

基于PUF与信封加密的1-of-n多设备口令恢复方案

汪思贤, 孟 坤, 王启源

北京信息科技大学计算机学院, 北京

收稿日期: 2026年8月25日; 录用日期: 2026年10月8日; 发布日期: 2026年10月16日

摘 要

随着在线账户数量增加, 口令管理系统被广泛用于生成、保存和自动填充站点口令, 但传统方案通常依赖低熵主口令或持久化根秘密, 存在离线猜测和秘密泄露风险。物理不可克隆函数(physical unclonable function, PUF)可按需派生设备相关秘密, 减少口令管理系统对用户记忆和根秘密持久化存储的依赖; 然而, 单一PUF设备损坏或遗失仍可能导致主秘密及全部站点口令无法恢复。针对这一问题, 提出一种基于PUF与信封加密的1-of-n多设备冗余恢复方案, 使任一可用完整成员均可独立恢复同一群主秘密, 无须Host、网络或其他成员同时在线。围绕该结构, 设计了群组初始化、单设备恢复、面对面入组和群组重建流程。安全性分析与Tamarin双成员符号模型验证表明, 在既定假设下, 方案能够保护群主秘密并检测篡改、重放和冒充行为, 所建立的10条安全引理均验证通过。该方案在保留PUF硬件信任根优势的同时, 缓解了单一PUF设备造成的口令恢复单点故障。

关键词

物理不可克隆函数, 口令管理, 信封加密, 多设备恢复

A 1-of-n Multi-Device Password Recovery Scheme Based on Physical Unclonable Functions and Envelope Encryption

Sixian Wang, Kun Meng, Qiyuan Wang

College of Computer Science, Beijing Information Science and Technology University, Beijing

Received: August 25, 2026; accepted: October 8, 2026; published: October 16, 2026

Abstract

With the increasing number of online accounts, password management systems are widely used to generate, store, and autofill site passwords. However, conventional solutions commonly rely on low-entropy master passwords or persistently stored root secrets, exposing them to offline guessing and secret-leakage risks. A physical unclonable function (PUF) can derive device-specific secrets on demand and reduce such dependence; nevertheless, damage to or loss of a single PUF device may make the master secret and all derived passwords unrecoverable. To address this problem, this paper proposes a PUF- and envelope-encryption-based 1-of-n multi-device recovery scheme, allowing any intact member to recover the same group master secret independently without requiring the host, network connectivity, or other members to be online. Group initialization, single-device recovery, face-to-face onboarding, and group rebuilding procedures are designed. Security analysis and a two-member Tamarin model show that, under the stated assumptions, the scheme protects the group master secret and detects tampering, replay, and impersonation. All ten security lemmas are verified. The scheme, while retaining the advantages of PUFs as hardware roots of trust, therefore mitigates the recovery single point of failure caused by reliance on a single PUF device.

Keywords

Physical Unclonable Function, Password Management, Envelope Encryption, Multi-Device Recovery

Copyright © 2026 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

口令仍是信息系统中最常用的身份认证方式。随着在线账户数量增加,用户容易采用弱口令或在不同站点复用口令。口令管理器通过加密存储或现场生成站点口令缓解了这一问题,但传统口令保险箱通常依赖低熵主口令;密文库泄露后,攻击者可能获得离线猜测条件[1]。FIDO2/Passkey 通过设备绑定或同步型凭据支持跨设备使用,但其恢复能力取决于设备或同步服务的安全设计[2][3];确定性口令管理器减少了静态口令存储,却仍需解决主秘密的可靠恢复问题[4][5]。

对于以主秘密为根生成站点口令的管理器,关键问题是如何在避免低熵主口令和根秘密长期存储风险的同时,稳定获得口令派生所需的秘密材料。PUF 可利用芯片制造差异,并结合稳定化机制按需派生设备相关秘密,从而减少对用户记忆和根秘密持久化存储的依赖[6]。然而,这种设备绑定也使系统的可用性依赖于承载 PUF 的硬件:若唯一设备损坏或遗失,其派生或保护的主秘密可能无法恢复,进而导致全部站点口令不可用。现有 PUF 口令生成与群组密钥方案主要面向单设备或物联网协商场景[7]-[11],尚未直接解决由另一独立 PUF 设备恢复同一口令集合的问题。因此,本文需要解决的是如何在保留 PUF 硬件信任根优势的同时,消除单一 PUF 设备造成的恢复单点故障。

对于以唯一 PUF 设备为恢复根的确定性口令方案,一旦设备损坏或遗失,其保护的主秘密及全部站点口令可能永久不可恢复。因此,本文关注的问题是:如何使多个具有独立 PUF 信任根的设备均能恢复同一口令集合,同时避免恢复过程依赖持续在线的中心服务或其他设备。

针对上述问题,本文提出一种基于 PUF 与信封加密的 1-of-n 多设备冗余恢复方案。多个设备分别利

用自身 PUF 派生包装密钥，并独立封装同一群主秘密 K ；任一可用完整成员在通过本地授权后，均可单独解封 K 并派生相同的站点口令。该结构不属于门限秘密共享，恢复时无须多台设备协作。Host 仅在初始化和成员维护阶段负责消息转发、成员信息汇总及公开数据存储，日常恢复不依赖 Host、网络或其他成员。

本文的主要工作如下：

(1) 提出基于独立 PUF 信任根和信封加密的多设备冗余恢复结构，使任一完整成员均可执行 1-of- n 离线恢复。

(2) 设计群组初始化、单设备恢复、面对面入组和群组重建流程，明确 Host 与成员设备的职责及信任边界，并分析方案的计算、存储和通信开销。

(3) 针对双成员初始化、单设备恢复和面对面入组建立 Tamarin 符号模型；在所建模型及其假设下，共验证 10 条安全引理，结果均为 verified。

2. 相关工作

以算代存方案不持久化站点口令，而在使用时依据主秘密和站点标识现场计算。Cambou 等提出的可寻址 PUF 生成器(addressable PUF generator, APG)及其多重哈希扩展将 PUF 用于无数据库口令生成[6][8]，但这类工作主要面向单设备或客户端 - 服务器结构；当唯一 PUF 设备不可用时，如何在不改变既有站点口令的情况下由另一独立 PUF 设备恢复同一主秘密，并非其直接目标。

基于 PUF 的群组密钥协商多面向物联网，普遍依赖中心化协调者或特定物理假设。Liu 等[9]令多个孪生超晶格 PUF 持有者共享同一挑战与辅助数据、各自本地恢复同一密钥；Barbareschi 等的 Group-Key PHEMAP[10]以 sink 节点为中心、依靠同步序列维持群组密钥；Feng 等[11]基于 PUF 导出的基向量在内积空间上构造可扩展的群组认证协议。

(t, n) 门限密码学将秘密或私钥能力分散到多个份额，恢复或签名通常需要至少 t 个参与方协作，相关标准化工作仍在推进[12]。加密货币钱包领域大量采用秘密共享或多方计算；Erinle 等[13]综述了钱包设计、漏洞与安全措施。本文采用 1-of- n 独立恢复：每个完整成员都能恢复完整 K ，因而不提供门限方案的“少于 t 份不泄密”性质，两类方案的可用性与失陷边界不同。

FIDO2/Passkey 提供抗钓鱼的公钥认证。Bindel 等[2]分析了 FIDO2、CTAP 2.1 与 WebAuthn 2；Büttner 与 Gruschka [3]比较了设备绑定与同步型凭据。同步型凭据便于跨设备恢复，但其安全与可用性依赖同步体系；设备绑定型凭据则不等同于多设备共享同一口令集合。Oesch 与 Ruoti [4]评估了十三款口令管理器的生成、存储和自动填充安全；Nair 与 Song [5]提出零存储秘密的多因素口令管理方案。这些工作与本文的单 PUF 故障恢复问题相关，但研究对象和信任假设并不相同。

密钥包装以一把密钥保护另一把密钥。Rogaway 与 Shrimpton [14]给出可证安全处理，NIST SP 800-38F [15]标准化了 AES-KW/KWP。本文的信封采用带关联数据的认证加密，而非把多信封安全性归因于密文“没有结构”。模糊提取器用于从带噪声源稳定生成近似均匀密钥及公开辅助数据；其安全性应按具体定义描述为：在给定 helper data 和攻击者先验信息后，提取结果与理想随机值足够接近[16]。这不等同于 helper data 在信息论意义上完全不泄露，也不能由输出长度直接推断 PUF 熵。

3. 预备知识与系统模型

本文方案的核心关系是：各成员设备利用自身 PUF 恢复设备根秘密并派生包装密钥，以独立信封封装同一群主秘密 K ，再由 K 确定性派生各站点口令。本章首先说明信封的组成及其所依赖的密码学原语，随后给出系统参与方、数据边界与攻击者能力。

3.1. 密码学原语

信封加密的基本思想是使用一把密钥保护另一把密钥[14][15]。在本文中,被封装的是 256 位群主秘密 K , 设备 N_i 的包装密钥为 k_i 。多个成员以各自独立的 k_i 分别封装同一个 K , 形成多个设备信封。信封中不保存具体站点口令; 设备解封 K 后, 再根据 K 、站点标识和账户标识确定性派生口令。因此, K 是整个口令集合的共同恢复根, 而信封是设备获得该恢复根的入口。

$\text{PUF}_i(C)$ 表示设备 N_i 对挑战 C 的响应。由于 PUF 输出可能受噪声和环境变化影响, 设备结合公开辅助数据 helper_i 重构稳定根秘密 $w_{\text{raw},i}$ [7] [16], 再通过 HKDF 及不同标签实施域分离[17]:

$$w_{\text{raw},i} = \text{Stabilize}(\text{PUF}_i(C_{\text{single}}), \text{helper}_i) \quad (1)$$

$$w_i = \text{HKDF}(w_{\text{raw},i}, \emptyset, \text{exp}, 32), \quad k_i = \text{HKDF}(w_i, \emptyset, \text{BID}_i \parallel \text{wrap}, 32) \quad (2)$$

其中, “exp” 和 “wrap” 为不同的域分离标签, BID_i 为设备公开标识。 helper_i 可以公开保存, 但 $w_{\text{raw},i}$ 和 k_i 不作明文持久化; 其安全性取决于给定 helper_i 和攻击者先验信息后, 稳定化输出仍具有足够的条件最小熵。 K 的 256 位长度也不构成对其实际熵的无条件声明。

设备 N_i 选择唯一的 nonce_i , 并使用 AES-256-GCM 形式的认证加密封装 K [18]。关联数据 ad_i 绑定协议标识、 BID_i 和 “envelope” 标签:

$$C_i = \text{AEAD.Enc}(k_i, \text{nonce}_i, K, \text{ad}_i) \quad (3)$$

$$K = \text{AEAD.Dec}(k_i, \text{nonce}_i, C_i, \text{ad}_i) \quad (4)$$

本文将 (nonce_i, C_i) 称为设备 N_i 的密钥信封; 恢复记录还包括公开的 helper_i 和 BID_i 。只有 AEAD 标签验证成功时才输出 K 。由于不同设备以独立包装密钥封装同一 K , 任一可用完整成员均可通过自身信封恢复 K , 无须其他成员同时在线, 这构成本文的 1-of- n 恢复结构。群组初始化与新成员入组还使用 Ed25519 签名验证消息来源[19], 并通过 X25519/ECDH 建立认证机密通道[20]; 这些公钥原语不参与日常的单设备离线恢复。

3.2. 系统模型与数据边界

系统包含用户、Host、PUF 成员设备 N_i 以及可由攻击者控制的网络 and 外部存储。成员设备执行 PUF 稳定化、密钥派生、签名、信封封装与解封以及站点口令派生; 用户在初始化和面对面入组时确认参与设备及短认证串, 并在日常使用前完成本地授权。

Host 仅在初始化和成员维护阶段转发消息、汇总成员表并保存公开记录, 不执行 PUF 计算, 也不应获得设备根秘密、包装密钥或 K 。外部存储可保存 helper_i 、 BID_i 、公钥、成员表、 nonce_i 和 C_i , 这些数据的机密性不作为方案成立的前提; 但其删除、替换或回滚可能破坏可用性。

PUF 原始响应、稳定根秘密 $w_{\text{raw},i}$ 、包装密钥 k_i 、签名私钥以及解封后的 K 仅在成员设备受控内存中短暂出现, 操作结束后应予擦除。初始化完成后, 只要本地能够取得与设备对应的公开恢复记录、PUF 仍可用且本地授权成立, 完整成员即可在不连接 Host、网络或其他成员的情况下恢复 K 并派生站点口令。

3.3. 威胁模型

攻击者可完全控制开放网络, 能够窃听、阻断、篡改、替换、重放和并行调度协议消息, 并可读取、删除或替换公开存储中的辅助数据、成员表、 nonce 和信封密文。攻击者还可获得全部公钥与公开协议参数, 并尝试在初始化或入组过程中冒充成员。

本文区分三类设备状态: 攻击者仅获得公开记录而不具备相应 PUF 能力时, K 的机密性依赖模糊提

取器、HKDF 和 AEAD 的安全性；攻击者取得设备但无法通过本地授权或受保护接口调用 PUF 时，安全性进一步依赖本地授权机制；攻击者完全控制任一当前或历史完整成员的固件、内存或 PUF 接口时，则可解封该成员持有的有效信封并获得对应 K ，进而威胁全部派生口令。

本文进一步考虑 PUF 建模、侧信道、故障注入及用户错误操作。方案仅使用设备内部的固定挑战 C_{single} ，且不对外输出原始响应，因此经典的基于大量挑战 - 响应对的远程建模攻击受到限制；但若攻击者控制固件、调试接口或 PUF 调用接口，仍可能收集信息并预测或提取设备根秘密。侧信道或故障注入也可能泄露 $w_{\text{raw},i}$ 、 k_i 或 K ，成功时均按完整成员失陷处理。用户可能跳过或错误核对 SAS，相关安全影响在第 5.1 节分析。其余安全结论仍以 nonce 不复用、关联数据一致，以及 PUF 和模糊提取器参数满足噪声与条件熵要求为前提。本方案不提供拒绝服务、旧状态回滚检测、细粒度撤销、前向保密或后妥协安全。

4. 方案设计

4.1. 密钥结构与总体思路

本方案采用 1-of-n 恢复结构：群组仅维护一个 256 位主秘密 K ，每个成员设备利用自身 PUF 派生独立包装密钥，并分别封装同一 K 。任一完整成员均可凭自身信封独立恢复 K ，无须其他成员同时在线；因此，该结构不是门限秘密共享，新成员加入也不会增加现有 K 的熵。

设备 N_i 由稳定根秘密派生签名种子 w'_i ，并先生成身份公私钥及公开标识 BID_i ，再将 BID_i 绑定到包装密钥和初始化贡献的域分离标签中：

$$sk_i = \text{Ed25519.KeyGen}(w'_i), pk_i = \text{Ed25519.Pub}(sk_i), BID_i = H(pk_i) \quad (5)$$

$$k_i = \text{HKDF}(w_i, \emptyset, BID_i \parallel \text{wrap}, 32), c_i = \text{HKDF}(w_i, \emptyset, BID_i \parallel \text{contrib}, 32) \quad (6)$$

式(5)避免以尚未生成的 BID_i 反向定义签名私钥；式(6)通过不同标签隔离包装与贡献用途[17] [21]。 w_i 、 k_i 、 c_i 和 sk_i 仅在设备受控内存中短暂存在，操作结束后应擦除。

4.2. 群组初始化与单设备恢复

群组初始化为一次性面对面操作，Host 仅负责汇集和转发。各设备首先提交 BID_i 与 pk_i ，Host 按 BID 排序形成成员表 M_{init} 并回发，具体流程如图 1 所示；各设备计算下式，用户在全部设备上核对其摘要或短认证串，以发现成员插入、替换或分叉。

$$M_{\text{digest}} = \text{SHA256}(\text{context}_{\text{init}} \parallel M_{\text{init}}) \quad (7)$$

确认成员表后，各设备使用 Ed25519 认证临时 X25519 公钥，并将双方身份、角色、会话标识和 M_{digest} 绑定到签名 transcript，建立端到端认证机密通道。设备经该通道交换 c_i ，按 BID 顺序计算 K 并广播 commit_K 比较结果：

$$K = \text{HKDF}(c_1 \parallel \dots \parallel c_n, M_{\text{digest}}, \text{groupK}, 32), \text{commit}_K = \text{SHA256}(\text{commit} \parallel K \parallel M_{\text{digest}}) \quad (8)$$

比较一致后，各设备以自身 k_i 生成 K 的信封并擦除其他成员贡献与 K 。该过程是对称密钥贡献式初始化，而非基于离散对数的分布式密钥生成[22]；Host 既不能获得 K ，也不能单独完成成员认证。

4.3. 成员入组与群组重建

新设备仅在面对面入组中获得当前 K 。新旧设备交换长期身份、临时 X25519 公钥与双方 nonce，对包含协议标签、old/new 角色、身份、公钥、nonce 和会话标识的同一 transcript 计算短认证串(SAS)；用

户在两端确认一致后，双方签名该 **transcript**，并由 ECDH 共享秘密经 HKDF 派生会话密钥。旧设备随后以 AEAD 仅传输一次 K ，新设备在签名与标签均验证成功后生成自身信封并擦除会话秘密[23]，具体内容如图 2 所示。远程入组不在本文协议范围内。

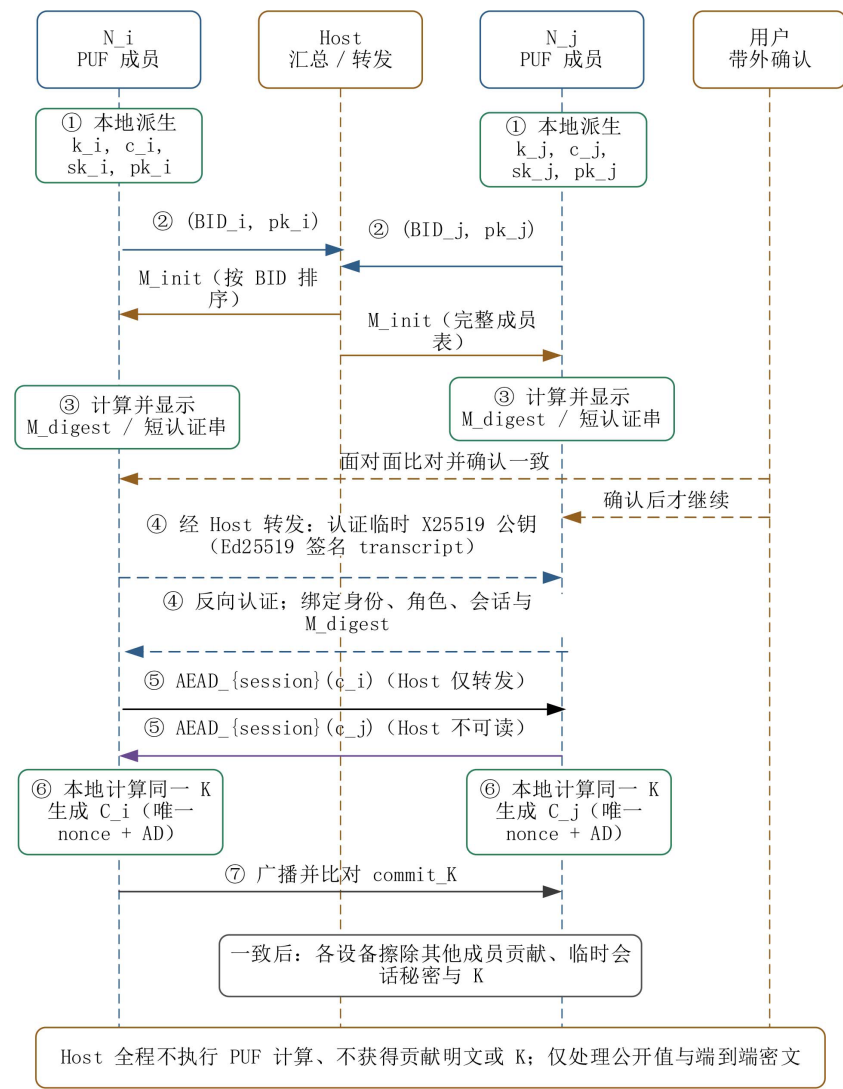


Figure 1. Dealer-free contributory group initialization
图 1. 无 dealer 贡献式群组初始化

成员表仅追加经认证的入组记录。若设备丢失、退出或怀疑泄露，剩余可信成员应重新执行初始化，生成 K' 及全部新信封；旧信封仍可恢复旧 K ，因此本方案不提供即时撤销、抗回滚、前向保密或后妥协安全。重建也不会自动使既有站点口令失效，用户仍需逐站点更新。

5. 安全性分析与形式化验证

本章结合非形式化分析与 Tamarin 符号验证评估协议安全性。相关结论均建立在第 3.3 节给出的威胁模型及密码学假设上，形式化验证用于检查协议消息流与安全目标，不等同于对 PUF 硬件、模糊提取器或具体实现的实证证明。

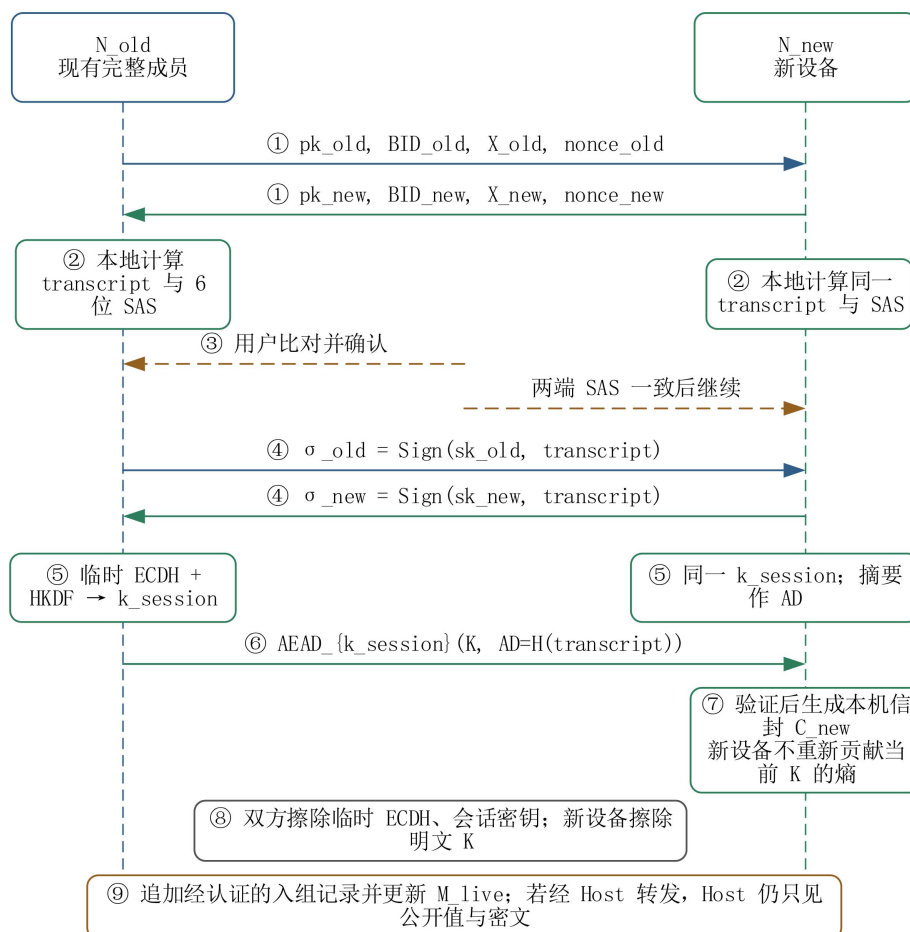


Figure 2. SAS-based face-to-face device onboarding

图 2. 基于 SAS 的面对面设备入组

5.1. 非形式化安全性分析

群主秘密 K 的机密性由 PUF 根秘密、HKDF 域分离和 AEAD 信封共同保证。攻击者仅获得 helper data、成员表、nonce 和全部信封时，不能在缺少有效包装密钥的情况下恢复 K ；若其通过 PUF 建模、侧信道或故障注入获得 $w_{\text{raw},i}$ 、 k_i 或解封后的 K ，则对应版本的 K 及其派生站点口令可能泄露。因此，1-of- n 结构提高恢复可用性的同时，也使任一完整成员成为共同 K 的潜在失陷点。实现中应避免对外暴露原始 PUF 响应，关闭或认证调试接口，限制 PUF 调用，将稳定化、密钥派生与解封置于受保护环境，并及时擦除中间状态；这些措施只能降低物理攻击风险，不构成协议层面对其完全抵抗的保证。

初始化时，用户面对面确认成员表摘要 M_{digest} ，各设备再通过绑定身份、角色和会话标识的认证机密通道交换贡献。Host 仅负责汇集与转发，无法读取贡献或独立计算 K ； commit_K 用于确认各设备所得 K 一致。单设备恢复时，设备经本地授权后重构包装密钥，仅在 AEAD 标签验证成功时输出 K ，且无需 Host、网络或其他成员在线。恶意成员或网络攻击者仍可通过阻断消息造成拒绝服务。

面对面入组将 SAS 确认、Ed25519 签名、临时 X25519/ECDH、HKDF 与 AEAD 组合使用，并把双方身份、角色、nonce 和会话标识写入同一 transcript。在用户正确核对 SAS 时，重放、替换或篡改消息将导致签名、SAS 或 AEAD 验证失败。若用户跳过核对或在 SAS 不一致时仍继续，带外认证将失效；由于签名公钥本身尚未绑定到预期设备，攻击者可能实施中间人攻击、冒充新成员取得 K 或造成成员视图

分叉。实现中应禁止跳过验证，优先要求将一端验证码输入另一端，并限制失败次数、实施退避且在失败后废弃当前 nonce 和会话；二维码或 NFC 可作为独立的面对面备用验证通道。六位 SAS 的安全性仅在用户实际核对且尝试次数受限时成立。

此外，不同站点口令由 K 结合规范化的站点、账户与策略参数经域分离派生，单个站点口令不应帮助计算其他输入域的口令。方案仍不提供恶意终端上的明文口令窃取防护、拒绝服务防护、旧状态回滚检测、细粒度撤销、前向保密或后妥协安全；群组重建生成 K' 后，既有站点口令仍需逐站点更新。

5.2. 形式化验证

本文采用 Tamarin [24]对 $n = 2$ 的群组初始化、单设备恢复和面对面入组进行符号建模。模型中的攻击者遵循 Dolev-Yao 网络模型[25]，可完全控制公开信道，并可通过 PUF_Compromise 事件获得被攻破设备的种子；该事件统一抽象成功的 PUF 建模、侧信道或故障攻击所造成的设备秘密泄露。HKDF、AEAD 和签名分别采用理想自由函数或内建密码学原语抽象。在 Tamarin 1.12.0 与 Maude 2.7.1 环境中对完整证明脚本进行本地回放，10 条引理均返回 verified。验证范围包括协议可执行性、PUF 种子与群主秘密机密性、SAS 唯一性、入组认证及会话唯一性，结果见表 1；其中入组认证相关结论以用户完成正确 SAS 核对为前提。

Table 1. Tamarin verification results

表 1. Tamarin 验证结果

引理	验证性质	结果
L1a、L1b	初始化后恢复与入组流程可执行	verified
kct_sources、seed_secret	密文来源与 PUF 种子保密	verified
L2、L3、L6	初始化、恢复和入组后的 K 机密性(允许显式 PUF 妥协例外)	verified
sas_unique、L4、L5	SAS 唯一性、入组认证及会话唯一性	verified

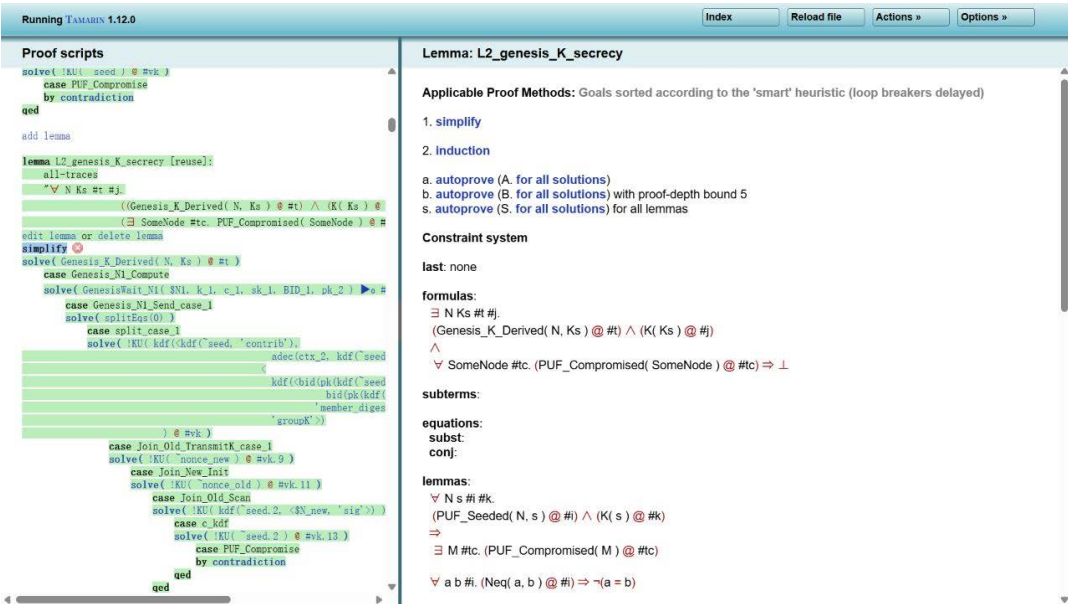


Figure 3. Proof interface of the L2_genesis_K_secretcy lemma

图 3. L2_genesis_K_secretcy 引理证明界面

图 3 给出了 L2_genesis_K_secretcy 引理的实际证明界面。综合 10 条引理的结果,可表述为:在所建立的符号模型及其理想化假设下,验证过程未发现违反上述目标性质的攻击轨迹。该结论不覆盖一般 n 的归纳证明、PUF 噪声与长期稳定性、真实密码实现、回滚、撤销或恶意固件;对于建模、侧信道或故障攻击,只验证其成功后由 PUF_Compromise 触发的条件性安全边界,不证明具体硬件具有物理抗攻击能力;用户跳过或错误接受 SAS 的情形亦不在现有模型保证范围内。

6. 结论

针对单一 PUF 设备损坏或遗失可能导致主秘密及全部站点口令无法恢复的问题,本文提出一种基于 PUF 与信封加密的 1-of- n 多设备冗余恢复方案。各成员设备利用自身 PUF 派生独立包装密钥,并分别封装同一群主秘密 K ,使任一可用完整成员均可在本地授权通过后独立恢复 K ,无须 Host、网络或其他成员同时在线。围绕该结构,本文设计了群组初始化、单设备恢复、面对面入组和群组重建流程,并明确了 Host 仅承担消息转发、成员信息汇总及公开数据管理。

安全性分析表明,在既定威胁模型和密码学假设下,方案能够保护公开数据泄露场景中的群主秘密,并对初始化、恢复及入组过程中的篡改、重放和冒充行为进行检测。Tamarin 验证结果显示,所建双成员符号模型中的 10 条安全引理均验证通过。后续工作将重点开展原型实现与 PUF 稳定性测试,并进一步研究细粒度撤销、状态回滚检测及设备妥协后的安全恢复机制。

参考文献

- [1] Gentles, J., Fields, M., Goodman, G. and Bhunia, S. (2025) Breaking the Vault: A Case Study of the 2022 LastPass Data Breach. <https://arxiv.org/abs/2502.04287>
- [2] Bindel, N., Cremers, C. and Zhao, M. (2023) FIDO2, CTAP 2.1, and Webauthn 2: Provable Security and Post-Quantum Instantiation. 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, 21-25 May 2023, 1471-1490. <https://doi.org/10.1109/sp46215.2023.10179454>
- [3] Büttner, A. and Gruschka, N. (2025) Device-Bound vs. Synced Credentials: A Comparative Evaluation of Passkey Authentication. *Proceedings of the 11th International Conference on Information Systems Security and Privacy*, 2, 651-659. <https://doi.org/10.5220/0013380600003899>
- [4] Oesch, S. and Ruoti, S. (2020) That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password Managers. 29th USENIX Security Symposium (USENIX Security '20), 12-14 August 2020, 2165-2182.
- [5] Nair, V. and Song, D. (2023) MFDPG: Multi-Factor Authenticated Password Management with Zero Stored Secrets. arXiv:2306.14746. <https://arxiv.org/abs/2306.14746>
- [6] Gao, Y., Al-Sarawi, S.F. and Abbott, D. (2020) Physical Unclonable Functions. *Nature Electronics*, 3, 81-91. <https://doi.org/10.1038/s41928-020-0372-5>
- [7] Cambou, B. (2018) Addressable PUF Generators for Database-Free Password Management System. 16th International Workshop on Cryptographic Architectures Embedded in Logic Devices (CryptArchi 2018), Guidel-Plages, 17-20 June 2018.
- [8] Assiri, S. and Cambou, B. (2021) Homomorphic Password Manager Using Multiple-Hash with PUF. In: Arai, K., Ed., *Advances in Intelligent Systems and Computing*, Springer International Publishing, 772-792. https://doi.org/10.1007/978-3-030-73100-7_55
- [9] Liu, J., Xie, J., Zhang, J., Liu, B., Chen, X. and Feng, H. (2023) A Secure Secret Key Agreement Scheme among Multiple Twinning Superlattice PUF Holders. *Sensors*, 23, Article 4704. <https://doi.org/10.3390/s23104704>
- [10] Barbareschi, M., Casola, V., Emmanuele, A. and Lombardi, D. (2024) A Lightweight PUF-Based Protocol for Dynamic and Secure Group Key Management in IOT. *IEEE Internet of Things Journal*, 11, 32969-32984. <https://doi.org/10.1109/jiot.2024.3418207>
- [11] Feng, P., Li, B., Han, B., Ma, Y., Hu, Y. and Zhao, R. (2026) A Scalable Group Authentication Protocol for IoT Based on PUF-Derived Bases in Inner Product Spaces. *Cybersecurity*, 9, Article No. 41. <https://doi.org/10.1186/s42400-025-00468-0>
- [12] Brandão, L.T.A.N. and Peralta, R. (2026) NIST First Call for Multi-Party Threshold Schemes: NIST IR 8214C. NIST.

-
- [13] Erinle, Y., Kethepalli, Y., Feng, Y., *et al.* (2023) SoK: Design, Vulnerabilities, and Security Measures of Cryptocurrency Wallets. arXiv:2307.12874. <https://arxiv.org/abs/2307.12874>
 - [14] Rogaway, P. and Shrimpton, T. (2006) A Provable-Security Treatment of the Key-Wrap Problem. In: Vaudenay, S., Ed., *Lecture Notes in Computer Science*, Springer, 373-390. https://doi.org/10.1007/11761679_23
 - [15] NIST (2012) Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping: NIST SP 800-38F. NIST.
 - [16] Canetti, R., Fuller, B., Paneth, O., Reyzin, L. and Smith, A. (2021) Reusable Fuzzy Extractors for Low-Entropy Distributions. *Journal of Cryptology*, **34**, Article No. 2. <https://doi.org/10.1007/s00145-020-09367-8>
 - [17] Krawczyk, H. and Eronen, P. (2010) HMAC-Based Extract-and-Expand Key Derivation Function (HKDF): RFC 5869. Internet Engineering Task Force.
 - [18] Dworkin, M. (2007) Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC: NIST SP 800-38D. NIST.
 - [19] Josefsson, S. and Liusvaara, I. (2017) Edwards-Curve Digital Signature Algorithm (EdDSA): RFC 8032. Internet Research Task Force.
 - [20] Langley, A., Hamburg, M. and Turner, S. (2016) Elliptic Curves for Security: RFC 7748. Internet Research Task Force.
 - [21] Krawczyk, H. (2010) Cryptographic Extraction and Key Derivation: The HKDF Scheme. In: Rabin, T., Ed., *Lecture Notes in Computer Science*, Springer, 631-648. https://doi.org/10.1007/978-3-642-14623-7_34
 - [22] Gennaro, R., Jarecki, S., Krawczyk, H. and Rabin, T. (2007) Secure Distributed Key Generation for Discrete-Log Based Cryptosystems. *Journal of Cryptology*, **20**, 51-83. <https://doi.org/10.1007/s00145-006-0347-3>
 - [23] Vaudenay, S. (2005) Secure Communications over Insecure Channels Based on Short Authenticated Strings. In: Shoup, V., Ed., *Lecture Notes in Computer Science*, Springer, 309-326. https://doi.org/10.1007/11535218_19
 - [24] Meier, S., Schmidt, B., Cremers, C. and Basin, D. (2013) The TAMARIN Prover for the Symbolic Analysis of Security Protocols. In: Sharygina, N. and Veith, H. Eds., *Lecture Notes in Computer Science*, Springer, 696-701. https://doi.org/10.1007/978-3-642-39799-8_48
 - [25] Dolev, D. and Yao, A. (1983) On the Security of Public Key Protocols. *IEEE Transactions on Information Theory*, **29**, 198-208. <https://doi.org/10.1109/tit.1983.1056650>