目录

TLS 证书加外部 PSK 的安全性分析
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

TLS 证书加外部 PSK 的安全性分析

本报告的其他语言版本：English。

rfc9973 · ProVerif+ Agent 报告

文稿	TLS 1.3 Extension for Using Certificates with an External Pre-Shared Key（协议定义）; The Transport Layer Security (TLS) Protocol Version 1.3（辅助）
检查的性质	17 条：14 条成立，2 条不成立（2 个攻击），1 条无答案
发现	无

1 协议和范围

该扩展允许共享预配置外部预共享密钥的客户端和服务器执行 TLS 1.3 握手：该密钥进入密钥编排，同时双方仍用证书相互认证。客户端持有自己的证书、签名密钥、外部 PSK 及其身份；服务器持有自己的证书、签名密钥和同一个 PSK。每一方在 hello 中发送新的 key share、PSK identity，客户端还发送 binder；服务器追加 EncryptedExtensions、CertificateRequest、自己的 Certificate、对 transcript 的 CertificateVerify 以及自己的 Finished，客户端则用自己的 Certificate、CertificateVerify 和 Finished 作答。交换结束后，每一方都知道对端经证书认证的身份、选定的 PSK identity，并且知道对端派生了相同的握手密钥。

参与方：

- **客户端**：持有本对的外部 PSK 及其证书。持有：cert(idC, spk(skC))、skC、外部 PSK、身份 pid。
- **服务器**：持有同一个外部 PSK 及其证书。持有：cert(idS, spk(skS))、skS、外部 PSK、身份 pid。

图 1 展示了文稿所规定的交换流程。

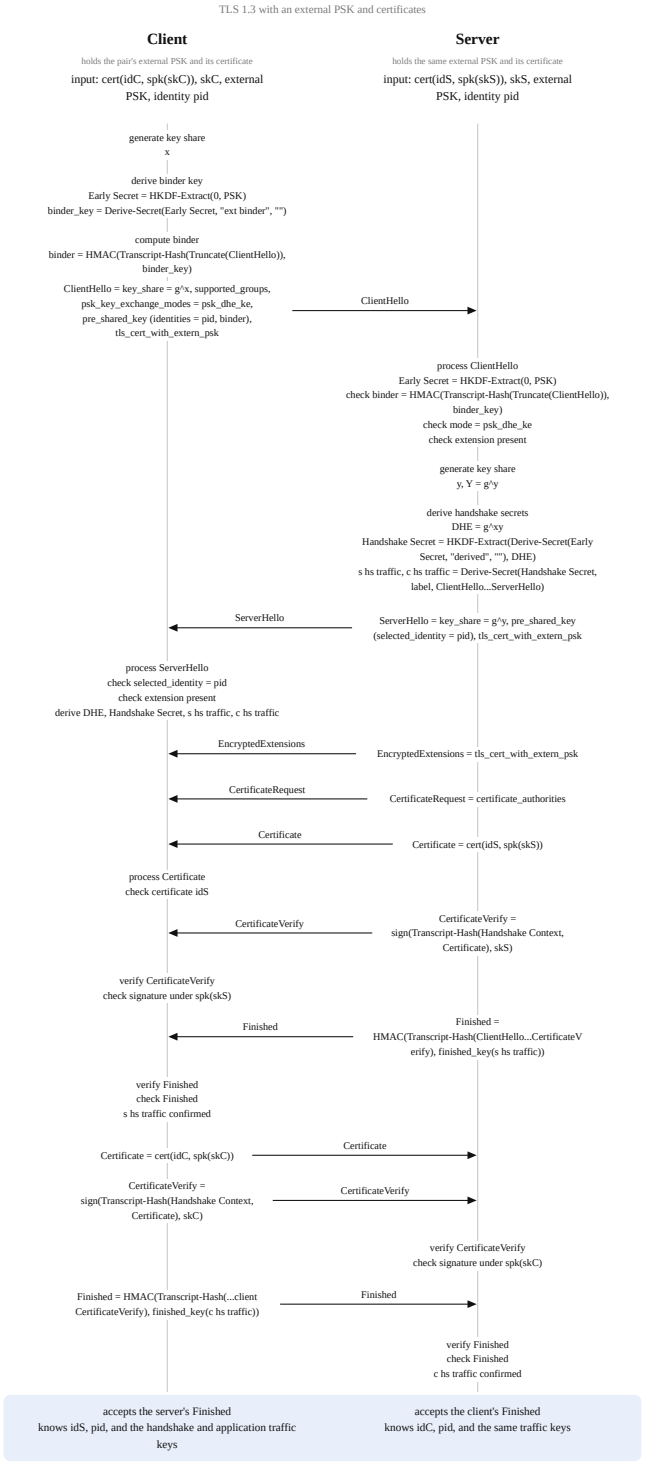


图 1. 文稿所规定的协议。

分析的范围见附录 D：分析了什么、省略了什么，以及依据文稿的哪些章节。

2 发现

没有发现。 分析没有发现文稿尚未写明或已排除的内容。第 3 节的表给出了每条性质的结果。

无发现：范围内文稿作为目标提出的每条性质都在模型上得到了证明，而不成立的两条性质恰好是规范自己写明的弱点。双向证书认证、transcript 一致、Finished 单次使用、身份绑定到证书密钥、psk_dhe_ke 的强制、PSK 与会话密钥的保密性、面对后续长期泄露的前向保密，以及当 (EC)DH 秘密可计算时会话密钥的存

活，全部成立。不成立的结果复现了文稿所述内容：既能计算 (EC)DH 秘密的 PSK 持有者可以解密录制的流量，明文的 PSK identity 则让观察者能够关联连接。有一条主张——被接受的 binder 是由客户端为同一个部分 ClientHello 生成的——被直接查询，但没有终止。结果基于一个符号模型，该模型将 HMAC、HKDF 和 AEAD 理想化，对 (EC)DH 只保留 g^xy = g^yx 这一条规律。共检查了 17 个目标。

3 检查过的性质

每行是一条提交给 ProVerif 的性质。结果是在分析者的协议模型上 ProVerif 给出的答案；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
A02	**通过证书进行服务器与客户端认证。** 每次客户端在握手完成时接受服务器身份 S，都存在一个以该客户端为意图对端的服务器运行；反向（服务器请求并验证客户端证书时）同理。	无	成立	高	是
A03	**握手参数协商一致。** 每次一方接受，都存在匹配的对端运行，角色、相互意图身份、所选 PSK identity、key_share 组与 cipher suite 一致。	无	成立	中	否
A04	**binder 或 Finished 不可重放。** 每次接受对应不同的对端运行；同一 ClientHello（含 binder）或同一 Finished 不能被接受两次。	无	成立	中	否
A06	**通过 binder 和 Finished 进行密钥确认。** 在确认接受点，预期对端对本次会话同一密钥有真实导出与匹配确认行为（binder 与 Finished 两个方向分别实例化）。	无	无答案	中	否
A07	**身份绑定到证书密钥。** 接受方认定的对端身份必须由该身份的证书私钥签名支撑，而非仅由 external PSK 知识支撑。	无	成立	中	是
A08	**扩展协商不可降级。** 接受方接受的扩展出现位置、伴随扩展集合、密钥交换模式、selected_identity 与 key_share 组均对应获批的对端提议与当前安全上下文。	无	成立	中	否
K01	**PSK 与流量密钥的保密性。** 攻击者不能导出 external PSK 或本次会话的握手/应用流量密钥；合法知悉者集合按实例固定。	无	成立	中	否
C01	**跨会话的前向保密。** 在会话完成并擦除临时 (EC)DH 私钥之后泄露长期秘密（证书私钥，以及按实例固定的 external PSK 使用范围），此前完成会话的流量密钥与载荷仍保密。	无	成立	高	否
C08	**(EC)DH 被攻破时 PSK 提供保护。** 在 (EC)DH 共享秘密被攻击者获得的假设下，只要 external PSK 未知且密钥派生未破，会话秘密仍不可导出。	(EC)DH 密钥协商 (会话期间（攻击者已获得共享秘密）)	成立	高	是
C03	**知晓 PSK 不构成窃听能力。** 在 external PSK 被攻击者（或组内其他成员）知道的假设下，由 (EC)DH 共享秘密保护的会话流量密钥与载荷仍保密。	external PSK 持有者（组内成员或攻击者） (会话建立前或期间)	成立	中	是
K04	**会话密钥分离。** external PSK 与 resumption PSK 的派生上下文分离；不同会话的流量密钥互不相同。	无	成立	低	否

ID	性质	假定的泄露	结果	价值	文稿是否已写
R05	**接受的配置策略。** 接受方接受的配置满足最低策略：psk_dhe_ke 模式、无 resumption PSK、无 early_data、证书认证存在。	无	成立	低	否
U01	**签名密钥与 PSK 泄露相互独立。** 分别检查签名私钥泄露与 PSK 泄露下的身份认证与会话密钥保密。	证书签名私钥或 external PSK（分别） (会话建立前或期间)	成立	中	否
U02	**binder 绑定身份与转录。** binder 与 PSK identity 绑定到本次 transcript 与证书身份。	无	成立	中	否
U03	**组合接受蕴含协商扩展。** 组合认证接受蕴含扩展已在双方协商。	无	成立	中	否
X01	**CRQC 获取的已记录流量密钥。** 如果攻击者获得 external PSK 并且还能计算 (EC)DH 共享秘密，它不得能派生已录制会话的会话流量密钥。	psk_leak 加上被攻破的 (EC)DH 密钥协商	攻击成立（文稿已写明）	低	是
X02	**外部 PSK 身份不可关联性。** 对两条连接的被动观察者不得能根据 ClientHello 中以明文携带的 external PSK identity 判断这两条连接来自同一个客户端。	无	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。

提出的问题，以及分析者的回答：

问题	回答	依据
Q1: 签名及 PSK 各自单独泄露时身份认证和密钥保密	任意一种泄露单独都不足够：仅签名密钥泄露不能让攻击者冒充服务器，因为客户端还需要 binder，而且它不提供会话密钥；仅 PSK 泄露既不能冒充也不提供会话密钥。只有 PSK 结合被攻破的 (EC)DH 协商才会暴露录制的流量，这正是文稿所述。	U01, A07, X01, C03
Q2: PSK identity/binder 与证书身份和 transcript 绑定	binder 通过 transcript 绑定到身份和部分 ClientHello，并且已证明双方对该 transcript 达成一致；仅针对 binder 本身的查询没有终止，所以这部分依赖于 transcript 一致性，而不是直接证明。	U02, A03, A06
Q3: 未协商本扩展不能错误按组合认证结果接受	是：在外部 PSK 下的证书认证接受只发生在 transcript 双方都携带扩展标记的会话中，因此一方不会被引导把未经协商的握手当作组合认证处理。	U03, A08

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给出了什么、未能给出什么，其中密码学被视为理想，与实现无关。

分析者指出，本分析不覆盖以下内容：

- 模型将 HMAC、HKDF 和 AEAD 理想化为理想的带密钥函数，因此这些原语的计算性攻破不在范围内。
- Diffie-Hellman 只用 g^xy = g^yx 这一条规律建模；攻击者在群中没有其他代数能力，因此找到的攻击是真实的，而证明只在该更弱攻击者下成立。
- 证书验证是每个身份固定一张证书：不建模到 CA 的证书链、吊销和密钥用途。
- transcript 是握手消息的理想化哈希，不是 RFC 9846 的逐字节编码。

- 按任务范围，不建模 resumption PSK、0-RTT、PSK 供应、组 PSK 和 HelloRetryRequest。
- 每对只建模一个 external PSK；不建模在多个会话中复用同一 PSK 的影响。
- 假定临时 (EC)DH 私钥在握手结束时销毁。
- 范围内没有一方在消息之间保留并改变的值，因此不需要有界展开，也不需要状态审查。

宿主记录的内容：

- 无答案：A06。
- A02、A03、A04、A06、A07、A08、K01、C01、C08、C03、K04、R05、U01、U02、U03、X01、X02 的答案依赖于模型简化的某个操作（附录 D）。
- 证明器没有给出结论的查询（附录 C）：A06: a06b。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”。
- 没带对照查询的证明（附录 C）：A02: a02, A08: r05, K01: k01psk, K04: k04, R05: r05。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。

每条性质还有什么未决之处，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、能否照现状使用，以及价值几何。

A02: 通过证书进行服务器与客户端认证

每次客户端在握手完成时接受服务器身份 S，都存在一个以该客户端为意图对端的服务器运行；反向（服务器请求并验证客户端证书时）同理。

客户端只有在服务器运行了同一份转录并用自己的证书中的密钥对其签名时，才接受完成的握手；服务器对客户端也是如此。当攻击者仅掌握网络、当它持有 external PSK、以及当它能计算 (EC)DH 共享秘密时，这一结论都成立。去掉签名检查会使两个方向都不成立，因此结果依赖于该检查。

- 结果：Holds；是否回答了所问：是；可用但有保留
- 价值 高：双向认证是该扩展的核心承诺，证明表明即使 PSK 已知或 (EC)DH 秘密可计算，它仍然成立。
- 文稿中已说明：是。文稿中的位置：s0034, s0035, s0052
- 依赖：证书验证被建模为每个身份一个固定证书；到 CA 的证书链和密钥用途在 TLS 之外，未被建模。；签名被理想化：只能用私钥生成。；客户端证书总是被发送，因为范围固定了两侧的证书认证。

A03: 握手参数协商一致

每次一方接受，都存在匹配的对端运行，角色、相互意图身份、所选 PSK identity、key_share 组与 cipher suite 一致。

双方的最终转录相同，因此它们在角色、所选 PSK identity、key share 和 cipher suite 上达成一致。这种一致由 binder、签名和 Finished 承载，它们都覆盖转录。

- 结果：Holds；是否回答了所问：是；可用但有保留
- 价值 中：对转录的一致使其他所有绑定有意义；该证明在理想化转录上成立。
- 文稿中已说明：否。所依据的原文：s0031, s0032, s0419
- 依赖：转录是握手消息的理想化哈希，而非 RFC 9846 的字节精确编码。；未建模 HelloRetryRequest 路径。

A04: binder 或 Finished 不可重放

每次接受对应不同的对端运行；同一 ClientHello（含 binder）或同一 Finished 不能被接受两次。

服务器和客户端都不能被诱使两次接受同一完成的握手。新鲜性来自转录覆盖的 key share，而不是来自计数器。

- 结果：Holds；是否回答了所问：是；可用但有保留
- 价值 中：一旦加入 PSK，重放完成的握手就是首先要测试的事情，而该扩展保持了这层保护。
- 文稿中已说明：否。所依据的原文：s0441, s0442
- 依赖：模型在消息之间不保留状态，因此接受仅受转录和 key share 的新鲜性约束。；转录是理想化哈希。

A06: 通过 binder 和 Finished 进行密钥确认

在确认接受点，预期对端对本次会话同一密钥有真实导出与匹配确认行为（binder 与 Finished 两个方向分别实例化）。

完成消息确认对端导出了相同的握手流量密钥，这通过证明被接受的 Finished 有匹配的发送方来体现，并且这一点在 PSK 泄露后仍然成立。binder 一侧是间接回答的：binder 是双方被证明达成一致的转录的一部分，因此被接受的 binder 属于该身份的一次客户端运行，但单独谈论 binder 的查询没有完成。

- 结果：无答案；是否回答了所问：部分；可用但有保留
- 价值 中：密钥确认是 PSK 有用的前提，但其两个主张之一没有直接答案。
- 文稿中已说明：否。所依据的原文：s0029, s0332, s0441
- 依赖：一个主张通过转录一致来回答，而不是通过直接查询。；HMAC 被理想化为带密钥的单向函数。
- 未决：关于被接受的 binder 是由客户端针对同一部分 ClientHello 计算的直接主张，曾针对 binder 值提出，但没有终止；答案转而依赖转录一致。

A07: 身份绑定到证书密钥

接受方认定的对端身份必须由该身份的证书私钥签名支撑，而非仅由 external PSK 知识支撑。

知道 external PSK 的一方仍然不能被接受为服务器：客户端保留证书和 CertificateVerify。文稿要求 PSK 不能是认证的唯一依据，模型确认了这一点。

- 结果：Holds；是否回答了所问：是；可用
- 价值 中：它机械地复现了规范的一项要求，并表明该扩展没有削弱对 PSK 持有者的认证。
- 文稿中已说明：是。文稿中的位置：main:465, s0052, s0058
- 依赖：证书验证是每个身份一个固定证书。；持有 PSK 的攻击者只被给予该对的 PSK，而不是证书私钥。

A08: 扩展协商不可降级

接受方接受的扩展出现位置、伴随扩展集合、密钥交换模式、selected_identity 与 key_share 组均对应获批的对端提议与当前安全上下文。

没有被接受的 ClientHello 使用纯 psk_ke 模式：服务器拒绝模式字段不是 psk_dhe_ke 的 ClientHello。组合握手本身可到达并被接受，因此该查询并非空洞。

- 结果：Holds；是否回答了所问：是；可用但有保留
- 价值 中：降级到 psk_ke 会移除 (EC)DH 的贡献，因此强制该模式正是该扩展的要点。
- 文稿中已说明：否。所依据的原文：s0022
- 依赖：模式字段是服务器比较的单个常量；客户端提供的模式列表未被建模。；未建模 HelloRetryRequest 路径。

K01: PSK 与流量密钥的保密性

攻击者不能导出 external PSK 或本次会话的握手/应用流量密钥；合法知悉者集合按实例固定。

网络上的攻击者既不知道 external PSK，也不知道会话的握手流量密钥，因为密钥同时依赖 PSK 和 (EC)DH 秘密，而它两者都没有。

- 结果：Holds；是否回答了所问：是；可用但有保留

- 价值 中：抵御网络的会话保密性是基本预期，该答案表明扩展保持了它。
- 文稿中已说明：否。所依据的原文：s0042, s0051, s0060
- 依赖：HMAC 和 HKDF 被理想化；HMAC 作为 PRF 被攻破的情形在模型之外。；DH 只携带规律 g^xy = g^yx，这给攻击者的信息少于真实群。

C01: 跨会话的前向保密

在会话完成并擦除临时 (EC)DH 私钥之后泄露长期秘密（证书私钥，以及按实例固定的 external PSK 使用范围），此前完成会话的流量密钥与载荷仍保密。

已完成会话的流量密钥在证书私钥和 external PSK 随后泄露时仍保密，因为长期值不给出临时 (EC)DH 秘密。

- 结果：Holds；是否回答了所问：是；可用但有保留
- 价值 高：这决定运营商能否安全地保留静态 PSK，并且针对文稿描述的单次使用情形得到了证明。
- 文稿中已说明：否。所依据的原文：s0053, s0054
- 依赖：假定握手结束后临时 (EC)DH 私钥即被销毁；泄露被放在之后的阶段。；每对一个 external PSK，不限制多少会话可以使用它。

C08: (EC)DH 被攻破时 PSK 提供保护

在 (EC)DH 共享秘密被攻击者获得的假设下，只要 external PSK 未知且密钥派生未破，会话秘密仍不可导出。

当攻击者能计算 (EC)DH 共享秘密但不知道 PSK 时，会话流量密钥仍无法获得，因为握手秘密需要两个输入。文稿这样说明，模型也确认了这一点。

- 结果：Holds；是否回答了所问：是；可用
- 价值 高：PSK 使流量免受未来量子攻击者威胁的主张是该扩展的主要动机，这里它是被检验而非被论证的。
- 文稿中已说明：是。文稿中的位置：main:474, s0053
- 依赖：被攻破的 (EC)DH 通过一个共享秘密公开的会话来建模；派生的其余部分被理想化。；攻击者没有被给予该会话的 PSK。

C03: 知晓 PSK 不构成窃听能力

在 external PSK 被攻击者（或组内其他成员）知道的假设下，由 (EC)DH 共享秘密保护的会话流量密钥与载荷仍保密。

知道 external PSK 但不知道 (EC)DH 共享秘密的一方无法读取会话流量，因为流量密钥也需要 (EC)DH 秘密。只有 (EC)DH 秘密也可计算的会话才会失守，而这正是文稿描述的情形。

- 结果：Holds；是否回答了所问：是；可用
- 价值 中：这是文稿为允许组 PSK 给出的论据，模型显示了它在何处不再成立。
- 文稿中已说明：是。文稿中的位置：main:524, s0059
- 依赖：PSK 持有者被建模为仅持有 PSK 的攻击者；失守情形额外加入一个 (EC)DH 秘密公开的会话。；组内成员没有被建模为自身的记录方。

K04: 会话密钥分离

external PSK 与 resumption PSK 的派生上下文分离；不同会话的流量密钥互不相同。

握手流量密钥只用于一份转录，因此两个会话不共享密钥。分离来自每份转录中新鲜的 key share。

- 结果：Holds；是否回答了所问：是；可用但有保留
- 价值 低：密钥分离是辅助性质，该答案没有说明 external 与 resumption 标签的区别，而模型没有这一标签。
- 文稿中已说明：否。所依据的原文：s0055, s0520
- 依赖：external 与 resumption PSK 没有通过标签分离，因为范围内不存在 resumption PSK。；转录是理想化哈希。

R05: 接受的配置策略

受理方接受的配置满足最低策略：psk_dhe_ke 模式、无 resumption PSK、无 early_data、证书认证存在。

一次被接受的握手使用了 psk_dhe_ke，并要求双方都进行证书认证。排除 resumption PSK 和 early_data 是元层面的：这些消息在模型中不存在，因此无法展示携带它们的任何运行。

- 结果：Holds；是否回答了所问：部分；可带保留使用
- 价值 低：答案确认了模式选择得到了强制执行，但策略的其余部分是由模型省略的内容来满足的。
- 文稿中已说明：否。所依据的原文：s0004, s0022, s0023
- 依据：Resumption PSK 和 early_data 被任务范围排除，因此相应的策略项未被测试。；客户端的模式列表是一个单一常量。
- 待解决：无 resumption PSK 和无 early_data 这两项按构造即为真，因为模型中没有这两条消息；这些主张是由模型回答的，而不是由协议回答的。

U01: 签名密钥与 PSK 泄露相互独立

分别检查签名私钥泄露与 PSK 泄露下的身份认证与会话密钥保密。

仅泄露签名私钥不能让攻击者冒充服务器，因为客户端还会检查 binder，而 binder 需要 PSK；单独泄露任一密钥都不能得到会话密钥。仅泄露 PSK 既不能冒充也不能得到会话密钥。

- 结果：Holds；是否回答了所问：是；可用
- 价值 中：它回答了哪个单一凭据对哪个目标重要，并表明两个因素确实是两个。
- 文稿中已说明：否。所依据的原文：s0042, s0052, s0058
- 依据：两种泄露在会话之前被分别建模。；每个身份一个证书私钥，不考虑吊销或过期。

U02: binder 绑定身份与转录

binder 与 PSK identity 绑定到本次 transcript 与证书身份。

binder 被双方被证明一致的 transcript 所覆盖，因此被接受的 binder 属于具有相同 PSK identity 和相同部分 ClientHello 的客户端运行，知道 PSK 并不能让攻击者绑定自己的握手。仅针对 binder 本身的直接查询没有得到答案。

- 结果：Holds；是否回答了所问：是；可带保留使用
- 价值 中：binder 是把 PSK 与握手绑在一起的东西；答案可靠，但对它的两个主张之一是间接的。
- 文稿中已说明：否。所依据的原文：s0031, s0032

- 依据：绑定是通过 transcript 一致性回答的，而不是通过对 binder 的直接查询。；HMAC 被理想化。
- 待解决：一个只谈论 binder 值、不涉及 transcript 其余部分的查询没有终止。

U03: 组合接受蕴含协商扩展

组合认证接受蕴含扩展已在双方协商。

在外置 PSK 下经证书认证的接受只发生在 transcript 在双方都携带扩展标记的会话内，因此不能诱使一方对未协商该扩展的握手接受组合结果。

- 结果：Holds；是否回答了所问：是；可带保留使用
- 价值 中：它排除了搭便车的情形，即一方认为已商定证书加 PSK 而另一方不这么认为。
- 文稿中已说明：否。所依据的原文：s0010, s0012
- 依据：扩展在 transcript 中是一个空标志，放置规则通过在两条消息中都要求它来建模。；对端在扩展放置错误时发送的拒绝未被建模。

X01: CRQC 获取的已记录流量密钥

如果攻击者获得外置 PSK 并且还能计算 (EC)DH 共享秘密，它必须不能推导出已记录会话的会话流量密钥。

持有外置 PSK 并且还能计算 (EC)DH 共享秘密的攻击者能推导出已记录会话的会话流量密钥；只有被攻破的协商而没有 PSK 则不能。这就是文稿针对拥有量子计算机的 PSK 持有者所述的弱点：一旦密钥协商失效，PSK 对其持有者不增加任何保护。

- 结果：攻击成立（文稿中已说明）；是否回答了所问：是；可用
- 价值 低：结果就是文稿已经说过的内容；在此复现是为了检查模型能看到它。
- 文稿中已说明：是。文稿中说明的位置：main:530, s0059, s0053
- 依据：被攻破的 (EC)DH 协商通过公布一个会话的共享秘密来建模。；该攻击针对已记录流量，需要同时具备 PSK 和被攻破的协商。

X02: 外部 PSK 身份不可关联性

对两个连接的被动观察者必须不能从 ClientHello 中以明文携带的外置 PSK identity 判断出这两个连接来自同一客户端。

外置 PSK identity 在 ClientHello 中以明文传输，因此观察同一客户端的两个连接的观察者能判断它们来自同一设备。ProVerif 无法证明该身份不可关联，并产生攻击者所做的测试。

- 结果：攻击成立（文稿中已说明）；是否回答了所问：是；可用
- 价值 中：文稿对此有警告，模型展示了确切的泄露点，这对他们推荐的缓解措施有用。
- 文稿中已说明：是。文稿中说明的位置：main:555, main:566, s0555, s0561
- 依据：ClientHello 总是携带该对的单一 PSK identity，因为范围固定了一个预配置的 PSK。；ProVerif 从不会把非干扰判为假；答案是它无法被证明，并附有攻击者测试的轨迹。

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，以及每个攻击及其分析者的判定。

目标	级别	界	查询	对照	攻击	主张
A02	proved		a02	3 of 4		4 proved
A03	proved		a02	checked		2 proved
A04	proved		a04	checked		2 proved
A06	proved		a02	checked		2 proved, 1 undecided
A07	proved		a07	checked		1 proved
A08	proved		r05			1 proved, 1 reachable
K01	proved		k01psk	1 of 2		2 proved
C01	proved		keysec_lt	checked		1 proved
C08	proved		c08	checked		1 proved
C03	proved		keysec_psk	checked		1 proved
K04	proved		k04			1 proved
R05	proved		r05			1 proved
U01	proved		u01auth	checked		3 proved
U02	proved		a02	checked		2 proved
U03	proved		a02r	checked		1 proved
X01	proved		c08	checked	x01 (holds_in_source)	1 proved, 1 attack
X02	none				track (holds_in_source)	1 attack

逐条主张，按分析者对每条主张的措辞；每条主张的答案是证明器给出的：

目标	主张	攻击者	回答	查询	对照
A02	服务器认证：只要客户端接受了服务器 Finished，就存在一个具有相同会话记录的服务器运行；仅此而已，不涉及网络之外的任何东西。	`network`	proved	a02	checked
A02	当攻击者能计算出 (EC)DH 共享秘密但不持有 PSK 时的服务器认证。	`dh_broken`	proved	a02	none
A02	客户端认证：只要服务器接受了客户端 Finished，就存在一个具有相同会话记录的客户端运行；仅此而已，不涉及网络之外的任何东西。	`network`	proved	a02r	checked
A02	当攻击者持有该对端的外部 PSK 时的服务器认证。	`psk_leak`	proved	a02	checked
A03	客户端视角下对会话记录（角色、PSK 身份、密钥份额、密码套件）的一致性。	`network`	proved	a02	checked
A03	服务器视角下对会话记录的一致性。	`network`	proved	a02r	checked

目标	主张	攻击者	回答	查询	对照
A04	客户端至多接受一次给定的服务器 Finished 会话记录（不会向客户端重放）。	network	proved	a04	checked
A04	服务器至多接受一次给定的客户端 Finished（及其携带 binder 的 ClientHello）会话记录。	network	proved	a04r	checked
A06	Finished 确认了握手流量密钥：接受方所对应的对端计算出了相同的流量秘密。	network	proved	a02	checked
A06	binder 为所选的外部 PSK 身份确认了共享的 binder 密钥：被接受的 binder 是由客户端针对同一身份和部分 ClientHello 计算得出的。	network	undecided	a06b	
A06	即使攻击者持有外部 PSK，Finished 仍确认握手流量密钥：被接受的 Finished 所对应的对端推导出了相同的流量秘密。	psk_leak	proved	a02	checked
A07	在已知外部 PSK 的情况下，客户端仍只接受具有相同会话记录的服务器运行：PSK 并非认证的唯一依据。	psk_leak	proved	a07	checked
A08	组合握手（扩展、psk_dhe_ke、binder、密钥份额）能够达成并被服务器接受。	network	reachable	a08	
A08	没有任何被接受的 ClientHello 携带纯 psk_ke 模式：服务器为初始握手选择 psk_dhe_ke。	network	proved	r05	none
K01	仅拥有网络的攻击者无法推导出外部 PSK。	network	proved	k01psk	none
K01	会话的握手流量密钥对仅拥有网络的攻击者保持机密。	network	proved	keysec_net	checked
C01	已完成会话的流量密钥对在会话之后获得证书私钥和外部 PSK 的攻击者保持机密。	longterm_after_session	proved	keysec_lt	checked
C08	只要攻击者不知道外部 PSK，即使它能计算出 (EC)DH 共享秘密，会话流量密钥仍保持机密。	dh_broken	proved	c08	checked
C03	对于知道外部 PSK 但不知道 (EC)DH 共享秘密的一方，会话流量密钥保持机密。	psk_leak	proved	keysec_psk	checked
K04	一个握手流量密钥只在一个会话记录中使用：不同会话的密钥互不相同。	network	proved	k04	none
R05	被接受的组合握手使用了 psk_dhe_ke；模型中不存在恢复 PSK 和 early_data，且要求证书认证。	network	proved	r05	none
U01	仅泄露服务器的签名私钥不会让攻击者冒充服务器：客户端还会检查 binder，而这需要 PSK。	sigkey_leak	proved	u01auth	checked
U01	仅泄露外部 PSK 既不会带来冒充，也不会带来会话流量密钥。	psk_leak	proved	a07	checked
U01	仅泄露签名私钥不会带来会话流量密钥。	sigkey_leak	proved	keysec_sk	checked
U02	被接受的 binder 属于由该身份的客户端所生成的会话记录（binder 被所商定的会话记录覆盖）。	network	proved	a02	checked
U02	即使攻击者持有外部 PSK，被接受的 binder 仍属于该身份的客户端会话记录，因此知道 PSK 并不能让它把自己的握手绑定到该身份上。	psk_leak	proved	a02	checked
U03	在外部 PSK 下的证书认证接受只发生在双方会话记录都携带该扩展标记的会话中。	network	proved	a02r	checked

目标	主张	攻击者	回答	查询	对照
X01	在持有外部 PSK 且能计算出 (EC)DH 共享秘密的情况下，攻击者能推导出已记录会话的会话流量密钥；这正是文稿所述持有 PSK 且拥有 CRQC 的攻击者所能做到的事。	`psk_leak`	attack (holds_in_source)	x01（c08 的对照查询）	
X01	仅拥有 (EC)DH 共享秘密而不拥有外部 PSK 时，已记录会话的流量密钥保持机密：仅凭该攻击者无法获得它们。	`dh_broken`	proved	c08	checked
X02	被动观察者能在 ClientHello 中以明文看到外部 PSK 身份，并能将同一客户端的两个连接关联起来。	`network`	attack (holds_in_source)	track	

“攻击者分不清用的是两个值里的哪一个”这类性质，证明器从不直接判为不成立。它没有证出来，并给出了一条攻击者能把两个值分开的轨迹，攻击按这条轨迹记录：track。

附录 D：分析是怎么跑的

由 LLM 分析者根据文稿构建协议模型，并把每个性质交给 ProVerif；第 3 节中的每个结果都是证明器给出的回答。

ProVerif+ Agent 会话 session-20261114T220941，2026-11-14。状态：已完成。模型：deepseek-v4-1-flash-261017。步数：46，证明器 797 秒，实际耗时 17 分钟，成本 0.156 USD。

上下文：宿主从对话中移除过时内容 1 次，共 442515 个字符（先前的推理，以及展示模型在最近一次更改之前状态的内容）。轨迹文件保留了全部内容。

ProVerif：运行了 135 次证明，107 次有定论，28 次无答案，784 秒，记录了 33 个回答。

分析了什么

协议	TLS 证书加外部 PSK
版本	rfc9973
分析范围	固定一组每对端独立预配置的高熵 external PSK、证书认证及 psk_dhe_ke；完整 binder、CertificateVerify 和 Finished；明确外部 PSK 不是 resumption PSK；排除 0-RTT、PSK provisioning、群组 PSK。
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	555 个编号原文单元（150113 字节），来自下列章节。本报告中诸如 s0001 的引用即为这些原文单元之一

分析所依据的文稿章节：

文稿	章节	标题
main	4	Extension Overview
main	5	Certificate with External PSK Extension
main	5.1	Companion Extensions
main	5.2	Authentication
main	5.3	Keying Material
main	7	Security Considerations
rfc9846	4	Handshake Protocol
rfc9846	4.1	The Transcript Hash
rfc9846	4.2	Key Exchange Messages
rfc9846	4.2.1	Cryptographic Negotiation
rfc9846	4.2.2	Client Hello
rfc9846	4.2.3	Server Hello
rfc9846	4.2.4	Hello Retry Request
rfc9846	4.3	Extensions
rfc9846	4.3.1	Supported Versions

文稿	章节	标题
rfc9846	4.3.2	Cookie
rfc9846	4.3.3	Signature Algorithms
rfc9846	4.3.4	Certificate Authorities
rfc9846	4.3.5	OID Filters
rfc9846	4.3.6	Post-Handshake Certificate-Based Client Authentication
rfc9846	4.3.7	Supported Groups
rfc9846	4.3.8	Key Share
rfc9846	4.3.8.1	Diffie-Hellman Parameters
rfc9846	4.3.8.2	ECDHE Parameters
rfc9846	4.3.9	Pre-Shared Key Exchange Modes
rfc9846	4.3.10	Early Data Indication
rfc9846	4.3.11	Pre-Shared Key Extension
rfc9846	4.3.11.1	Ticket Age
rfc9846	4.3.11.2	PSK Binder
rfc9846	4.3.11.3	Processing Order
rfc9846	4.4	Server Parameters
rfc9846	4.4.1	Encrypted Extensions
rfc9846	4.4.2	Certificate Request
rfc9846	4.5	Authentication Messages
rfc9846	4.5.1	Certificate
rfc9846	4.5.1.1	OCSP Status and SCT Extensions
rfc9846	4.5.1.2	Certificate Selection
rfc9846	4.5.1.3	Receiving a Certificate Message
rfc9846	4.5.2	Certificate Verify
rfc9846	4.5.3	Finished
rfc9846	4.6	End of Early Data
rfc9846	4.7	Post-Handshake Messages
rfc9846	4.7.1	New Session Ticket Message
rfc9846	4.7.2	Post-Handshake Authentication
rfc9846	4.7.3	Key and Initialization Vector Update
rfc9846	7	Cryptographic Computations
rfc9846	7.1	Key Schedule
rfc9846	7.2	Updating Traffic Secrets
rfc9846	7.3	Traffic Key Calculation
rfc9846	7.4	Asymmetric Shared Secret Calculation
rfc9846	7.4.1	Finite Field Diffie-Hellman

文稿	章节	标题
rfc9846	7.4.2	Elliptic Curve Diffie-Hellman
rfc9846	7.5	Exporters

源文包在文稿中定位到的协议目的：固定一组每对端独立预配置的高熵 external PSK、证书认证及 psk_dhe_ke；完整 binder、CertificateVerify 和 Finished；明确外部 PSK 不是 resumption PSK；排除 0-RTT、PSK provisioning、群组 PSK。

对照文稿定性质

在写出查询之前，分析者把起草的性质清单对照文稿本身关于协议目的的表述逐条核对。名称、性质所涉对象以及文稿的说法均为分析者的解读；所引位置在文稿中确实存在。

ID	简称	对象	文稿怎么说	出处
A02	通过证书进行服务器与客户端认证	客户端确信由其证书指名的服务器执行了握手；服务器在验证客户端证书时确信客户端的证书身份	认证依赖于用证书公钥验证的签名，且不受 PSK 影响（s0007、s0034、s0035、s0052）。	s0007、s0034、s0035、s0052
A03	握手参数协商一致	双方最终得到相同的转录：相同的角色、身份、选定的 PSK 身份、key_share 群组、密码套件	密钥调度、binder 和签名绑定转录（s0006、s0031、s0032、s0037、s0038）。	s0006、s0031、s0032、s0037、s0038
A04	binder 或 Finished 不可重放	服务器对每个携带 binder 的 ClientHello 和每个客户端 Finished 至多接受一次；客户端对每个服务器 Finished 至多接受一次	Binder 和 Finished 绑定 PSK 与当前握手（s0032、s0441、s0442）；转录携带新鲜的 key share（s0003、s0010）。	s0003、s0010、s0032、s0441、s0442
A06	通过 binder 和 Finished 进行密钥确认	接受方所面对的对端派生出了相同的 binder 密钥和本次会话相同的握手流量密钥	Binder 验证确认了该身份共享密钥（s0029、s0032）；Finished 认证握手和计算出的密钥（s0441、s0443）。	s0029、s0032、s0441、s0443
A07	身份绑定到证书密钥	接受方最终认定的身份由证书私钥下的签名支撑，而不是由 PSK 知识支撑	外部 PSK 不得作为认证的唯一依据；知道 PSK 不足以冒充（s0052、s0058）。	s0052、s0058
A08	扩展协商不可降级	只有当扩展及其伴随扩展和 psk_dhe_ke 同时出现在 ClientHello 和 ServerHello 中时才完成	要求伴随扩展；扩展未出现在 ClientHello 则不得出现在 ServerHello；服务器选择 psk_dhe_ke（s0003、s0005、s0010、s0022）。	s0003、s0005、s0010、s0022
K01	PSK 与流量密钥的保密性	外部 PSK 以及握手和应用流量密钥不被网络上的攻击者获取	保护外部 PSK（s0042）；保密目标继续成立（s0051、s0060）。	s0042、s0051、s0060

ID	简称	对象	文稿怎么说	出处
C01	跨会话的前向保密	已完成会话的流量密钥和载荷在攻击者事后获取长期秘密后仍然保密	临时密钥在会话结束前销毁；前向保密讨论（s0053、s0054、s0055）。	s0053、s0054、s0055
C08	(EC)DH 被攻破时 PSK 提供保护	当攻击者能计算 (EC)DH 共享秘密但不知道 PSK 时，会话秘密仍不可推导	只要攻击者缺少 PSK，即使计算出 (EC)DH 共享秘密也无法推导会话秘密（s0053）。	s0053
C03	知晓 PSK 不构成窃听能力	持有外部 PSK 但不掌握 (EC)DH 秘密的一方无法获取会话流量密钥和载荷	保密性依赖于 (EC)DH 共享秘密，因此知道 PSK 不足以窃听（s0059）。	s0059
K04	会话密钥分离	不同会话的流量密钥互不相同；外部 PSK 与 resumption PSK 相互隔离	PSK 绑定到单一哈希和 KDF（s0008、s0061）；binder 标签将外部 PSK 与 resumption 区分开（s0520）；一次性 PSK 保持会话分离（s0055）。	s0008、s0061、s0520、s0055
R05	接受的配置策略	被接受的组合握手使用了 psk_dhe_ke、无 resumption PSK、无 early_data、使用证书认证	要求 psk_dhe_ke（s0022）；resumption PSK 必须中止（s0023）；early_data 必须中止（s0004）；PSK 不得作为唯一依据（s0052）。	s0022、s0023、s0004、s0052
U01	签名密钥与 PSK 泄露相互独立	单独泄露签名私钥与单独泄露 PSK 分别对认证和会话密钥保密性意味着什么	PSK 不得作为认证的唯一依据（s0052）；PSK 泄露只对 CRQC 暴露内容（s0042）；知道 PSK 不足以冒充（s0058）。	s0042、s0052、s0058
U02	binder 绑定身份与转录	被接受的 binder 是客户端针对同一身份和同一部分 ClientHello 计算出的	binder 在截至 identities 字段的部分转录上确认该身份的共享密钥（s0029、s0031、s0032）。	s0029、s0031、s0032
U03	组合接受蕴含协商扩展	外部 PSK 下的证书认证接受只发生在双方协商了该扩展的会话中	只有当扩展出现在 ClientHello 且服务器持有被提供的 PSK 时，扩展才会出现在 ServerHello（s0010、s0012、s0018）。	s0010、s0012、s0018
X01	CRQC 获取的已记录流量密钥	客户端和服务器已记录的会话流量	文稿表述相反：持有外部 PSK 和 CRQC 的攻击者能像群组成员一样解密已存储的流量（s0059）。作为该弱点所破坏的性质补充。	s0059

ID	简称	对象	文稿怎么说	出处
X02	外部 PSK 身份不可关联性	ClientHello 中以明文携带的外部 PSK 身份	跨连接重复使用同一身份会让观察者跟踪客户端；明文 PSK 身份有助于跟踪（s0555、s0561）。作为该弱点所破坏的性质补充。	s0555

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

宿主把文稿中说明协议保护什么、防范什么的章节逐段列出，共 26 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 23 段，没选 3 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:392-392	A02, A03, K01, C01, C08, C03, `network`, `psk_leak`, `dh_broken`, `longterm_after_session`	
P02	main:394-399	A02, A08, R05, U03	
P03	main:401-405	K01, C01, C08, C03, `psk_leak`	
P04	main:407-410	X02	
P05	main:412-421	证明器问不了	s0044：PSK 生成所用 PRNG 的强度；熵不是迹性质
P06	main:423-437	证明器问不了	s0045：对称密钥长度与 Grover 算法；计算强度
P07	main:439-441	证明器问不了	s0046：外部 PSK 的最小长度；密钥长度不是迹性质
P08	main:443-452	A02, A03, A06, A07, K01, C08, C03	
P09 至 P11	main:454-458	K01, C08	
P12	main:460-463	K01, C08, C03	
P13	main:465-472	A07, A02, `psk_leak`	
P14	main:474-487	C08, `dh_broken`	
P15 至 P18	main:489-512	X01, C01, K04, `psk_leak`, `dh_broken`, `longterm_after_session`	
P19	main:514-522	A07, C03, `psk_leak`	
P20	main:524-532	C03, X01, `psk_leak`, `dh_broken`	
P21	main:534-538	K01, C08, C03	
P22	main:540-547	K04	
P23	main:551-553	X02	
P24	main:555-559	X02	
P25	main:561-568	X02	

段落	出处	定为	不选的原因
P26	rfc9846:4676-4677	A02, A03, K01, C01, C08, `network`, `psk_leak`, `sigkey_leak`, `longterm_after_session`, `dh_broken`	

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 39 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 24 项，没设的 15 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	客户端	参与方	`sigkey_leak`	
S02	服务器	参与方	`sigkey_leak`	
S03	PSK 组内其他成员	参与方	`psk_leak`	
S04	PSK 组内成员	参与方	`psk_leak`	
S05	证书身份	值	攻击者得不到更多	证书身份是公开的
S06	external PSK 身份	值	攻击者得不到更多	PSK 身份以明文传输（s0561）
S07	所选 external PSK identity	值	攻击者得不到更多	selected_identity 是明文索引
S08	key_share 组	值	攻击者得不到更多	key_share 组是公开的协商参数
S09	cipher suite	值	攻击者得不到更多	cipher suite 是公开的协商参数
S10	transcript	值	攻击者得不到更多	transcript 是公开的握手数据；其完整性才是目标
S11	binder	值	`psk_leak`	
S12	Finished	值	`psk_leak`	
S13	binder_key	值	`psk_leak`, `longterm_after_session`	
S14	finished_key	值	`psk_leak`	
S15	握手流量密钥	值	`dh_broken`, `longterm_after_session`	
S16	证书私钥	值	`sigkey_leak`, `longterm_after_session`	
S17	external PSK	值	`psk_leak`, `longterm_after_session`	
S18	tls_cert_with_extern_psk 扩展	值	攻击者得不到更多	该扩展是空的明文标志
S19	psk_key_exchange_modes	值	攻击者得不到更多	模式字段是明文
S20	selected_identity	值	攻击者得不到更多	selected_identity 是明文
S21	key_share	值	攻击者得不到更多	key share 是公开的；共享秘密对应 dh_broken
S22	Early Secret	值	`psk_leak`, `longterm_after_session`	
S23	Handshake Secret	值	`dh_broken`	
S24	Main Secret	值	`dh_broken`, `psk_leak`	

ID	参与方或值	类别	攻击者条件	不设的原因
S25	握手与应用流量密钥	值	`psk_leak`, `dh_broken`, `longterm_after_session`	
S26	已完成会话的流量密钥与载荷	值	`longterm_after_session`	
S27	临时 (EC)DH 私钥	值	`dh_broken`	
S28	会话秘密	值	`dh_broken`, `psk_leak`	
S29	(EC)DH 共享秘密	值	`dh_broken`	
S30	会话流量密钥与载荷	值	`psk_leak`	
S31	会话流量密钥	值	`dh_broken`, `psk_leak`, `longterm_after_session`	
S32	resumption PSK	值	不在范围内	任务排除了 resumption PSK，模型中也没有它
S33	密钥交换模式	值	攻击者得不到更多	模式字段是明文；R05 要求被接受的运行使用了 psk_dhe_ke
S34	PSK 类型	值	攻击者得不到更多	PSK 类型只是标签，不是攻击者持有的值
S35	early_data 标志	值	攻击者得不到更多	early_data 标志是明文，必须被拒绝（s0004）；R05 要求被接受的运行未携带它
S36	证书认证	值	`sigkey_leak`	
S37	证书签名私钥	值	`sigkey_leak`, `longterm_after_session`	
S38	会话密钥	值	`dh_broken`, `psk_leak`, `longterm_after_session`	
S39	PSK identity	值	攻击者得不到更多	PSK 身份是明文；其暴露破坏的正是不可关联性目标

每条性质在各攻击者条件下的答案

攻击者由分析者在编写查询之前设定；每个答案都在其中某一个攻击者下记录。单元格是证明器在该攻击者下对该性质给出的答案；“无答案”指该性质在该攻击者集合下，证明器留下的主张未决，或没有记录任何内容；空单元格指分析者没有为该性质设定该攻击者。

攻击者	持有什么	依据	出处
`network`	只有网络：它读取、丢弃、修改和发送消息，不持有任何一方的秘密		
`psk_leak`	该对端的 external PSK，在会话之前或期间；除此之外什么都没有	规范并未要求 PSK 只被客户端和服务器知晓，并讨论了组内知晓和失窃（s0058, s0059）。	s0058, s0059
`sigkey_leak`	服务器的证书签名私钥（以及单独的客户端证书签名私钥），在会话之前或期间；不包括 PSK	认证依赖用证书公钥验证的签名，因此该私钥保护的是认证（s0007, s0034, s0052）。	s0007, s0034, s0052
`longterm_after_session`	在会话完成后获得的证书私钥和 external PSK	前向保密讨论假定临时密钥已消失，并追问之后长期材料的泄露会带来什么（s0053, s0054, s0055）。	s0053, s0054, s0055
`dh_broken`	一次会话的 (EC)DH 共享秘密，可由公开的 key share 计算得出；不包括 external PSK	文稿假定 (EC)DH 密钥协商已被攻破，而 PSK 仍然未知（s0053, s0054）。	s0053, s0054

ID	network	psk_leak	sigkey_leak	longterm_after_session	dh_broken
A02	成立	成立			成立
A03	成立				
A04	成立				
A06	无答案	成立			
A07		成立			
A08	成立				
K01	成立				
C01				成立	
C08					成立
C03		成立			
K04	成立				
R05	成立				
U01		成立	成立		
U02	成立	成立			
U03	成立				
X01		不成立			成立
X02	不成立				

原文和目标

Source: 555 units, 150113 bytes, frozen in source-delivery-01.json. Targets: 15 approved (A02, A03, A04, A06, A07, A08, K01, C01, C08, C03, K04, R05, U01, U02, U03); the questions asked: 3. The list of targets was approved as drafted, beforehand, with --approve-targets.

Decisions the host took by its documented default (task `decisions: auto`), for you to check:

- approve_package: 批准源文包 protocol-2ae552d7044c652af21e3e484e2a

This step as it reports itself: 1 requests (1 failed), 0.000 USD, 68847 tokens in and 6161 out, 40 s.

关于证明器和模型的说明

- A02: answered in ProVerif, and the analyst names dh_algebra for this target
- A03: answered in ProVerif, and the analyst names dh_algebra for this target
- A04: answered in ProVerif, and the analyst names dh_algebra for this target
- A06: answered in ProVerif, and the analyst names dh_algebra for this target
- A07: answered in ProVerif, and the analyst names dh_algebra for this target
- A08: answered in ProVerif, and the analyst names dh_algebra for this target
- K01: answered in ProVerif, and the analyst names dh_algebra for this target
- C01: answered in ProVerif, and the analyst names dh_algebra for this target
- C08: answered in ProVerif, and the analyst names dh_algebra for this target
- C03: answered in ProVerif, and the analyst names dh_algebra for this target

- K04: answered in ProVerif, and the analyst names dh_algebra for this target
- R05: answered in ProVerif, and the analyst names dh_algebra for this target
- U01: answered in ProVerif, and the analyst names dh_algebra for this target
- U02: answered in ProVerif, and the analyst names dh_algebra for this target
- U03: answered in ProVerif, and the analyst names dh_algebra for this target
- X01: answered in ProVerif, and the analyst names dh_algebra for this target
- X02: answered in ProVerif, and the analyst names dh_algebra for this target

简化代数的 ProVerif 模型（xor、dh_algebra、other_algebra）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，在那里得到的攻击也是攻击。遗漏了对会变化的值所做检查的 ProVerif 模型（changing_state）会让参与方接受更多：在那里得到的证明成立，而在那里得到的攻击可能只是缺少了该检查。Tamarin+ Agent 则按原样对它们建模。

分析者为各目标命名的内容：

step	targets	features	reason
40	A02, A03, A04, A06, A07, A08, K01, C01, C08, C03, K04, R05, U01, U02, U03, X01, X02	dh_algebra, many_sessions, plain_primitives	密钥编排在理想化的 HMAC/HKDF 和 AEAD 之上，为每个带标签的派生使用一个构造子，而 (EC)DH 共享秘密只用 g^xy = g^yx 这一条定律建模，因此攻击者拥有的代数能力少于真实群。每条性质都针对任意数量的会话提出，而泄露建模了各个攻击者所泄露的长期值。

分析者的结束语

正常流程存在，在 model.pv 上回答了十七个目标。已证明：双向证书认证（在外部 PSK 已知或 (EC)DH 共享秘密可计算时同样成立）、双向的会话记录一致、双向 Finished 的单次使用、由 Finished 完成密钥确认、身份绑定到证书密钥、psk_dhe_ke 的强制执行、PSK 与会话密钥对网络的保密性、会话后证书密钥和 PSK 泄露时的前向保密、(EC)DH 秘密可计算时会话密钥的存活、会话密钥不被重用，以及签名密钥和 PSK 各自的独立泄露都不会导致冒充，也不会泄露会话密钥。必须失败的对照查询在存在变体处均被证伪（a02ctl、a02rctl、keysec_ctl、c01ctl、x01）。有两个性质不成立，二者都是文稿本身已陈述的弱点，因此予以记录，没有新的发现：能够同时计算 (EC)DH 共享秘密的 PSK 持有者可解密录制的流量（X01，s0059），明文 PSK 身份会关联连接（X02，s0555/s0561）。其余工作受阻的原因：关于被接受的 binder 由客户端针对同一部分 ClientHello 计算得到的直接主张未在 ProVerif 中终止（记为无答案；会话记录一致间接承载了它），且 (EC)DH 代数被简化为 g^xy = g^yx 外加一个理想化的共享秘密函数，因此对代数建模的 Tamarin+ Agent 可以解决最后这部分。所有结果都是符号性的：HMAC、HKDF 和 AEAD 都是理想的带密钥函数。