CMS复合KEM加密剖面的安全分析

draft-ietf-lamps-cms-composite-kem-04 — ProVerif+ 代理 报告

文稿	用于加密信件语法(CMS)的合成ML-KEM(协议定义)); 使用密钥封装机制(KEM) 加密信件语法中的算法(CMS) (辅助))
检查的性质	13 条：8 条成立，5 条不成立（5 个攻击）
发现	无

目录

1 协议和范围
2 发现
3 检查过的性质
4 本次分析的局限
附录 A：逐条性质的解读
附录 C：主张和证明器的答案
附录 D：分析是怎么跑的

1 协议和范围

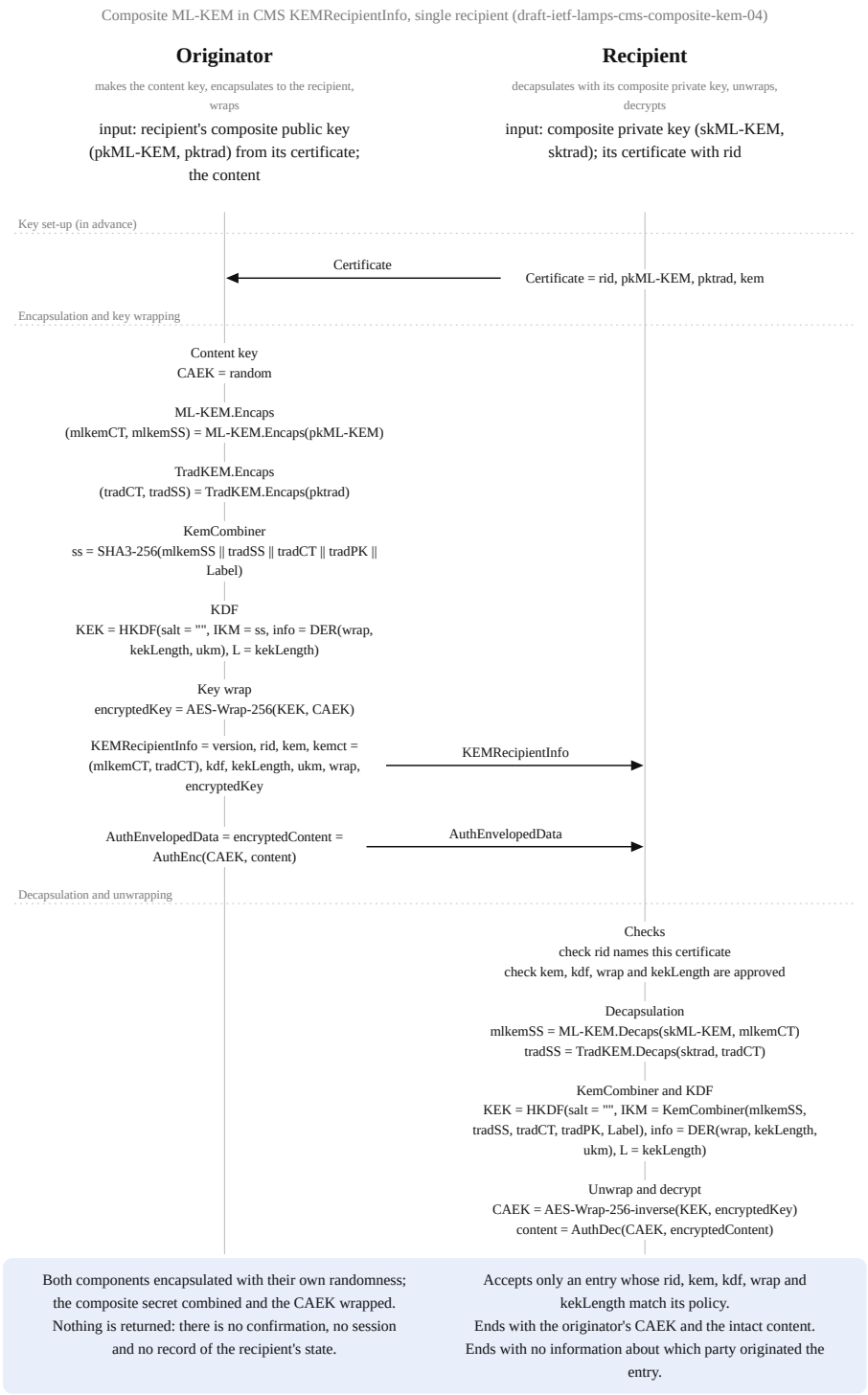
该剖面图载有发端人到一个收件人之间的内容认证加密密钥。CMSAuthEnvelopedData,使用其中一种复合材料ML-KEM区注册的算法3草案案文。 发端人持有收款人经认证的复合公用密钥,aML-KEM公用密钥和传统的公用密钥,使内容键本身、封装在两个部件上并发送一个KEMRecipientInfo带有包裹的密钥和加密内容。接收者持有匹配的复合私钥, aML-KEM解封密钥和传统的私人密钥。

当交换结束时,接收方持有发端人的内容密钥和发端人的内容,对于它所处理的条目,它没有任何关于哪一方发送该条目的信息。 发端人不会学到什么回馈:简介没有回应,没有密钥确认,也没有会话保留.

双方:

- **设计器**:制作内容密钥,封装给接收者,包裹. 持有:接收人从其证书中提取的复合公用密钥(pkML-KEM,pktrad); 2. 内容。
- **接收**:用其复合私钥,未包装,解密来解封. 持有:复合私人密钥(skML-KEM,sktrad); 它的证书与清除。

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。

在分析范围范围内,剖面图给出了它要给出的:双向密钥加密密钥,内容密钥和内容远离网络攻击者,密钥加密密钥绑定在ukm,密码文本和生成密钥的套件上,一个断开的组件让密钥完好无损,一个被披露的消息密钥只传达到该消息. 没有发现:每个失败的模型复制在文档中都有说明,即接收方可以将一个被接受的条目归属于任何一方,稍后对复合私钥的披露会打开已完成的信息,失去两个组件的密钥都会丢失每个与密钥配对一起保护的信息. 在这13个目标中,证据涵盖9个目标,其余的声称是源头的攻击。 证明基于理想化的原始: 复合KEM,结合器,密钥衍生,密钥包和内容加密都是具有反向定律且没有代数的构造器,因此构件安全性,碰撞阻力和密码优点是假设的. Tamarin+ Agent,即模拟组件及其代数的原样,需要将结果携带到算法本身.

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
K01	**密钥和私人密钥保密。** 对文稿点名的每个秘密（接收方组合 KEM 私钥、由 KEM 共享秘密派生的成对 KEK、CEK/CAEK、消息认证密钥），未持有相应泄露的攻击者不能从协议流量推导出该值；在组合 KEM 私钥泄露时，记录文稿所述的全部消息受危及这一后果。	收件人(受保护会议期间或之后的任何时候披露)	攻击成立（文稿已写明）	中	是
K02	**CAEK美元项下的保密费用。** 在 CEK/CAEK 下加密的内容只有预期接收方可读；不持有接收方私钥或 CEK/CAEK 的攻击者不能恢复内容。	无	成立	中	是
K04	**KEK不同衍生背景的分离。** 针对不同 关闭算法、不同 kekLength、不同 语句 ukm 或不同组合 KEM密钥对派生的 KEK互不相同；一个上下文的 KEK不能当作另一上下文的 KEK使用。	无	成立	低	是
A03	**关于KEK和身份的接收协议。** 接收方接受 KEMRecipientInfo 并派生 KEK 时，存在一个匹配的发起方运行，它向接收方公钥封装并派生出相同的共享秘密与 KEK，且接收方身份一致。	无	成立	低	否
A08	**KEMRecipientInfo00 个田,装入KEK号公路。** 接收方仅在 kem;kdf; wrap 标识、kekLength 与 0ukm 与获批上下文一致、且正是绑定进 KEK 派生的值时，才接受该 KEMRecipientInfo.	无	成立	低	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
D01	**无原产地认证的连带完整性。** 接收方接受的已认证内容对应发起方的真实发送且未被未持有消息认证密钥或 CAEK 的攻击者修改；AEAD 完整性不被解释为对任意发送者身份的认证。	无	攻击成立（文稿已写明）	中	是
C08	**Hybrid安全,一个部件断裂。** 在组合 KEM 的一个分量失效（其私钥被泄露）而另一分量完好时，成对共享秘密与 KEK 仍对攻击者保密。	收件人(受保护会话之前或期间的中断)	成立	中	是
C08.8	**CEK 部分或全部渗漏下的保密。** 在传统分量私钥泄露、ML-KEM 私钥泄露或两者同时泄露的条件下，检查 CEK/CAEK 是否仍对攻击者保密。	接收者(会话期间或之后人)	攻击成立（文稿已写明）	中	是
A08.9	**Combiner绑定标签,密码文本,密钥.** 接收方接受的 KEMRecipientInfo中，kem. kdf. 包装标识、kekLength(单位:千美元)与接收方公钥/证书一致，并作为 KEK派生的上下文输入。	无	成立	低	是
D01.10	**AEAD没有发件人认证。** 接收方接受的受保护内容对应允许发送方（持有相应密钥的一方）的真实发送，且未被篡改；AEAD 完整性不被解释为对任意发送者身份的认证。	无	攻击成立（文稿已写明）	中	是
X01	**受孕者封装新鲜度。** 发端人的两个KEMRecipientInfo条目共享一个KEM共享的秘密或封装随机性:如果两个发送的条目带有相同的复合共享秘密,它们就是同一个条目.	无	成立	低	是
X02	**泄漏限于一个信息。** 一份电文的KEK或CEK/CAEK的披露不披露任何其他电文的内容; 只有当收件人的复合私人密钥被披露时,才能了解另一电文的内容。	攻击者在会话中获取的密钥加密密钥,内容加密密钥和会话中一条消息的内容认证加密密钥(例如通过从党的记忆中读取).	成立	中	是
X03	**过去电文的保密性。** 内容和内容CEK/CAEK当接收方的复合密钥仅在会话结束后才披露时,已完成的会话将保密。	接收者整个复合ML-KEM的私人密钥,i. e. 在受保护的会话期间或之后的任何时候向攻击者披露的两种元件私钥。	攻击成立（文稿已写明）	中	是

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

文稿写明而起草的清单里没有、由分析者补充的目标（见附录 D）：X01, X02, X03.

所问之问,及分析师之答:

问题	回答	依据
Q1: 单分量泄露时 CEK 保密及双泄露控制	由于综合密钥的一个部分被披露,另一个部分完好无损,接收者条目的内容密钥在两个方向上都保密; 只有当两个组件密钥被披露时,内容密钥和内容才会掉落,控制运行会显示这些内容.	C08, C08.8
Q2: 组合器公钥/密文/算法 ID 上下文绑定	套件标签和两个密码文本被捆绑在复合密钥中,并通过它插入密钥加密密钥,因此在一个套件下或用不同的密码文本制作的条目,从不产生另一个条目的密钥加密密钥; ML-KEM密码和公用密钥的绑定 仅靠解封,如引用的组合器草稿所说,组合器在模型中被理想化.	A08.9, A08, K04, A03
Q3: 不得把 AEAD 完整性解释为任意发送者身份认证	接受者获得完整性但无发送者认证:持有接受者证书的一方可以凭自己选择的内容使接受者接受的条目,模型复制了该条目,RFC 9629声明.	D01, D01.10

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:

- 综合KEM是理想化的:ML-KEM和传统构件是抽象的封装功能,其共同的秘密是公钥和新鲜硬币的函数,因此任一构件的选择密码安全是假设的,没有被证明.
- 组合器是自由注射式构造器,而不是SHA3-256,因此碰撞,密码文本的第二预画阻力和绑定的等级被假定为去掉; 在参考草案之后,ML-KEM密码和公钥不是明确的组合器输入,只能通过解封来捆绑,模型象征性地复制.
- HKDF,AES 密钥包装和内容加密是理想的构造器,其单反法则; 2. 它们的强度和组件算法的强度都在模型之外.
- 接受方的复合公用密钥假设为真实的:证书内容,验证和公用密钥的替换没有建模.
- 内容加密的相关数据是一个常数,所以加密本身对CMS字段进行认证的不检查.
- 模拟一个内容类型(认证-输入-数据)和每个条目一个接收者; 签名属性, S/MIME 能力, 多个收件人和内容加密配置文件被忽略 。
- 该模型没有任何价值可以改变整个消息,因此对已交付的条目的重播,接受令和重传既没有被证明,也没有被否定.
- 随机数的质量,时间和其他侧通道,以及猜测的概率,都超出了可以问到的象征性证明器的范畴.
- 传统成分并非仿制为Diffie-Hellman:该模型给攻击者以低于X25519或ECDH的代数定律,因此发现的攻击仍将是攻击,而证据则是针对较弱的攻击者的证据.
- 私钥披露模式为交换后移交的两个元件密钥; 部分披露所储存的关键材料仅作为整个组成部分的模式。

主持人记录的是什么:

- 解读后答案有所改变,分别为:K04,A03,A08,A08.9,D01,X01.

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.

K01:密钥和私钥保密

对文稿点名的每个秘密（接收方组合 KEM 私钥、由 KEM 共享秘密派生的成对 KEK、CEK/CAEK、消息认证密钥），未持有相应泄露的攻击者不能从协议流量推导出该值；在组合 KEM 私钥泄露时，记录文稿所述的全部消息受危及这一后果。

网络上的攻击者读取一个条目的每个字段,既不获得双向密钥加密密钥,也不获得内容密钥,也不获得收件人的私人密钥. 它获得它们的一个案例是文档的状态:一旦收件人的复合私人密钥被披露,它就会将条目的两个密码解析,获得密钥加密密钥,并恢复内容密钥和内容,对于每一个用该密钥保护的电文.

- 结果:攻击停留(在文件中说明); 回答问题:是的; 可用备注
- 价值介质:与所列理想化有关的保密证明; 披露结果就是文件所描述的,现在机械地用给出内容密钥的确切步骤来显示。
- 在文件中说明:是的。 在文件里说: 494,rfc9629:568,s0067
- 休息时间:复合KEM,结合器,HKDF,AES密钥包装和内容加密是理想的构建器. ; 披露模式为移交两个组成部分的私人密钥; 认证数据内容类型的电文-认证密钥没有单独的对应器,因为在AuthEnvelopedData中,内容-认证-加密密钥携带该密钥。 ; 每一份保密证明都有其控制力,同样的查询没有排除披露,结果失败.
- 下一步:网络攻击者不再有任何进展; 元件的代数需要Tamarin+ Agent.

K02: CAEK号机车的内容保密

在 CEK/CAEK 下加密的内容只有预期接收方可读；不持有接收方私钥或 CEK/CAEK 的攻击者不能恢复内容。

一个条目的内容不由只拥有网络的攻击者读取:它既不持有接收者的私人密钥,也不持有内容密钥,没有接收者获得的密钥加密密钥的解包失败. 内容只在收件人的复合私密密钥,或消息本身的内容密钥被披露时才会掉落.

- 结果:持有; 回答问题:是的; 可用备注
- 数值介质:以所列理想化为中心值的保密证明; 文件需要它,所以这不是一个新结果。
- 在文件中说明:是的。 文件所言:主文:490,s0067,s0078,s0087
- 内容加密是一种理想的认证加密,具有一种反向定律; 没有密码属性是模拟的 。 ; 相关数据是一个常数,因此加密本身保护的字段没有被检查.
- 下一步:Tamarin+ Agent会解决理想化原始人的力量.

K04:KEK 不同衍生背景的分离

针对不同 关闭算法、不同 kekLength、不同 语句 ukm或不同组合 KEM密钥对派生的 KEK互不相同；一个上下文的 KEK不能当作另一上下文的 KEK使用。

此目标的答案在此读取后有所改变.

两个以相同的密钥加密密钥结尾的条目是同一个条目,因此不同的ukm值,不同的套件和不同的复合密钥对从不给出相同的密钥加密密钥,也没有一个可以结转到另一个上下文. 条目中包含的 ukm 正好是密钥加密密钥所衍生的值, 且一个带有更改的 ukm 的条目不会产生该密钥 。

- 结果:持有; 回答问题:部分; 可用备注
- 值低:它从将密钥衍生器和结合器作为注射式构造器来对待,四个上下文字段之一没有被行使.
- 在文件中说明:是的。 文件中说:rfc9629:378,s0116,s0117,s0124,s0034
- 休息时间:只有ukm不同; 密钥-wrap算法和密钥长度是剖面图的常数,因此它们分离的部分跟从剖面图而不是被行使. ; 键的衍生和结合器是注射式构造器,这就是使等键意味着输入的等值. ; 这两种说法都有其控制权,一旦两个事件不再与一个条目挂钩,就失败了.
- 开放:只有ukm在模型中存在差异:包装和kekLength是剖面图的单一授权值,而跨键对的分离只表现在两个模型套件之间.
- 下一步:一个带有数个密钥包算法和密钥长度的模型将锻炼分离的其余部分.

A03:关于KEK和身份的收款协议

接收方接受 KEMRecipientInfo 并派生 KEK 时， 存在一个匹配的发起方运行， 它向接收方公钥封装并派生出相同的共享秘密与 KEK， 且接收方身份一致。

此目标的答案在此读取后有所改变.

当收件人接受一个已交付的条目时,它会到达与发端人相同的密钥加密密钥,内容密钥和内容,在收件人身份和与条目名称的套件下,所以该条目不会与另一个收件人的或另一个套件的相混淆. 这上面没有说是谁送入的:信件是跟入,不是和党.

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:协议的根据是,鉴于该条目,具有决定性意义,而且文件没有说明认证目标,所以这是我对目的的操作解读,而不是说明财产。
- 在文件中说明:否。 资料来源:s0002、s0078、s0102。
- 补充:主张涉及已交付的、其密码标明的条目; 它没有说一个真正的起源者站在它的后面。 ; 身份约束是结构性的:每个接受者将接受者标识与自己的标识进行比较,每个套件使用自己的标签. ; 其控制,即发端人从未发送的对一个条目要求的相同信件,均告失败.
- 下一步:地址收件人以外的缔约方接受的条目需要第二个套房共享密钥; 该模型只显示地址接收者案件。

A08: KEMRecipientInfo 捆绑在KEK型机车中的田地.

接收方仅在 kem;kdf; wrap 标识、kekLength 与 ukm 与获批上下文一致、且正是绑定进 KEK 派生的值时， 才接受该 KEMRecipientInfo.

此目标的答案在此读取后有所改变.

收件人所接受的上下文值是密钥加密密钥的出处:一个其ukm或密码文本被更改的条目不能产生发端人的密钥加密密钥,一个带有另一套房标识符的条目只能被该套房的收件人接受. 接收者拒绝任何其识别码与其批准的套件不符的物件.

- 结果:持有; 回答问题:部分; 可用备注
- 数值低:它来自将收到的上下文字段作为输入的密钥,只有 ukm 运行。
- 在文件中说明:是的。 文件中说:rfc9629:378,主线:368,s0106,s0116,s0117,s0124
- 剩余:标识符检查是结构与剖面常数的比较; 用于接受若干套房的接收者没有建模。 ; 绑定为 ukm 显示,这是每个消息都不同的一个上下文字段 。 ; 这两种说法都有其控制权,一旦两个事件不再与一个条目挂钩,

就失败了.

- 打开: kem, kdf 和 包裹标识符以及 kekLength 是本配置文件中的单值, 所以模型检查它们但不能更改它们; ukm 是上下文字段,其约束力被行使。
- 下一步:一个模型中的若干密钥包算法和密钥长度可以解决其余问题。

A08.9: 组合器绑定标签,密码文本,密钥

接收方接受的 KEMRecipientInfo中， kem. kdf. 包装标识、kekLength(单位:千美元)与接收方公钥/证书一致, 并作为 KEK派生的上下文输入。

此目标的答案在此读取后有所改变.

套件标签和两个密码文本是复合密件的输入,因此在一个套件下制作的条目,或者有不同的密码文本,从不产生另一个条目的密钥加密密钥. ML-KEM密码和公用密钥的装订只来自解封,而不是来自明确的联合输入,这就是被引用的记录草案的设计决定.

- 结果:持有; 回答问题:部分; 可用备注
- 价值低:结合器的输入是不同的构建者论据,而文件则说明约束性财产本身。
- 在文件中说明:是的。 文件上写着: 草稿-itf-lamps-pq-composite-kem: 2588, s0012, s0041, s0066
- 休息:联合体是自由注射式构造器,而不是散列式,所以绑定结果依赖于注射力,而不是碰撞阻力. ; 拆卸时使用的传统公用密钥是接收人自己的; 2. 草案要求解首器从带子中取出的要求,假定已得到满足。 ; 这两种说法都有其控制权,一旦两个条目不再被同一个密钥捆绑,则无效.
- open:碰撞和密码文本的第二预录阻力被理想化的结合器假设为去掉. ; ML-KEM密码和公用密钥只能通过斩首来捆绑,如引用的草案所述.
- 下一步:Tamarin+ Agent需要散列和传统密钥交换的代数特性更进一步.

D01: 内容完整性,不进行原产地认证

接收方接受的已认证内容对应发起方的真实发送且未被未持有消息认证密钥或 CAEK 的攻击者修改; AEAD 完整性不被解释为对任意发送者身份的认证。

此目标的答案在此读取后有所改变.

对于发端人发送的条目,收件人接受的内容是发端人自己的:网络上的攻击者不能将内容替换为解密的条目. 然而,诚信就到此为止,因为没有发端人发送的条目被接受的同样容易,因此接收者无法从攻击者编造的条目中说出诚实的信息.

- 结果:攻击停留(在文件中说明); 回答问题:是的; 可用备注
- 值介质:完整性的一半与列出的理想化在一起,缺失的起源认证以机械的方式复制,其确切状况,是攻击者可以读到的证书.
- 在文件中说明:是的。 文件上写着:rfc9629:563,s0067,s0002
- 休息:内容加密的相关数据是常数,因此加密本身保护的字段没有被检查. ; 发端人是否是接受人信任的一方,完全不在模型之外.
- 下一步:不再进一步; 缺乏原产地认证属于CMS和KEM接收者,而不是复合建筑。

D01.10: AEAD没有发件人认证

接收方接受的受保护内容对应允许发送方（持有相应密钥的一方）的真实发送， 且未被篡改； AEAD 完整性不被解释为对任意发送者身份的认证。

收件人无法确定哪一方发送了接受的条目:持有收件人证书的人将证书封装到其公钥上,获取自己的密钥加密密钥,并发送收件人接受的内容. 发端人的认证必须来自CMS本身,例如签字,而不是密钥运输。

- 结果:攻击停留(在文件中说明); 回答问题:是的; 可用
- 值介质:一个有记录的KEM个收件人信息的财产,在此显示在本简介自己的消息流上; 这是使用剖面图的条件,而不是复合建筑的一个缺陷。
- 在文件中说明:是的。 文件上写着:rfc9629:563,s0002
- 补习:领受人证书按设计公开; 该模型公布两个收件人的公用密钥。 ; 内容加密是理想化的,因此结果只涉及密钥传输.
- 下一步:本概况无进一步内容; 添加签名的剖面图将是一种不同的分析。

C08:混合安保,一个部件断裂

在组合 KEM 的一个分量失效（其私钥被泄露）而另一分量完好时， 成对共享秘密与 KEK 仍对攻击者保密。

随着一个复合密钥的ML-KEM密钥或另一个传统密钥的披露,每个密钥的另一构件完好无损,这些收件人条目的密钥加密密钥和内容密钥保持秘密:攻击者计算一个构件的密钥而不是另一个,联合器是一条途径. 混合财产的双向控股,只有披露同一密钥对的两个组件密钥才让密钥掉落.

- 结果:持有; 回答问题:是的; 可用备注
- 价值介质:通过对所列部件和组合器的理想化来证明特征的中央保障; 文档上写着,所以它确认而不是发现。
- 在文件中说明:是的。 文件上写着: 草稿 - ietf - lamps - pq - composite - kem: 2588, s0066, s0075
- 剩余部分:两个单一组成部分的披露是仿照两个仿制的密钥对,因此,每个主张都对一个破碎的部件和同一个密钥对的另一部件进行了测试。 ; 组合器、关键衍生物和组件是理想的; 结果是混合论点的象征性对应,而不是论点本身。 ; 每项主张都有其控制权,一旦整个复合密钥被披露,该控制权即告失效。
- 下一步:用于组件代数和第二序假设的Tamarin+代理.

C08.8:CEK部分或全部渗漏情况下的保密

在传统分量私钥泄露、ML-KEM 私钥泄露或两者同时泄露的条件下， 检查 CEK/CAEK 是否仍对攻击者保密。

一个破碎的元件,无论是哪个方向,都使收件人条目的内容密钥无法到达,而一个复合密钥的两个元件密钥的披露则赋予每个条目的内容密钥和内容以该密钥保护. 因此,如问题所预期,单漏案和双漏案不同。

- 结果:攻击停留(在文件中说明); 回答问题:是的; 可用备注
- 价值介质:它以已核实的个案和记录的损失来回答问题,代价是所列的理想化。
- 在文件中说明:是的。 文件说:主机:494,rfc9629:568,s0066,s0067
- 休息:单元件的披露放在两个模型的密钥对上,因此两个单元件的漏泄都无法与另一个组合成一个完整的密钥. ; 综合KEM及其结合器被理想化.
- 下一步:部分披露存储关键材料的模型将覆盖一个部件存储部分的漏泄。

X01:每个接收者的封装新鲜度

发端人的2个KEMRecipientInfo条目共享一个KEM共享的秘密或封装随机性:如果两个发送的条目带有相同的复合共享秘密,它们就是同一个条目.

此目标的答案在此读取后有所改变.

发端人没有两个条目共享密钥加密密钥或内容密钥: 带有相同复合共享密钥的条目为同一条目,因此封装随机性与共享密钥永远不能重复用于另一个条目或另一个收件人.

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:根据硬币每面面值为新鲜,构件为注射式; 这一要求在文件中作了说明。
- 在文件中说明:是的。 文件上写着:rfc9629:575,s0069,s0072
- 休息:新鲜度是结构性的:每个发端人会自己铸造硬币,所以结果取决于构造者是注射的. ; 该模型每个条目有一个内容密钥,如简介所示,没有故意重复使用的情况。 ; 其控制, 2个预期共享密钥的不受限制的条目,失败 。
- 下一步:不再进一步; 同一接受方的第二场辩论不会改变这一论点。

X02:漏水仅限一条信息

披露KEK条电文或其中一条电文的CEK/CAEK条不披露任何其他电文的内容; 只有当收件人的复合私人密钥被披露时,才能了解另一电文的内容。

获得密钥加密密钥和一个消息的内容密钥的攻击者解密了该消息,而别无其他:其他每一个消息的内容仍然需要自己的密钥或收件人的复合私人密钥. 隔离之所以坚持,是因为每个消息都得到了自己的封装和内容密钥.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:一个已声明的保证与其确切条件,即仅一个消息的密钥,以机械方式显示。
- 在文件中说明:是的。 文件上写着:rfc9629:569,s0067,s0116
- 休息:一个消息的密钥的披露由发布其密钥加密密钥和内容密钥的会话模拟. ; 每条信息都有新鲜的硬币和一个新鲜的内容密钥,这就是孤立的基础.
- 下一步:如果部件的代数对隔离很重要,则需要Tamarin+剂。

X03:过去电文的前向保密

当接收方的复合私钥仅在会话结束后才被披露时,已完成会话的内容和CEK/CAEK是保密的.

已经完成的会话通过披露随后发生的收件人的复合私密密钥来打开:存储的密码文本被解封,内容密钥和内容随之而来. 剖面图不给前向保密,文档称私密密钥会损害所有与之相保护的信息.

- 结果:攻击停留(在文件中说明); 回答问题:是的; 可用
- 数值介质:文件中说明没有预先保密; 该模型在此配置图上显示它,并精确的步骤将打开一个已完成的会话。
- 在文件中说明:是的。 文件上说: 494,s0067
- 补充:披露模式为交换后的第二阶段,作为两个组成部分的私钥。 ; 该条目的密码文本被假定保存下来,网络上任何一方都可以做到这一点.
- 下一步:没有更进一步:配置文件没有可以恢复秘密的鼠标或重键。

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
K01	proved		kek_secret	检查	ctl_cek (holds_in_source)	证实3,1次攻击
K02	proved		m_secret	检查		证明:1
K04	proved		kek_inj	检查		证明:4
A03	proved		说吧	检查		证明:2
A08	proved		ukm_bound	检查		证明:4
D01	proved		说吧	检查	伪造(holds_in_source)	证实2,1次攻击
C08	proved		one_mlkem	检查		证明:2
C08.8	proved		one_mlkem	检查	ctl_cek (holds_in_source)	证实2,1次攻击
A08.9	proved		kek_inj	检查		证明:4
D01.10	reachable		运行		伪造(holds_in_source)	1次攻击
X01	proved		kek_inj	检查		证明:2
X02	proved		限制	检查		证明:1
X03	reachable		运行		ctl_cek (holds_in_source)	1次攻击

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
K01	发端人条目的对称KEK不是由只有网络,在会话期间或会话之后的攻击者获得的(控制,没有相位限制的相同查询,一旦私钥被披露就会失败).	`network`	proved	kek_secret	检查
K01	发端人入口的CEK/CAEK在AuthEnvelopedData中也携带了消息认证,但只有网络的攻击者并不获得.	`network`	proved	cek_secret	检查
K01	接收方的复合私钥不是从流量中衍生出来的; 2. 攻击者只有在它被披露时才到达它(控制:没有排除的话,查询失败)。	`network`	proved	sk_secret	检查
K01	披露接收方的复合私钥使攻击者获得了使用该密钥保护的条目的CEK/CAEK,其内容是:文件上写明的披露后果.	`composite_key_leak`	攻击 (holds_in_source)	ctl_cek(控制 cek_secret) (中文(简体)).	
K02	根据CEK/CAEK号加密的发端人条目的内容不是由既不持有收件人私人密钥也不持有CEK/CAEK号密钥的攻击者获取的.	`network`	proved	m_secret	检查
K04	两个发端人条目产生相同的结果KEK是同一个条目: 不同的 ukm 、 不同的套件标识符 或不同的复合密钥配对 永远不会给出相同的KEK,所以一个KEK无法从一个衍生上下文结转到另一个上下文(控制: 两个不受限制的条目不共享 a)KEK).	`network`	proved	kek_inj	检查
K04	KEK型源于KEMRecipientInfo型机车所携带的ukm,因此一个带不同ukm的条目不会产生发端人的KEK型机车:接受的上下文和衍生的KEK型机车属于一起(控制:不附带两个事件涉及一个条目的条件,接受不同的ukm型机车).	`network`	proved	ukm_bound	检查

目标	主张	攻击者	回答	查询	对照
K04	两个产生相同KEK的发端人条目是同一个条目:不同的ukm,不同的套件标识符或不同的复合密钥配对从不给出相同的KEK,因此一个KEK不能从一个衍生上下文结转到另一个衍生上下文.	network	proved	kek_inj	检查
K04	KEK系来源于KEMRecipientInfo系携带的ukm,因此一个带有不同ukm的条目不会产生发端人的KEK:接受的上下文和衍生的KEK属于一起.	network	proved	ukm_bound	检查
A03	当接收人接受交付的KEMRecipientInfo时,它到达发端人的KEK,CEK以及该条目的内容,它所接受的接收人身份和套件标识是条目名称(控制:接收任何发端人发送的条目时没有这种匹配的发送).	network	proved	说吧	检查
A03	当接收人接受交付的KEMRecipientInfo时,它会到达发端人的KEK,CEK以及该条目的内容,它所接受的接收人身份和套件标识是该条目的名称.	network	proved	说吧	检查
A08	条目中携带的ukm正是约束在KEK衍生物中的值:一个被更改的ukm不会产生被接受的KEK,因此接收者从不接受KEK衍生物以外的上下文(控制:不附带两个事件涉及一个条目的条件,接受不同的ukm).	network	proved	ukm_bound	检查
A08	条目中携带的密码文字(kemct)和套件标识符是绑定在KEK的值:一个带有替换的密码文字或另一个套件标识符的条目与发端人的KEK(控制:不附带两个事件涉及一个条目的条件,其他密码文字在同一ukm下被接受)一起不接受.	network	proved	ct_bound	检查
A08	条目中包含的ukm正是约束在KEK衍生物中的值:其ukm被更改的条目不会产生被接受的KEK,因此接受者从不接受KEK衍生物以外的上下文.	network	proved	ukm_bound	检查
A08	条目中携带的密码文字(kemct)和套件标识符是绑定在KEK的值:一个带有替换的密码文字或另一个套件标识符的条目与发端人的KEK不一并接受.	network	proved	ct_bound	检查
D01	接收者接受一个没有发端人发送的条目,包含攻击者选择的内容: 完整性 AuthEnvelopedData提供不给出来源认证.	network	攻击 (holds_in_source)	伪造	
D01	对于发端人交付的条目,接收人接受的内容是发端人自己的内容:网络攻击者不能将不同的内容替换为解密的条目(控制:不接受发端人发送的条目,因此发送的条件就是包含债权的内容).	network	proved	说吧	检查
D01	对于发端人交付的条目,收件人接受的内容是发端人自己的内容:网络上的攻击者不能将不同的内容替换为解密的条目.	network	proved	说吧	检查
C08	随着一个复合密钥的ML-KEM解首密钥被披露,而同一密钥的传统组成部分完好无损,接收者的条目中的KEK和CEK仍然保密(控制:不完全披露除外,查询失败)。	mlkem_key_leak	proved	one_mlkem	检查
C08	随着复合密钥传统部分的私钥被披露,同一密钥的ML-KEM密钥完好无损,该接收方条目中的KEK和CEK保密.	trad_key_leak	proved	one_trad	检查
C08.8	一个破损的部件——ML-KEM拆卸密钥——没有披露接收人条目中的CEK/CAEK,而该密钥的传统部件仍然完好无损。	mlkem_key_leak	proved	one_mlkem	检查
C08.8	一个破损的部件,即传统的私人密钥,没有披露接收人条目中的CEK/CAEK,而同一密钥中的ML-KEM密钥仍然完好无损。	trad_key_leak	proved	one_trad	检查

目标	主张	攻击者	回答	查询	对照
C08.8	在披露复合密钥的两个元件私人密钥时,收回用该密钥保护的条目中的CEK/CAEK。	composite_key_leak	攻击 (holds_in_source)	ctl_cek(控制 cek_secret) (中文 (简体)).	
A08.9	套装标签是联合器的输入:两个条目的KEK重合带同一个套装标识符和同一个接收器,因此在一个套装下制作的密码从不产生另一个套装的KEK(控制:两个不受约束的条目不共享一个KEK).	network	proved	kek_inj	检查
A08.9	传统的密码文字和通过ML-KEM解封,在条目中携带的ML-KEM密码文字是计算复合密件的密码:一个带有替换密码文字的条目不能产生接受的KEK(控制:不附带两个事件涉及一个条目的条件,其他密码文字被接受).	network	proved	ct_bound	检查
A08.9	每套Label是组合器的输入:两个条目的KEK重合带有相同的套件标识符和同一个接收器,因此在一个套件下制作的密码从不产生另一个套件的KEK.	network	proved	kek_inj	检查
A08.9	传统的密码文字和通过ML-KEM拆封,在条目中携带的ML-KEM密码文字是计算复合机密的密码:用替换的密码文字的条目不能产生可接受的KEK。	network	proved	ct_bound	检查
D01.10	接受方无法确定哪一方是接受的条目:持有接受方证书的任何一方都可以使接受方接受的条目.	network	攻击 (holds_in_source)	伪造	
X01	发端人没有两条KEMRecipientInfo的条目共用KEK或CEK:携带相同复合共享密件的条目是同一条目,因此每个接收人封装随机性,共享密件永不重复使用(控制:两条不受限制的条目不共用KEK或CEK).	network	proved	kek_inj	检查
X01	发端人没有2个KEMRecipientInfo条目共用KEK或CEK: 携带相同复合共享密件的条目是同一条目,因此每封封装随机性,共享密件从不重复使用.	network	proved	kek_inj	检查
X02	向攻击者披露的一条信息中的KEK和CEK不披露任何其他信息的内容; 3. 只有当收件人的复合私人密钥被披露时,才能到达另一电文的内容。 攻击者持有网络外的KEK和CEK的一条信息.	network	proved	限制	检查
X03	已经完成的会话的内容和CEK在随后披露收件人的复合私人密钥后被收回:没有远期保密.	composite_key_leak	攻击 (holds_in_source)	ctl_cek(控制 cek_secret) (中文 (简体)).	

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-20261114T233225, 2026-11-14. 状态: 完成 。 型号:deepseek-v4-1-flash-261017. 台阶:46,校对:4 s,壁16 min,耗资0.137 USD.

ProVerif:71 证明运行,71 决定,0 未答,3 s,43 答录.

分析了什么

协议	CMS 复合KEM 加密剖面图
版本	draft-ietf-lamps-cms-composite-kem-04
分析范围	固定草案明确注册的一种 ML-KEM+传统分量组合；单接收者 AuthEnvelopedData； 接收公钥已认证， 独立分量随机性和规范组合器输入/域分离 保留；算法计算性质不在符号结论内。不得挑选文稿不存在的套件。
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124个编号段落(22283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	CMS号机车使用合成ML-KEM号机车
主体	2.1	第RecipientInfo号公约
主体	2.2	基本构成部分
主体	2.2.1	使用基于HKDF-的密钥衍生函数
主体	2.3	证书公约
主体	2.4	SMIME 能力属性公约
主体	3	标识符
主体	4	安全考虑
rfc9629	2	KEM 处理概况.
rfc9629	3	KEM 收件人信息
rfc9629	5	密钥衍生

协议的目的是在文档中将其定位为源步骤:固定草案明确注册的一种 ML-KEM+传统分量组合；单接收者 AuthEnvelopedData；接收公钥已认证， 独立分量随机性和规范组合器输入/域分离保留；算法计算性质不在符号结论内。不得挑选文稿不存在的套件。

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
K01	密钥和私钥保密	接受者的综合ML-KEM私钥, 双向KEK,则CEK/CAEK(单位:千美元)AuthEnvelopedData也携带信件认证),远离只拥有网络的攻击者;以及公开私密密钥的既定后果,损害了所保护的每一项信息。	s0067项主要规定,执行应准确保护这些价值,并说明披露的后果; rfc9629第7节也这么说,并补充说,KEK/CEK/CAEK妥协仅限于一条信息.	主机:490,主机:494,rfc9629:568,s0067,s0078,s0079,s0109,s0123
K02	CAEK中的内容保密性	内容及保护它的CEK/CAEK号车,远离攻击者,攻击者既不持有接收者的斩首密钥,也不持有CEK/CAEK号车.	s0002/s0005:KEM综合设备将CEK/CAEK从发端人转让给接收人; s0078和s0087: CEK由发端人生成,每个接收者都用它解密内容; s0067将CEK/CAEK列为保护值.	主机:490、s0002、s0005、s0067、s0078、s0087
K04	KEK 不同衍生背景的分离	配对 KEK:KEKs 衍生给不同的包装算法,不同的kekLength,不同的ukm或不同的复合键对必须不同,所以一个上下文的KEK不能作为另一个上下文的KEK.	s0116/s0117从KEMRecipientInfo元件(rap, kekLength, ukm)中建造了KDF信息输入器; s0124要求所有KDF投入对产出产生影响; s0034要求L与包装密钥尺寸一致得到确认.	rfc9629:378, s0014, s0034, s0116, s0117, s0119, s0120, s0121, s0124
A03	KEK和身份的收款协议	接收人:当接受交付的KEMRecipientInfo,其KEK,CEK及其内容为该条目的发端人时,在摆脱中的接收人身份是其证书被使用者.	文件没有说明明确的认证目标; 要求来自目的、转让、转让、转让、CEK给预定接受者的建议(s0002,s0005,s0078与s0084/s0089),并且从消除中命名收件人的证书和密钥(s0102).	s0002, s0005, s0078, s0084, s0089, s0102
A08	KEMRecipientInfo00 个田地进入KEK号公路	Kem, kdf 和包装标识符,kekLength和 ukm 接收人接受一个KEMRecipientInfo,并且这些精确的数值是约束在KEK推论.	s0106:实施MUST确认kekLength符合包装算法; 3. s0116/s0117:KDF型机车的信息输入由这些场馆建造,s0124型机车需要所有输入来影响输出; s0014/s0020 任务HKDF-SHA256和AES-Wrap-256; s0034需要确认L; s0019 落叶乌克姆免费.	主场:296,主场:368,rfc9629:378,s0012,s0014,s0019,s0020,s0034,s0106,s0116,s0117,s0124
D01	没有原产地认证的内容完整性	接收者接受的认证内容:没有被网络攻击者修改,而接收者得不到对哪个方发源的保证.	rfc9629 第7节规定,KEM算法不提供数据来源认证,因此内容从未知来源完整地交付; 2. 第s0067号主论指出,关键披露可以允许修改经认证的内容。	rfc9629:563, s0002, s0067
C08	混合安保,一个部分断裂	当攻击者掌握一个复合组件的私人密钥,而另一个组件完好无损时,复合组件共享的秘密,结果的KEK和内容.	s0066号主要文件规定,KEM号综合草案的安全考虑适用,草案规定,一个部分被打破时,合并的秘密保密; s0075号主机警告重用密钥。	s0066, s0075
C08.8	CEK 部分或全部渗漏下的保密	密码CEK/CAEK页:1KEK(b) 披露复合部件的一个或两个私人密钥; 用户询问单漏和双漏的情况。	与C08相同:s0066号主机服从于KEM号综合草案,其联合说明包含一个断裂部分; 第s0067号和第rfc9629号主判决第7节规定了私人密钥披露的全部后果。	s0066, s0067, s0075

ID	简称	对象	文稿怎么说	出处
A08.9	组合器绑定标签、密码文本、密钥	KEM联合器生产的复合共享密件:它必须捆绑套件Label,传统密钥和传统公钥,并通过ML-KEM拆卸ML-KEM密钥和公钥.	s0012要求Kem持有第3节的ML-KEM OIDs和s0044..s0059节的复合设备之一,每个套房登记一个明显的OID; 联合体本身在引用的KEM复合体草案(s0041)中作了具体说明,s0066号主体是适用的。	s0012, s0041, s0048, s0053, s0066
D01.10	AEAD没有发件人认证	发端人的身份,即使内容完好无损,接受人也无法从接受的AuthEnvelopedData中确定.	rfc9629节 7行 563:KEM算法不提供数据源认证,因此内容从未知来源完整地交付.	rfc9629:563, s0002, s0067
X01	每个接收者封装新鲜度	发端人的每封装,其新鲜的随机性和复合共享秘密:一个条目的任何内容都不可能被另一个条目重复使用.	rfc9629 第7节(574-587行)要求每个接收者有一个新的KEM共享秘密,包括KEM使用的任何随机值,并禁止用于任何其他目的的再利用; 主机s0069/s0072需要独立的组件随机性.	rfc9629:575
X02	漏水局限于一个信息	其他信息的内容,当一个信息KEK或 时 间 CEK/CAEK到达攻击者。	rfc9629 第7节(行568-572):KEK号,CEK号或CAEK号的妥协可能导致单条电文的加密内容的披露,而KEM号私钥的妥协则可能披露所有与之保护的内容.	rfc9629:569
X03	过去消息的前向保密	内容和完成的会话的CEK/CAEK,与会话结束后发生的对接收者的复合私钥的披露相对应.	s0067号主要文件指出,披露ML-KEM号综合私人密钥可能导致所有用该密钥保护的信息妥协,即没有这种财产; rfc9629节 7线 568-570说同样.	主机: 494

分析者依据文稿补充的性质：X01, X02, X03.

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 84 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 48 段，没选 36 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	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2531-2534	C08, K01, `composite_key_leak`	
P02 至 P06	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2538-2578	C08	
P07 至 P09	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2582-2586	A08.9	
P10	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2588-2596	C08, A08.9	
P11	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2598-2602	A08.9	

段落	出处	定为	不选的原因
P12 至 P18	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2604-2628	A08.9	
P19	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2632-2633	证明器问不了	它引入了计算概念词汇表; 引言本身没有说明协议的任何财产。
P20	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2635-2649	A08.9	
P21	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2653-2655	C08	
P22	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2657-2662	C08	
P23 至 P26	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2666-2692	A08.9	
P27	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2694-2697	A08.9	
P28 至 P31	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2701-2728	证明器问不了	Ciphertext 第二次图像前阻力是一个计算属性,涉及找到两个解封为同一秘密的密码; 符号模型使构造器具有注入性,不能问它。
P32	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2731-2735	A08.9	
P33	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2737-2741	A08.9	
P34	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2745-2749	没有陈述目标	它警告不要将这种结合器应用到其他组件算法:一种设计限制,而不是这种交换的属性.
P35	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2753-2757	C08	
P36	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2759-2764	没有陈述目标	将单算法密钥再利用与混合设置进行比较; 它说没有这种交换的财产。
P37 至 P40	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2766-2791	C08, A08.9	
P41	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2795-2806	不在范围内	向验证局提供关于对组件密钥的吊销检查的指导意见; 证书管理超出任务范围 。
P42 至 P43	(原始内容存档于2019-09-22) (中文(简体)). Draft-itf-lamps-pq-composite-kem: 2810-2827	没有陈述目标	综合证书中算法的折旧政策; 它没有说明可以询问证明器的信息流的属性。
P44	主机: 486-488	C08, K01, D01	

段落	出处	定为	不选的原因
P45	主机: 490-501	K01, K02, D01, `composite_key_leak`, `kek_leak`	
P46	主机: 503-504	没有陈述目标	指向SP800-57的关键管理指导,说明本身无.
P47 至 P50	主机: 506-532	证明器问不了	伪随机性弱的生成器和关于其他输出的信息封装随机性是概率和生成器质量问题; 一个象征性的证明器没有概率攻击者。
P51	主机: 534-536	C08, A08.9	
P52	主机: 538-545	证明器问不了	通过计时或中间运算的侧式通道在可以询问的符号证明器之外.
P53	主机: 547-550	A08.9	
P54	rfc5083:308-310	K02, D01	
P55	rfc5083:312-317	证明器问不了	关于反模式加密强度的声明,与CBC相比; a 计算密码属性。
P56	rfc5083:325-328	K02	
P57	rfc5083:330-337	X02	
P58	rfc5083:339-348	证明器问不了	随机生成 CAEKs , 粘贴和非粘贴, 以及生成器的质量不是属性 符号验证器可以询问 。
P59	rfc5083:350-355	不在范围内	签名属性和内容跟踪的信息-digest属性:签名属性不是模型配置的一部分.
P60	rfc5083:357-369	不在范围内	按网关进行非主动加密流量和简洁文字分析:在模拟交换之外的一个业务问题。
P61	rfc5652:2837-2839	没有陈述目标	它说明了CMS提供的一般情况; 此配置文件没有属性 。
P62	rfc5652:2841-2842	不在范围内	保护签名者的私钥和签名数据的假名: CMS的签名部分在这个加密配置外.
P63	rfc5652:2844-2849	K01, K02, `composite_key_leak`, `kek_leak`	
P64	rfc5652:2851-2855	D01, K01	
P65	rfc5652:2864-2872	D01, D01.10	
P66	rfc5652:2874-2877	D01.10	
P67	rfc5652:2879-2889	证明器问不了	随机生成CEKs,MAC键,IVs和铺垫; 发电机质量在象征性模型之外.
P68	rfc5652:2891-2903	证明器问不了	有效的安全是两种算法中较弱者的安全:关于密码强度的语句,而不是关于痕迹的语句.
P69	rfc5652:2905-2911	没有陈述目标	算法随着时间的推移而减弱,执行应当模块化:建议,而不是交换的财产.
P70	rfc5652:2917-2927	不在范围内	反签名未签名属性; CMS属性在此加密剖面之外.
P71	rfc5869:355-360	没有陈述目标	介绍HKDF自己的安全考虑,指另一份文件; 协议没有规定任何财产。
P72	rfc5869:362-371	证明器问不了	HKDF背后的基本散列的强度和建模选择是计算假设,是不能问起的象征性证明器.
P73	rfc9629:542-543	K01, K02, D01	

段落	出处	定为	不选的原因
P74	rfc9629:545-554	证明器问不了	IND-CCA2安全性和藤崎-小本变换是计算属性; 2. 象征的模型 理想化KEM 代替。
P75	rfc9629:556-556	证明器问不了	KDF型机车应至少提供KEM型机车的安全级别:关于优势的说明.
P76	rfc9629:558-561	证明器问不了	与KEM的关卡相对的密钥加密算法的选择和大小:关于长处的说明.
P77	rfc9629:563-566	D01, D01.10	
P78	rfc9629:568-572	K01, K02, X02, `composite_key_leak`, `kek_leak`	
P79	rfc9629:574-587	X01	
P80	rfc9629:589-598	证明器问不了	随机生成的CEKs,CAEKs和MAC键和发电机质量不能象征性地要求.
P81 至 P83	rfc9629:600-620	证明器问不了	密钥加密,内容加密或MAC算法对齐的有效安全性:关于密码强度的语句.
P84	rfc9629:622-629	没有陈述目标	算法随时间推移而减弱,执行应当模块化:向执行者提供咨询.

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 35 条没选，分析者把它们逐条过了一遍：作为性质在这里检查，或者写明原因不检查。检查了 12 条，没检查 23 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
K03	强保密／秘密值不可区分性	K01, K02	
A01	对端曾参与性（寿命)	A03	
A02	弱一致性认证	A03, D01.10	
A04	单射一致性认证	D01.10	
A05	隐式密钥认证	K01, K02	
A06	显式密钥确认	不适用	剖面图没有密钥确认信息:发端人从未收到任何回信,因此没有任何信息可以证实收件人持有该密钥.
A07	身份—凭据—密钥绑定	A03, A08	
R01	认证／挑战新鲜性	不适用	简介没有质疑、柜台、时间戳或罚单; 没有新鲜的东西可以证明
R02	消息级抗重放	D01.10	
R03	业务操作至多一次	不适用	简介没有进行可两次收费、消费或分配的业务活动。
R04	消息接受顺序／窗口安全	不适用	本配置文件中没有序列号,计数器或接受窗口.
R05	抗降级／安全策略保持	A08, A08.9	
C01	前向保密性（FS）	X03	
C02	抗密钥泄露冒充（KCI）	不适用	发端人根本不持有长期证书,因此没有可以用来冒充其身份的对等密钥.
C03	已知密钥安全／泄露隔离	X02	
C04	临时秘密／部分状态泄露韧性	C08	

条目	目录里的性质	作为哪条性质检查	不检查的原因
C05	泄露后安全恢复（PCS）	不适用	没有鼠标,没有重键,也没有长寿的会话:每条消息都是新鲜的一弹封装.
C06	注册凭据泄露后的增强认证	不适用	此配置文件中不存在密码和增强认证机制 。
C07	抗离线字典攻击	不适用	没有使用密码或其他低通密,因此没有离线字典攻击表面.
Z01	授权执行正确性	不适用	剖面文件没有授权决定:接受者只是解密它所能解密的东西.
Z02	委托权限不扩张	不适用	没有授权或代理机制。
Z03	授权与身份／会话／操作绑定	不适用	没有与用户、服务或操作绑定的授权标志。
Z04	撤销与过期生效	不在范围内	撤销和证书有效性是任务所忽略的证书管理问题; 草案仅将其作为CA项指导意见加以讨论。
Z05	跨租户／跨服务安全隔离	不适用	简介中没有多租户或跨服务结构。
S01	加密 0nonce 唯一性 (中文(简体)).	X01	
S02	重传／密钥重安装安全	不适用	没有安装或重新安装过密钥: 每个消息都是独立的 。
S03	抗回滚与状态单调性	不适用	配置文件没有保存可回滚的版本或缓存状态 。
S04	跨阶段安全上下文一致性	不适用	简介只有一个阶段:一个发端人,一个条目,一个交付.
S05	终止与旧状态失效	不适用	没有会议终止; 没有什么比信息活得更久
P01	身份匿名性	不适用	接收者在清除时得名,其证明在清除时得名; 配置文件没有匿名模式。
P02	会话不可关联性	不适用	信件带有收件人的标识符,且设计上不能连接; 2. 档案里没有什么目标
P03	用户／凭据存在性隐藏	不适用	没有查询或发现交换,其答复可以列举用户或证书。
V01	条件性进展／错误恢复	证明器问不了	进展和错误的恢复是活性问题,无法问到一个基于痕量的验证器.
V02	无非预期死锁	证明器问不了	死锁自由不是可以问到的ProVerif的财产; 它不能说跑步总是完成。
V03	受限资源滥用／抗放大	证明器问不了	扩大资源需要一种成本模式; 一个象征性的证明器 算上事件,没有别的。

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 18 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 7 项，没设的 11 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	发端人	参与方	攻击者得不到更多	发端人没有长期的秘密:在其位置上的攻击者已经可以将任何内容通过网络发送给接收者,这是D01.10声明的内容.
S02	接收者	参与方	`composite_key_leak`	
S03	综合ML-KEM私人密钥	值	`composite_key_leak`	
S04	双向KEK	值	`kek_leak`	
S05	CEK/CAEK	值	`kek_leak`	

ID	参与方或值	类别	攻击者条件	不设的原因
S06	消息认证密钥	值	kek_leak	
S07	内容	值	攻击者得不到更多	了解一个消息的简洁字句不会产生任何关键信息,也不会产生任何其他信息; 目标属性仍然值得询问,而且没有受到影响。
S08	上下文字段	值	攻击者得不到更多	包裹,kekLength和 ukm 旅行在KEMRecipientInfo 本身, 并且已经对网络攻击者公开。
S09	双向共享密钥	值	kek_leak	
S10	收件人身份	值	攻击者得不到更多	接收人的身份在清除和公开证明中携带; 网络攻击者已经掌握了
S11	基姆 OID	值	攻击者得不到更多	KEM OID是信息中携带的公共算法标识符.
S12	kdf OID (英语).	值	攻击者得不到更多	KDF OID是信息中携带的公共算法标识符.
S13	包装 OID	值	攻击者得不到更多	包裹 OID 是一个公用算法标识符 包含在消息中。
S14	kekLength	值	攻击者得不到更多	kekLength是信息中携带的公用整数.
S15	语句 ukm	值	攻击者得不到更多	ukm在设计上是公开的:s0019对它不设任何要求,并以清晰的文字传送.
S16	认证内容	值	攻击者得不到更多	经认证的内容是信息有效载荷; 持有它不给密钥 也没有其他信息。
S17	CAEK	值	kek_leak	
S18	接收公钥	值	攻击者得不到更多	收件人的复合公用密钥在其证书中公布,并由发端人使用; 2. 网络攻击者已经掌握了

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		
composite_key_leak	接收者整个复合ML-KEM的私人密钥,i. e. 在受保护的会话期间或之后的任何时候向攻击者披露的两种元件私钥。	第s0067号主论指出,披露综合ML-KEM私人密钥可能导致所有用该密钥保护的电文妥协,因此,必须在该披露下对财产进行核对。	主机:494,s0067
mlkem_key_leak	只有接收者的ML-KEM解首密钥,传统部件的私人密钥仍然完好无损.	s0066号主要文件使综合KEM草案的安全考虑得以适用,该草案分析了一个组件算法被完全打破的情况; 用户问题1 问这个案件。	s0066, s0075
trad_key_leak	只有传统部件的私人密钥(X25519或ECDH),ML-KEM的解封密钥仍然完好.	s0066号主干法适用的单裂构件分析的对称性案例; 2. 用户问题1 要求它。	s0066, s0075
kek_leak	攻击者在会话中获取的密钥加密密钥,内容加密密钥和会话中一条消息的内容认证加密密钥(例如通过从党的记忆中读取).	rfc9629 第7节将KEK列为必须保护的价值观之一,并说其妥协可能披露单一信息的内容; s0067号主机说,披露密钥加密密钥,内容加密密钥或CAEK可能损害相关的加密内容.	rfc9629:569,主机:496,s0067

ID	network	composite_key_leak	mlkem_key_leak	trad_key_leak	kek_leak
K01	成立	不成立			

ID	network	composite_key_leak	mlkem_key_leak	trad_key_leak	kek_leak
K02	成立				
K04	成立				
A03	成立				
A08	成立				
D01	不成立				
C08			成立	成立	
C08.8		不成立	成立	成立	
A08.9	成立				
D01.10	不成立				
X01	成立				
X02	成立				
X03		不成立			

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：
31	K01, K02, K04, A03, A08, A08.9, D01, D01.10, C08, C08.8, X01, X02, X03	plain_primitives, many_sessions, long_flow	每个答案都基于理想原始: KEM合成器是两个抽象的KEMs,其共同的秘密是公钥和新鲜硬币的功能,联合器是自由注射式的构造器,HKDF,AES密钥包和AEAD是理想的构造器,具有其单一的反向定律. 不使用独家或Diffie-Hellman代数,因此传统元件作为不透明KEM处理,模型给予攻击者少于真实的X25519或ECDH执行. 在两个套房的任何发端人和接收人会议中,都询问财产情况,并分两阶段进行私钥披露。

分析员的结语

CMS综合KEM简介是仿照来源单位的,所有13个目标都得到了答复。 该模型有一个发端人和两个不同的复合套房的两位接受者(ML-KEM768-X25519,ML-KEM1024-ECDH-P384); 综合KEM是两个带有自己硬币的抽象组件,组合器遵循被引用的草稿(两者都是组件机密,tradCT,tradPK,每套Label),密钥加密密钥来自HKDF的包裹,kekLength和ukm,内容密钥被包裹,在理想的内容加密下使用. 第二阶段披露复合密钥,一个会场公布自己的密钥加密和内容密钥,将两个单元元件的漏泄放在两个不同的密钥对上,这样每个单元件的主张都用另一元件进行测试,结果完好无损. 被证明,每个控件都有失败的:密钥加密密钥,内容密钥和内容是网络攻击者的秘密; 2. 接收人以发件人的密钥、内容、身份和交付物品的套件为终点; ukm 和密码文本是绑定在密钥加密密钥中的值; 混合财产持有一个部分在两个方向上均被打破; 条目从不共享密钥; 而漏出的信息密钥只传达到此信息. 掌握来源的攻击:接收者接受一个没有发送发件人的条目(记录,RFC 9629 第7节),一个已完成的会话由后来的私钥披露(记录,主记录,第4节)开启,失去两个组件密钥都会丢失每条与密钥对一起保护的信息. 没有新的发现。 更多的是:KEM组件,结合器,密钥衍生和密码优势被理想化,传统组件没有Diffie-Hellman代数,因此将结果带给算法需要Tamarin+Agent; 这里的信息没有值变化,所以没有应用有界限的模式或状态审查; 而包算法和密钥长度都是剖面常数,所以只有 ukm 被作为上下文字段行使.