：它读取、丢弃、修改和发送消息，不持有任何一方的秘密		
`ltk_after`	用户的 AKA 长期密钥 K 及其派生的一切（CK、IK、CK'、IK'、MK、K_aut、K_encr），在受攻击的会话结束之后获得。	文稿讨论了 USIM 上 AKA 长期密钥的失守，并要求过去的会话保持受保护；s0056 指出，保留的 skR 加上长期密钥即可恢复会话密钥。	rfc9678:929, s0056, s0028
`ltk_active`	用户在运行之前和运行期间的 AKA 长期密钥，在路径上被主动使用。	第 10 节：持有长期密钥的攻击者仍然可以移除 hybrid KEM 提议，RFC 9678 7.2 指出这样的攻击者可以伪造协商并冒充任何一方。	main:585, s0057
`dishonest_server`	网络/AAA 侧不诚实或已失守的一方，它从 AD 获得该用户的有效 AKA 认证向量，因此能算出该向量的 K_aut，并可以用有效的 AT_MAC 发送任意 AT_KDF_FS 列表。	RFC 3748 7.13 讨论了认证者与后端认证服务器的分离及其所需的信任；RFC 9048 7.2 描述了一个服务网络，它让一次运行成功，然后滥用密钥。任务范围声明 AAA/AKA 向量源可信，因此该攻击者仅在文稿提出它的地方使用。	rfc3748:2832, rfc9048:1358
`one_component`	两个 hybrid 组件之一（X25519 组件或 ML-KEM 组件）的共享秘密，另一个组件完好。	Hybrid 密钥交换的意图是即使除一个组件算法之外的所有组件都被攻破也保持安全；hybrid KEM 草案说明了组件算法必须具备的安全性质。	draft-irtf-cfrg-hybrid-kems:1031, s0021
`mk_hybrid_reveal`	会话的 MK_HYBRID 或 hybrid 共享秘密 ss，在运行之后披露。	用户的问题 Q1 假设 hybrid MSK 组件被披露；文稿未讨论这一点。	s0038

ID	`network`	`ltk_after`	`ltk_active`	`dishonest_server`	`one_component`	`mk_hybrid_reveal`
A03	不成立					
A04	成立					
A08	成立					
K01	成立	成立				
C01		成立				
C08					成立	
R05	成立			成立		

ID	network	ltk_after	ltk_active	dishonest_server	one_component	mk_hybrid_reveal
R01	成立					
A06	成立					
K01.10						不成立
R05.11	成立			成立		
A03.12	不成立					
X01	成立					

原文和目标

来源：147 个原文单元，33631 字节，已冻结于 source-delivery-01.json。 目标：9 个已批准（A03、A04、A08、K01、C01、C08、R05、R01、A06）；提出的问题：3 个。 目标清单事先按草稿获批，使用 --approve-targets。

宿主按其文档化默认值做出的决定（任务 `decisions: auto`），供你核查：

- approve_package：批准源文包 protocol-3ad9877a4632fe52f364bd17e792

本步骤的自述：1 次请求（1 次失败），0.000 美元，输入 27975 个 token，输出 4139 个，24 秒。

关于证明器和模型的说明

- R01：在 ProVerif 中给出了答案，分析者为此目标命名了 changing_state

一个简化代数（xor、dh_algebra、other_algebra）的 ProVerif 模型给攻击者的能力弱于真实运算：在那里得到的证明是针对更弱攻击者的证明，在那里得到的攻击就是攻击。一个省略了对变化值检查（changing_state）的 ProVerif 模型会让各方接受更多：在那里得到的证明成立，在那里得到的攻击可能只是缺少了那项检查。Tamarin+ Agent 按原样对这些建模。

按步数给出的界是对 bounded.pv 的答案：这是分析者的第二个 ProVerif 模型，其中保存变化值的一方被展开到该步数，并保留其检查。该模型所做的少于协议所做的，所以性质只对这些步数成立，不能推得更远；在那里发现的攻击就是攻击。步数由分析者说明。

分析者的状态审阅

这一部分是分析者自己对原文的解读，不是证明器的答案。"shown by ProVerif"下的"yes"表示 ProVerif 在展开模型中找到了带有这些步数的轨迹，因此这些步数是可能的；它们是否破坏了某个目标，只由答案表中的一次攻击来说明，它们还付出了什么代价则是分析者的解读。"nothing found"说明查看了哪些模式，并不证明任何东西。

值	由谁保存	何时变化	何时检查	参考
SQN（AUTN 中携带的 AKA 序列号）以及用户已接受的最高 SQN	对端（USIM/AD 一侧：对端中的 USIM 以及签发向量的 AD）	USIM 在验证了一个它接受的 AUTN 之后提高其存储值，即每次接受 AKA'-Challenge 时提高一次；AD 每签发一个向量就提高放入该向量的值	在每次 AKA'-Challenge 时，对端在检查 AUTN MAC 之后，将从 AUTN 中恢复的 SQN 与其保存的值比较，当 SQN 不可接受时拒绝	s0021、s0028、s0035
混合 KEM 私钥 skR 和服务器的封装状态（skx、skk），以及对端的封装秘密（rx、rk）	EAP 服务器和对端，在一次交换期间	每个 AT_PUB_HYBRID 都会生成新的密钥对，因此每次挑战使用不同的 skR/pkR；对端的封装随机数每次响应都是新的	服务器只用 skR 解封装与其所发送 pkR 相匹配的回复；对端从不重用其秘密	s0033、s0040、s0056

值	由谁保存	何时变化	何时检查	参考
一次完成的运行所派生的密钥 MK_HYBRID、MSK、EMSK 和 K_re	对端和 EAP 服务器	每次完成的完整认证都会派生新值；MSK 被安装到下层一次	不做比较；对端在收到 EAP-Success 时安装其 MSK，不检查服务器是否派生了相同的值	s0031、s0038
AT_KDF_FS 协商的状态（提供的列表、选定的值、回显的列表）	EAP 服务器和对端，在一次交换期间	选定的值被插入 AT_PUB_HYBRID 中回显列表的头部，对端将其与提供给它的列表比较	对端在 AT_MAC 保护下将回显列表与首次提供比较，并要求选定的值排在首位	s0015、s0018、s0028

模式	结果	目标	shown by ProVerif	步数
replay	候选		否：未用 ProVerif 尝试	攻击者记录发往该用户的 EAP-Request/AKA'-Challenge，其中包含 RAND、AUTN 以及带有 pkR 的 AT_PUB_HYBRID。/ 对端完成运行并发送其响应；攻击者丢弃该响应，并从自己的存储中投递 EAP-Success。/ 针对同一用户的第二次认证开始；攻击者原样投递所记录的 EAP-Request/AKA'-Challenge。/ 在没有序列号比较的情况下，对端再次验证 AUTN，封装到同一个 pkR，接受，于是攻击者在一个挑战上获得了第二次运行。
repeat_one_time_action	未发现任何东西			所关注的一次性动作是派生并安装会话密钥，以及只使用 pkR 一次。对同一个对端响应的两次接受被 model.pv 上的 A04 排除（每次服务器接受都有各自的、已验证的对端运行），对同一个挑战的两次接受被 bounded.pv 上的 R01 排除。同一个挑战的一次运行若要产生两次服务器接受，就需要在一个 pkR 下有两个对端响应，而服务器无法获得，因为它只解封装它收到的单个回复，且 A04 成立。
desynchronisation	未发现任何东西			AD 提高其签发的序列号，而对端只接受大于它保存的值，因此被拒绝的运行不会改变对端的值，下一个向量仍然携带更大的值：两者之间不会产生差距，也不需要恢复步骤。bounded.pv 显示第二次运行在第一次以 SQN 1 完成之后以 SQN 2 完成。
update_before_check	候选		否：未用 ProVerif 尝试	USIM 验证挑战的 AUTN MAC 并接受其 SQN，提高它保存的值；此时对端尚未发送其响应。/ 攻击者丢弃对端的 AKA'-Challenge 响应，因此服务器永不完成，也永不接受。/ 对端存储的序列号已经前移，尽管没有任何运行完成；该对端再也不能接受同一个挑战。
no_rollback_on_failure	候选		否：未用 ProVerif 尝试	对端验证 AUTN 并接受该挑战；其保存的序列号向前移动。/ 该运行被放弃（攻击者丢弃响应，或服务器停止），因此服务器一侧没有安装任何密钥。/ 对端保持着已推进的值，而会话并不存在；此时旧挑战的录制副本会被拒绝。
race_between_sessions	未发现任何东西			同一用户的两个并发运行正是 replay 候选所利用的，而在有序列号比较的情况下，对同一个挑战的第二次接受被排除（R01，bounded.pv）。EAP 对每个对端一次只有一个会话；模型中的两个对端运行是顺序的，一个把其值交给下一个，这是更严格的顺序。同一存储值上真正并发的一对运行超出了此处可向 ProVerif 提出的范围。
distinguishable_failure	候选		否：未用 ProVerif 尝试	一个持有记录向量的不诚实服务器向它怀疑的用户身份发送带有该向量的 EAP-Request/AKA'-Challenge。/ AUTN MAC 在对端处验证通过，而序列号已陈旧，因此对端回复 EAP-Response/AKA'-Synchronization-Failure。/ 如果该向量不是发给该用户的，对端则回复 EAP-Response/AKA'-Authentication-Reject，因为其 AUTN MAC 在该身份的密钥下无法验证。/ 两条失败消息不同，且都带有 AT_MAC，因此该答复告诉不诚实服务器：所记录的向量属于该用户。

模式	结果	目标	shown by ProVerif	步数
wrap_or_window	未发现任何东西			草案没有定义序列号的接受规则，也没有给出窗口，因此这些文稿中没有可建模的内容；48 位回绕需要 2^48 次认证，在任何模型中都无法达到。要解决这一点，需要 3GPP TS 33.102 中的 AKA 序列号规则，这超出了原文单元的范围，并且必须由 Tamarin+ Agent 写出整数规则来完成。

分析者为各目标命名的内容：

步骤	目标	特征	原因
33	A03, A04, A06, A08, K01, C01, C08, R05, R05.11, A03.12, X01, K01.10	plain_primitives, many_sessions	这些目标依赖 PRF'/KDF、MAC、AKA 算法以及一个双分量 KEM 抽象，它们都被建模为理想函数；混合 KEM 是一个符号化的封装，包含两个独立分量，不涉及 Diffie-Hellman 代数，因此不作出任何计算性或后量子主张。每条保密性、一致性以及降级查询都在无界的对等方、服务器和 AD 会话数量上提出，因此结果适用于这些角色的任意多次运行。
33	R01	changing_state	R01 要求对等方接受的证据来自一次新鲜的挑战。新鲜性依赖于 RAND/AUTN 以及 USIM 保存、更新并比较的序列号，而模型省略了这些，因此对等方接受每一个它能认证的挑战，而为此目标记录的正是缺失的那项检查。对于一个会变化的值的半答案，必须在展开的模型上给出。

分析者的结语

混合 EAP-AKA' 完整认证的模型（draft-ietf-emu-hybrid-pqc-eapaka-02），包含对等方+USIM、EAP 服务器、诚实的归属 AAA 向量源以及持有有效向量的不诚实服务器；model.pv 能够运行，全部十三个目标都有记录的答案。

已确立：对等方接受的挑战和 AT_PUB_HYBRID 来自服务器（A03 主张 a，A03.12 主张 a），回显的 AT_KDF_FS 列表就是所提供的那个（A08），每次服务器接受都有其对等方的独立运行（A04），密钥确认双向成立（A06），没有混合公钥被重用（X01）。会话密钥（MK_HYBRID/MSK/EMSK）在运行期间保持保密，并且在运行后 AKA 长期密钥被披露的情况下也保持保密（K01, C01），并且能经受住一个混合分量被攻破（C08）—— 所有这些都在理想化的 PRF'/KDF/MAC 和符号化的双分量 KEM 下得到证明。要求混合 KEM 的对等方无法被推向仅 ECDHE，无论是由网络还是由持有有效向量的不诚实服务器（R05, R05.11），被证伪的对照查询表明，允许回退的对等方确实会接受被剥离的提议。

失败结果全部记录在文稿中，因此没有新的发现：对等方在未受保护的 EAP-Success 上派生密钥并完成，而服务器没有接受任何东西（A03/A03.12 主张 b，RFC 4187 第 12.8 节）；披露 MK_HYBRID 按定义会得到 MSK/EMSK，仅披露 ss 则不会（K01.10）。一次挑战的重放（R01）是将 USIM 序列号从 model.pv 中省略所造成的产物；在 bounded.pv 上，AD 先发出 SQN 1 再发出 SQN 2，对等方比较最后接受的值，同一查询在两次展开的运行中得到了验证。

阻碍：序列号接受窗口和 48 位回绕不在这些文稿中，需要 Tamarin+ Agent 配合 3GPP TS 33.102 规则；AUTN 验证与提升已存储 SQN 的顺序未作规定，因此 update_before_check 和 no_rollback_on_failure 仍为未确认的候选；失败消息的可区分性（Synchronization-Failure 与 Authentication-Reject 揭示出记录的向量是真实的）是一个候选发现，但没有模型查询；分片、重认证以及擦除保留的 skR 未被建模；八个一致性和新鲜性证明没有对照查询，因为必须失败的那个变体需要攻击者主动持有 AKA 长期密钥，而模型中不包含这种情况。