IKEv2个多中间键交换器的安全分析

rfc9370 — ProVerif+ 代理 报告

文稿	互联网密钥交换协议版本2(IKEv2)中的多键交换(协议定义)); 互联网密钥交换协议版本2(IKEv2)(辅助)); 互联网密钥交换协议的中间交换版本 2 (IKEv2) (辅助))
检查的性质	15 条：9 条成立，0 条不成立，6 条没有答案
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

IKEv2具有多个中间密钥交换器(RFC9370,使用IKE_INTERMEDIATE交换RFC9242(a) 建立一个IKESA发起者和答复者之间分三个阶段进行。IKE_SA_INIT谈判古典主义(A) :EC)DH键交换外加两个额外的量子后键交换方法,并携带初始键交换有效载荷和非切。 二个IKE_INTERMEDIATE交换然后运行, 每一个带一个新鲜的ML-KEM从发起人得到的公钥和从响应者得到的新封装,两者都延伸了链条IKESA键。

各方持有长期身份和签名的私人密钥; 发起者还持有其身份 IDi, 仅行驶在加密的有效载荷内。 在两次中间交换后,IKE_AUTH携带了这两条签名,双方签字的octets包括IntAuth,中间交换的累计值加上IKE_AUTH电文ID.

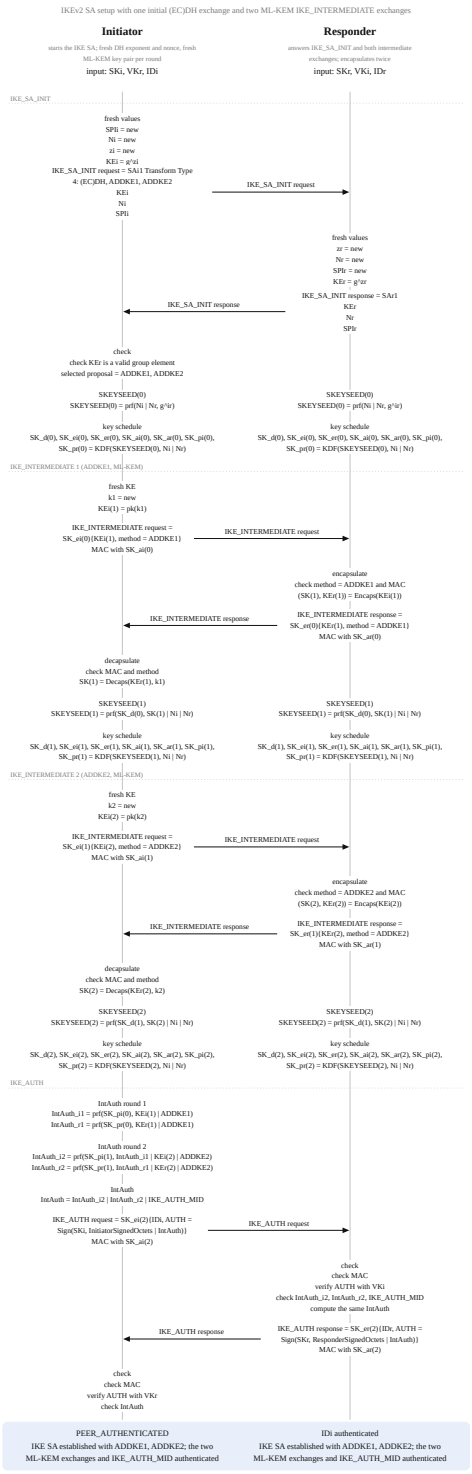
IKE_SA_INIT 衍生出 SKEYSEED(0), 来源于秘密的 (EC)DH, 非斯和 SPIs, 将其分为 SK_d,SK_ei,SK_er,SK_ai,SK_ar,SK_pi和SK_pr. 每个中间交换机将自己的KEM共享密钥折叠成SKEYSEED(n), 生成n的密钥保护了回合n+1的电文,所以每个额外的交换机都与上一代的SK_pi(n)/SK_pr(n)进行验证.

当交换结束时,双方都确信对等方运行着相同的IKE SA,并有相同的经商附加方法,顺序相同,每回合相同的密钥交换有效载荷,以及相同的IntAuth值和IKE_AUTH消息ID. 两轮的ML-KEM秘密是截然不同的,上一代的签名覆盖了全程.

双方:

- **发起者**:开始使用IKE SA; 新鲜DH expresent和nonce,新鲜ML-KEM 每轮密钥对. 持有量:SKi,VKr,IDi.
- **答复**:答复IKE_SA_INIT和中间交换; 封装两次。 持有量:SKr,VKi,IDr.

图1显示交易所,如文件所示。



- 图1。 指定协议 。 *

分析的范围载于附录D:分析的内容、遗漏的内容和文件的章节。

2 发现

没有发现。 分析发现文件没有说明或搁置任何内容。 款次中的表格3对每一个财产都有结果。

模拟协议提供了协议、注入和有记录的保证,其目的是:仅针对网络上的攻击者IKE_AUTH运行时采用了商定的额外关键交换方法,其中既包括关键交换有效载荷,也包括相同的交换方法。IntAuth数值。 证明器为任何几场会议确立了这一点,并且还确定:IKE_INTERMEDIATE回合从不共享一个KEM暗号。 关键秘密和妥协问题没有答案:IKESA密钥,用于泄漏ML-KEM部分,对于一个收获下来的古典秘密,对于一代人的密钥,对于发起人的身份保密,证明器说,它不能证明财产,但也没有找到痕迹,所以这些是开放的而不是破损的。 没有发现: 这里没有什么是文件尚未说明的弱点 。 结果是建立在具有理想化的象征性模式之上KEM, prf, (英语).MAC和签名,日期:EC)DH只有一个法则 和一个没有信息的模式ID计数器,没有窗口,也没有每个会话的状态变化。

3 检查过的性质

每行是一块财产,投入到ProVerif. 结果是ProVerif对分析师的协议模型的回答; 价值以及文件是否已经说明结果是分析员的判断,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	**关于IKE SA运行的协议。** 每当发起方（或响应方）在 IKE_AUTH 完成后接受 IKE SA，就存在一个对端真实运行，其角色、意图身份、协商的 ADDKE 算法序列、各轮 KEi(n)/KEr(n) 内容与最终 SKEYSEED 派生一致。	无	成立	中	是
A04	**不重复接受一个对等跑步。** 每次本方 IKE_AUTH成功接受都对应一个不同的对端真实运行；同一对端运行不能被接受两次，消息ID与 IKE_AUTH_MID必须与本次运行一致。	无	成立	中	是
A08	**夹在记录稿上的中间子弹。** IKE_AUTH 成功后接受的 ADDKE 算法序列、各轮顺序与 IntAuth 覆盖的转录，必须与双方在 IKE_SA_INIT 中协商的结果一致，且第 n 轮 KE 方法字段匹配第 n 个协商算法。	无	成立	中	是
K01	**决 定IKESA密钥保密。** 最终 IKESA密钥（SKEYSEED、SK_d、SK_ei/er, (英语).SK_ai/ar, (帮助)SK_pi(四月) (中文(简体)).不能被攻击者推导；即使攻击者获得某一个后续 ML-KEM封装得到的共享秘密 SK(n)，只要其余分量未被攻破，最终密钥仍保密。	单个后续 ML-KEM 封装共享秘密 SK(n) (在 IKE_AUTH 完成之后泄露)	无答案	低	是
K04	**不同用途和生成的密钥分离。** 每一轮 IKE_INTERMEDIATE 派生出的 SK_d(n)、SK_ai(n)/SK_ar(n)、SK_ei(n)/SK_er(n)、SK_pi(n)/SK_pr(n) 在用途、方向与轮次上相互分离；同一轮的保护密钥与认证密钥来自同一代。	无	无答案	低	是
C01	**会后保密。** 在 IKE_AUTH 完成并擦除会话状态之后，泄露长期签名私钥（或 654001) 以及经典 (EC) DH 共享秘密 g^ir, 都不能使攻击者恢复此前完成的 IKE SA 密钥。	长期签名私钥与经典 DH 共享秘密 (IKE_AUTH 完成并擦除状态之后)	无答案	低	是
C08	**一个破损的部件没有打破SA。** 当经典 (EC)DH 分量或某一个后续 ML-KEM 分量被攻破时，只要其余分量未被攻破，最终 IKE SA 密钥仍保密。	经典 DH 分量或单个 ML-KEM 分量 (派生之后)	无答案	低	是
R01	**电文ID新鲜的。** IKE_AUTH成功所依赖的 消息ID与 IKE_AUTH_MID必须是本次运行的新鲜值，旧运行的证据不能被接受。	无	成立	低	是
R02	**每条电文接受一次。** 同一逻辑 IKE_INTERMEDIATE 或 IKE_AUTH 消息在单个 IKE SA 内至多被接受一次。	无	成立	中	是
R04	**按顺序排列的中间回合,没有跳过。** IKE_INTERMEDIATE 的接受顺序必须符合 变形型 值顺序与 Message ID 递增规则，且每个附加密钥交换完整完成后才能开始下一个。	无	成立	中	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
A08.11	**ADDKE发子弹装配至AUTH号机车.** IKE_AUTH 成功后接受的 ADDKE 算法序列、各轮顺序与 IntAuth 覆盖的转录，必须与双方在 IKE_SA_INIT 中协商的结果一致，且第 n 轮 KE 方法字段匹配第 n 个协商算法。	无	成立	中	是
K01.12	**最终密钥在KEM泄漏下。** 即使攻击者获得某一个后续 ML-KEM 封装得到的共享秘密 SK(n)，只要其余分量未被攻破，最终 IKE SA 密钥仍保密。	单个后续 ML-KEM 封装共享秘密 SK(n) (在 IKE_AUTH 完成之后泄露)	无答案	低	是
A04.13	**无弹片或跑步。** 每次本方 IKE_AUTH 成功接受都对应一个不同的、完整的对端真实运行；攻击者不能通过拼接不同轮次报文或跳过某一轮使认证成功。	无	成立	中	是
X01	distinct distinctKEM每个回合的秘密。 ** 两者IKE_INTERMEDIATE一轮IKESA使用新鲜KEM密钥对和新封装的随机性,所以他们共享的秘密SK(1和(a)和(b)SK(2——是不同的价值观; 任何重复的算法选择都不能使一个回合的秘密站成为另一个回合的秘密站。	无	成立	中	是
X02	**启动身份保密。** 网络上的被动攻击者无法知道IKE_AUTH交换机携带的两种发起者身份中的哪一种,因为IDi只在加密有效载荷内飞行。	无	无答案	低	不确定

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.

所问之问,及分析师之答:

问题	回答	依据
Q1: 中间交换顺序/算法与最终 AUTH 绑定	是:增加关键交换回合和IKE_AUTH消息ID被绑定为IntAuth,这两个IKE_AUTH签名封面,所以接受的运行在与这些子弹的关键交换有效载荷谈判的顺序中使用了商定的额外方法,仅针对网络上的攻击者。	A08.11, A08, R04
Q2: 单个后续 KEM 秘密 泄露时最终 IKE SA 密钥保密 7 secret secret	这个模型没有回答:持有一个ML-KEM共享秘密的攻击者没有模型,而查询只能要求网络攻击者,它回到那里没有结果,没有痕迹,所以它必须用一个有明确泄露的有界限的模型或Tamarin+ Agent来解决.	K01.12, K01, C08
Q3: 跨轮次报文拼接与缺轮次不能产生成功认证	否:接受在对等运行时进行注射,两轮都反馈了IntAuth,两者的签名都覆盖,因此网络上的攻击者不能连发不同回合或运行的信息,也不能跳过一回合,并获得IKE_AUTH的接受.	A04.13, A04, A08

4 本次分析的局限

这里的一个结果就是协议模型的结果:它描述了特定的信息和检查给出的或未能给出的,以密码学为理想,没有关于执行的内容.

正如分析师所说,这一分析没有涵盖的内容是:

- 符号模型:没有计算担保,没有量子后主张. 其属性为理想化原始人的属性,而非ML-KEM,PRF,MAC或签名计划.
- Diffie-Hellman以单定律g^xy=g^yx为模型; 2. 在模型中,除了这个定律之外,不可能进行代数攻击。
- KEM封装是共享秘密,方法及公钥的私用功能,其封装为反; 2. 隐性拒绝,错误的密码和ML-KEM编码不是模型化的.
- 没有SA有效载荷谈判,没有提案匹配和降级检查:另外两种关键交换方法都是固定常数,因此不检查候选人之间的谈判.

- 没有信息ID计数器,没有重复请求的窗口,也没有再发送的计时器:IKE_AUTH的新鲜度通过新SPIs和非ces的注入来回答,而不是通过IKEv2的ID状态.
- IKE SA号和CHILD_SA号没有更新或重置密钥; CREATE_CHILD_SA超出了模型范围.
- 折中问题(一个泄露了ML-KEM秘密,一个收割的古典DH秘密,一代密钥,一个加密密钥,一个泄露的长期签名密钥)是无法模拟的:复制的应答器内部的泄露使ProVerif出现分歧,因此这些询问只与网络攻击者一起询问.
- 拥有固定对同伴身份的发起者和答复者; 除了复制角色外,不审查跨会场连接和多党派设置。
- 倡议者的身份保密被要求为不干涉两个候选身份,ProVerif既未证明,也未提供线索。

主持人记录的是什么:

- 无回答:K01,K04,C01,C08,K01.12,X02.
- 证明器没有给出结论的查询（附录 C）： K01: skd2, K04: skai1, K04: skd2, C01: sks2, C08: skd2, K01.12: skd2, X02: id_conf。 这条性质问过了， 证明器既没有证明它也没有找到攻击， 所以结果写“无答案”。

附录A中列出了每个财产的开口情况以及解决这些财产的办法。

附录 A：逐条性质的解读

分析师自己对证明器的答案的解读,而不是对证明器的答案:答案对协议的意义,读取的基础,是否可以按原样使用,价值如何.

A03:关于IKE SA运行的协议

每当发起方（或响应方）在 IKE_AUTH 完成后接受 IKE SA，就存在一个对端真实运行，其角色、意图身份、协商的 ADDKE 算法序列、各轮 KEi(n)/KEr(n) 内容与最终 SKEYSEED 派生一致。

两个方向都坚持:每当响应者接受IKE_AUTH请求时,发出同一会话的发起人运行,每当响应者接受IKE_AUTH响应时,响应者运行时发送. 被接受的IntAuth价值链既包括中间交换,也包括IKE_AUTH信息ID,因此同行运行的会话相同,而不仅仅是具有相同识别符的会话. 网络上的攻击者不能让任何一方接受同行没有参与的运行。

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:这是指定的协议的中央认证属性; 证据是机械的,但依赖于理想化的签名和IntAuth抽象.
- 在文件中说明:是的。 文件上说:rfc9242:283,s0481,s0482,s0486
- 休息 : 签名是理想化的: 校验只在匹配密钥的精确签名的octets上成功. ; IntAuth从RFC 9242中抽象出来,是两发弹关键交换有效载荷、谈判方法和ID号电文的棱镜链; 可选的 A 和 P 块会倒塌到链条中。 ; 加密,MAC和prf是理想的原始,所以模型没有显示真实的有效载荷编码是毫不含糊的. ; 这两个角色都是复制的,对等身份是固定的,因此对于这对对等的任意次数的会话都表现出一致.

A04:不重复接受一次同行赛

每次本方 IKE_AUTH 成功接受都对应一个不同的对端真实运行；同一对端运行不能被接受两次， 新闻 ID 与 IKE_AUTH_MID 必须与本次运行一致。

双方的接受是注射性的:每个被接受的IKE_AUTH对应不同的对等者运行,因此一个对等者运行不能被接受两次. IKE_AUTH的ID号电文在IntAuth号内携带,因此在两个签名内都携带,因此一个运行的电文不能被呈现为属于另一个运行的电文. 网络上的攻击者不能将旧的IKE_AUTH重播为第二次接受.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:IKE_AUTH的重播保护是一项已申明的要求; 证据是机械的 并且它与 ID 真实信息的关系 仅通过模型的新值。
- 在文件中说明:是的。 文件上写着:rfc9242:205,s0487
- 休息:在接受事件之后证明注射性; 其新鲜的SPIi、SPIr和Nonce确定了同行竞选。 ; 该模型没有信息ID计数器,也没有窗口,因此通过新鲜会话值而不是通过IKEv2消息ID状态排除了双重接受. ; 签名、prf和IntAuth抽象与协议财产一样是理想化的。
- 开放:真实消息ID规则是否拒绝每一次重播IKE_AUTH,包括接受窗口内的重播.
- 下一步:一个带ID号电文的模型未卷进几个步骤就能解决窗口案件.

A08:装有记录的中弹

IKE_AUTH 成功后接受的 ADDKE 算法序列、各轮顺序与 IntAuth 覆盖的转录，必须与双方在 IKE_SA_INIT 中协商的结果一致，且第 n 轮 KE 方法字段匹配第 n 个协商算法。

响应者接受的IntAuth值是一个prf链,覆盖第1轮的关键交换有效载荷和密码,第2轮的关键交换有效载荷和密码,以及两种谈判方法,所以公认的顺序,顺序和内容是谈判方法. IKE_AUTH两个签名都带有这一价值,每个角色在使用前将N轮的方法领域与n次谈判的方法进行比较. 网络上的攻击者不能替代一种方法、重新排列子弹或交换有效载荷而不使签名失效。

- 结果:持有; 回答问题:是的; 可用备注
- 数值介质:附加交换机的转写装订值为IntAuth; 结果是模型理想化下的机械证明.
- 在文件中说明:是的。 文件上写着:rfc9242:286,s0483,s0488
- 休息:通过将方法领域与谈判方法进行比较,在结构上执行轮对方法的约束,第一回合为alg1,第二回合为alg2; 该模型不为不同的方法构建术语。 ; 另外两种方法是固定不变的,因此,几个候选人之间没有谈判模式。 ; 签名和prf被理想化,IntAuth的可选A和P块被坍塌.

A08.11:ADDKE发子弹装配至AUTH号机车.

IKE_AUTH 成功后接受的 ADDKE 算法序列、各轮顺序与 IntAuth 覆盖的转录，必须与双方在 IKE_SA_INIT 中协商的结果一致，且第 n 轮 KE 方法字段匹配第 n 个协商算法。

对第一个问题:是的,所接受的额外密钥交换顺序和圆形顺序与AUTH的交换以及之前的谈判内容相联. 两回合内容和两种谈判方法进入IntAuth,IntAuth进入双方签字的octets,IKE_AUTH电文ID的携带价值相同. 网络上的攻击者不能得到接受其中间内容不同于谈判内容的运行。

- 结果:持有; 回答问题:是的; 可用备注
- 价值介质:在与记录带约束力的财产相同的提示下,用经证明的保证来回答用户的问题.
- 在文件中说明:是的。 文件上写着:rfc9242:286,s0483,s0488
- 休息:与抄本装订的地产相同的理想化,它回答了同样的问题:理想化的签名和prf,IntAuth抽象自RFC 9242,固定的附加方法. ; 每轮方法检查是在方法领域进行平等测试,而不是完全的转换比较.

A04.13:无弹片或跑步

每次本方 IKE_AUTH 成功接受都对应一个不同的、完整的对端真实运行；攻击者不能通过拼接不同轮次报文或跳过某一轮使认证成功。

问第三个问题:不要乱打乱打,不要跳转。 两轮中间弹都装入IntAuth,IntAuth都装入了IKE_AUTH的签名,接受是注射式的,所以一个被接受的IKE_AUTH总是对应一个完整的对等跑. 网络上的攻击者不能将不同回合或不同回合的信息合并成接受.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:用证明的保证回答用户的问题; 回合的顺序部分由角色的结构而不是通过查询来执行.
- 在文件中说明:是的。 文件上写着:rfc9242:286,s0487
- 休息:对新会话值的注入,对重播属性而言。 ; 回合是每个角色的顺序语句,所以模型不能表达出一个不规则的回合; 命令参数不是一个单独的查询。 ; 理想的签名,prf,MAC和加密。

K01:最后的IKE SA 密钥保密

最终 IKESA密钥（SKEYSEED、SK_d、SK_ei/er, (英语).SK_ai/ar, (帮助)SK_pi(四月) (中文(简体)).不能被攻击者推导；即使攻击者获得某一个后续 ML-KEM封装得到的共享秘密 SK(n)，只要其余分量未被攻破，最终密钥仍保密。

最终的IKE SA 键没有显示为秘密,也没有显示可衍生. 仅对网络攻击者而言,证明器无法证明财产,也找不到攻击的痕迹; 对于一个持有ML-KEM共享秘密的攻击者来说,这个模型甚至无法被问及,因为复制的响应者内部一个会话组件的泄露使得搜索出现分歧. 这些文件所争论的仍然是一个论点:只要至少一个交换的秘密是未知的,SKEYSEED是不可妥协的.

- 结果:没有答复; 回答问题:未确定; 无法使用
- 价值低:既不是证据,也不是攻击,而且目标的一个决定性案例,即一个泄露了KEM组件,根本没有模型化.
- 在文件中说明:是的。 文件中说: 910、s0106、s0108
- 休息:该模型不给攻击者任何会话组件; 只有网络攻击者问了问题 答案谈到那个攻击者 ; 关键衍生法采用理想化的prf和kdf; 一个新组件保护最终密钥的论据是计算性的。 ; 不确定的答案是证明器将不同会话的步数结合起来的过度近似; 它后面没有痕迹。
- 公开:一个泄露了ML-KEM共享秘密是否留下了最终的IKE SA密钥. ; 网络攻击者能否单独获得任何最终的密钥.
- 下一步:一个有明确泄露一个元件的定界模型,或者在Tamarin+ Agent中一个有揭示元件的相同问题,会解决它.

K01.12:一个KEM泄漏的终极密钥

即使攻击者获得某一个后续 ML-KEM 封装得到的共享秘密 SK(n)，只要其余分量未被攻破，最终 IKE SA 密钥仍保密。

对于第二个问题,没有证明的答案:目标被设定为拥有一个ML-KEM共同秘密的攻击者,攻击者不在模型中,没有任何记录代表它. 设计论点是,链条将一个新的秘密折叠到每代人中,这样一个破碎的组件就不会折断其他组件,这就是文件所描述的,以及一个有界限的或代数模型需要确认的. 仅针对网络攻击者的同样的查询没有定论。

- 结果:没有答复; 回答问题:未确定; 无法使用
- 价值低:模型未回答问题; 仅重述意图论证的形状。
- 在文件中说明:是的。 文件中说: 910、s0106、s0108
- 休息:目标的攻击者不是模型化的:模型中不存在会话组件的漏泄. ; 对网络唯一版本的无定论的回答是一个没有痕迹的过度近似. ; 理想的普雷夫和kdf.
- 打开:整个问题,对攻击者来说是目标名称.
- 下一步:模拟泄漏,定界或用Tamarin+ Agent,再要求最后的密钥.

K04:不同用途和生成的密钥分离

每一轮 IKE_INTERMEDIATE 派生出的 SK_d(n)、SK_ai(n)/SK_ar(n)、SK_ei(n)/SK_er(n)、SK_pi(n)/SK_pr(n) 在用途、方向与轮次上相互分离；同一轮的保护密钥与认证密钥来自同一代。

密钥分离是通过给每个用途和每代自己的密钥块的提取器来构建到模型中的,因此,任何密钥在策略上都不是另一个密钥. 是否知道一个世代的密钥或一个加密密钥揭示了另一个没有被回答:模型没有将这些值交给攻击者,两个查询都毫无结果地返回了. 因此,所需文件的分离在结构上被复制,但没有对攻击者进行测试。

- 结果:没有答复; 回答问题:未确定; 无法使用
- 价值低:两项主张均无证明器答复; 分离是模型的一种假设,而不是结果.
- 在文件中说明:是的。 文件上说: 910,s0107
- 休息:分化提取器和每代区块通过构造进行分离,因此模型无法表达真正的衍生弱点. ; 模型中没有一代的密钥被泄露,因此两个查询都只为网络攻击者运行. ; 理想的普雷夫和kdf.
- open:持有generation-1密钥的攻击者能否获得生成的2. ; 一代的加密密钥是否揭示其完整性密钥 。

- 下一步:在定界模型中泄露一代人对攻击者的密钥,再问两个问题,或者使用 Tamarin+ Agent,它能容忍揭示的值.

C01:会后预先保密

在 IKE_AUTH 完成并擦除会话状态之后，泄露长期签名私钥（或 654001) 以及经典 (EC) DH 共享秘密 g^ir, 都不能使攻击者恢复此前完成的 70IKE SA 密钥。

已完成的IKE SA的远期保密既不能如所示,也不能如已破损。 意向设计,即后来的量子计算机学习古典秘密仍然无法解密存档的会话,是文件所声称的,但给攻击者的古典秘密的查询没有得到回答. 对网络攻击者来说,证明器没有定论,也没有留下任何痕迹。

- 结果:没有答复; 回答问题:未确定; 无法使用
- 价值低:决定性的攻击者,一个持有收获的古典秘密的人,不在模型中; 财产没有固定的,也没有固定的。
- 在文件中说明:是的。 文件上说: 925,s0106
- 休息:古典秘诀不授予攻击者,因此询问中谈到攻击者不持有. ; 至少有一个ML-KEM元组件必须保持隐藏,prf是量子抗药性,而象征模型只假定如此. ; 理想的普雷夫和kdf.
- 开放:用于模拟会话的收获和解密阻力。
- 下一步:用被揭示的古典秘密来问问题,在一个有界限的模型或Tamarin+ Agent中.

C08:一个断开的部件没有断开SA

当经典 (EC)DH 分量或某一个后续 ML-KEM 分量被攻破时，只要其余分量未被攻破，最终 IKE SA 密钥仍保密。

一个破碎的部件没有破碎的SA号的说法没有得到回答:古典DH案和1KEM-号部件的案子都没有作为攻击者出现在模型中,对于网络攻击者来说,这两个查询都没有定论,没有找到任何线索. 模型在结构上显示的是,每一代人将一个新的秘密折叠到链条中,即文件所依赖的机制. 这个机制是否针对一个真正持有一个组件的攻击者,在这里是开放的.

- 结果:没有答复; 回答问题:未确定; 无法使用
- 数值低:没有证明答案; 所披露的复合主张需求的组成部分。
- 在文件中说明:是的。 文件所言:主文:910,s0104,s0106,s0107
- 休息:没有显示组件; 两个查询都只为网络攻击者运行。 ; 两种附加方法都是固定常数,因此两种回合都使用相同的算法,因而是相同的公钥材料,是没有模型化的. ; 理想的普雷夫和kdf.
- 开放:两种说法的读数:古典构件破损,1个KEM构件破损.
- 下一步:一个有边界的漏泄模型,或者Tamarin+代理,带有显示的值,如同关于最终键的问题.

R01:消息ID新鲜度

IKE_AUTH 成功所依赖的 新闻 ID 与 IKE_AUTH_MID 必须是本次运行的新鲜值，旧运行的证据不能被接受。

新鲜度为IKE_AUTH,仅以模型可携带的形式显示:接受在会场新鲜度SPIi,SPIr和nonce上注入,IKE_AUTH的ID的电文在署名值IntAuth内. ID留言柜台对窗口的检查没有在模型中,因此对于一个仍然适合窗口的旧留言,没有说什么.

- 结果:持有; 回答问题:部分; 可用备注
- 价值低:所述财产涉及信息ID规则,该模式没有执行; 所证明的是一种较弱的新鲜财产。
- 在文件中说明:是的。 文件上写着:rfc9242:205,s0132,s0487

- 休息时间:没有消息ID计数器,没有窗口,也没有重传逻辑:新鲜度依赖于新鲜的会话值和注射. ; 理想的签名和prf; IntAuth摘录于RFC 9242.
- 公开:信息ID规则是否拒绝一个适合窗口内部的重播的IKE_AUTH.
- 下一步:在捆绑的模型中解开ID信件计数器,并在窗口内重放一个旧请求.

R02:每条电文接受一次

同一逻辑 IKE_INTERMEDIATE 或 IKE_AUTH 消息在单个 IKE SA 内至多被接受一次。

重新播放的IKE_AUTH请求没有两次被接受:接受的签名覆盖了这次运行新鲜的SPIr,非ce和接受在对等运行时注入. 中间电文也一样,因为每个电文都用一个不同的一代的密钥加以保护,并带有这个运行的标识符. 该模型没有信息ID状态,所以答案是重放到一个新的或平行的会话,而不是在一个窗口内重放.

- 结果:持有; 回答问题:部分; 可用备注
- 值介质:模型假设下有意义的重播结果,弱于完整信息ID规则.
- 在文件中说明:是的。 文件上写着:rfc9242:205,s0132
- 休息: 新鲜会话值和注入态,而不是信件ID状态. ; 理想加密,MAC,prf和签名.
- 开机:重播在1台IKESA的接收窗口内.
- 下一步:与ID新电文相同的捆绑电文ID型号.

R04:中弹顺序,无跳过

IKE_INTERMEDIATE 的接受顺序必须符合 变形型 值顺序与 Message ID 递增规则， 且每个附加密钥交换完整完成后才能开始下一个。

IKE_AUTH仅在两个中间交换完成后才能被接受: IntAuth将第二回合连到第一回合,两者都输入已签名的octets,角色按顺序运行这些回合,因此跳转的回合或不同的顺序不能产生一个被接受的运行. 相对于谈判方法的顺序来自每轮方法检查。 没有任何明确的信息ID订单是模拟的,因此一回合内重排的电文的订单没有被检查.

- 结果:持有; 回答问题:是的; 可用备注
- 数值介质:已证实对已完成的子弹装订IKE_AUTH,但警告说,在一回合内订购是结构性的。
- 在文件中说明:是的。 文件上说:rfc9242:286,s0022,s0468,s0469
- 顺序作用程序执行命令; 该模型不能表达出一个超出命令的回合。 ; 每轮方法检查是一种平等测试,两种附加方法都是固定常数. ; 摘自RFC 9242的IntAuth; 理想化的签名和prf.

X01:每轮明显KEM次秘密.

两发IKE_INTERMEDIATE发的IKE SA使用新鲜的KEM密钥对和新鲜封装随机性,因此其共享的机密SK(1)和SK(2)是不同的值; 任何重复的算法选择都不能使一个回合的秘密站成为另一个回合的秘密站。

两个中间交换从未共享一个ML-KEM秘密:发起人为每轮制作一个新鲜的密钥对,响应者封装了新鲜的密钥,因此两个共享的秘密在每次运行中都是不同的价值. 这阻止了设计警告的失败,其中一个共享的秘密会比两个独立组件被计算两次. 它为两轮的任何届会和任何交替举行。

- 结果:持有; 回答问题:是的; 可用
- 价值介质:设计的一个结构属性,被机械地证明:关键链和混合参数所依赖的两个秘密的区别.
- 在文件中说明:是的。 文件中说: 252、s0025、s0043
- 休息:封装是共享秘密、方法和公用密钥的私人功能; 新鲜度来自模型的新名称. ; 真实的ML-KEM封装一个公钥能否两次还回同样的秘密,是象征模型假定的计算问题.

X02:发起人身份保密

网络上的被动攻击者无法知道IKE_AUTH交换机携带的两种发起人身份中的哪一种,因为IDi只行驶在加密有效载荷内。

该模型既没有显示发起人的身份被被动攻击者隐藏,也没有显示其泄露. 在设计中,IDi及其产生的价值只在加密的IKE_AUTH有效载荷内飞行,而这正是保密的基础。 证明器无法证明不干涉; 它的衍生需要古典秘密 和KEM的秘密 一次也没有产生痕迹, 所以这不是攻击。

- 结果:没有答复; 回答问题:未确定; 无法使用
- 数值低:没有答案; 模型最强大的支持是 身份在加密的有效载荷内
- 在文件中说明:不明确。 资料来源:s0471、s0482。
- 休息:加密是理想化的,所以答案只是关于象征的藏书IDi,而不是关于大小和图案等流量分析. ; 证明器从来不说不干预是虚假的; 没有定论的答案既不意味着证据,也不意味着攻击。 ; 只有两个候选身份和一个固定的应答者身份是模拟的。
- 打开:被动攻击者能否分辨出两个发起者的身份.
- 下一步:一个使IKE_AUTH代密钥无法到达攻击者,即Tamarin+ Agent的密钥的密钥将解决观测等效问题的模式.

附录 C：主张和证明器的答案

证明器对每个目标的记录:所达到的关卡,到达它的查询,是否检查了控制,以及攻击与分析师对每个目标的判决.

目标	级别	界	查询	对照	攻击	主张
A03	proved		auth_resp	检查		证明:2
A04	proved		inj_resp	检查		证明:2
A08	proved		auth_resp	检查		证明:1
K01	无					2 未决定
K04	无					2 未决定
C01	无					1 未决定
C08	无					2 未决定
R01	proved		inj_resp	检查		证明:1
R02	proved		inj_resp	检查		证明:1
R04	proved		auth_resp	检查		证明:1
A08.11	proved		auth_resp	检查		证明:1
K01.12	无					1 未决定
A04.13	proved		inj_resp	检查		证明:1
X01	proved		same_kem	检查		证明:1
X02	无					1 未决定

以分析师对每项主张的措辞提出的主张; 每一个答案都是证明器的:

目标	主张	攻击者	回答	查询	对照
A03	发起方:当发起方接受IKE_AUTH响应时,一些响应方运行发送了相同的(SPIi,SPIr)和相同的IntAuth值,它们将IKE_INTERMEDIATE发和IKE_AUTH电文ID连锁. 攻击者只有网络	network	proved	auth_init	检查
A03	响应方:每当响应方接受IKE_AUTH请求时,一些发起方会发出完全相同的(SPIi,SPIr)和相同的IntAuth值; IntAuth值是IKE_INTERMEDIATE弹(pk(k1),ct1,alg1,pk(k2),ct2,alg2)和IKE_AUTH_MID弹的棱镜链,所以对等者运行同一会话. 攻击者只有网络	network	proved	auth_resp	检查
A04	响应方:每个被接受的IKE_AUTH请求对应一个单独的发起方运行,因此一个对等方运行无法被接受两次; IntAuth内携带的IKE_AUTH_MID价值属于该跑道。 攻击者只有网络	network	proved	inj_resp	检查
A04	启动方:每个接受的IKE_AUTH响应对应一个截然不同的响应方运行,因此同一响应方运行无法被接受两次. 攻击者只有网络	network	proved	inj_init	检查
A08	被接受的IntAuth是两轮内装物(pk(k1),ct1,alg1,pk(k2),ct2,alg2)和IKE_AUTH电文ID的棱镜链,所以被接受的ADDKE序列,圆序和KE有效载荷是谈判的; 4. N回合的方法字段与N-th谈判算法相比较。 攻击者只有网络	network	proved	auth_resp	检查
K01	最终的IKE SA 关键材料(SK_d和上一代的SK_*),单靠网络攻击者无法得出. ProVerif回答无法证明(结论性):它没有找到痕迹,因此既没有证据,也没有攻击. 攻击者只有网络	network	undecided	skd2	

目标	主张	攻击者	回答	查询	对照
K01	由于IKE_INTERMEDIATE共享的秘密SK(n)在IKE_AUTH之后泄露,最终的SK_d仍然保密. 该模型不将该组件交给攻击者(不能在不失去终止的情况下添加泄漏过程),因此仅与网络攻击者询问; ProVerif回答无法证明(结论性):它没有找到痕迹,因此既没有证据,也没有攻击. 攻击者掌握着会议的一个ML-KEM共同秘密。	kem_component	undecided	skd2	
K04	只知道generation-1加密密钥 SK_ei(1)没有揭示generation-1完整性密钥 SK_ai(1):一个世代的密钥由同一块的明显提取器分离. 该型号没有将SK_ei(1)交给攻击者; ProVerif回答不能被证明(结论性):它没有找到痕迹,所以既没有证据,也没有攻击. 攻击者持有SK_ei(1).	enc1_key	undecided	skai1	
K04	编号generation-2的密钥仅从所有generation-1的密钥中衍生出来:SK_d(2)通过SKEYSEED(2)从新鲜的SK(2)和之前的SK_d(1)衍生出来. 该型号没有将generation-1的密钥交给攻击者; ProVerif回答不能被证明(结论性):它没有找到痕迹,所以既没有证据,也没有攻击. 攻击者持有所有generation-1键.	gen1_keys	undecided	skd2	
C01	IKE_AUTH完成后,学习古典(EC)DH共享的秘密g^ir(从铁丝网中收获)并不能给出完成的会话的SK_s. 型号不将g^ir 交给攻击者; ProVerif回答无法证明(结论性):它没有找到痕迹,因此既没有证据,也没有攻击. 攻击者举行会场仪式。	classical_dh	undecided	sks2	
C08	随着古典式(EC)DH组件的破损,最终的SK_d仍然保密,因为ML-KEM组件仍然保护着它. 型号不将g^ir 交给攻击者; ProVerif回答无法证明(结论性):它没有找到痕迹,因此既没有证据,也没有攻击. 攻击者举行会场仪式。	classical_dh	undecided	skd2	
C08	随着一个ML-KEM共享的秘密SK(n)被打破,最终的SK_d依然保密,因为其他组件仍然保护它. 该型号没有将SK(n)交给攻击者; ProVerif回答无法证明(结论性):它没有找到痕迹,因此既没有证据,也没有攻击. 攻击者掌握着会议的一个ML-KEM共同秘密。	kem_component	undecided	skd2	
R01	一个接受的IKE_AUTH,带有Message-ID-类似值是新鲜的:接受在对等运行中注入,所以一个旧运行的IKE_AUTH证据不再被接受. 该型号没有Message-ID柜台或窗口; SPIi/SPIr/Nr和IntAuth中的 IKE_AUTH_MID, 以注入方式答复了这一申诉。 攻击者只有网络	network	proved	inj_resp	检查
R02	回放方:一个重播或拼接的IKE_AUTH消息不能被任何回放方接受,因为接受的签名覆盖了SPIi,新鲜的SPIr和Nr这个运行,接受事件是注射式的. 信息ID/窗口状态没有模拟; 新鲜度取决于会议新鲜度SPIr/nr。攻击者只有网络	network	proved	inj_resp	检查
R04	IKE_INTERMEDIATE两回合均按顺序完成后才能接受 IKE_AUTH:IntAuth 连锁圆 1 进入2 回合,两者都为已签名的octets配音,角色流程作为顺序语句发布各回合,因此任何回合都无法跳过,任何回合都无法被无序接受. 攻击者只有网络	network	proved	auth_resp	检查
A08.11	(用户问题Q1) 被接受的IntAuth号记录片将两发IKE_INTERMEDIATE发装入IKE_SA_INIT号谈判:两发KE有效载荷,谈判的ADDKE算法按顺序排列,IKE_AUTH号电报ID全部装入IntAuth号供货,两发 IKE_AUTH号签名均覆盖. 攻击者只有网络	network	proved	auth_resp	检查
K01.12	(用户问题Q2) 在IKE_AUTH后泄露了一个IKE_INTERMEDIATE共享的秘密SK(n),最终的IKE SA密钥保密. 该模型只给予攻击者网络(复制反应器的一个泄漏过程使ProVerif出现偏差); ProVerif回答无法证明(结论性):它没有找到痕迹,所以既没有证据,也没有攻击. 攻击者掌握了会议的一个ML-KEM共同秘密。	kem_component	undecided	skd2	
A04.13	(用户问题Q3) 一个接受的IKE_AUTH是一个截然不同且完整的对等运行:没有拼凑的回合或运行的回合,也没有跳转的回合,因为两回合都反馈了IntAuth,IntAuth两个签名,接受的事件都是注入的. 攻击者只有网络	network	proved	inj_resp	检查

目标	主张	攻击者	回答	查询	对照
X01	两发IKE_INTERMEDIATE发的一发IKE SA使用新鲜的KEM密钥对和新鲜的封装随机性,所以任何事件都不可能像SK(1)和SK(2):一发的密令永远不能代表另一发的密令. 攻击者只有网络	network	proved	same_kem	检查
X02	被动攻击者无法知道IKE_AUTH交换机携带的两种发起者身份中的哪一种; IDi和prf(SK_pi,IDi)只在加密有效载荷内行驶,存在可到达的运行,发出IKE_AUTH请求. ProVerif回答不能证明(结论性)不干涉:其产生需要DH秘密和KEM两个秘密同时产生,没有产生痕迹,所以这不是攻击. 攻击者只有网络	network	undecided	id_conf	

附录 D：分析是怎么跑的

LLM名分析员从文件中建立了协议模型,将每个财产归入ProVerif; 第3节中的每一个结果都是证明器的答案.

ProVerif+ 代理会话 session-20261115T080535, 2026-11-15. 状态: 完成 。 型号:deepseek-v4-1-flash-261017. 台阶:61,校对:607 s,壁27 min,耗资0.331 USD.

背景:对话是从分析师的2次笔记中重新开始的。 轨迹文件保存了一切

ProVerif:54 证明运行,35 决定,19 未答,474 s,12 答录.

分析了什么

协议	IKEv2 多个中间键交换器
版本	rfc9370
分析范围	初始 DH加两个不同新鲜 ML-KEM封装的有界 IKE_INTERMEDIATE，再签名认证；保留 ADDKE协商、顺序号、逐次 密钥更新和 中间认证,绝不把两个相同长期 KEM密钥当独立分量；排除 CHILD_SA。
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	以下各节的500个编号段落(177184字节). 本报告中的s0001等参考文献就是其中一段。

文件各节的分析依据如下:

文稿	章节	标题
主体	2	多个密钥交换
主体	2.1	设计概览
主体	2.2	协议细节
主体	2.2.1	IKE_SA_INIT回合:谈判
主体	2.2.2	IKE_INTERMEDIATE回合:额外的密钥交换
主体	2.2.3	IKE_AUTH 交易所
主体	2.2.4	CREATE_CHILD_SA 交易所
主体	2.2.5	与 IKEv2 扩展的相互作用
主体	2.2.5.1	与无子女儿童的互动 IKE SA
主体	3	IANA 考虑
主体	4	安全考虑
rfc7296	2	IKE 礼宾细节和变动
rfc7296	2.1	使用再传送计时器
rfc7296	2.2	信件使用序列号 ID
rfc7296	2.3	重叠请求的窗口大小
rfc7296	2.4	状态同步和连接超时
rfc7296	2.5	版本编号和转发兼容性
rfc7296	2.6	IKE SA SPIs和饼干

文稿	章节	标题
rfc7296	2.6.1	COOKIE和INVALID_KE_PAYLOAD的相互作用
rfc7296	2.7	密码算法谈判
rfc7296	2.8	重键
rfc7296	2.8.1	同时期儿童 SA 重新键入
rfc7296	2.8.2	同时 IKE SA 重键
rfc7296	2.8.3	重修IKE SA对重修
rfc7296	2.9	交通选择谈判
rfc7296	2.9.1	交通选择者侵犯自有政策
rfc7296	2.9.2	Rekeying 中的交通选择器
rfc7296	2.10	诺斯
rfc7296	2.11	地址和端口敏捷度
rfc7296	2.12	Diffie-Hellman 指示器的重新使用
rfc7296	2.13	生成密钥材料
rfc7296	2.14	生成IKE SA型机车的密钥材料
rfc7296	2.15	IKE SA号机车的认证
rfc7296	2.16	广泛认证协议方法
rfc7296	2.17	制作儿童密钥材料 SAs
rfc7296	2.18	重键IKESAs使用aCREATE_CHILD_SA交换
rfc7296	2.19	请求远程网络内部地址
rfc7296	2.20	请求对等版本
rfc7296	2.21	处理错误
rfc7296	2.21.1	IKE_SA_INIT中处理错误
rfc7296	2.21.2	IKE_AUTH中处理错误
rfc7296	2.21.3	IKE SA 后处理错误已认证
rfc7296	2.21.4	处理错误 IKE SA
rfc7296	2.22	IPComp
rfc7296	2.23	NAT 倾斜
rfc7296	2.23.1	运输方式 NAT Traversal
rfc7296	2.24	明确通知(ECN)
rfc7296	2.25	交换碰撞
rfc7296	2.25.1	恢复或关闭时的碰撞 SAs
rfc7296	2.25.2	收回或关闭时碰撞 IKE SAs
rfc9242	3	中间交换细节
rfc9242	3.1	支持中间交换谈判
rfc9242	3.2	使用中间交换器
rfc9242	3.3	IKE_INTERMEDIATE 外汇保护和认证

文稿	章节	标题
rfc9242	3.3.1	保护IKE_INTERMEDIATE件信件
rfc9242	3.3.2	IKE_INTERMEDIATE交易所的认证
rfc9242	3.4	IKE_INTERMEDIATE 交换器处理错误

协议的目的是在文档中将其定位为源步骤:初始 DH 加两个不同新鲜 ML-KEM 封装的有界 IKE_INTERMEDIATE，再签名认证；保留 ADDKE协商、顺序号、逐次 密钥更新和 中间认证,绝不把两个相同长期 KEM密钥当独立分量；排除 CHILD_SA。

对照文稿定性质

在写出查询之前,分析师根据文件本身所说的协议的目的设定了已起草的属性清单. 名称、财产是什么 以及文件上所说的 是分析师的读物; 文档中存在指定位置。

ID	简称	对象	文稿怎么说	出处
A03	IKE SA运行协议	发起方 和响应方:双方在IKE_AUTH后接受IKESA后,均保证同行以IKE_INTERMEDIATE相同的内容和ID的IKE_AUTH电文运行同一会话.	同行认证一次,IKE_AUTH次,AUTH次,覆盖IKE_SA_INIT条信息加上IntAuth链条,每IKE_INTERMEDIATE条信息(s0481,s0482,s0486,s0488). 至此中间数据未经校验(rfc9242 5).	s0022, s0041, s0046, s0048, s0481, s0482, s0486, s0488
A04	不重复接受一个对等运行	发起方 和响应方:最多接受一次同行选举; IKE_AUTH_MID号和ID号电文属于这次运行.	IDs信息遵循了RFC 7296 2.2规则,IKE_AUTH的第一个ID信息比最后一个中间信息多一个(s0469); IKE_AUTH_MID是IntAuth(s0487)的一部分.	s0132, s0469, s0487
A08	夹在记录稿上的中弹	发起方 和响应方:接受的ADDKE顺序,圆序和KEi(n)/KEr(n)的内容是谈判的内容,回合n带有n-谈判的方法.	回合按其变形类型顺序排列,每回合在下一轮之前完成(s0022); 关键交换法领域MUST与N级谈判交换(s0041); IntAuth每条电文的链条(s0483,s0488).	s0022, s0025, s0041, s0483, s0487, s0488
K01	最后的IKE SA 密钥保密	发起方 财务报告和财务报告响应方 对一个网络攻击者持有一个ML-KEM分享了会议的秘密。	SKEYSEED(n) = prf(SK_d(n-1)),SK(n) → Ni → Nr),7个键为prf+ SKEYSEED(n) (s0043,s0044,s0045); a 失密的PQC算法不得损害最终的秘密(s0104).	s0043, s0044, s0045, s0104, s0106
K04	跨用途和生成的密钥分离	发起方 和响应方:一代人的保护,完整性和AUTH密钥是分开的,没有generation-2密钥仅从一代人1就跟随.	这7个关键是按用途区分的显著的prf+产出(s0045); a 圆形使用最近计算的密钥,其保护和认证密钥总是同一代(s0476,s0498)。	s0045, s0046, s0476, s0498
C01	会后前保密	发起方 财务报告和财务报告响应方: 已完成IKESA古典时的密钥保密(Q)EC)DH秘密被获取,尽管AUTH签名是公开的。	量子攻击器可以从古典交换器中学习SK(x),而后量子元件保持SKEYSEED不妥协(s0106,s0108); DH 责任人使用后被删除.	s0106, s0108, s0290
C08	一个破碎的部件没有破碎的SA	发起方 和响应方:随着古典元件或一个ML-KEM元件破解了最后的密钥保持秘密.	多个密钥交换形成共享密钥,这样一个密钥的妥协不会损害结果(s0104,s0106,s0107).	s0104, s0106, s0107

ID	简称	对象	文稿怎么说	出处
R01	信息 ID新鲜度	响应方:已接受的IKE_INTERMEDIATE/IKE_AUTH号电文的ID是下一个未使用的价值.	消息IDs已经1第一次报告IKE_INTERMEDIATE和增加,以及执行MUST核实(E)s0469);IKE_AUTH_MID是第一个IKE_AUTH圆(N)s0487).	s0132, s0469, s0487
R02	每条电文接受一次	响应方:相同IKE_INTERMEDIATE或IKE_AUTH的电文最多在IKE SA内接受一次.	重播必须从(s0114)中收回,"信息ID"规则禁止重用ID(s0469).	s0114, s0132, s0469
R04	按顺序进行中间回合,没有跳过	响应方:第i轮在第i+1回合前接受,每轮在下一轮之前完成,第IKE_AUTH轮在最后一轮之前不接受.	回合按其变形型顺序进行,每轮MUST在下一轮(s0022)前完全完成; 4. 它们在IKE_AUTH(s0468)之前是顺序和完整的。	s0022, s0468, s0469
A08.11	ADDKE发装至AUTH的子弹.	发起方 和响应方 (用户问题Q1):接受的ADDKE序列,圆令和IntAuth是谈判的笔录.	与A08相同; 问题在于中间回合是否与最后的AUTH回合挂钩。	s0022, s0041, s0483, s0488
K01.12	最后一个密钥在KEM泄漏中	发起方 和响应方 (用户问题Q2):有一个KEM秘密泄露了最终的IKE SA密钥保密.	与部分妥协案(s0104,s0106)的K01相同.	s0043, s0045, s0106
A04.13	没有弹夹或运行	发起方 和响应方 (用户问题Q3):回合或跑步不能被拼接,一回合不能跳过.	IntAuth是轮回上的一个prf链条,顺序为+IKE_AUTH_MID(s0483,s0488)和AUTH在它上签下(s0482).	s0022, s0468, s0482, s0483, s0488
X01	每轮有KEM个秘密	发起方 和响应方:输入SKEYSEED(1)和SKEYSEED(2)的值为SK(1)和SK(2).	新的电源密钥对和密码文本是:REQUIRED每种类型ML-KEM交换和答复者MUST NOT重复使用随机性(draft-ietf-ipsecme-ikev2-mlkem3线条335-338); 反应者ADDKE选择MUST NOT包含重复的算法(E)s0025).	draft-ietf-ipsecme-ikev2-mlkem:335, s0025, s0043
X02	启动身份保密	发起方:IKE_AUTH请求中的身份IDi,签名的octets中的prf(SK_pi,IDi).	IKEv2尽量减少了向未经认证的同龄人披露,但发起人先自我识别,而响应者或冒充其身份的人可以探测发起人的身份(rfc7296 5,第6478-6488行); IDi在加密有效载荷内飞行。	rfc7296:6478, s0471, s0482

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 54 段；分析者对每一段说明了去向：定为性质、定为攻击者条件，或者为什么都不选。选了 13 段，没选 41 段。列哪些段落由标准的章节结构决定；每一段的去向是分析者的判断。

段落	出处	定为	不选的原因
P01	draft-ietf-ipsecme-ikev2-mlkem:320-321	没有陈述目标	它只说适用RFC 9242和RFC 9370的安全考虑; 这两段分别列出。
P02	draft-ietf-ipsecme-ikev2-mlkem:323-338	X01, K01, C08	

段落	出处	定为	不选的原因
P03 至 P04	draft-ietf-ipsecme-ikev2-mlkem:340-346	X01	
P05	draft-ietf-ipsecme-ikev2-mlkem:350-350	没有陈述目标	页面页脚和运行标题的草稿.
P06	draft-ietf-ipsecme-ikev2-mlkem:353-358	没有陈述目标	指向另一个文档的指针; 它没有说明该协议的目标。
P07	draft-ietf-ipsecme-ikev2-mlkem:360-361	没有陈述目标	指向执行准则。
P08	draft-ietf-ipsecme-ikev2-mlkem:363-367	K01, C08, `kem_component`	
P09	draft-ietf-ipsecme-ikev2-mlkem:369-383	A08, C08, `classical_dh`	
P10	draft-ietf-ipsecme-ikev2-mlkem:385-395	没有陈述目标	向操作员提供禁用建议 。
P11 至 P14	draft-ietf-ipsecme-ikev2-mlkem:397-429	不在范围内	无子女IKE SAs,CREATE_CHILD_SA重键和 IKE_FOLLOWUP_KE被排除在这项任务之外.
P15	主机: 883-891	K01, C01, C08, `classical_dh`, `kem_component`	
P16	主机: 893-908	证明器问不了	变形型的格罗弗(Grover on Transform Transform Types 1-3)是原始人的力量.
P17	主机: 910-916	C01, C08, `classical_dh`	
P18	主机: 918-923	没有陈述目标	额外密钥交换的秩序对于安全无关紧要; 仅向实施者提供建议。
P19	主机: 925-932	C01, `classical_dh`	
P20	主机: 934-942	证明器问不了	认证步骤是古典的 原始的力量; 模式标志和验证 完美,并限制记录它。
P21	主机: 944-954	没有陈述目标	讨论为什么量子后的真实性不那么迫切.
P22	主机: 956-961	证明器问不了	增加的DoS暴露是一个资源问题.
P23	主机: 963-980	不在范围内	无子女SA和CREATE_CHILD_SA/IKE_FOLLOWUP_KE除外.
P24	rfc7296:6478-6488	X02, A03	
P25	rfc7296:6490-6494	不在范围内	EAP认证不是模拟运行的一部分.
P26	rfc7296:6496-6500	不在范围内	重复的CREATE_CHILD_SA重键没有新的DH被排除在外.
P27 至 P29	rfc7296:6502-6527	证明器问不了	迪菲-赫尔曼团体的实力是原始人的力量.
P30	rfc7296:6529-6530	C01	
P31	rfc7296:6532-6538	证明器问不了	DoS 未经认证的同行是一个资源问题.
P32	rfc7296:6540-6542	证明器问不了	PRF输出大小是一个原始参数.
P33	rfc7296:6544-6549	X01	
P34	rfc7296:6551-6556	没有陈述目标	设计原理指针外加禁止NONE完整性和ENCR_NULL加密的规则.

段落	出处	定为	不选的原因
P35	rfc7296:6558-6563	不在范围内	预共享密钥和低内涵秘密是替代认证模式; 模拟运行使用签名。
P36 至 P37	rfc7296:6565-6580	不在范围内	NAT检测不是模拟运行的一部分.
P38 至 P39	rfc7296:6582-6612	不在范围内	EAP认证不是模拟运行的一部分.
P40	rfc7296:6614-6619	证明器问不了	IP重新组装耗尽是一个资源问题.
P41 至 P42	rfc7296:6621-6633	不在范围内	入境管制和PAD涉及儿童SA批准,这里不包括。
P43 至 P50	rfc7296:6637-6696	不在范围内	交通选择者授权涉及儿童SAs和PAD,这里不包括.
P51	rfc9242:463-470	A03, A08, K01	
P52	rfc9242:472-477	没有陈述目标	IKE条支离破碎; 模型将信息作为一个整体处理。
P53	rfc9242:479-499	证明器问不了	认证前还原资源支出是一个DoS问题.
P54	rfc9242:501-514	A08, C08, `classical_dh`	

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 13 条，没检查 19 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	有效载荷保密属于Child SAs,在此排除.
K03	强保密／秘密值不可区分性	K01	
D01	消息完整性与数据来源真实性	A03, A08	
A01	对端曾参与性（寿命)	A03	
A02	弱一致性认证	A03	
A05	隐式密钥认证	K01, A03	
A06	显式密钥确认	不适用	IKE_AUTH 认证同行; 它没有明确确认拥有密钥。
A07	身份—凭据—密钥绑定	A03	
R03	业务操作至多一次	不适用	不得经营营业,开具账单或分配资源.
R05	抗降级／安全策略保持	不在范围内	模拟运行修正了每次运行中的谈判算法,因此在此不能要求对提案进行按路径降级; 限制记录它。
C02	抗密钥泄露冒充（KCI）	不在范围内	每个缔约方有一个长期签名密钥,一个同行无法像另一个伙伴一样签名; 本条目所说的方向需要一方的长期密钥作为攻击者输入,这样它就可以在同一个文件的协议目标中冒充该方.
C03	已知密钥安全／泄露隔离	K04	
C04	临时秘密／部分状态泄露韧性	K01, C08	
C05	泄露后安全恢复（PCS）	不适用	没有转折或妥协后恢复。
C06	注册凭据泄露后的增强认证	不适用	第PAKE号或登记记录。
C07	抗离线字典攻击	不在范围内	模拟运行使用签名; 带有低内涵密钥的预共享密钥模式不是建模的.

条目	目录里的性质	作为哪条性质检查	不检查的原因
Z01	授权执行正确性	不适用	IKE SA 个单位没有授权、授权、撤销或租赁。
Z02	委托权限不扩张	不适用	IKE SA 个单位没有授权、授权、撤销或租赁。
Z03	授权与身份／会话／操作绑定	不适用	IKE SA 个单位没有授权、授权、撤销或租赁。
Z04	撤销与过期生效	不适用	IKE SA 个单位没有授权、授权、撤销或租赁。
Z05	跨租户／跨服务安全隔离	不适用	IKE SA 个单位没有授权、授权、撤销或租赁。
S01	加密 0nonce 唯一性 (中文(简体)).	证明器问不了	这些文件没有界定AEAD非衍生物,也没有建模。
S02	重传／密钥重安装安全	R02	
S03	抗回滚与状态单调性	R01, R04	
S04	跨阶段安全上下文一致性	A08	
S05	终止与旧状态失效	R02	
P01	身份匿名性	X02	
P02	会话不可关联性	不适用	每一次运行都使用新鲜的SPIs和nonces,没有稳定的每个用户手柄可以连接.
P03	用户／凭据存在性隐藏	不适用	答复者只在交换之后回答; 没有查询显示是否存在用户或证书 。
V01	条件性进展／错误恢复	证明器问不了	进展、僵局和资源扩展没有经过微量证明。
V02	无非预期死锁	证明器问不了	进展、僵局和资源扩展没有经过微量证明。
V03	受限资源滥用／抗放大	证明器问不了	进展、僵局和资源扩展没有经过微量证明。

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 23 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 10 项，没设的 13 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	一个不诚实的发起人知道发起人的长期密钥和它自己运行的每一个秘密,所以约定和运行的密钥根据定义是失去的; 这些文件在不诚实的同行面前都没有要求。
S02	响应方	参与方	按定义全部失守	与应机S01相同.
S03	攻击者	参与方	攻击者得不到更多	攻击者是网络已经赋予其能力的参与者.
S04	IKE SA 密钥材料（SKEYSEED(n) SK_d SK_ei/er.SK_ai/ar.SK_pi/pr) (中文(简体)).	值	`kem_component`, `classical_dh`, `gen1_keys`, `enc1_key`	
S05	协商的 ADDKE 算法序列	值	攻击者得不到更多	算法序列、圆序、KE有效载荷、IDs、IKE_AUTH_MID和IntAuth链是网络或密钥持有人已经拥有的价值; 单枪匹马地关着他们,没有密钥
S06	各轮 KE 载荷	值	攻击者得不到更多	算法序列、圆序、KE有效载荷、IDs、IKE_AUTH_MID和IntAuth链是网络或密钥持有人已经拥有的价值; 单枪匹马地关着他们,没有密钥

ID	参与方或值	类别	攻击者条件	不设的原因
S07	电文 ID	值	攻击者得不到更多	算法序列、圆序、KE有效载荷、IDs、IKE_AUTH_MID和IntAuth链是网络或密钥持有人已经拥有的价值; 单枪匹马地关着他们,没有密钥
S08	IKE_AUTH_MID	值	攻击者得不到更多	算法序列、圆序、KE有效载荷、IDs、IKE_AUTH_MID和IntAuth链是网络或密钥持有人已经拥有的价值; 单枪匹马地关着他们,没有密钥
S09	IntAuth 链	值	攻击者得不到更多	算法序列、圆序、KE有效载荷、IDs、IKE_AUTH_MID和IntAuth链是网络或密钥持有人已经拥有的价值; 单枪匹马地关着他们,没有密钥
S10	ADDKE 算法序列	值	攻击者得不到更多	算法序列、圆序、KE有效载荷、IDs、IKE_AUTH_MID和IntAuth链是网络或密钥持有人已经拥有的价值; 单枪匹马地关着他们,没有密钥
S11	轮次顺序	值	攻击者得不到更多	算法序列、圆序、KE有效载荷、IDs、IKE_AUTH_MID和IntAuth链是网络或密钥持有人已经拥有的价值; 单枪匹马地关着他们,没有密钥
S12	IntAuth 转录	值	攻击者得不到更多	算法序列、圆序、KE有效载荷、IDs、IKE_AUTH_MID和IntAuth链是网络或密钥持有人已经拥有的价值; 单枪匹马地关着他们,没有密钥
S13	SKEYSEED	值	`kem_component`, `classical_dh`, `gen1_keys`, `enc1_key`	
S14	SK_d	值	`kem_component`, `classical_dh`, `gen1_keys`, `enc1_key`	
S15	SK_ei/SK_er	值	`kem_component`, `classical_dh`, `gen1_keys`, `enc1_key`	
S16	SK_ai/SK_ar	值	`kem_component`, `classical_dh`, `gen1_keys`, `enc1_key`	
S17	SK_pi/SK_pr	值	`kem_component`, `classical_dh`, `gen1_keys`, `enc1_key`	
S18	各轮 SK	值	`kem_component`, `classical_dh`, `gen1_keys`, `enc1_key`	
S19	各代 SK_d、SK_a、SK_e、SK_p	值	`kem_component`, `classical_dh`, `gen1_keys`, `enc1_key`	
S20	已完成的 IKE SA 密钥	值	`kem_component`, `classical_dh`, `gen1_keys`, `enc1_key`	
S21	最终 IKE SA 密钥	值	`kem_component`, `classical_dh`, `gen1_keys`, `enc1_key`	

ID	参与方或值	类别	攻击者条件	不设的原因
S22	IKE_INTERMEDIATE 消息	值	攻击者得不到更多	网络攻击者持有的IKE_INTERMEDIATE和IKE_AUTH讯息; 篡改属于协议目标。
S23	IKE_AUTH 消息	值	攻击者得不到更多	网络攻击者持有的IKE_INTERMEDIATE和IKE_AUTH讯息; 篡改属于协议目标。

每条性质在各攻击者条件下的答案

攻击者是分析师的,在写出询问之前设定的; 每一个答案都记录在其中之一下。 牢房是攻击者的财产的证明器答案; "无答"是攻击者设定的,用于证明器未裁定索偿或无记录的财产; 2. 空单元格是分析师没有为财产设定的攻击者。

攻击者	持有什么	依据	出处
network	只有网络:它读、丢、更改和发送消息,并且不为一方保密		
kem_component	IKE_INTERMEDIATE轮会议中共有的秘密SK(n),该轮会议完成了IKE_AUTH次; 其他组件和长期签名密钥保持不变	扩展必须在现有或未来的PQC密钥交换算法(s0104)妥协后幸存下来,这种妥协不得损害最终的SKEYSEED(s0106).	s0104, s0106
classical_dh	古典式(EC)DH 共享会话的秘密 g^ir,从线上录制,以后可以用密码学上相关的量子计算机计算.	量子攻击器在通过古典密钥交换(s0106)获得时,可以学习SK(x). 主要重点是防止收获和减少(s0108)。	s0106, s0108
gen1_keys	所有generation-1 IKE SA 一次会话的密钥 (SK_d(1)SK_ei(1)SK_er(1)SK_ai(1)SK_ar(1)SK_pi(1) SK_pr(1))),回合后读出一方的记忆.	每IKE_INTERMEDIATE个从SKEYSEED(n)(s0045)产生全新的一整代密钥,下一轮使用最近计算的密钥(s0476).	s0045, s0476, s0498
enc1_key	仅一个会话的generation-1加密密钥 SK_ei(1)	SK_ei保护回合的发起者信息(s0039,s0475), 因此部分解读一党状态可以单独曝光.	s0039, s0475

ID	network	kem_component	classical_dh	gen1_keys	enc1_key
A03	成立				
A04	成立				
A08	成立				
K01	无答案	无答案			
K04				无答案	无答案
C01			无答案		
C08		无答案	无答案		
R01	成立				
R02	成立				
R04	成立				
A08.11	成立				
K01.12		无答案			
A04.13	成立				
X01	成立				
X02	无答案				

关于证明和模型的说明

分析师给目标取了什么名字?

步骤	目标	特性	原因：
52	A03, A04, A08, A08.11, A04.13, K01, K01.12, K04, C01, C08, R01, R02, R04, X01, X02	plain_primitives, many_sessions, 其他 (中文 (简体)).	该型号将ML-KEM封装,prf/kdf,MAC,加密和签名视为理想原始,只使用Diffie-Hellman作为与单定律g^xy=g^yx的普通密钥协议; 在两个角色的任意一个会话中询问属性。 IKEv2 Message ID 计数器,重叠请求窗口和每一方的一次性密钥流没有建模,因此R01/R02 答案依赖于注入值而不是新鲜的会话值; 没有目标依赖于一个计数器或一个替换的密钥,所以没有使用有边框的模型.

分析员的结语

所有15个目标在为它们设定的每个攻击者下都得到回答,报告是完整的(阅读,数字,注释). 仅针对网络攻击者证实:双向协议(A03),注射接受IKE_AUTH(A04,A04.13,R02),将两发IKE_INTERMEDIATE发装订至AUTH交换台(A08,A08.11,R04),新鲜度IKE_AUTH通过会场新鲜值(R01),以及两个ML-KEM共同秘密的区别(X01). 每个证据都包含一个伸展力 lemma作为它的控制。

开放,无ProVerif的回复:最终的IKE SA密钥保密(K01,K01.12),一个破碎的部件没有打破SA(C08),丰收和解密前向保密(C01),跨代和使用的密钥分离(K04),发起身份保密(X02). 对于所有这ProVerif都毫无痕迹地回答`cannot be proved`:既不是证据,也不是攻击.

阻碍这些答案的是模型,而不是协议。 在复制的响应器内漏出一个会话元件,使得ProVerif分化,因此妥协目标只要求网络攻击器; 信息ID的计数器和窗口不是模拟的,它通过新的会话值将R01/R02限制在新鲜度上。 不需要有限度的模式或国家审查,因为没有目标依赖于柜台或替换的密钥。 Tamarin+ Agent 直接处理显示值和代数,将结算K01,K01.12,C01,C08,K04和X02。

没有发现:没有伪造目标,因此没有显示文件尚未说明的弱点,报告印有"没有发现"字样. 证明的结果是保证文件要求的,按照理想化的ML-KEM、prf、MAC和签名的象征性模式,并且(EC)DH被降格为单一的法律。