IKE_INTERMEDIATE 中 IKEv2 PPK 的安全性分析

本报告的其他语言版本：English。

rfc9867 · ProVerif+ Agent 报告

文稿	Mixing Preshared Keys in the IKE_INTERMEDIATE and CREATE_CHILD_SA Exchanges of the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-Quantum Security （协议定义）; Internet Key Exchange Protocol Version 2 (IKEv2)（辅助）; Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2)（辅助）
检查的性质	11 条：9 条成立，2 条不成立（3 个攻击）
发现	1；另在附录 B 复现已知结论： 1

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

IKEv2 在 IKE_INTERMEDIATE 交换中协商后量子预共享密钥，目的是让初始 IKE SA 本身（而不仅是后续交换）能够抵御量子攻击者。发起方和响应方先运行 IKE_SA_INIT，协商算法、交换 nonce，并根据 Diffie-Hellman 派生第一代 IKE SA 密钥。随后它们运行一次 IKE_INTERMEDIATE 交换：发起方提供 PPK 身份和 PPK Confirmation，响应方回复它选定的身份，之后双方根据 SKEYSEED' = prf+(PPK, SK_d) 重新计算所有 IKE SA 密钥。接下来的 IKE_AUTH 交换通过长期凭据对等方进行认证，认证基于一个签名块，其中包含双方的 nonce、身份以及中间交换的内容，其载荷受 PPK 派生密钥保护。

交换结束后，每一方都确信：对端确实针对这些 nonce、SPI 和中间转录运行了该交换；即使攻击者能计算 Diffie-Hellman 共享秘密，没有 PPK 也无法读取或伪造 IKE_AUTH 载荷。发起方还得到保证：响应方要么确认了它提供的某个 PPK 身份，要么在发起方要求 PPK 保护时建立失败。

参与方：

- **发起方**：提出 PPK，要求 PPK 保护。持有：自己的签名密钥；带有其 PPK_ID 的 PPK。
- **响应方**：选择 PPK 身份。持有：自己的签名密钥；该 PPK_ID 对应的 PPK；PPK 强制或可选策略。

图 1 展示了文稿所规定的交换。

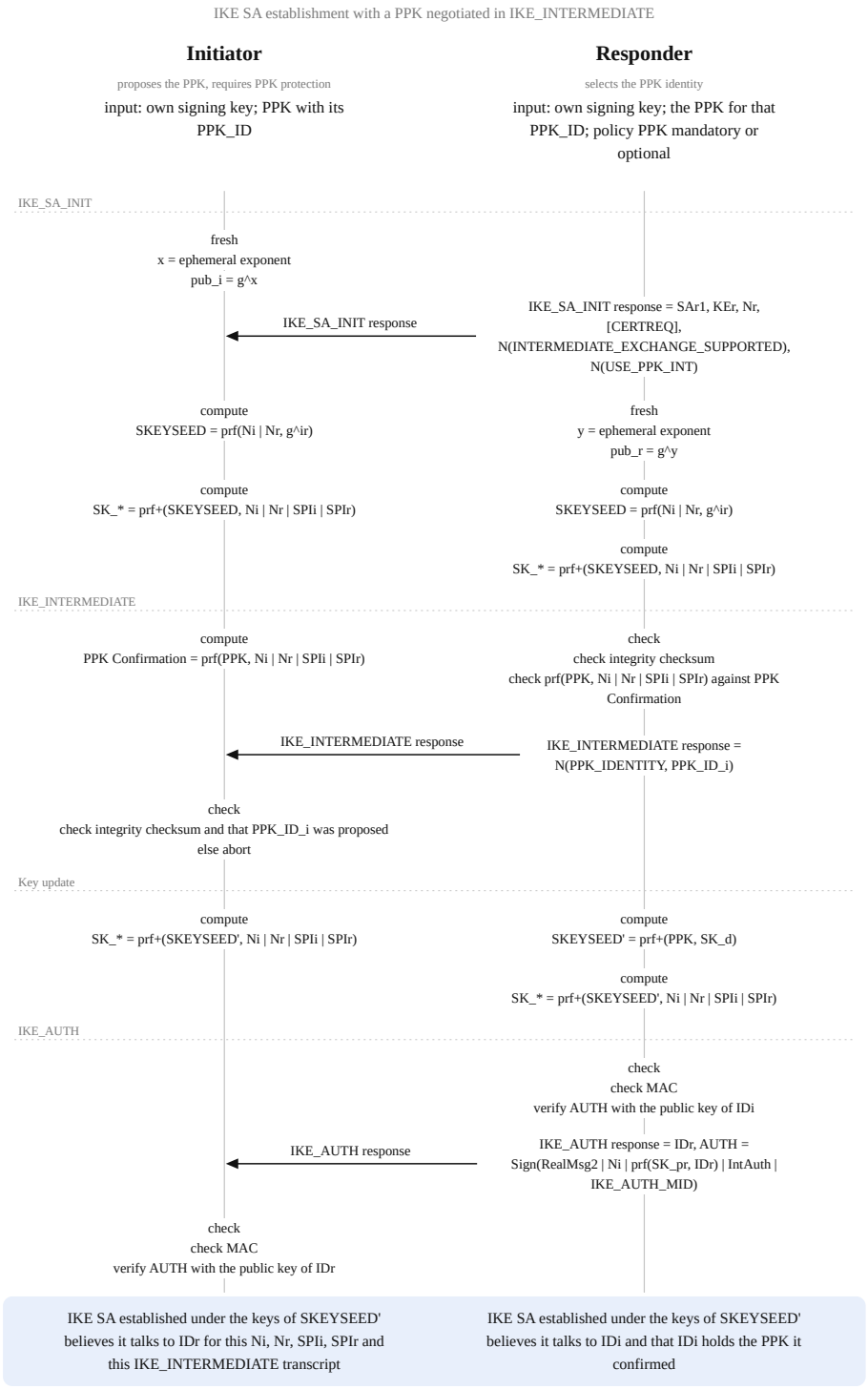


图 1. 文稿所规定的协议。

分析范围见附录 D：分析了什么、省略了什么，以及它基于文稿的哪些章节。

2 发现

分析有 1 项发现：以下内容文稿未写明。其中 1 项文稿是否写明不明确。文稿已写明的 1 项结果不计入，见附录 B。

在分析范围内，RFC 9867 兑现了其承诺：在拥有 PPK 秘密的情况下，IKE_AUTH 认证和由 SKEYSEED' 重新计算的 IKE SA 密钥都能抵御已攻破 Diffie-Hellman 和签名算法的攻击者，网络攻击者既不能伪造也不能重放 IKE_AUTH。第 3.1 节的策略规则也采用失败关闭：强制策略的响应方在没有确认 PPK 时绝不完成 IKE SA，要求 PPK 的发起方绝不接受无 PPK 的会话。文稿未说明的一点仍暴露在外：PPK_ID 和 PPK Confirmation 在 IKE_INTERMEDIATE 中传输，而该交换只受 IKE_SA_INIT 密钥保护，因此后量子攻击者，或自行应答 IKE_SA_INIT 的网络攻击者，可以读取它们。低熵 PPK 字典攻击的后果是已知结果，此处以其确切条件重述。所有结果都来自一个符号模型，该模型理想化原语，将后量子攻击者获得的 g^ir 视为转录的公开函数，且不建模 Key Exchange 载荷验证、Message ID 计数器或身份到 PPK 的策略。

攻击图使用图 1 的列。红色表示攻击者的行为。黄色标记某方发送了规定交换在该时点本不应有的消息，以及攻击所破坏的结果。

2.1 PPK 身份和确认在量子攻击者可攻破的密钥下传输

类型	协议规范本身的弱点
是否新发现	不确定：文稿只写了一部分，或没能检索 (rfc9242:463, rfc8784:567)
价值	中
涉及的性质	X01 （见第 3 节）
原文	s0013, s0016, s0031, s0561
依据	ProVerif attack queries `x01_crqc`, `x01_net`; Figures 2 and 3

发生了什么。 发起方在 IKE_INTERMEDIATE 请求中发送其 PPK_ID 和 PPK Confirmation，仅受 IKE_SA_INIT 产生的第一代 IKE SA 密钥保护。能计算该共享秘密的攻击者（量子计算机即可做到）从线路上读取这两个值。网络攻击者通过自行应答 IKE_SA_INIT 请求可以更廉价地获得同样的值，因为此时它就是该交换的 Diffie-Hellman 对端。

攻击者需要什么。 一台能计算 IKE_SA_INIT 共享秘密的量子计算机，而这正是整个扩展设计要抵御的；或者，对于第二条路径，只需能用自己的群元素应答 IKE_SA_INIT。

攻击者能得到什么。 攻击者得知会话使用哪个 PPK 组，并获得该会话的 prf(PPK, Ni|Nr|SPIi|SPIr)。该值使其能离线测试 PPK 猜测，因此人们自行选择而非生成的 PPK 可被恢复，会话的量子保护随之丧失。PPK 本身及由其混合的密钥不会暴露。

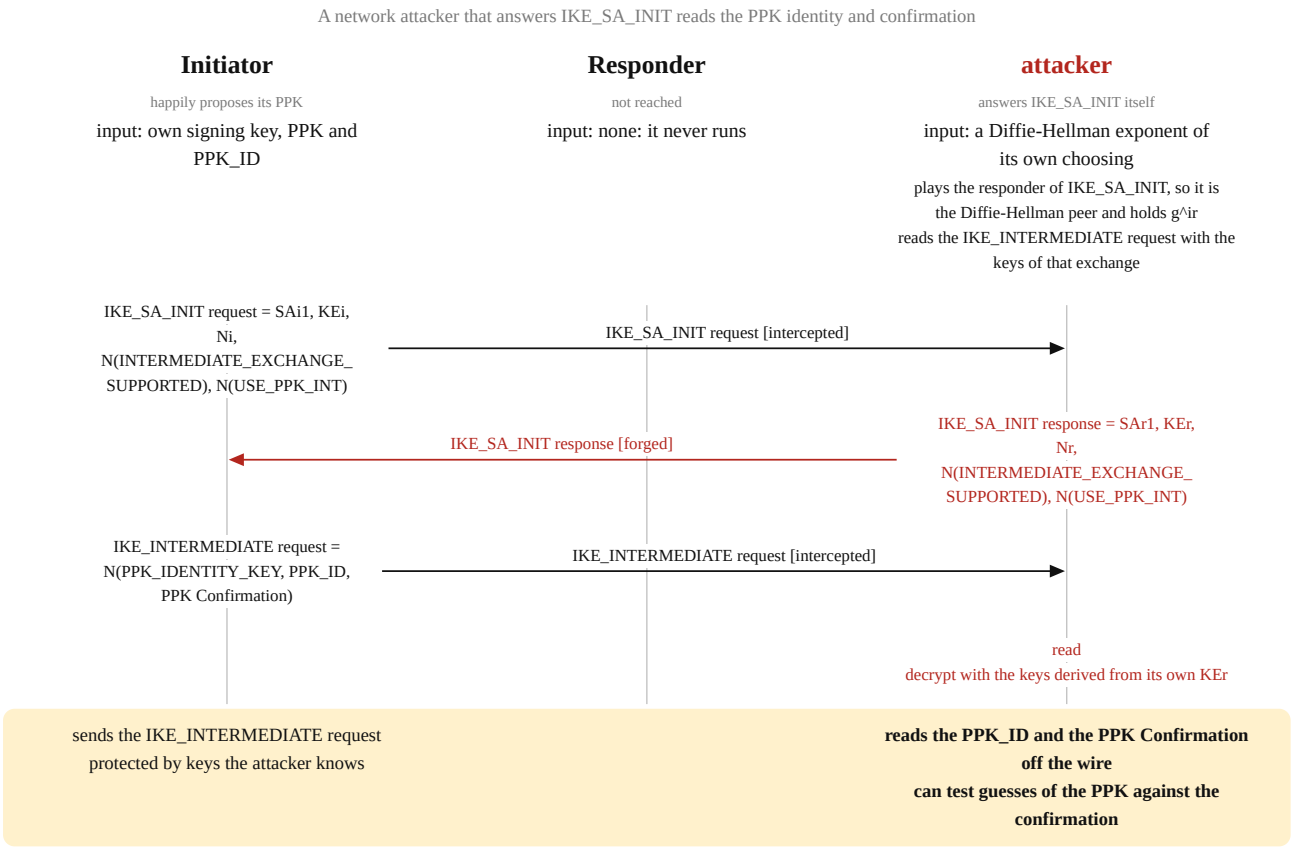


图 2. 应答 IKE_SA_INIT 的网络攻击者读取 PPK 身份和确认。性质 X01；攻击查询 x01_net。

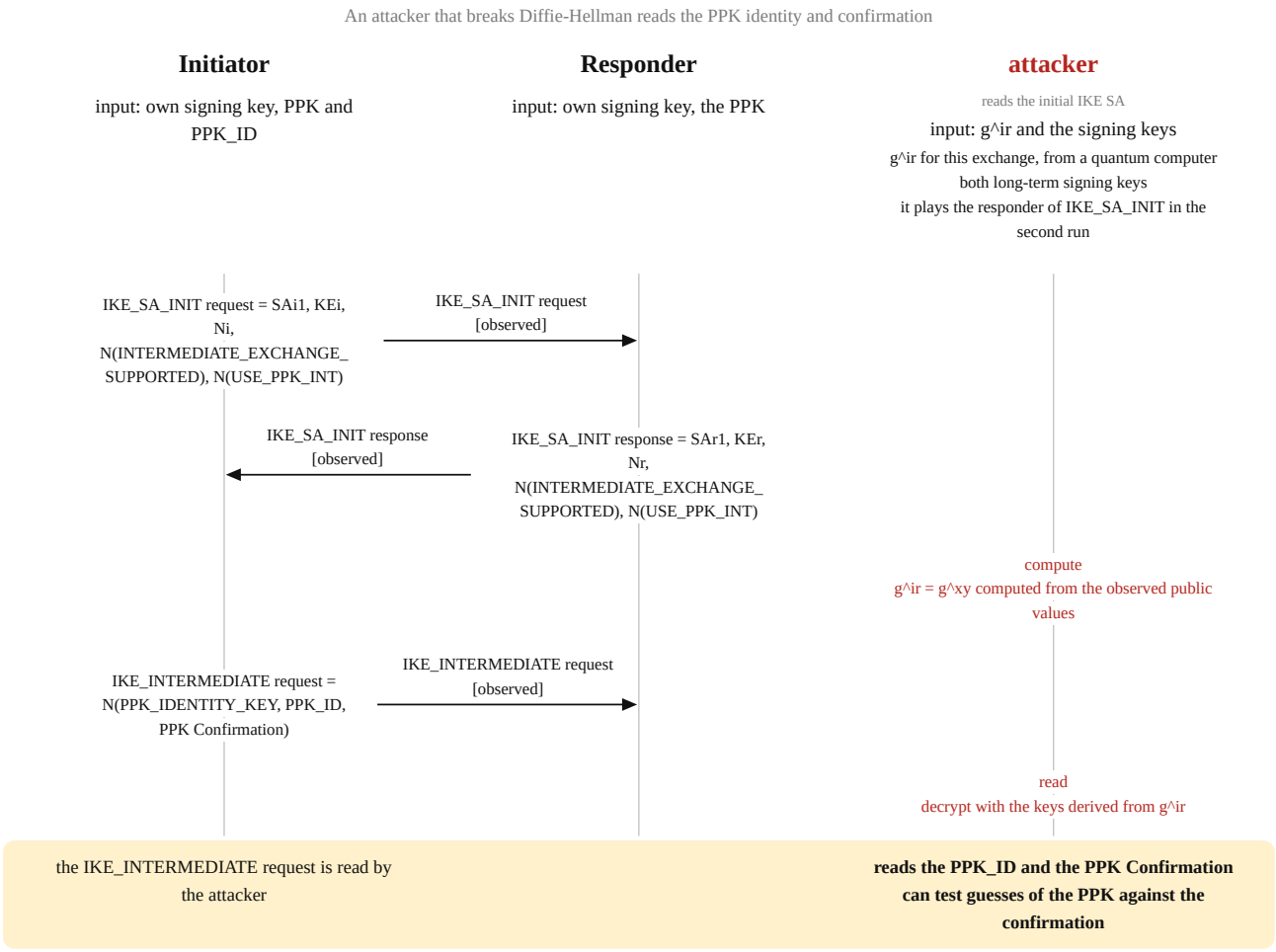


图 3. 攻破 Diffie-Hellman 的攻击者读取 PPK 身份和确认。性质 X01；攻击查询 x01_crqc, x01_net。

拟议修改。 无。任何消息改动都无法消除这种暴露：在 PPK 被混合之前，中间交换只能受量子攻击者可攻破的密钥保护，因此在那里发送的任何依赖 PPK 的值按设计就是可读的。补救措施是部署要求（如 RFC 8784 所述，使用至少 256 位的随机 PPK）并保持确认消息简短，而不是更改协议消息让模型去检查。

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	**IKE_AUTH 接受的匹配运行。** 每次发起方或响应方在 IKE_AUTH 中接受对端认证时，都存在一个匹配的对端真实运行，角色、双方意图身份以及 PPK_ID、Ni、Nr、SPIi、SPIr、IntAuth 一致。	无	成立	高	是
A04	**每次接受的独立对等方运行。** 每次 IKE_AUTH 成功接受都对应一个不同的对端真实运行；同一 IKE_INTERMEDIATE/IKE_AUTH 转录不能被重复接受为新的成功会话。	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
A08	**绑定到本会话的 PPK 字段。** 接受的 PPK_ID、PPK Confirmation、IntAuth 与 IKE_AUTH_MID 对应本次 IKE_SA_INIT 的 Ni、Nr、SPIi、SPIr 及本次 IKE_INTERMEDIATE 转录，并与 IKE_AUTH 中认证的身份一致。	无	成立	中	否
K01	**PPK 派生 IKE SA 密钥的保密性。** 攻击者不能推导出 PPK 值，也不能推导出由 PPK 与 SK_d 派生的 IKE SA 密钥 SK_d、SK_ei、SK_er、SK_ai、SK_ar、SK_pi、SK_pr。	无	成立	高	是
R05	**强制策略下无无 PPK 会话。** 在 PPK 强制策略下，若响应方没有匹配的 PPK 或值不匹配，IKE SA 建立必须失败；在可选策略下，若发起方要求 PPK 保护，未使用 PPK 的会话不得被发起方接受为成功的 PPK 会话。	无	成立	中	是
C04	**Diffie-Hellman 失效时 IKE_AUTH 受保护。** 攻击者获得 IKE_SA_INIT 的 Diffie-Hellman 共享秘密 g^ir 但未获得 PPK 时，不能推导出 IKE_AUTH 消息内容以及由 SKEYSEED' 派生的新 IKE SA 密钥。	IKE_SA_INIT 的 Diffie-Hellman 共享秘密 g^ir (IKE_SA_INIT 完成后、IKE_INTERMEDIATE 与 IKE_AUTH 之前或期间)	成立	中	是
A08.7	**如 Q1 所问的 PPK 绑定。** 接受的 PPK_ID、PPK Confirmation、IntAuth 与 IKE_AUTH_MID 对应本次 IKE_SA_INIT 的 Ni、Nr、SPIi、SPIr 及本次 IKE_INTERMEDIATE 转录，并与 IKE_AUTH 中认证的身份一致。	无	成立	中	否
U01	**如 Q2 所问的 DH 失效。** 攻击者获得 g^ir 但未获得 PPK 时，不能推导出 IKE_AUTH 内容以及由 SKEYSEED' 派生的新 IKE SA 密钥。	IKE_SA_INIT 的 Diffie-Hellman 共享秘密 g^ir (IKE_SA_INIT 完成后、IKE_INTERMEDIATE 与 IKE_AUTH 之前或期间)	成立	中	是
R05.9	**如 Q3 所问的 PPK 策略。** 在 PPK 强制策略下，若响应方没有匹配的 PPK 或值不匹配，IKE SA 建立必须失败；在可选策略下，若发起方要求 PPK 保护，未使用 PPK 的会话不得被发起方接受为成功的 PPK 会话。	无	成立	中	是
X01	**DH 失效下 PPK 字段隐藏。** 能解密初始 IKE SA（知晓 g^ir）的攻击者不会得知发起方提出的 PPK_ID 或它在 IKE_INTERMEDIATE 中发送的 PPK Confirmation 值。	IKE_SA_INIT 共享秘密 g^ir（因此可读取初始 IKE SA 的每条加密消息）及双方长期签名密钥，从会话开始起；对称原语仍不可及	不成立（2 个攻击）	中	不确定
X02	**PPK 不可通过离线猜测恢复。** 获得 PPK Confirmation 值的攻击者（通过在 IKE_SA_INIT/IKE_INTERMEDIATE 中冒充响应方）不能离线针对该值测试人为选择的 PPK 猜测并恢复 PPK。	若干候选 PPK 值，以及通过冒充响应方在 IKE_SA_INIT 中并读取 IKE_INTERMEDIATE 请求所获得的一次 IKE_INTERMEDIATE 交换的 PPK Confirmation 值；可离线测试猜测	攻击成立（文稿已写明）	低	是

“攻击成立（文稿已写明）”：证明器找到了这个攻击，而文稿自己已经写明它存在。这条性质不成立；这是已知结果，不算发现（附录 B）。

文稿写明而起草的清单里没有、由分析者补充的目标（见附录 D）：X01, X02.

所提出的问题与分析者的回答：

问题	回答	依据
Q1: PPK 标识与 intermediate transcript/身份绑定	是：响应方接受的 PPK_ID 与 PPK Confirmation 属于该会话的 Ni、Nr、SPIi 和 SPIr，IntAuth 绑定意味着完成 IKE_AUTH 的对端就是发送 intermediate 请求的一方；与对端身份的关联只针对单一身份进行检查，因此第 3.1 节的身份到 PPK 策略仍然悬而未决。	A08, A08.7, A03
Q2: 在 DH 已泄露而 PPK 未泄露时 IKE_AUTH 内容与新密钥保密	是：在 IKE_SA_INIT 共享密钥已知而 PPK 保密的情况下，既无法推导出 IKE_AUTH 内容，也无法推导出由 SKEYSEED' 重新计算的密钥，这正是要在 IKE_AUTH 之前混入 PPK 的意义所在。	C04, U01, K01
Q3: 回退策略和认证失败不会被当作成功的 PPK 会话	是，就文稿所述策略而言：强制要求 PPK 的响应方在未确认 PPK 时绝不会完成 IKE SA，要求 PPK 的发起方绝不会接受无 PPK 的会话。对照查询表明，容忍缺失 PPK 的对端确实会完成这样的会话。	R05, R05.9

4 本次分析的局限

这里的结果是协议模型上的结果：它说明所规定的消息和检查给出或未能给出什么，其中密码学被视为理想化的，且不涉及任何实现。

按分析者的陈述，本分析不覆盖以下内容：

- 符号模型：不涉及计算安全性，也不涉及对原语的量子攻击，除了通过公开 g^ir 和签名密钥所建模的那部分之外。
- 未对 Key Exchange 载荷校验建模，因此攻击者可以通过选择群元素成为任意交换的 Diffie-Hellman 对端；真实实现会拒绝非法的公开值。
- 消息 ID 被建模为固定常量：RFC 9242 第 3.2 节的序列规则、RFC 7296 第 2.3 节的接受窗口以及重传均未建模。
- 单一发起方身份和至多两个 PPK 值：主文稿 s0029 中的身份到 PPK 策略（SHOULD abort，MAY continue）未被覆盖。
- 仅有一个 IKE_INTERMEDIATE 交换；多个交换、CREATE_CHILD_SA、密钥更新、NAT 穿越、分片和 EAP 均超出范围。
- PPK Confirmation 取完整的 prf 输出而非其前八个八位组，IntAuth 取内层载荷而非 RFC 9242 第 3.3.2 节的字节布局。
- 可用性性质，例如 RFC 8784 第 6 节和 RFC 9242 第 5 节的 DoS 建议，无法向证明器提出。

每条性质仍悬而未决之处，以及什么能够解决它，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、该解读依据什么、能否按原样使用，以及它的价值何在。

A03: IKE_AUTH 接受的匹配运行

每次发起方或响应方在 IKE_AUTH 中接受对端认证时，都存在一个匹配的对端真实运行，角色、双方意图身份以及 PPK_ID、Ni、Nr、SPIi、SPIr、IntAuth 一致。

IKE_AUTH 认证在两个方向上都是可靠的：只有针对相同 nonce、SPI 和 intermediate transcript 运行过该交换的对端才会接受 AUTH 载荷。即使攻击者知道 IKE_SA_INIT 共享密钥和两个长期签名密钥，该保证依然成立，因为签名数据中承载 prf(SK_pi, IDi) 的部分来自由 PPK 推导出的 SK_pi，而这样的攻击者并不拥有它。面对网络攻击者，同样的对应关系也成立。

- 结果：成立；回答了所问：是；可带注意事项使用
- 价值 高：主文稿指出，即便面对主动攻击者，IKE_AUTH 交换也是量子安全的，因为 PPK 被混入密钥并用于认证；本分析对已经攻破 Diffie-Hellman 和签名的攻击者机械地复现了这一点。
- 文稿中已陈述：是。文稿中的位置：s0039, s0377, s0568, s0574
- 依据：Diffie-Hellman 以单一法则 g^xy = g^yx 建模，签名不可伪造性被理想化：签名只能由签名密钥生成。；后量子攻击者通过将 g^ir 设为转录的公开函数并公开两个长期签名密钥来建模；未建模任何真实的密码分析。；AUTH 被建模为对 RealMessage1 或 RealMessage2、对端 nonce、prf(SK_p, ID) 和 IntAuth 的签名；RFC 7296 第 2.15 节和 RFC 9242 第 3.3.2 节的字节布局被抽象化。；未对接收到的 Key Exchange 载荷的校验建模，因此任何群元素都被接受为对端的公开值。；每个角色只有一个身份：身份与其被允许的 PPK 之间的关联（主文稿 s0029）未建模。；对照查询仅在后量子攻击者的无 PPK 路径上被证伪，这表明正是 PPK 承载了该结果。
- 悬而未决：当 PPK 与多个对端共享且响应方可能以未与已认证身份关联的 PPK 继续时（主文稿 s0029），同样结论是否成立。
- 下一步：对两个发起方身份、两个 PPK 以及主文稿 s0029 的响应方策略建模，以观察持有某一个 PPK 的后量子攻击者能否以另一身份完成 IKE_AUTH。

A04: 每次接受的独立对等方运行

每次 IKE_AUTH 成功接受都对应一个不同的对端真实运行；同一 IKE_INTERMEDIATE/IKE_AUTH 转录不能被重复接受为新的成功会话。

没有任何已记录的 IKE_INTERMEDIATE/IKE_AUTH 转录会被接受两次：每次接受受 PPK 保护的 IKE SA 都对应着对端的一次不同运行。正是对两个 nonce、SPI、IntAuth 和 IKE_AUTH 消息 ID 的绑定阻止了重放，并且该性质对网络攻击者以及已攻破 Diffie-Hellman 和签名的攻击者都成立。

- 结果：成立；回答了所问：是；可带注意事项使用
- 价值 中：文稿要求在校验 IKE_INTERMEDIATE 中的消息 ID（rfc9242 s0555）并将 IKE_AUTH_MID 绑定进 IntAuth，但没有明确写出认证的单射性；结果正是这些规则所达成的。
- 文稿中已陈述：不明确。所依据的原文：s0377, s0555, s0569, s0573
- 依据：消息 ID 被建模为固定常量，而非采用 RFC 9242 第 3.2 节排序规则的计数器，因此序列检查本身未建模。；与 A03 相同的原语理想化。；单射性针对响应方接受发起方 AUTH 的情形给出；另一方向通过非单射的对应关系给出。；对照为移除 PPK 保护的同一性质，该性质被证伪。

- 悬而未决：消息 ID 的接受窗口与重传行为（RFC 7296 第 2.2 和 2.3 节）未建模。
- 下一步：对双方的消息 ID 计数器以及 RFC 9242 第 3.2 节的规则建模，以检查该检查本身。

A08: 绑定到本会话的 PPK 字段

接受的 PPK_ID、PPK Confirmation、IntAuth 与 IKE_AUTH_MID 对应本次 IKE_SA_INIT 的 Ni、Nr、SPIi、SPIr 及本次 IKE_INTERMEDIATE 转录，并与 IKE_AUTH 中认证的身份一致。

响应方接受的 PPK 协商与本 IKE SA 绑定：PPK Confirmation 针对 Ni、Nr、SPIi 和 SPIr 进行校验，IntAuth 将 intermediate 消息绑定进标识对端的 AUTH 载荷。该主张中身份一侧只针对单一发起方身份进行检查，因此身份与其被授权 PPK 之间的关联未被覆盖。

- 结果：成立；回答了所问：部分；可带注意事项使用
- 价值 中：在文稿中检索了 PPK、会话参数与身份之间的关联：主文稿 s0013-s0014 定义了基于会话值的确认，rfc9242 s0568-s0574 绑定了 intermediate 转录，主文稿 s0029 指出响应方可能只在稍后才会注意到 PPK 与身份不匹配。没有任何原文将该组合绑定陈述为一条性质，也没有任何原文陈述其不成立。
- 文稿中已陈述：否。所依据的原文：s0013, s0014, s0018, s0029, s0568, s0573
- 依据：一个 PPK 和一个发起方身份，因此主文稿 s0029 的策略问题未建模。；PPK Confirmation 被建模为完整的 prf 输出，而非截断为八个八位组。；RFC 9242 第 3.3.2 节的 A 和 P 块被抽象为消息的内层载荷。
- 悬而未决：发起方提出多个 PPK 身份的情形（主文稿 s0016）以及主文稿 s0029 的身份到 PPK 策略。
- 下一步：对两个 PPK 身份和两个发起方身份建模，以在后量子攻击者下检查主文稿 s0029 的策略。

A08.7: 如 Q1 所问的 PPK 绑定

接受的 PPK_ID、PPK Confirmation、IntAuth 与 IKE_AUTH_MID 对应本次 IKE_SA_INIT 的 Ni、Nr、SPIi、SPIr 及本次 IKE_INTERMEDIATE 转录，并与 IKE_AUTH 中认证的身份一致。

对于问题 Q1，同样的结果成立：接受的 PPK_ID 与 PPK Confirmation 属于本 IKE SA 的 nonce 和 SPI，且完成 IKE_AUTH 的对端就是发送 intermediate 请求的一方。该绑定的身份一侧仅能达到所建模的单一身份所允许的强度。

- 结果：Holds；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：没有原文单元将这种组合绑定陈述为一条性质，也没有说它不成立；相关片段位于 main s0013-s0014 和 rfc9242 s0568-s0574。
- 文稿中是否陈述：否。所依据的原文：s0013、s0014、s0018、s0029、s0568、s0573
- 依据：与 A08 相同的理想化和单一身份。；PPK Confirmation 在模型中未被截断。
- 未决：若干拟议的 PPK 身份以及身份到 PPK 的策略。
- 下一步：添加第二个身份和第二个 PPK，以测试 main s0029 的策略。

K01: PPK 派生 IKE SA 密钥的保密性

攻击者不能推导出 PPK 值，也不能推导出由 PPK 与 SK_d 派生的 IKE SA 密钥 SK_d、SK_ei、SK_er、SK_ai、SK_ar、SK_pi、SK_pr。

PPK 本身在两种情况下都对攻击者未知，并且由 SKEYSEED' = prf+(PPK, SK_d) 重新计算的 IKE SA 密钥无法从整个会话记录中推导出来，即使攻击者知道 g^ir 和两个签名密钥也不行。对于网络攻击者同样成立，而且在这里保护是双重冗余的，因为它也不知道 g^ir。

- 结果：Holds；是否回答了所问：是；可在有保留条件的情况下使用

- 价值高：RFC 8784 指出，当 PPK 具有足够熵时，SK_d 是 PPK 的函数，量子攻击者无法恢复它；分析针对 RFC 9867 密钥调度复现了这一点。
- 文稿中是否陈述：是。文稿中何处陈述：s0033、s0035、s0036
- 依据：prf 和 prf+ 被理想化为单向函数，每个标签的输出相互独立；实际构造将密钥作为一个 prf+ 流的切片。；密钥在一个已确认 PPK 的会话中被证明为秘密；运行结束时的 PPK 揭示使它们可被恢复，对照查询表明了这一点。；SK_d 仅用于派生 Child SA 密钥，超出本范围，且不在显式密钥测试之内。
- 未决：对于之后执行 CREATE_CHILD_SA 重新生成密钥的 IKE SA，其密钥是否同样成立，这超出本范围。
- 下一步：将模型扩展到 CREATE_CHILD_SA，以检查 PPK 派生的 SK_d 是否保护重新生成密钥后的密钥。

R05: 强制策略下无无 PPK 会话

在 PPK 强制策略下，若响应方没有匹配的 PPK 或值不匹配，IKE SA 建立必须失败；在可选策略下，若发起方要求 PPK 保护，未使用 PPK 的会话不得被发起方接受为成功的 PPK 会话。

失败关闭规则有效：在强制要求 PPK 的策略下，当 PPK 未被确认时，响应方从不完成 IKE SA；而要求 PPK 保护的发起方从不把无 PPK 的会话视为受 PPK 保护的会话。两个结果都针对规范所规定的分支，对照查询表明，容忍缺失 PPK 的对端确实会完成这样的会话，因此差异在于策略检查而非模型。

- 结果：Holds；是否回答了所问：是；可在有保留条件的情况下使用
- 价值中：RFC 8784 指出，当至少一个对端强制要求 PPK 时，拥有量子计算机的攻击者所发起的降级会被检测到；而在可选策略下，配置错误会在没有量子保护的情况下建立 IKE SA；两者均被复现。
- 文稿中是否陈述：是。文稿中何处陈述：s0021、s0023、s0025
- 依据：策略分支依据 main s0021、s0023 和 s0025 建模，并包含 s0021 的失败分支；RFC 8784 第 6 节的重传和 DoS 处理未建模。；不匹配情况使用第二个 PPK 值，代表配置错误的一对，而非攻击者猜测 PPK。；当已确认的 PPK 未列在对端身份下时（main s0029），响应方是否在 IKE_AUTH 中中止，未建模。
- 未决：main s0029 的 MAY-continue 选项，以及 RFC 8784 第 6 节讨论的中止与等待行为。
- 下一步：对 main s0029 的身份到 PPK 策略建模，以观察 MAY 选项给攻击者带来了什么。

R05.9：如 Q3 所问的 PPK 策略

在 PPK 强制策略下，若响应方没有匹配的 PPK 或值不匹配，IKE SA 建立必须失败；在可选策略下，若发起方要求 PPK 保护，未使用 PPK 的会话不得被发起方接受为成功的 PPK 会话。

关于问题 Q3：在规范所陈述的策略下，失败答案和回退到普通 IKEv2 都不会被视为成功的 PPK 会话。强制策略的响应方以 AUTHENTICATION_FAILED 停止，而要求 PPK 的发起方会中止而不是继续。

- 结果：Holds；是否回答了所问：是；可在有保留条件的情况下使用
- 价值中：复现了 RFC 8784 的陈述，即当至少一个对端强制要求 PPK 时，降级会被检测到。
- 文稿中是否陈述：是。文稿中何处陈述：s0021、s0023、s0025
- 依据：与 R05 相同的策略分支建模。；RFC 8784 第 6 节的 DoS 和重传建议未建模，因此模型对滥用中止没有任何说明。
- 未决：注入不带 USE_PPK_INT 的响应导致的 DoS 后果（RFC 8784 第 6 节）。
- 下一步：对重传行为建模，以检查 RFC 8784 第 6 节的可用性建议。

X01: DH 失效下 PPK 字段隐藏

能够解密初始 IKE SA（知道 g^ir）的攻击者不会获知发起方提出的 PPK_ID，也不会获知其在 IKE_INTERMEDIATE 中发送的 PPK Confirmation 值。

IKE_INTERMEDIATE 请求仅受 IKE_SA_INIT 产生的密钥保护，因此任何能读取该交换的人都能读取 PPK_ID 和 PPK Confirmation：知道 g^ir 的量子攻击者从线路上读取它们，而网络攻击者通过自己应答 IKE_SA_INIT 从而成为 Diffie-Hellman 对端来读取它们。泄露的是使用了哪个 PPK 组，以及一个可用来测试 PPK 猜测的值，而不是 PPK 本身。

- 结果：不成立（2 个攻击）；是否回答了所问：是；可在有保留条件的情况下使用
- 价值中：RFC 9242 指出中间数据受到保护，可抵御被动窃听者；RFC 8784 指出解密初始 IKE SA 的量子攻击者能看到除受 PPK 保护的密钥之外的一切；主文稿没有说明中间交换暴露了什么，因此该后果是隐含的而非陈述的。
- 文稿中是否陈述：不明确。所依据的原文：s0013、s0016、s0561
- 依据：确认值被建模为完整的 prf 输出，而非其前八个八位组。；允许网络攻击者用其选择的群元素应答 IKE_SA_INIT，而执行校验的实现会拒绝这一点。；按照通知的设计，PPK_ID 被视为非秘密。
- 未决：八个八位组的确认值暴露在实践中是否重要，这取决于 PPK 熵，是一个计算问题。
- 下一步：询问计算证明器或密码学论证：八个八位组的确认值和 PPK_ID 在每个会话中的泄露，在多个会话中允许什么。

X02: PPK 不可通过离线猜测恢复

获得 PPK Confirmation 值（通过在 IKE_SA_INIT/IKE_INTERMEDIATE 中冒充响应方）的攻击者，不能离线针对它测试对人类选择的 PPK 的猜测并恢复 PPK。

人们选择的 PPK（而非随机的 256 位值）可以通过针对一次交换的 PPK Confirmation 测试猜测来恢复，而攻击者通过冒充响应方获得该确认值。对于 RFC 8784 所要求大小的随机 PPK，这不可行，因此该结果重述了部署要求。

- 结果：攻击成立（文稿中已陈述）；是否回答了所问：是；可在有保留条件的情况下使用
- 价值低：RFC 8784 在其安全考虑中指出，冒充服务器的攻击者即使使用传统计算机，也能对可能的 PPK 值进行字典搜索；并且从口令或名称派生 PPK 是不安全的。
- 文稿中是否陈述：是。文稿中何处陈述：s0013
- 依据：字典攻击者通过弱秘密测试建模，该测试假设攻击者能针对其见过的值测试猜测。；确认值在模型中未被截断；实际的八个八位组截断限制每次测试，而非阻止它。
- 下一步：无：对 PPK 熵的要求就是补救措施，且已经陈述。

C04: Diffie-Hellman 失效时 IKE_AUTH 受保护

攻击者获得 IKE_SA_INIT 的 Diffie-Hellman 共享秘密 g^ir 但未获得 PPK 时，不能推导出 IKE_AUTH 消息内容以及由 SKEYSEED' 派生的新 IKE SA 密钥。

知道 g^ir 但不知道 PPK 的量子攻击者既不能获得新的 IKE SA 密钥，也不能获得 IKE_AUTH 载荷。原因是 SKEYSEED' 由 PPK 和先前的 SK_d 计算得出，因此仅持有旧共享秘密的攻击者无法跟进密钥更新。

- 结果：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：RFC 8784 指出，解密初始 IKE SA 的量子攻击者能看到除受 PPK 保护的密钥之外的一切；本次分析在 RFC 9867 的 IKE_AUTH 上复现了这一点。
- 文稿中已说明：是。文稿中的位置：s0033、s0035、s0039

- 依据：按 RFC 8784 的要求，假定 PPK 是秘密的且具有高熵。；prf+ 被理想化，并且保密性通过一项显式测试来证明：攻击者交出它声称知道的密钥。；攻击者被赋予 g^ir，作为转录的公开函数，这比此处建模的任何真实量子攻击都更强。
- 待解决：身份和其余 IKE_AUTH 字段是否对该攻击者隐藏：模型把整个载荷作为一个整体来保护。
- 下一步：在模型中拆分 IKE_AUTH 的各个字段，以报告后量子攻击者能获知其中哪些字段。

U01: 如 Q2 所问的 DH 失效

攻击者获得 g^ir 但未获得 PPK 时，不能推导出 IKE_AUTH 内容以及由 SKEYSEED' 派生的新 IKE SA 密钥。

对于问题 Q2，答案与 C04 相同：在 g^ir 泄露且 PPK 保密的情况下，IKE_AUTH 内容和新 IKE SA 密钥都无法推导出来。PPK 混合是 IKE_AUTH 之前的最后一个动作，因此用旧密钥保护的内容不会带入其中。

- 结果：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：与 C04 相同的 RFC 8784 陈述。
- 文稿中已说明：是。文稿中的位置：s0033、s0035
- 依据：与 C04 相同的理想化：高熵的秘密 PPK、理想化的 prf+，以及在后量子世界中公开的 g^ir。
- 待解决：IKE_INTERMEDIATE 交换本身不受此类攻击者保护；参见关于 PPK 字段的发现。
- 下一步：此主张无需下一步；中间交换的暴露由关于 PPK 字段的单独目标覆盖。

附录 B：复现的已知结论

如果某项性质如文稿已经陈述的那样不成立，或者文稿将其搁置，那就不算发现。以下属于这一类：分析在模型上复现了它，并给出了确切条件。

B.1 低熵 PPK 可从一次确认中恢复，而文稿要求它不可被恢复

类型	协议规范本身的弱点
文稿出处	rfc8784:541
价值	低
涉及的性质	X02, X01 （见第 3 节）
原文	s0013
依据	ProVerif 攻击查询 `x02_guess`

发生了什么。 PPK 确认值是 prf(PPK, Ni|Nr|SPIi|SPIr) 截断到八个八位组，任何扮演 IKE_SA_INIT 响应方的参与方都能获得它。持有几个看似合理的 PPK 值的攻击者可以离线将这些值与那个值进行比对测试，从而得知其中之一是否是正在使用的 PPK。

攻击者需要什么。 能够应答 IKE_SA_INIT 请求并读取随后的 IKE_INTERMEDIATE 请求，这是任何在途攻击者都具备的，外加一个取自小候选集的 PPK。

攻击者能得到什么。 对于由人选择的 PPK，该 SA 的量子保护就会丧失，攻击者随后可以相互冒充对等方，因为认证既绑定到签名也绑定到 PPK。

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，以及每项攻击及分析者的判定。

目标	级别	界	查询	对照	攻击	主张
A03	proved		auth_net	checked		4 proved
A04	proved		inj_net	checked		2 proved
A08	proved		auth_net	checked		2 proved
K01	proved		ppk_sec	checked		4 proved
R05	proved		r05_mand	checked		2 proved
C04	proved		keys_crqc	checked		1 proved
A08.7	proved		auth_net	checked		2 proved
U01	proved		keys_crqc	checked		1 proved
R05.9	proved		r05_mand	checked		2 proved
X01	none				x01_crqc (holds_in_source); x01_net (holds_in_source)	2 attack
X02	none				x02_guess (holds_in_source)	1 attack

逐项主张，按分析者对每项主张的措辞；每项的答案是证明器给出的：

目标	主张	攻击者	回答	查询	对照
A03	在仅网络攻击者下，响应方仅在匹配的发起方运行为相同的 Ni、Nr、SPIi、SPIr 和相同的 IKE_INTERMEDIATE 转录发送了该 AUTH 载荷时，才在 IKE_AUTH 中接受发起方的 AUTH 载荷。	`network`	proved	auth_net	checked
A03	即使攻击者知道 g^ir 和双方长期签名密钥，只要 PPK 保密，响应方的匹配运行保证仍然成立。	`crqc`	proved	auth_crqc	checked
A03	在仅网络攻击者下，发起方仅在匹配的响应方运行为相同的 Ni、Nr、SPIi、SPIr 和相同的 IKE_INTERMEDIATE 转录发送了该 AUTH 载荷时，才在 IKE_AUTH 中接受响应方的 AUTH 载荷。	`network`	proved	authr_net	checked
A03	即使攻击者知道 g^ir 和长期签名密钥，只要 PPK 保密，发起方的匹配运行保证仍然成立。	`crqc`	proved	authr_crqc	checked
A04	在仅网络攻击者下，PPK 保护的 IKE SA 中响应方的每次 IKE_AUTH 接受都对应不同的发起方运行：相同的 IKE_INTERMEDIATE/IKE_AUTH 转录不会被接受两次。	`network`	proved	inj_net	checked
A04	PPK 保护的 IKE SA 中 IKE_AUTH 接受的单射性对于知道 g^ir 和长期签名密钥且不知道 PPK 的攻击者也成立。	`crqc`	proved	inj_crqc	checked
A08	响应方接受的 PPK 协商（PPK_ID 和 PPK 确认值）属于此 IKE SA 的 Ni、Nr、SPIi、SPIr，并且它在 IKE_AUTH 中认证的对等方身份就是发送该 IKE_INTERMEDIATE 请求的那个。	`network`	proved	auth_net	checked
A08	被接受的 PPK 字段、IKE_INTERMEDIATE 转录（IntAuth）与已认证身份之间的绑定对于知道 g^ir 和长期签名密钥的攻击者也成立。	`crqc`	proved	auth_crqc	checked

目标	主张	攻击者	回答	查询	对照
K01	由 SKEYSEED' = prf+(PPK, SK_d) 重新计算的 SK_ei、SK_er、SK_ai、SK_ar、SK_pi 和 SK_pr 不能被仅网络攻击者推导出来。	`network`	proved	keys_net	checked
K01	即使对于知道 g^ir 和长期签名密钥的攻击者，由 PPK 派生的 IKE SA 密钥 SK_* 仍不可推导。	`crqc`	proved	keys_crqc	checked
K01	PPK 值本身不能被仅网络攻击者推导出来。	`network`	proved	ppk_sec	checked
K01	PPK 值不能被知道 g^ir 和长期签名密钥的攻击者推导出来。	`crqc`	proved	ppk_sec	checked
R05	在强制 PPK 的响应方策略下，当拟议的 PPK 未被确认时不会完成任何 IKE SA（而是 AUTHENTICATION_FAILED）。	`network`	proved	r05_mand	checked
R05	在可选的响应方策略下，要求 PPK 保护的发起方绝不会完成未协商 PPK 的会话。	`network`	proved	r05_req	checked
C04	在 g^ir 已知且 PPK 保密的情况下，由 SKEYSEED' 派生的新 IKE SA 密钥保持隐藏，因此用它们保护的 IKE_AUTH 内容不可读。	`crqc`	proved	keys_crqc	checked
A08.7	Q1：被接受的 PPK_ID、PPK 确认值和 IntAuth 对应于此 IKE_SA_INIT 的 nonce 和 SPI 以及 IKE_AUTH 中认证的身份，在仅网络攻击者下。	`network`	proved	auth_net	checked
A08.7	Q1：对于知道 g^ir 和长期签名密钥但不知道 PPK 的攻击者，同样的绑定成立。	`crqc`	proved	auth_crqc	checked
U01	Q2：在 g^ir 泄露且 PPK 保密的情况下，IKE_AUTH 内容和新 IKE SA 密钥不可推导。	`crqc`	proved	keys_crqc	checked
R05.9	Q3：在强制 PPK 策略下，当拟议的 PPK 未被确认时不会完成任何 IKE SA；响应方回答 AUTHENTICATION_FAILED。	`network`	proved	r05_mand	checked
R05.9	Q3：要求 PPK 保护的发起方绝不会把无 PPK 的会话视为成功的 PPK 会话。	`network`	proved	r05_req	checked
X01	能读取初始 IKE SA 的攻击者会获知 IKE_INTERMEDIATE 中发送的 PPK_ID 和 PPK 确认值。	`crqc`	attack (holds_in_source)	x01_crqc	
X01	在 IKE_SA_INIT 中冒充响应方的网络攻击者会获知 PPK_ID 和 PPK 确认值。	`network`	attack (holds_in_source)	x01_net	
X02	由人选择的 PPK 可以通过将猜测离线比对到攻击者冒充响应方所获得的 PPK 确认值来恢复。	`dictionary`	attack (holds_in_source)	x02_guess	

附录 D：分析是怎么跑的

LLM 分析者根据文稿构建协议模型，并把每项性质交给 ProVerif；第 3 节中的每个结果都是证明器的答案。

分析了什么

协议	IKEv2 PPK in IKE_INTERMEDIATE
版本	rfc9867
分析范围	固定一个 IKE_INTERMEDIATE PPK 协商后签名 IKE_AUTH；完整使用本 RFC 的 key update/认证绑定；区分 PPK 强制和可选策略。排除 CREATE_CHILD_SA 和多次 intermediate。
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	586 个编号原文单元（194124 字节），来自下列章节。本报告中的 s0001 这类引用就是其中之一

分析所依据的文稿章节：

文稿	章节	标题
main	3.1	Creating Initial IKE SA
main	3.1.1	Computing IKE SA Keys
main	4	Security Considerations
rfc7296	1	Introduction
rfc7296	1.1	Usage Scenarios
rfc7296	1.1.1	Security Gateway to Security Gateway in Tunnel Mode
rfc7296	1.1.2	Endpoint-to-Endpoint Transport Mode
rfc7296	1.1.3	Endpoint to Security Gateway in Tunnel Mode
rfc7296	1.1.4	Other Scenarios
rfc7296	1.2	The Initial Exchanges
rfc7296	1.3	The CREATE_CHILD_SA Exchange
rfc7296	1.3.1	Creating New Child SAs with the CREATE_CHILD_SA Exchange
rfc7296	1.3.2	Rekeying IKE SAs with the CREATE_CHILD_SA Exchange
rfc7296	1.3.3	Rekeying Child SAs with the CREATE_CHILD_SA Exchange
rfc7296	1.4	The INFORMATIONAL Exchange
rfc7296	1.4.1	Deleting an SA with INFORMATIONAL Exchanges
rfc7296	1.5	Informational Messages outside of an IKE SA
rfc7296	1.6	Requirements Terminology
rfc7296	1.7	Significant Differences between RFC 4306 and RFC 5996
rfc7296	1.8	Differences between RFC 5996 and This Document
rfc7296	2	IKE Protocol Details and Variations
rfc7296	2.1	Use of Retransmission Timers

文稿	章节	标题
rfc7296	2.2	Use of Sequence Numbers for Message ID
rfc7296	2.3	Window Size for Overlapping Requests
rfc7296	2.4	State Synchronization and Connection Timeouts
rfc7296	2.5	Version Numbers and Forward Compatibility
rfc7296	2.6	IKE SA SPIs and Cookies
rfc7296	2.6.1	Interaction of COOKIE and INVALID_KE_PAYLOAD
rfc7296	2.7	Cryptographic Algorithm Negotiation
rfc7296	2.8	Rekeying
rfc7296	2.8.1	Simultaneous Child SA Rekeying
rfc7296	2.8.2	Simultaneous IKE SA Rekeying
rfc7296	2.8.3	Rekeying the IKE SA versus Reauthentication
rfc7296	2.9	Traffic Selector Negotiation
rfc7296	2.9.1	Traffic Selectors Violating Own Policy
rfc7296	2.9.2	Traffic Selectors in Rekeying
rfc7296	2.10	Nonces
rfc7296	2.11	Address and Port Agility
rfc7296	2.12	Reuse of Diffie-Hellman Exponentials
rfc7296	2.13	Generating Keying Material
rfc7296	2.14	Generating Keying Material for the IKE SA
rfc7296	2.15	Authentication of the IKE SA
rfc7296	2.16	Extensible Authentication Protocol Methods
rfc7296	2.17	Generating Keying Material for Child SAs
rfc7296	2.18	Rekeying IKE SAs Using a CREATE_CHILD_SA Exchange
rfc7296	2.19	Requesting an Internal Address on a Remote Network
rfc7296	2.20	Requesting the Peer's Version
rfc7296	2.21	Error Handling
rfc7296	2.21.1	Error Handling in IKE_SA_INIT
rfc7296	2.21.2	Error Handling in IKE_AUTH
rfc7296	2.21.3	Error Handling after IKE SA is Authenticated
rfc7296	2.21.4	Error Handling Outside IKE SA
rfc7296	2.22	IPComp
rfc7296	2.23	NAT Traversal
rfc7296	2.23.1	Transport Mode NAT Traversal
rfc7296	2.24	Explicit Congestion Notification (ECN)
rfc7296	2.25	Exchange Collisions
rfc7296	2.25.1	Collisions while Rekeying or Closing Child SAs

文稿	章节	标题
rfc7296	2.25.2	Collisions while Rekeying or Closing IKE SAs
rfc9242	3	Intermediate Exchange Details
rfc9242	3.1	Support for Intermediate Exchange Negotiation
rfc9242	3.2	Using Intermediate Exchange
rfc9242	3.3	The IKE_INTERMEDIATE Exchange Protection and Authentication
rfc9242	3.3.1	Protection of IKE_INTERMEDIATE Messages
rfc9242	3.3.2	Authentication of IKE_INTERMEDIATE Exchanges
rfc9242	3.4	Error Handling in the IKE_INTERMEDIATE Exchange

源文步骤在文稿中为协议定位的用途是：固定一个 IKE_INTERMEDIATE PPK 协商后签名 IKE_AUTH；完整使用本 RFC 的 key update/认证绑定；区分 PPK 强制和可选策略。排除 CREATE_CHILD_SA 和多次 intermediate。

对照文稿定性质

在编写查询之前，分析者先把草拟的性质清单与文稿本身对协议用途的说明作了对照。名称、每条性质所涉及的内容以及文稿的说法都出自分析者的解读；文中所指的位置在文稿中确实存在。

ID	简称	对象	文稿怎么说	出处
A03	IKE_AUTH 接受的匹配运行	发起方和响应方各自在 IKE_AUTH 中接受对端的 AUTH 载荷时，都确信对端以相同角色、身份、PPK_ID、Ni、Nr、SPIi、SPIr 和 IntAuth 进行了一次匹配运行。	主文稿称，初始 IKE SA（包括 IKE_AUTH 交换）即使面对主动攻击者也是量子安全的，因为 PPK 被混入 SK_* 并用于认证；AUTH 载荷是对 IKE SA 的认证（rfc7296 s0377），由 IntAuth 绑定到 IKE_INTERMEDIATE 内容（rfc9242 s0565-s0574）。	s0039, s0377, s0565, s0568, s0574
A04	每次接受的独立对等方运行	给定 IKE SA 建立的每次被接受的 IKE_AUTH 都对应着对端的一次不同运行：同一份 IKE_INTERMEDIATE/IKE_AUTH 记录不会被当作新的成功会话接受两次。	消息 ID 必须在 IKE_INTERMEDIATE 中校验（rfc9242 s0555），且 IKE_AUTH_MID 是 IntAuth 的一部分（rfc9242 s0569, s0573）；AUTH 载荷对两个 nonce 都签名（rfc7296 s0377）。文稿没有逐字写明单射性。	s0377, s0555, s0569, s0573
A08	绑定到本会话的 PPK 字段	响应方对 PPK_ID 和 PPK Confirmation 的接受，以及双方对 IntAuth 和 IKE_AUTH_MID 的接受，都对应本次 IKE_SA_INIT 的 Ni、Nr、SPIi、SPIr 以及本次 IKE_INTERMEDIATE 记录，并与 IKE_AUTH 中认证的身份一致。	PPK Confirmation 是 prf(PPK, Ni|Nr|SPIi|SPIr)，让响应方检查自己是否对给定 PPK_ID 持有同一 PPK（main s0013, s0014）；IntAuth 把 IKE_INTERMEDIATE 消息绑定进 AUTH（rfc9242 s0568-s0574）。响应方可能直到 IKE_AUTH 才发现该 PPK 与发起方身份并无关联（main s0029）。	s0013, s0014, s0018, s0029, s0568, s0573

ID	简称	对象	文稿怎么说	出处
K01	PPK 派生 IKE SA 密钥的保密性	PPK 以及由它重新计算的 IKE SA 密钥（SKEYSEED'、SK_d、SK_ei、SK_er、SK_ai、SK_ar、SK_pi、SK_pr）对攻击者保密。	SKEYSEED' = prf+(PPK, SK_d)，SK_* 密钥在 IKE_AUTH 之前由它重新计算（main s0032-s0037）；rfc8784 指出 SK_d 是 PPK 的函数，并假定 PPK 具有高熵，量子攻击者无法恢复它（rfc8784:556）。	rfc8784:556, s0032, s0033, s0034, s0035, s0036
R05	强制策略下无无 PPK 会话	在 PPK 强制的响应方策略下，若没有任何提议的 PPK 匹配，则绝不创建 IKE SA（而是 AUTHENTICATION_FAILED）；在可选策略下，要求 PPK 保护的发起方不会把无 PPK 会话当作成功的 PPK 保护会话接受。	主文稿 s0021（强制：AUTHENTICATION_FAILED 并中止）、s0023-s0025（可选：无 PPK_IDENTITY，且若量子抗性是要求，发起方必须中止）、s0006 和 s0027（表 1）、s0020（未提议的身份是致命的）；rfc8784:619-627 指出，当至少一方强制使用 PPK 时，拥有量子计算机的攻击者实施的降级会被检测到。	rfc8784:619, s0006, s0020, s0021, s0023, s0025, s0027
C04	Diffie-Hellman 失效时 IKE_AUTH 受保护	IKE_AUTH 内容以及由 SKEYSEED' 派生的 IKE SA 密钥，对知道 IKE_SA_INIT 共享秘密 g^ir 但不知道 PPK 的攻击者保持隐藏。	主文稿 s0032-s0036 在 IKE_AUTH 之前把 PPK 混入 SK_d，s0039 声明 IKE_AUTH 交换即使面对主动攻击者也是量子安全的；rfc8784:567 指出，解密了初始 IKE SA 的量子攻击者能看到除受 PPK 保护的密钥之外的一切。	rfc8784:567, s0032, s0035, s0036, s0039
A08.7	如 Q1 所问的 PPK 绑定	与 A08 相同的性质，由用户作为问题 Q1 提出：被接受的 PPK_ID、PPK Confirmation、IntAuth 和 IKE_AUTH_MID 属于本次 IKE_SA_INIT 的 nonce 和 SPI、本次 IKE_INTERMEDIATE 记录，以及 IKE_AUTH 中认证的身份。	main s0013, s0014, s0018, s0029；rfc9242 s0568-s0574。	s0013, s0014, s0018, s0029, s0568, s0573
U01	如 Q2 所问的 DH 失效	与 C04 相同的性质，由用户作为问题 Q2 提出：在 g^ir 泄露而 PPK 保密的情况下，IKE_AUTH 内容和新的 IKE SA 密钥不可推导。	main s0032-s0036, s0039；rfc8784:556, rfc8784:567。	rfc8784:567, s0032, s0035, s0039
R05.9	如 Q3 所问的 PPK 策略	与 R05 相同的性质，由用户作为问题 Q3 提出：回退和认证失败不得被当作成功的 PPK 会话。	main s0021, s0023, s0025, s0027；rfc8784:619-627, rfc8784:646-650（在可选策略且配置错误时，SA 会在没有量子保护的情况下被创建）。	rfc8784:619, s0021, s0023, s0025, s0027
X01	DH 失效下 PPK 字段隐藏	发起方 IKE_INTERMEDIATE 请求中的 PPK_ID 和 PPK Confirmation，对能读取初始 IKE SA 的攻击者保密	RFC 9242 指出，IKE_INTERMEDIATE 数据由 Encrypted 载荷保护，免受被动窃听者窥探，并且只在 IKE_AUTH 中被认证（rfc9242:463）；RFC 8784 指出，解密初始 IKE SA 的量子攻击者能看到其上交换的一切信息，但受 PPK 保护的密钥除外（rfc8784:567）。主文稿没有说明 IKE_INTERMEDIATE 的 PPK 字段会暴露什么。	rfc9242:463, rfc8784:567, s0013, s0016, s0561

ID	简称	对象	文稿怎么说	出处
X02	PPK 不可通过离线猜测恢复	由人选择的 PPK 值，对能对 PPK Confirmation 发起离线字典攻击的攻击者保密	RFC 8784 指出，冒充服务器的攻击者可以用传统计算机对可能的 PPK 值进行字典搜索；PPK 必须具有至少 256 比特熵；从口令或名称派生它并不安全（rfc8784:541-554）；RFC 7296 对预共享密钥有同样的说法（rfc7296:6558）。	rfc8784:541, rfc7296:6558

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 46 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 8 段，没选 38 段。列哪些段落由标准的章节结构决定；每一段的去向是分析者的判断。

段落	出处	定为	不选的原因
P01	main:479-485	A03, K01, C04, U01, X01, `crqc`	
P02	main:487-488	没有陈述目标	它只指向 RFC 9242 中相关的安全问题；目标本身在该文档的段落中陈述。
P03	main:490-493	证明器问不了	它陈述了关于 CRQC 下对称原语强度的信念，符号证明器无法被问及这一点；它仅用于限定 crqc 攻击者。
P04	rfc7296:6478-6488	不在范围内	它涉及探测未认证对端的身份和 CERTREQ/证书；本文未对证书和对端身份探测场景建模。
P05	rfc7296:6490-6494	不在范围内	EAP 认证被排除在本任务范围之外。
P06	rfc7296:6496-6500	不在范围内	它涉及不进行 Diffie-Hellman 的重复 CREATE_CHILD_SA 重密钥，本任务将其排除。
P07	rfc7296:6502-6514	证明器问不了	它估计 Diffie-Hellman 组的密码学强度，符号模型无法表达这一点。
P08	rfc7296:6516-6519	证明器问不了	同一主题：Diffie-Hellman 组和 PRF 的强度与选择。
P09	rfc7296:6525-6527	没有陈述目标	它称赞可扩展框架并提到椭圆曲线组；没有必须成立或可被攻击的内容。
P10	rfc7296:6529-6530	没有陈述目标	它是一项假设：实现在使用后擦除 DH 指数；在模型中，网络世界里的指数从不交给攻击者，这是更强的解读。
P11	rfc7296:6532-6538	证明器问不了	它涉及对来自未认证对端的 DoS 的鲁棒性，这是可用性问题，超出证明器可被问及的范围。
P12	rfc7296:6540-6542	证明器问不了	它是对 PRF 输出大小的下界，属于原语强度。
P13	rfc7296:6544-6549	证明器问不了	它是对各参与方随机性的要求，不是迹的性质。
P14	rfc7296:6551-6556	证明器问不了	它限制可以协商哪些算法（不允许 NONE 完整性、不允许 ENCR_NULL），属于原语强度。
P15	rfc7296:6558-6563	X02, `dictionary`	

段落	出处	定为	不选的原因
P16	rfc7296:6565-6572	不在范围内	它涉及 NAT_DETECTION 通知和内部地址泄露；NAT 穿越不在建模流程内。
P17	rfc7296:6578-6580	不在范围内	它延续 NAT_DETECTION 地址泄露的讨论。
P18	rfc7296:6582-6606	不在范围内	它涉及不生成密钥的 EAP 方法，排除在范围之外。
P19	rfc7296:6608-6612	不在范围内	它涉及 EAP 服务器认证要求，排除在范围之外。
P20	rfc7296:6614-6619	证明器问不了	它涉及用长消息耗尽重组缓冲区，这是可用性问题。
P21	rfc7296:6621-6625	没有陈述目标	它是关于准入控制和信任锚的部署建议，不是协议迹的性质。
P22	rfc7296:6631-6633	没有陈述目标	它说明对等端身份和凭据的明确安全策略是必要的；它没有陈述要证明的性质。
P23	rfc7296:6637-6643	不在范围内	Child SA 的流量选择器授权排除在范围之外。
P24 至 P30	rfc7296:6645-6696	不在范围内	第 5.1 节其余部分涉及流量选择器授权，本任务将其排除。
P31	rfc8784:541-554	X02, `dictionary`	
P32	rfc8784:556-565	K01, C04, U01, `crqc`	
P33	rfc8784:567-572	C04, U01, X01, `crqc`	
P34	rfc8784:574-584	不在范围内	它涉及在发送敏感信息之前重密钥 IKE SA 以及无子 SA 的 IKE SA（RFC 6023），本任务将其排除。
P35	rfc8784:586-591	证明器问不了	它是关于哪些对称算法是量子安全的建议，属于原语强度。
P36 至 P39	rfc8784:593-617	证明器问不了	它列出了不应使用的算法密钥大小和 PRF，属于原语强度。
P40	rfc8784:619-627	R05, R05.9, `crqc`	
P41	rfc8784:629-644	证明器问不了	它涉及使发起方中止的 DoS/注入攻击以及重传时序，属于可用性问题，证明器无法被问及。
P42	rfc8784:646-650	R05, R05.9	
P43	rfc9242:463-470	X01, `crqc`	
P44	rfc9242:472-477	没有陈述目标	它涉及大型中间交换的 IKE 分片，不在建模流程内（引用了 RFC 7383）。
P45	rfc9242:479-499	证明器问不了	它涉及恶意发起方传输数据后中止的 DoS 攻击，属于可用性和代价性质。
P46	rfc9242:501-514	没有陈述目标	它涉及错误处理以及诊断与 DoS 之间的权衡；它没有陈述证明器可被问及的交换性质。

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 29 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 25 项。清单来自性质本身；每一项怎么处理是分析者的判断。

ID	参与方或值	类别	攻击者条件	不设的原因
S01	发起方	参与方	按定义全部失守	不诚实的发起方持有自己的长期签名密钥和它与对方共享的 PPK；有了这些，冒充该身份本身并不构成协议失败。任务没有要求防范交出自己的凭据的对端，而在只建模一个身份的情况下也无法再提出更多要求。
S02	响应方	参与方	按定义全部失守	不诚实的响应方持有 PPK 和自己的签名密钥，因此发起方对该对端的保证以及 PPK 派生密钥的保密性按定义即告失守；没有任何目标要求防范本身已失陷的对端。
S03	IKE SA 身份绑定	值	攻击者得不到更多	身份绑定是双方验证的内容；攻击者持有它得不到任何无法从转录中自行算出的东西。
S04	PPK_ID 与 PPK 确认值	值	`dictionary`	
S05	IKE_SA_INIT 非数与 SPI	值	攻击者得不到更多	Nonces、SPIs、Message IDs、IKE_INTERMEDIATE 与 IKE_AUTH 转录、IntAuth 和 PPK_ID 都在线路上传输；攻击者持有它们并不拥有网络攻击者所缺的东西，而且 PPK_ID 也不是秘密。
S06	IKE_INTERMEDIATE 转录	值	攻击者得不到更多	Nonces、SPIs、Message IDs、IKE_INTERMEDIATE 与 IKE_AUTH 转录、IntAuth 和 PPK_ID 都在线路上传输；攻击者持有它们并不拥有网络攻击者所缺的东西，而且 PPK_ID 也不是秘密。
S07	IKE_AUTH 转录	值	攻击者得不到更多	Nonces、SPIs、Message IDs、IKE_INTERMEDIATE 与 IKE_AUTH 转录、IntAuth 和 PPK_ID 都在线路上传输；攻击者持有它们并不拥有网络攻击者所缺的东西，而且 PPK_ID 也不是秘密。
S08	IntAuth 与 IKE_AUTH_MID	值	攻击者得不到更多	Nonces、SPIs、Message IDs、IKE_INTERMEDIATE 与 IKE_AUTH 转录、IntAuth 和 PPK_ID 都在线路上传输；攻击者持有它们并不拥有网络攻击者所缺的东西，而且 PPK_ID 也不是秘密。
S09	Message ID	值	攻击者得不到更多	Nonces、SPIs、Message IDs、IKE_INTERMEDIATE 与 IKE_AUTH 转录、IntAuth 和 PPK_ID 都在线路上传输；攻击者持有它们并不拥有网络攻击者所缺的东西，而且 PPK_ID 也不是秘密。
S10	PPK_ID	值	攻击者得不到更多	Nonces、SPIs、Message IDs、IKE_INTERMEDIATE 与 IKE_AUTH 转录、IntAuth 和 PPK_ID 都在线路上传输；攻击者持有它们并不拥有网络攻击者所缺的东西，而且 PPK_ID 也不是秘密。
S11	PPK Confirmation	值	`dictionary`	
S12	IntAuth	值	攻击者得不到更多	IntAuth、IKE_AUTH_MID 和身份都在线路上（位于加密载荷内）；持有它们不会给攻击者增添任何网络攻击者所没有的东西。
S13	IKE_AUTH_MID	值	攻击者得不到更多	IntAuth、IKE_AUTH_MID 和身份都在线路上（位于加密载荷内）；持有它们不会给攻击者增添任何网络攻击者所没有的东西。
S14	身份 IDi/IDr	值	攻击者得不到更多	IntAuth、IKE_AUTH_MID 和身份都在线路上（位于加密载荷内）；持有它们不会给攻击者增添任何网络攻击者所没有的东西。
S15	PPK	值	`ppk_revealed`	
S16	SKEYSEED'	值	按定义全部失守	持有 SKEYSEED' 或任一 SK_* 密钥的攻击者，恰好拥有保密性目标所说它不得拥有的东西；该性质按定义即告失守，也没有任何目标询问密钥被交出时会发生什么。

ID	参与方或值	类别	攻击者条件	不设的原因
S17	SK_d	值	按定义全部失守	持有 SKEYSEED' 或任一 SK_* 密钥的攻击者，恰好拥有保密性目标所说它不得拥有的东西；该性质按定义即告失守，也没有任何目标询问密钥被交出时会发生什么。
S18	SK_ei	值	按定义全部失守	持有 SKEYSEED' 或任一 SK_* 密钥的攻击者，恰好拥有保密性目标所说它不得拥有的东西；该性质按定义即告失守，也没有任何目标询问密钥被交出时会发生什么。
S19	SK_er	值	按定义全部失守	持有 SKEYSEED' 或任一 SK_* 密钥的攻击者，恰好拥有保密性目标所说它不得拥有的东西；该性质按定义即告失守，也没有任何目标询问密钥被交出时会发生什么。
S20	SK_ai	值	按定义全部失守	持有 SKEYSEED' 或任一 SK_* 密钥的攻击者，恰好拥有保密性目标所说它不得拥有的东西；该性质按定义即告失守，也没有任何目标询问密钥被交出时会发生什么。
S21	SK_ar	值	按定义全部失守	持有 SKEYSEED' 或任一 SK_* 密钥的攻击者，恰好拥有保密性目标所说它不得拥有的东西；该性质按定义即告失守，也没有任何目标询问密钥被交出时会发生什么。
S22	SK_pi	值	按定义全部失守	持有 SKEYSEED' 或任一 SK_* 密钥的攻击者，恰好拥有保密性目标所说它不得拥有的东西；该性质按定义即告失守，也没有任何目标询问密钥被交出时会发生什么。
S23	SK_pr	值	按定义全部失守	持有 SKEYSEED' 或任一 SK_* 密钥的攻击者，恰好拥有保密性目标所说它不得拥有的东西；该性质按定义即告失守，也没有任何目标询问密钥被交出时会发生什么。
S24	PPK 策略	值	攻击者得不到更多	PPK 策略、PPK_IDENTITY 通知和 AUTHENTICATION_FAILED 通知都不是秘密；持有它们不会带来超出网络攻击者的优势。
S25	PPK_IDENTITY 通知	值	攻击者得不到更多	PPK 策略、PPK_IDENTITY 通知和 AUTHENTICATION_FAILED 通知都不是秘密；持有它们不会带来超出网络攻击者的优势。
S26	AUTHENTICATION_FAILED 通知	值	攻击者得不到更多	PPK 策略、PPK_IDENTITY 通知和 AUTHENTICATION_FAILED 通知都不是秘密；持有它们不会带来超出网络攻击者的优势。
S27	g^ir	值	`crqc`	
S28	IKE_AUTH 内容	值	按定义全部失守	持有 IKE_AUTH 内容或新 IKE SA 密钥的攻击者已经破坏了 C04 和 K01 所要求的保密性；该目标询问的是攻击者能否推导出它们，因此持有它们正是对目标的否定，而不是另一类攻击者。
S29	新 IKE SA 密钥	值	按定义全部失守	持有 IKE_AUTH 内容或新 IKE SA 密钥的攻击者已经破坏了 C04 和 K01 所要求的保密性；该目标询问的是攻击者能否推导出它们，因此持有它们正是对目标的否定，而不是另一类攻击者。

每条性质在各攻击者条件下的答案

攻击者由分析者设定，且在编写查询之前就已确定；每个答案都记录在其中某一个攻击者之下。单元格是证明器在该攻击者下对该性质的答案；“无答案”表示证明器使某项主张悬而未决或没有记录任何内容的攻击者设定；空单元格表示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`	仅网络：它读取、丢弃、更改和发送消息，不持有任何一方的秘密		

攻击者	持有什么	依据	出处
`crqc`	从会话开始时起就持有 IKE_SA_INIT 共享秘密 g^ir（因此它能读取初始 IKE SA 的每条加密消息）以及双方的长期签名密钥；对称原语仍不可企及	主要文献 s0039 声称 IKE_AUTH 交换即使在主动攻击者面前也具有量子安全性，而 s0041 称只有对称原语被认为不受 CRQC 影响；rfc8784:567 描述了一个解密初始 IKE SA 的量子攻击者。	rfc8784:567, s0039, s0041
`dictionary`	若干候选 PPK 值，以及一次 IKE_INTERMEDIATE 交换的 PPK Confirmation 值，通过在 IKE_SA_INIT 中冒充响应方并读取 IKE_INTERMEDIATE 请求而获得；它可以离线检验猜测	rfc8784:541-554（冒充服务器的攻击者对可能的 PPK 值进行字典搜索）和 rfc7296:6558（低熵预共享密钥）。	rfc8784:541, rfc7296:6558
`ppk_revealed`	PPK 本身，作为泄露的长期共享秘密	RFC 8784 指出每个密钥的量子安全性都依赖于 PPK（rfc8784:556）；此处用它表明 K01 和 C04 的证明完全依赖于 PPK。	rfc8784:556

ID	`network`	`crqc`	`dictionary`	`ppk_revealed`
A03	成立	成立		
A04	成立	成立		
A08	成立	成立		
K01	成立	成立		
R05	成立			
C04		成立		
A08.7	成立	成立		
U01		成立		
R05.9	成立			
X01	不成立	不成立		
X02			不成立	

原文和目标

原文：586 个原文单元，194124 字节，冻结于 source-delivery-01.json。 目标：已批准 7 个（A03、A04、A08、K01、R05、C04、U01）；提出的问题：3 个。 目标清单已在事先按草稿获批，使用 --approve-targets。

宿主按其记录的默认设置（任务 `decisions: auto`）做出的决定，供你核对：

- approve_package：批准源文包 protocol-f7069cbdfce35279198aba406f93

本步骤的自报情况：1 次请求（1 次失败），0.000 美元，输入 84068 tokens，输出 5032 tokens，耗时 31 秒。

关于证明器和模型的说明

分析者为目标命名了什么：

步骤	目标	特征	原因
42	A03, A04, A08, A08.7, K01, R05, R05.9, C04, U01, X01, X02	plain_primitives, many_sessions, other	该模型只使用哈希、带密钥的 PRF/KDF、AEAD 式加密加 MAC、签名，以及 Diffie-Hellman 作为仅依赖单一法则 g^xy = g^yx 的明文密钥协商；答案不依赖该法则之外的任何代数法则。所有性质都对任意数量的会话提出：两个角色都被复制。此外：协议中 PPK Confirmation 和 AUTH 载荷在传输时被截断/序列化，符号模型无法表达这一点；后量子攻击者是通过让 g^ir 成为记录轨迹的公开函数并公开长期签名密钥来建模的，而不是对原语建模量子攻击。

分析者的总结说明

构建的模型：一次 IKE_SA_INIT 运行、一次携带 PPK_IDENTITY_KEY 的 IKE_INTERMEDIATE、PPK 密钥更新（SKEYSEED' = prf+(PPK, SK_d)）以及带 RFC 9242 IntAuth 的签名 IKE_AUTH，并为强制/可选响应方以及要求 PPK 的发起方设有策略分支。两个攻击者世界在同一文件中并行运行：仅网络攻击者，以及通过让 g^ir 成为记录轨迹的公开函数并公开两个签名密钥来建模的后量子攻击者。

十一个目标，全部有答案（记录 22 个答案，均在最终文本上重新验证）。已证明：针对网络攻击者以及已攻破 Diffie-Hellman 和签名的攻击者，IKE_AUTH 对应关系的两个方向（A03）；两个世界中 IKE_AUTH 接受的单射性（A04）；PPK_ID/confirmation 到会话的绑定以及身份绑定（A08、A08.7，部分：仅一个身份）；两个攻击者均无法到达 PPK 及由 PPK 派生的 SK_* 密钥（K01）；当 g^ir 已知时，IKE_AUTH 内容和新密钥均不可推导（C04、U01）；第 3.1 节的失败关闭策略规则（R05、R05.9）。每个证明都附带一个 ProVerif 证伪的对照查询。

两个攻击，均在文稿中为至少具备我的攻击者所需能力的攻击者命名，因此仅作报告而不作为新发现呈现：只要初始 IKE SA 可读，IKE_INTERMEDIATE 的 PPK_ID 和 PPK Confirmation 就可读，后量子攻击者具备此能力，网络攻击者通过自行应答 IKE_SA_INIT 也能获得同样能力（X01，新颖性不明确）；以及人工选择的 PPK 会遭到针对该 confirmation 的离线猜测（X02，记录于 RFC 8784 第 6 节）。

阻碍更多结论的因素：模型理想化了原语，给后量子攻击者 g^ir 而不是攻击原语，未建模 Key Exchange 载荷验证、Message ID 计数器、多次 IKE_INTERMEDIATE 交换、多个 PPK 身份或第 3.1 节的身份到 PPK 策略，且无法讨论可用性；PPK Confirmation 被建模为完整的 prf 输出而非其前八个八位组。使用有界状态和显式字节布局的 Tamarin 将解决 Message ID 和截断问题。