中国科学: 信息科学 2022 年 第 52 卷 第 12 期: 2336–2350
SCIENTIA SINICA Informationis
论文

一种基于 PUF 的可证明安全消息认证算法及应用

张效林, 谷大武*

上海交通大学电子信息与电气工程学院, 上海 200240

* 通信作者. E-mail: dwgu@sjtu.edu.cn

收稿日期: 2021–08–04; 修回日期: 2021–10–13; 接受日期: 2021–12–01; 网络出版日期: 2022–12–05

国家自然科学基金 (批准号: 62072307) 资助项目

摘要 消息认证码 (message authentication code, MAC) 是一种对称密码算法, 能检查消息的完整性与来源合法性, 可广泛用于各类信息系统. 然而, 当运行 MAC 算法的设备受到物理攻击时, 攻击者可通过读取存储器或电路调试等手段获取算法密钥并生成合法的消息认证码, 从而危害系统安全. 为此, 本文提出了 PUF-MAC, 一种基于物理不可克隆函数 (physically unclonable function, PUF) 和 Hash 函数的 MAC 算法. PUF 是一种具有结构不可克隆性与输出不可预测性的数据映射实体, 不同 PUF 实体映射间的差异来源于生产时物理环境的微小变化. 通信双方可使用 PUF 生成共享密钥. 在标准模型下, 本文归约证明了 PUF-MAC 算法在适应性选择消息攻击下满足存在性不可伪造 (existential unforgeability under chosen message attack, EUF-CMA), 且算法的 EUF-CMA 安全性依赖于 Hash 的弱抗碰撞性以及 PUF 的 EUF-CMA 安全性. 同时, 本文基于 PUF-MAC 算法设计了一种满足前后向安全性的密钥协商方案和双向身份认证协议, 体现了 PUF-MAC 良好的实用性. 理论分析表明, 与其他 MAC 算法相比, PUF-MAC 结构轻量且实现简单, 无需预先存储大量的 PUF 响应. PUF 的引入使攻击者即使获取算法密钥, 也无法生成合法的消息认证码, 保证了通信系统的安全.

关键词 消息认证码, 密钥管理, 物理不可克隆函数, 身份认证

1 引言

1.1 研究背景

近年来, “新基建” 背景下工业互联网与传统物联网迎来了快速发展与产业升级, 随之而来的新兴技术, 如智能家居、无人机等, 得到了应用与关注. 为保障通信时数据的完整性与可靠性, 消息认证码 (message authentication code, MAC) 算法被广泛用于不同产品与系统中, 如 Google Cloud [1)]等.

1) Google. HMAC keys in cloud storage. [2021-07-06]. https://cloud.google.com/storage/docs/authentication/hmackeys.

引用格式: 张效林, 谷大武. 一种基于 PUF 的可证明安全消息认证算法及应用. 中国科学: 信息科学, 2022, 52: 2336–2350, doi: 10.1360/SSI-2021-0261
Zhang X L, Gu D W. A PUF-based provably secure message authentication algorithm and application (in Chinese). Sci Sin Inform, 2022, 52: 2336–2350, doi: 10.1360/SSI-2021-0261

现有 MAC 算法主要包括 HMAC [1] 与 CBC-MAC [2], 其中 HMAC 于 RFC2104 [3] 中被标准化, 并以 FIPS 198-1 [4] 的形式在 IPSec 与 SSL 等协议中使用. 在物联网等系统中, 终端设备面临着被入侵与拆解的风险, 为抵御物理攻击, MAC 算法的密钥等敏感数据在应用时需被安全存储, 例如存放在只可一次编程的非易失内存 (one time progammable NVM, OTP NVM) 中. 但此类方案仅能实现局部数据安全, 攻击者可拆解与调试其余电路, 并在本地单独运行目标设备, 从而也能伪造合法的签密数据, 如消息认证码等. 另外, 在 OTP NVM 等方案中, 长期密钥的使用可能遭受能量侧信道分析 [5,6] 等攻击. 因此 MAC 算法在应用时, 双方还应实现动态的密钥协商与更新.

针对以上问题, 本文提出了一种基于物理不可克隆函数 (physically unclonable function, PUF) 的 MAC 算法, 即 PUF-MAC. PUF 由 Pappu 提出的物理单向函数 [7] 演变而来, 是一种具有数据映射功能的物理实体, 能将激励 C 不可预测地映射到响应 R. 每个 PUF 实例 puf 均不相同且无法复制, 其映射方式与所处环境的电气、光线、温度等条件有关. 因此集成在不同设备中的 puf 可利用制造过程中的随机工艺偏差获得唯一的映射 $f: C \to R$. 一旦制作流程结束, puf 将与该设备及其内部硬件融为一体. 设备用户能以激励响应对 (challenge response pair, CRP) 的形式使用 PUF, 一个或一组 CRP 对应着唯一的 puf, 以此可实现对网络中消息的认证与溯源.

PUF 实现轻量, 可快速稳定地生成大量 CRP [8~10], 能减少资源受限设备的计算开销. 因此, 在物联网、移动互联网等情景中, 可基于 PUF 这类新型原语设计安全算法与协议, 以解决应用时的密钥管理问题并减少资源占用.

1.2 相关研究现状

MAC 是一种对称密码算法, 一般基于 Hash 函数或分组密码算法. Bellare 等 [1] 为 Hash 函数引入密钥后设计了 NMAC 与 HMAC 算法, 其中 HMAC 由两层 Hash 组成, 实现时可直接替换为 SHA256, SM3 等算法; 基于 Hash 的方案还有 UMAC, VMAC 等. FIPS 则标准化了基于分组密码的 CBC-MAC, 如 DAA [2], 即为基于 DES 的 CBC-MAC, 该算法会将最后一个分组的加密结果作为输出. CMAC [11] 在结构上与 CBC-MAC 相似, 但无需初始向量 (initialization vector, IV). 此外, 还有基于异或运算的 XOR-MAC [12]、基于有限域上运算的 GMAC [13] 以及使用格雷码 (Gray code) 且能并行计算的 PMAC [14] 等. Boneh 等 [15] 则定义了 MAC 算法的后量子安全模型并给出了一种后量子 MAC 算法.

PUF 可看作一种单向函数, 在密码学语义下可抽象出不同的安全性质与模型. Armknecht 等 [16] 根据 PUF 的单向性等特点, 定义了 PUF 模型下的不可区分性、伪随机性、不可伪造性等安全性质. Brzuska 等 [17] 与 Badrinarayanan 等 [18] 还讨论了 PUF 在密码协议 UC (universally composable) 安全证明框架中的表现与性质.

抽象出的各种安全性质可用于基于 PUF 的密码算法与协议的设计中. 对于身份认证, Delvaux 等 [19] 总结了 PUF 认证协议的安全问题, 并对 21 个协议展开分析. Chatterjee 等 [20] 与 Chuang 等 [21] 针对网络节点需存储大量 CRP 的问题, 设计了一种适用于多终端系统的身份认证协议; Nimmy 等 [22] 则在文献 [20] 的基础上提出了一种抗建模攻击的轻量认证协议. Mahalat 等 [23] 基于 PUF 设计了一种 WiFi 认证协议以抵御传统网络面临的 MAC 地址欺骗、去认证 (de-authentication) 等攻击. Gope 等 [24] 和 Chatterjee 等 [25] 分别基于 PUF 提出了一种高效的匿名认证协议. 在各种新型网络系统中, PUF 仍可作为安全认证协议的重要组件. Alladi 等 [26] 与 Nyangaresi 等 [27] 针对无人机与地面站、无人机间的认证问题, 设计了基于 PUF 的认证协议. Jiang 等 [28] 与 Renault 等 [29] 则提出了车联网中的 PUF 认证协议. Falcone 等 [30] 则使用 PUF 来解决供应链系统中的产品溯源问题.

对于密钥协商, Qureshi 等 [31] 提出了 PUF-RAKE, 一种具有 CRP 混淆机制的密钥交换协议, 能

在多个节点之间快速协商出密钥. Mall 等 [32] 提出了 EuDaimon, 一种基于 PUF 的会话密钥协商方案, 使用户经一次认证后即可访问云服务器或其他远程节点. Mahmood 等 [33] 基于 PUF 设计了一种多认证服务器情景下的端到端密钥协商方案, 并给出了随机预言机模型下的安全性证明.

对于消息认证, Bolotnyy 等 [34] 仅使用 PUF 设计了一种用于 RFID 系统的 MAC 算法, 但该算法的存储与通信开销过大, 且缺乏安全性证明. Resende 等 [35] 针对本地数据的安全存储等情景, 结合 Hash 函数与 PUF 设计了一种 MAC 算法并给出了标准模型下的安全证明, 但其中消息认证码的生成与验证需由同一方完成, 即仅能本地使用, 应用局限性较大. 而在 Zheng 等 [36] 及 Jung 等 [37] 设计的协议中, PUF 响应直接被用作 HMAC 的密钥. 因此验证方需预先安全地存储大量 PUF 激励, 这会对轻量级平台带来较大存储负担. 上述方案中 PUF 的引入虽能解决密钥的安全存储问题, 但在方案应用的可扩展性和实用性上具有局限性. 因此, 本文将基于 PUF 与 Hash 函数构造一种无需预先存储大量 PUF 响应、适用于双方的实用 MAC 算法, 并给出标准模型下的安全性证明.

1.3 本文的主要工作与结果

• 本文提出了 PUF-MAC, 一种基于 PUF 的 MAC 算法. 该算法由 Hash 函数与 PUF 组成, 结构简单, 可用于移动设备、物联网终端等资源受限平台中, 且无需预先存储大量的 PUF 响应. 在密钥被窃取的条件下, 该 MAC 算法依然安全.

• 本文将算法的选择消息攻击的存在不可伪造安全性 (existential unforgeability under chosen message attack, EUF-CMA) 归约到 PUF 的 EUF-CMA 安全性以及 Hash 函数的弱抗碰撞性上, 从而在标准模型下证明了 PUF-MAC 的安全性, 理论验证了算法的可用性.

• 本文使用 PUF-MAC 算法设计了一种密钥协商方案与双向身份认证协议. 其中, 该密钥协商方案可实现 PUF-MAC 算法本身在不安全信道中的密钥更新与协商, 并满足前后向安全性; 身份认证协议则能防止攻击者冒用合法用户的身份进行通信.

第 2 节介绍 MAC 与 PUF 的相关定义; 第 3 节介绍 PUF-MAC 算法的组成与构造, 并给出安全性证明; 第 4 节给出 PUF-MAC 的应用; 第 5 对 PUF-MAC 进行对比分析; 第 6 节对全文进行总结.

2 预备知识

2.1 MAC

定义1 MAC 可表示为一个由 3 个多项式时间算法组成的元组 (KeyGen, Mac, Vrfy), 定义如下.

• KeyGen: 根据选定的安全参数 n 均匀地输出长度为 n 的密钥 $k \leftarrow \mathrm{KeyGen}(1^n)$;

• Mac: 接收输入 $k \in \{0,1\}^n, M \in \{0,1\}^m$, 输出 $\mathrm{tag} \in \{0,1\}^*$, 其中 tag 为 M 对应的消息认证码, 即 $\mathrm{tag} \leftarrow \mathrm{Mac}_k(M)$;

• Vrfy: 接收输入 $k \in \{0,1\}^n, \mathrm{tag} \in \{0,1\}^*, M \in \{0,1\}^m$, 输出为一比特 $b \in \{0,1\}$; 对于 $\forall k, M$, 都有 $\mathrm{Vrfy}_k(\mathrm{Mac}_k(M), M)) = 1$.

2.2 PUF 的相关定义

PUF 一般可分为数字电路 PUF、模拟电路 PUF 与非电子 PUF; 其中数字电路 PUF 易于集成至 IC 器件内, 是目前应用最广泛的 PUF.

2.2.1 理想 PUF 与非理想 PUF

定义2 理想 PUF (ideal PUF) [19] 是一函数实体集合 $\mathcal{P}$, 在给定集成电路版图和制造流程的条件下, 对于 $\forall \text{puf} \in \mathcal{P}, C \in \{0,1\}^n$, 有 $R = \text{puf}(C) \in \{0,1\}^n$ 且位于均匀分布 $\mathbb{U}_n$ 上. 若令 $\mathcal{R} = (R_1, \ldots, R_q)$ 为 C 对应的 q 次响应, 则有 $\forall a, b \in [1,q], R_a = R_b$. puf 的产生取决于若干有界环境参数, 如电压、温度等.

定义3 非理想 PUF (non-ideal PUF) [19] 是一函数实体集合 $\mathcal{P}^*$, 在给定集成电路版图和制造流程的条件下, 对于 $\forall \text{puf} \in \mathcal{P}^*, C \in \{0,1\}^n$, 有 $R = \text{puf}(C)$. 其中 $R \in \{0,1\}^n$ 位于分布 $\mathbb{D}_n$, 最小熵 $H_\infty(\mathbb{D}_n) \geqslant \alpha_{\mathbb{D}}$ ($\alpha_{\mathbb{D}}$ 一般令 $\alpha_{\mathbb{D}} = 0$). 若令 $\mathcal{R} = (R_1, \ldots, R_q)$ 为 C 对应的 q 次响应, 则有 $\forall a, b \in [1,q]$, 汉明距离 $\text{HD}(R_a, R_b) \leqslant \delta$ (δ 为一较小值). puf 的产生取决于若干有界环境参数, 如电压、温度等.

任何针对 PUF 的主动攻击 (如侵入式的物理攻击) 都会改变 PUF 所在设备的硬件结构与 PUF 运行时的电气环境, 从而会改变 puf 的映射方式, 使其不可用或成为一个新的 PUF 实例 puf′ [38].

2.2.2 模糊提取器与 PUF

定义4 模糊提取器 (fuzzy extractor, FE) 可表示为 (Gen, Rep), 其中 $\text{Gen}: \{0,1\}^n \to \{0,1\}^k \times \{0,1\}^n$, $\text{Rep}: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$. 对于 $(w,z) \leftarrow \text{Gen}(y)$, 其中 $(w,z) \in \{0,1\}^k \times \{0,1\}^n, y \in \{0,1\}^n$, 若存在 $y' \in \{0,1\}^n$ 且 $\text{HD}(y,y') \leqslant \delta$, 则有 $\text{Rep}(w,y') = z$.

由定义 4 可知, 当 FE 与非理想 PUF 组合时, puf 将具有确定性映射的特点, 即若 $R_a = \text{puf}(C)$, $(w,r) = \text{Gen}(R_a)$, 对于 $\forall R_b \in \mathcal{R}, \text{HD}(R_a, R_b) \leqslant \delta$, 都有 $\text{Rep}(w, R_b) = r$.

2.3 安全性定义

2.3.1 MAC 安全性定义

伪随机函数 (pseudorandom function, PRF) 可用于构造 MAC 算法, PRF 安全性也是 MAC 的重要安全目标. 首先给出 PRF 的一般定义.

定义5 PRF: 对于函数集合 $\mathcal{F}$, 有 $\forall f \in \mathcal{F}, f: \{0,1\}^n \to \{0,1\}^n$, 且输出分布为 $\mathbb{P}_n$. 对于任意的概率多项式时间 (probabilistic polynomial time, PPT) 的区分器 $\mathcal{A}$, 若 $\mathcal{A}$ 适应性地向 $\mathcal{F}$ 提交多次输入 x_i 并获得输出 y_i 后, $\mathcal{A}$ 根据输出 y_i 区分情况 I, II 的优势, 则称 $\mathcal{F}$ 在 $\mathbb{P}_n$ 上是 PRF 的.

I. $y_i = f(x_i), f \xleftarrow{\$} \mathcal{F}$;

II. $y_i \xleftarrow{\$} \{0,1\}^n$.

若 MAC 算法满足定义 5 中的 PRF 安全性, 则满足 EUF-CMA, 定义如下.

定义6 EUF-CMA: 对于一 MAC 算法 $\mathcal{O} = (\text{KeyGen}, \text{Mac}, \text{Vrfy})$, PPT 敌手 $\mathcal{A}$ 在时间 t 内可选择消息 $M_i \in \{0,1\}^m$ 并向 $\mathcal{O}$ 查询 $\text{tag}_i = \text{Mac}_k(M_i)$. 在 q 次查询后, 若 $\mathcal{A}$ 输出 (M^*, tag^*) 且 $M^* \notin \{M_1, \ldots, M_q\}, \text{Vrfy}_k(\text{tag}^*, M^*) = 1$ 的优势 $\text{Adv}_{\mathcal{A}}^{\text{EUF-CMA}} = \Pr\left[\mathcal{A}^{\text{EUF-CMA}}\text{成功}\right] = \epsilon_M$ 是可忽略的, 则称 $\mathcal{O}$ 满足 EUF-CMA 安全性. 此时 $\mathcal{O}$ 可称为 $(\epsilon_M, t, q, n) -$ secure MAC.

2.3.2 PUF 的安全性定义

EUF-CMA 也可用于刻画 PUF 的安全性, 定义如下.

定义7 PUF 的 EUF-CMA 安全性: 对 $\forall \text{puf}$, PPT 敌手 $\mathcal{A}$ 在时间 t 内可选择 $C_i \in \{0,1\}^n$ 并向 puf 查询响应 $R_i = \text{puf}(C_i)$. 在 q 次查询后, 若 $\mathcal{A}$ 输出 (C^*, R^*) 且 $C^* \notin \{C_1, \ldots, C_q\}, \text{HD}(\text{puf}(C^*), R^*) \leqslant \delta$ 的优势 $\text{Adv}_{\mathcal{A}}^{\text{EUF-CMA}} = \epsilon_P$ 是可忽略的, 则称 puf 满足 EUF-CMA 安全性.

定义 7 对理想 PUF 与非理想 PUF 均适用. 对于理想 PUF, 可令 $\delta = 0$. 此时满足 EUF-CMA 安全性的 PUF 可称为 (ϵ_P, t, q, n) – secure PUF.

2.3.3 Hash 函数安全性定义

定义8 弱抗碰撞 (weakly collision resistant) Hash 函数 [1]: 对于带密钥的 Hash 函数 $H(\circ, K)$, PPT 敌手 $\mathcal{A}$ 在未知密钥 K 时, 在时间 t 内可查询 q 次 Hash 值 $h_i = H(M_i, K) \in \{0,1\}^n$. 若 $\mathcal{A}$ 最终输出 (M^*, M_j) 且 $H(M^*, K) = H(M_j, K), M^* \notin \{M_1, \ldots, M_q\}, j \in [1, q]$ 的优势 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{wCR}} = \epsilon_H$ 是可忽略的, 则 $H(\circ, K)$ 具有弱抗碰撞性. 此时称 $H(\circ, K)$ 为 (ϵ_H, t, q, n) – secure Hash.

3 PUF-MAC

3.1 系统模型

算法模型. PUF-MAC 由 3 个多项式时间算法 (KeyGen, Mac, Vrfy) 组成. 其中 KeyGen 需要双方在离线或安全信道中进行; Mac 与 Vrfy 如定义 1, 用于生成和验证消息认证码.

安全假设. PUF-MAC 应实现通信数据的完整性与可靠性, 使接收方能验证消息是否完整以及是否由可信方发送. 因此 PUF-MAC 应满足定义 6 的 EUF-CMA 安全性. 对于试图攻破算法安全性的敌手, 其目标是在时间 t 内至多通过 q 次 MAC 查询来伪造一对能通过验证的 (M^*, tag^*).

同时, 本文假设通信环境中的攻击者具有拆解设备的能力, 但攻击者不能在模拟环境中单独对部分电路重新供电与调试, 因为这将改变设备中 PUF 的硬件环境以及运行状态, 使其不可用或成为一个新的 PUF 实例 [38, 39]. 因此, 对于已拆解的设备, 攻击者无法从 NVM 等存储器或 PUF 中获取与算法有关的原始状态信息; 对于未拆解的设备, 攻击者可作为中间人嗅探网络数据流量.

下面首先基于定义 2 的理想 PUF 给出 PUF-MAC 的构造.

3.2 基于理想 PUF 的 MAC 算法

运行 PUF-MAC 算法的双方 A, B 各自分别拥有 $\mathrm{puf}_A : \{0,1\}^n \to \{0,1\}^n, \mathrm{puf}_B : \{0,1\}^n \to \{0,1\}^n$ 以及 Hash 函数 $H : \{0,1\}^* \to \{0,1\}^n$ 和一预先任选的、相同的初始激励 $C_0 \in \{0,1\}^n$.

I. KeyGen. A, B 首先在本地分别生成 $R_A = \mathrm{puf}_A(C_0)$, $R_B = \mathrm{puf}_B(C_0)$. 之后 A, B 将自己的响应发送给对方, 实现 PUF 响应的交换. 最终, 双方各自可计算 $T = R_A \oplus R_B$. KeyGen 算法结束后, 双方在本地存储密钥 $K = (C_0, T)$.

II. Mac. 若 A 需生成 M 的消息认证码, 则进行如下步骤.

(a) A 根据 C_0 与 puf_A 重新生成 R_A, 从而有 $R_B = T \oplus R_A$;

(b) A 计算 $C_A = H(M||R_A)$, 并生成响应 $R'_A = \mathrm{puf}_A(C_A)$;

(c) A 得到消息认证码 $\mathrm{tag} = (t, \sigma)$; 其中 $t = H(C_A||R'_A), \sigma = H(R_A||R_B) \oplus R'_A$;

(d) A 将 (M, tag) 发送给 B, Mac 算法结束, 示意图如图 1 所示.

III. Vrfy. B 收到 (M, tag) 后, 进行如下步骤完成对 M 的验证.

(a) B 根据 C_0 与 puf_B 重新生成 R_B, 从而有 $R_A = T \oplus R_B$;

(b) B 计算 $C_A = H(M||R_A)$, 并利用 σ 得到 $R'_A = \sigma \oplus H(R_A||R_B)$;

(c) B 将 C_A, R'_A 代入 $t' = H(C_A||R'_A)$, 验证 t' 是否等于 t; 若相等则说明 M 未经篡改且由合法系统实体发送.

综上, A, B 双方使用 PUF-MAC 算法进行通信的示意图如图 2 所示.

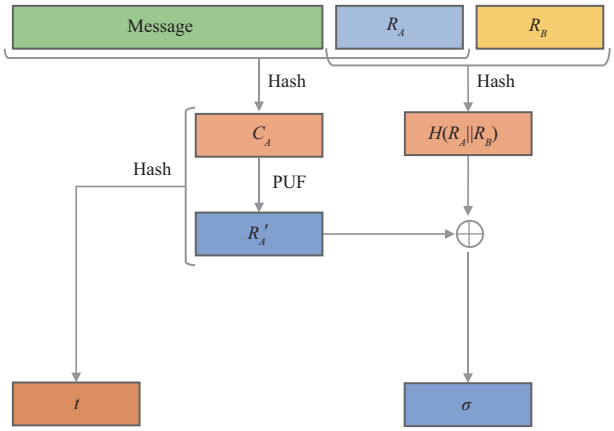

图 1 (网络版彩图) Mac 算法流程

Figure 1 (Color online) Workflow of Mac in PUF-MAC

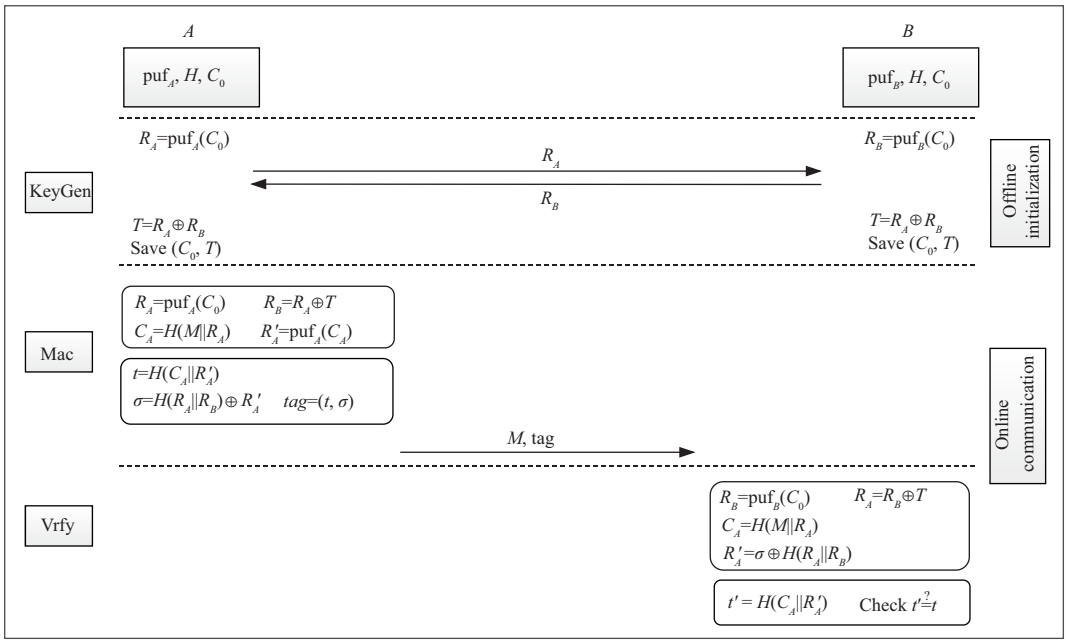

图 2 PUF-MAC 算法流程

Figure 2 Procedure of PUF-MAC

3.3 安全性分析

根据 3.1 小节中的假设, PUF-MAC 算法应满足 EUF-CMA 安全性; 根据定义 7, 本文将基于伪造 PUF 的 CRP 是困难的这一假设, 给出 PUF-MAC 的 EUF-CMA 安全性证明, 即有如下定理.

定理1 若 PUF 是 $(\epsilon_P, t, q, n)-$secure PUF, 以及 H 是 $(\epsilon_H, t, q, n)-$secure Hash, 那么 PUF-MAC 是 $(\epsilon_M, t, q, n)-$secure MAC.

为证明定理 1, 即证明若存在 PPT 敌手 $\mathcal{A}$ 能攻破 PUF-MAC 的 EUF-CMA 安全性, 则存在多项式时间算法可构造 PPT 敌手 $\mathcal{B}$, 使 $\mathcal{B}$ 能攻破 PUF 的 EUF-CMA 安全性或 Hash 的弱抗碰撞性.

证明 敌手 $\mathcal{B}$ 会将敌手 $\mathcal{A}$ 作为子程序, 并为其模拟 PUF-MAC 算法; 敌手 $\mathcal{B}$ 将与一拥有 PUF 使用权限的挑战者 $\mathcal{C}$ 进行交互. 此外, 存在一验证者 $\mathcal{V}$ 接收输入 (M, tag), 与 $\mathcal{C}$ 交互以输出 (M, tag) 的验证结果. 由 $\mathcal{A}$ 构造 $\mathcal{B}$ 的过程如下.

阶段 I. 在该阶段, $\mathcal{A}$ 将向 $\mathcal{B}$ 提交若干次 MAC 预言机查询, $\mathcal{B}$ 会向 $\mathcal{C}$ 提交若干次 PUF 预言机查询.

(a) $\mathcal{B}$ 首先选取 $r_0, r_1 \xleftarrow{\$} \mathbb{U}_n$, 并发送给 $\mathcal{V}$.

(b) $\mathcal{A}$ 生成消息 M_i 并提交给 $\mathcal{B}$;

(c) $\mathcal{B}$ 根据 M_i 计算 $C_i = H(M_i||r_0)$, $\mathcal{B}$ 将 C_i 提交给 $\mathcal{C}$;

(d) $\mathcal{C}$ 调用 puf 生成响应 $R_i = \text{puf}(C_i)$, 并返回给 $\mathcal{B}$;

(e) $\mathcal{B}$ 计算 $t_i = H(C_i||R_i)$ 以及 $\sigma_i = H(r_0||r_1) \oplus R_i$, 返回 $\text{tag}_i = (t_i, \sigma_i)$ 给 $\mathcal{A}$;

阶段 II. 经 q 次 MAC 查询后, $\mathcal{A}$ 将输出对 PUF-MAC 的攻击结果, 并由 $\mathcal{V}$ 进行验证.

(a) $\mathcal{A}$ 输出 $\text{output}_A = (M^*, \text{tag}^*)$ 并发送给 $\mathcal{V}$ 与 $\mathcal{B}$, 其中 $M^* \notin \{M_1, \ldots, M_q\}$;

(b) $\mathcal{V}$ 收到 (M^*, tag^*) 后, 计算 $C^* = H(M^*||r_0)$;

(c) $\mathcal{V}$ 运行 PUF-MAC 的 Mac 算法: $\mathcal{V}$ 发送 C^* 给拥有 puf 的挑战者 $\mathcal{C}$ 以获取合法响应 $R^{*'} = \text{puf}(C^*)$. 之后, $\mathcal{V}$ 计算 $t^{*'} = H(C^*||R^{*'}), \sigma^{*'} = H(r_0||r_1) \oplus R^{*'}$, 从而得到 $\text{tag}^{*'} = (t^{*'}, \sigma^{*'})$;

(d) $\mathcal{V}$ 运行 PUF-MAC 的 Vrfy 算法: $\mathcal{V}$ 计算 $R^* = \sigma^* \oplus H(r_0||r_1), t^* = H(C^*||R^*)$. 最后, $\mathcal{V}$ 比较 t^* 是否等于 $t^{*'}$, 若相等则输出 1, 其他情况则输出 0;

阶段 III. 在该阶段 $\mathcal{B}$ 会根据 $\mathcal{A}$ 的输出, 输出针对 PUF 的攻击结果. 同时还将分析 $\mathcal{A}$ 攻破算法 EUF-CMA 安全性的优势. 令 $\mathcal{A}$ 攻破 PUF-MAC 的优势为 ϵ_M, $\mathcal{B}$ 攻破 PUF 的优势为 ϵ_P, ϵ_H 为任意 PPT 敌手找到 H 上碰撞的概率.

(a) $\mathcal{B}$ 得到 output_A, 计算 $C^* = H(M^*||r_0), R^* = \sigma^* \oplus H(r_0||r_1)$, 输出 $\text{output}_B = (C^*, R^*)$;

(b) 考虑敌手 $\mathcal{B}$ 会失败的情况:

(i) 敌手 $\mathcal{A}$ 失败, 即 $\mathcal{V}$ 输出 0;

(ii) 敌手 $\mathcal{A}$ 输出无效, 输出的 M^* 在 H 上发生了碰撞, 即 $\exists j \in [1, q]$ 使得 $C_j = C^*$;

(iii) 敌手 $\mathcal{A}$ 成功, 即 $\mathcal{V}$ 输出 1, 但 $\text{output}_B = (C^*, R^*)$ 不是关于 puf 的合法 CRP;

(c) 敌手 $\mathcal{B}$ 失败的概率至多为上述 3 种情况概率之和, 如下所示:

$$1 - \epsilon_P \leqslant \Pr[\mathcal{A} \text{ 失败}] + \Pr[M^* \text{ 发生碰撞}] + \Pr[\mathcal{A} \text{ 成功} \cap R^* \neq R^{*'}], \tag{1}$$

其中, $\Pr[\mathcal{A} \text{ 失败}] = 1 - \epsilon_M$, $\Pr[M^* \text{ 发生碰撞}] = \epsilon_H$. 而当且仅当 $\mathcal{V}$ 输出 1, 即 $t^* = t^{*'}$ 时 $\mathcal{A}$ 才能成功; 因此 $\Pr[\mathcal{A} \text{ 成功} \cap R^* \neq R^{*'}] = \Pr[t^* = t^{*'} \cap R^* \neq R^{*'}] = \Pr[t^* = t^{*'}] \cdot \Pr[R^* \neq R^{*'} \mid t^* = t^{*'}] = \epsilon_M \cdot \epsilon_H$. 代入式 (1) 可得

$$1 - \epsilon_P \leqslant 1 - \epsilon_M + \epsilon_H + \epsilon_M \cdot \epsilon_H.$$

因此敌手 $\mathcal{A}$ 攻破 PUF-MAC 算法 EUF-CMA 安全性的优势如下所示:

$$\epsilon_M \leqslant \frac{\epsilon_H + \epsilon_P}{1 - \epsilon_H}. \tag{2}$$

上述构造过程证明了当攻破 PUF EUF-CMA 的优势与 H 发生弱碰撞的概率是可忽略时, 攻破 PUF-MAC 算法 EUF-CMA 的概率也是可忽略的, 从而定理 1 得证.

注释1 $\mathcal{A}$ 与 $\mathcal{B}$ 实现 MAC 预言机的交互时, $\mathcal{A}$ 未知 r_0, r_1, 且 $\mathcal{B}$ 为 $\mathcal{A}$ 返回的 tag_i 中 σ_i 符合响应分布 $\mathbb{U}_n$; 因此 $\mathcal{B}$ 为 $\mathcal{A}$ 模拟的预言机与真实 PUF-MAC 算法相同, 满足 $\mathcal{A}$ 攻破算法所需的环境.

注释2 当 Hash 函数 H 为 $(\epsilon_H, t, q, n)-$secure Hash 时, $\mathcal{B}$ 计算 $C_i = H(M_i||r_0)$ 发生碰撞的概率是可忽略的. 而在攻破 PUF EUF-CMA 安全性的游戏中, 敌手不能输出已查询过的激励. 因此, 在这种条件下 $\mathcal{B}$ 与挑战者 $\mathcal{C}$ 间的交互过程与攻破 PUF EUF-CMA 安全性的过程相同. output_B 即为针对 PUF 的选择消息攻击输出结果.

注释3 验证者 $\mathcal{V}$ 为确认 $\mathcal{A}$ 输出的 tag^* 是否合法, 需首先查询 puf 以获得 M^* 真正对应的 $\text{tag}^{*'} = (t^{*'}, \sigma^{*'})$, 并由 Vrfy 算法计算 t^* 后再与 $t^{*'}$ 比较, 完成验证. 与 3.2 小节中的 Vrfy 算法相比, 一方面, 若 $\mathcal{V}$ 获得 $t^{*'}$ 后直接将其与 t^* 比较, 则会与 Vrfy 的流程不同, 从而使 $\mathcal{V}$ 模拟的验证过程无效. 另一方面, 为确保验证结果的正确性, $\mathcal{V}$ 应以 $t^{*'}$ 而非 $\mathcal{A}$ 输出的 t^* 作为验证时比较的根据. 这等价于将 $\mathcal{A}$ 输出 tag^* 中的 t^* 替换为 $t^{*'}$ 后再对其执行 Vrfy 算法.

注释4 上述证明中敌手的运行时间取决于 Hash 函数与 PUF 的计算效率, 而二者均有多项式时间实现的实例. 因此敌手 $\mathcal{A}, \mathcal{B}$ 能在时间 t 内完成预言机查询, 从而该构造过程也是多项式时间的.

注释5 根据安全假设, 实际中攻击者能采取物理入侵等手段读取设备存储器, 从而能获取算法的共享密钥 (C_0, T). 但攻击者无法克隆设备中的 puf, 并且也不能对设备重新供电模拟运行, 因为这会改变 puf 的工作环境, 进而改变 puf 的性质, 导致其在同一激励下无法输出原有的响应. 因此在能成功实施物理攻击的条件下, 攻击者依然不能获取算法正常运行时的任一合法 PUF 响应, 上述安全性归约证明依然成立, 此时 PUF-MAC 算法仍是安全的.

综上, 本文给出了 PUF-MAC 在标准模型下的安全性归约, 证明了当 PUF 满足 EUF-CMA 安全性且 H 具有弱抗碰撞性时, PUF-MAC 算法就能满足 EUF-CMA 安全性.

3.4 基于非理想 PUF 的 MAC 算法

当使用非理想 PUF 构造 PUF-MAC 时, 需引入模糊提取器来实现 PUF-FE 构造, 从而实现数据的确定性映射, 其余流程则与 3.2 小节相同. 而根据定义 4, 攻击者在不能调用和访问 PUF 的条件下, 即使获取辅助校验数据 w 也难以恢复对应的响应 R. 因此 3.3 小节中的安全性证明依然适用于该算法. 模糊提取器的引入可以增强 PUF 的鲁棒性, 以减小器件老化等因素对 MAC 算法正确性造成的影响.

A, B 双方使用基于非理想 PUF 的 MAC 算法通信的示意图如图 3 所示.

4 PUF-MAC 的应用

4.1 基于 PUF-MAC 的密钥更新与协商

A, B 双方初始时除 puf, H 和 C_0 之外, 还分别拥有上一轮协商中对方的 PUF 响应 R_{LB}, R_{LA}. 首次协商时可令 $R_{LB} = R_B, R_{LA} = R_A$. 该方案分为密钥生成与密钥更新两阶段, 如图 4 所示.

I. 密钥生成. 该阶段与图 2 中的 KeyGen 相同, A, B 交换 R_A, R_B 后各自计算密钥 (C_0, T).

II. 密钥更新. 若由 A 发起共享密钥 (C_0, T) 的更新时, 可进行如下步骤:

(a) A 由 $R_A = \text{puf}_A(C_0)$ 与 T 可得 R_B, 生成 $R_{TA} = \text{puf}_A(C_0 \oplus R_{LB})$, 从而令 $M_A = R_{TA} \oplus H(R_{LA}||R_{LB})$. 之后 A 调用 Mac 算法计算 M_A 的消息认证码 tag_A 并发送给 B;

(b) B 收到消息后调用 Vrfy 算法可验证 tag_A, 从而能根据 R_B 解算出 R_{TA};

(c) B 生成 R_{TB}, 令 $M_{AB} = R_{TA} \oplus R_{TB}, M_B = R_{TB} \oplus H(R_{TA}||R_{LB})$; 之后, B 计算 C_1 并得到 $R'_B = \text{puf}_B(C_1)$, 并由 Mac 算法可得 $\text{tag}_B = (t_B, \sigma_B)$. 最终 B 发送 M_B, tag_B 给 A;

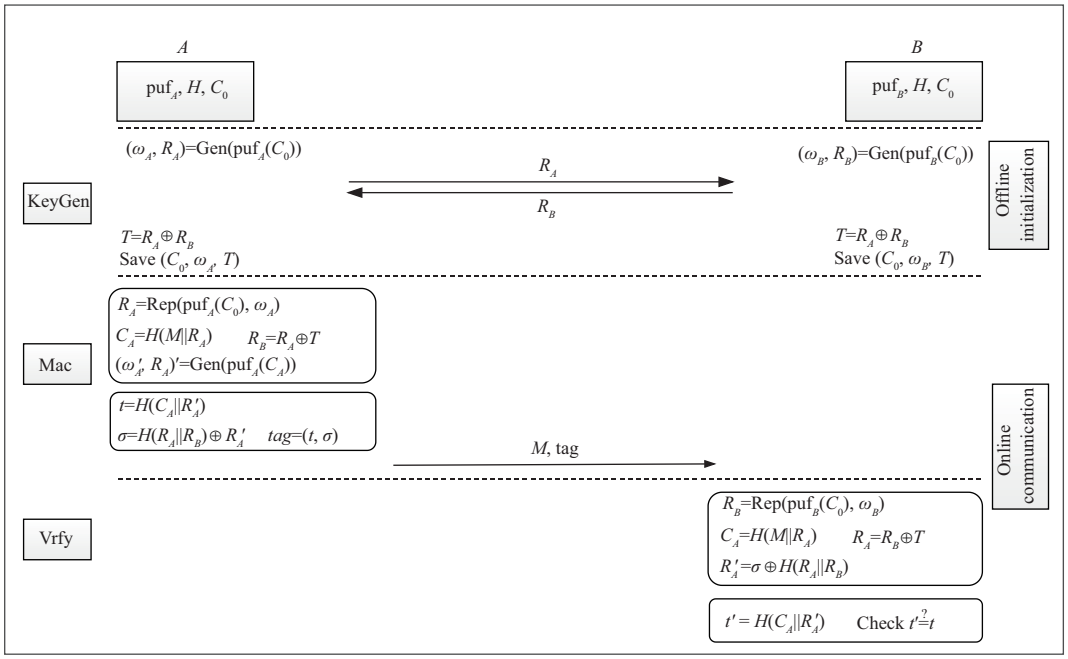

图 3 基于非理想 PUF 的 MAC 算法流程

Figure 3 Procedure of non ideal PUF-MAC

(d) A 收到消息后首先由 R_A, R_{TA} 解算出 R_{TB}, 从而计算 M_{AB} 与 C_1. 其次, A 可根据 Vrfy 算法验证 t_B, 若验证通过, 则 A 将 R'_B 作为 B 的新响应; 否则中止协议.

(e) 同步骤 (c), A 依次计算 R'_A, t_A, σ_A, 并发送 $M'_A = H(R_{TA}||R_{TB})$, $\mathrm{tag}'_A = (t_A, \sigma_A)$ 给 B;

(f) 同步骤 (d), B 对 M'_A 进行验证以确认 A 已收到 R_{TB} 与 R'_B, 而 B 会将 R'_A 作为新响应. 由此, A, B 可分别获得新的密钥 $(C_1, T_{\mathrm{new}} = R'_A \oplus R'_B)$. 下一轮协商中则有 $R_{LB} = R'_B, R_{LA} = R'_A$.

该方案的主要计算过程与 PUF-MAC 相同, 但需保存响应 R'_A, R'_B 以计算共享密钥. 由于 PUF 的单向性与不可预测性, 在无法调用 PUF 的条件下, 攻击者即使已知当前密钥 T 也无法预测新密钥 T_{new} 或还原历史密钥 T_{old}. 因此该方案满足前向与后向安全性, 适用于不安全环境中的密钥协商.

4.2 基于 PUF-MAC 的身份认证协议

除密钥协商外, 本文还将基于 PUF-MAC 设计一种双向身份认证协议, 如图 5 所示. 令字符串 $\mathrm{ID}_A, \mathrm{ID}_B$ 分别表示协议中双方 A, B 的身份. 该身份认证协议包括准备与认证两阶段, 内容如下.

I. 准备. 同 4.1 小节, 该阶段 A, B 交换响应后可得共享值 $(C_0, T = R_A \oplus R_B)$.

II. 认证. 若 A, B 需相互认证对方的身份, 则进行如下步骤.

(a) A 由当前时间 TS 计算 $R_A^T = R_A \oplus \mathrm{TS}$, 即令 $T' = T \oplus \mathrm{TS}$, 其中 TS 可序列化成长度为 n 的比特串. A 可得 $M_A = \mathrm{ID}_A||\mathrm{TS}$, 并使用 Mac 算法得到对应的 $\mathrm{tag}_A = (t_A, \sigma_A)$. 计算时 R_A 应替换为 R_A^T, 其余步骤保持不变. 最终 A 发送 M_A, tag_A 给 B;

(b) B 首先检查收到消息中 TS 的新鲜性以抵御重放攻击, 之后令 $T' = T \oplus \mathrm{TS}$, 并由 M_A 与 R_B 得 $R_A^T = T' \oplus R_B$; B 根据 Vrfy 算法使用 R_A^T 对 tag_A 进行验证. 若验证成功则 A 通过认证, 否则认证失败, 协议中止.

(c) 其次, B 由当前时间 TS′ 计算 $R_B^T = R_B \oplus \mathrm{TS}'$, 即有 $T'' = T' \oplus \mathrm{TS}'$. 同步骤 (a), B 可根据

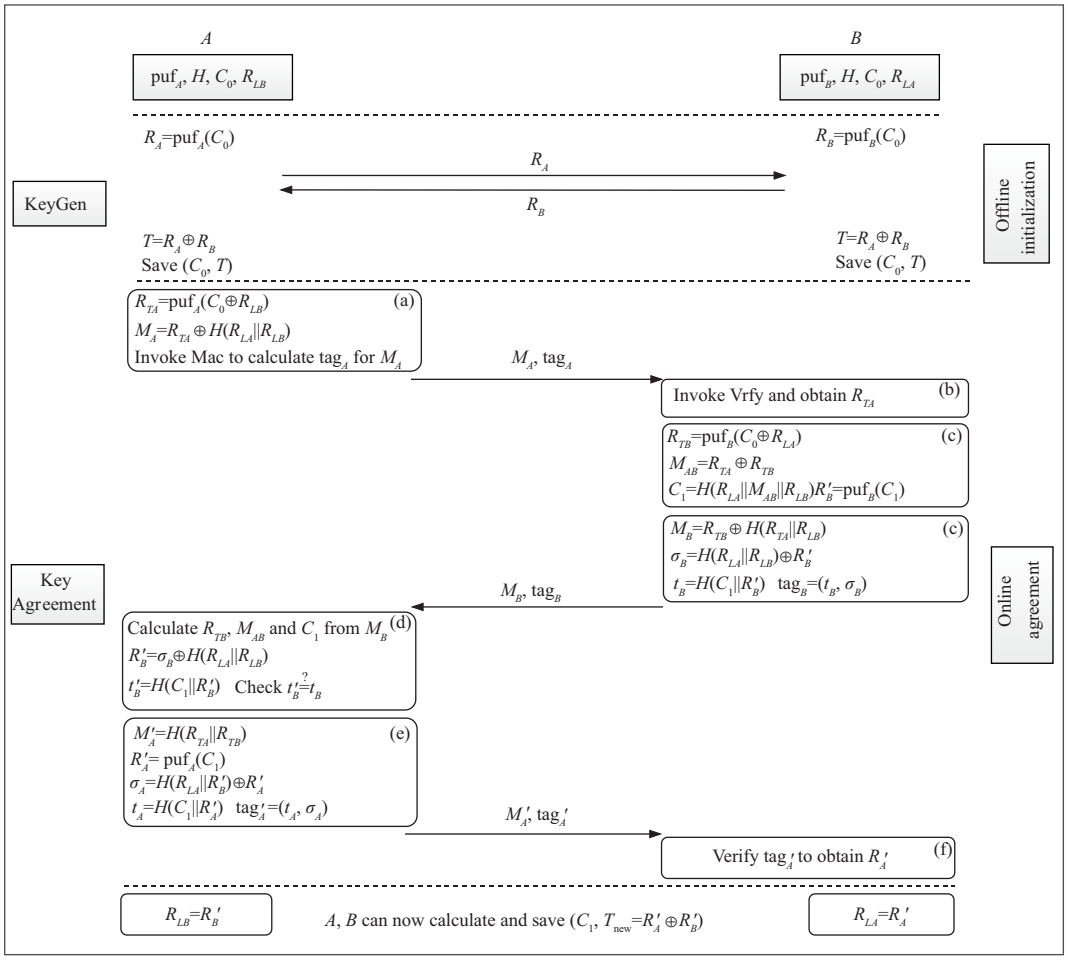

图 4 基于 PUF-MAC 的密钥更新与协商

Figure 4 Procedure of PUF-MAC based key agreement protocol

Mac 算法使用 R_A^T, R_B^T 计算 M_B 的消息认证码 tag_B. B 最终发送 M_B, tag_B 给 A;

(d) 同理, A 由 TS′ 与 R_A^T 可得 R_B^T, 并使用 Vrfy 算法验证 tag_B. 若验证成功则 B 通过认证.

该双向认证协议可用于设备的配对认证等情景. 当攻击者试图假冒某一方身份通过认证时, 需伪造 TS 与 ID 的消息认证码, 在无法调用 puf 的条件下, 攻击者需伪造 PUF 响应或找到 H 上的碰撞. 因此, 当 PUF 满足 EUF-CMA 安全性且 H 满足弱抗碰撞性时, 该身份认证协议可抵御假冒攻击. 另外, TS 与 TS′ 保证了认证消息与验证结果的新鲜性, 可抵御重放攻击.

PUF-MAC 算法以及对应的密钥协商和身份认证协议具有相同的算法组成与运算结构, 且通信双方需执行的预操作相同 (即交换 PUF 响应)、预存储向量相同 (即 $(C_0, R_A \oplus R_B)$). 因此本文设计的 PUF-MAC 算法经一次部署和初始化后, 可在同一系统中实现消息认证、密钥协商以及身份认证的功能, 从而形成一个完整的信息系统安全协议框架.

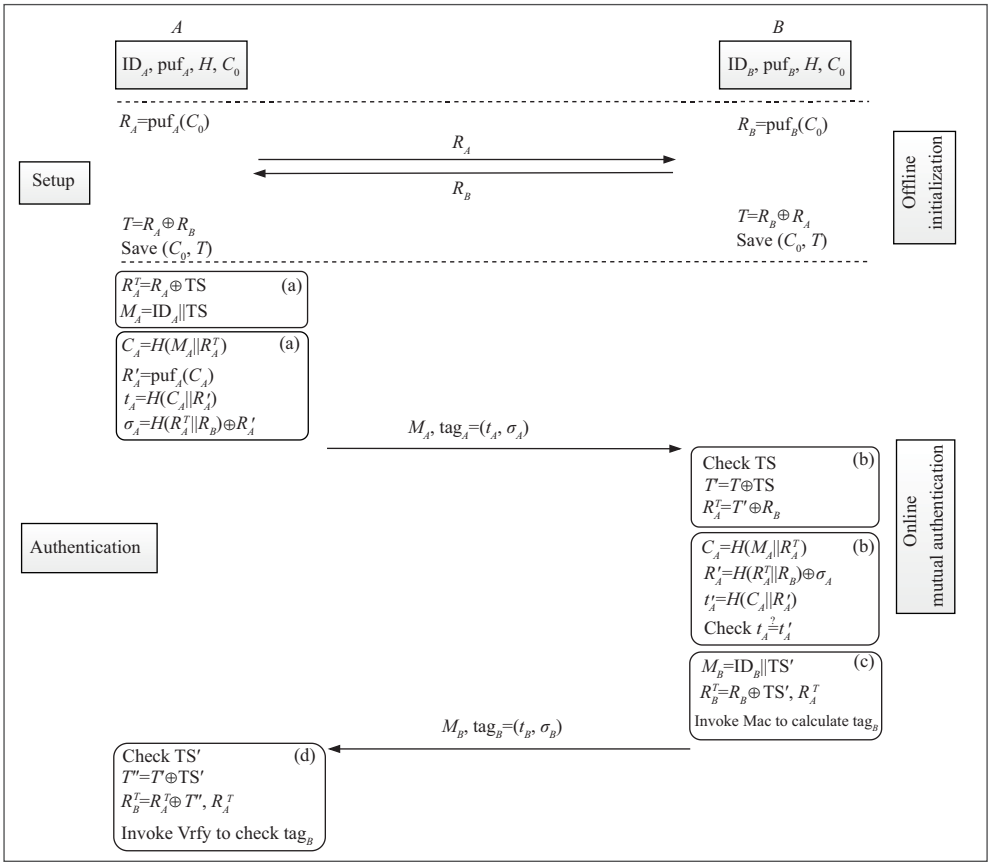

图 5　基于 PUF-MAC 的身份认证协议

Figure 5　Procedure of PUF MAC-based authentication protocol

表 1　基于 PUF 的 MAC 算法间的对比

Table 1　Comparison of different PUF-based MACs

Scheme	Ref. [34]	Ref. [35] (for local use only)	Ref. [36]	PUF-MAC
Primitives used	PUF	Hash, PUF	Hash, PUF	Hash, PUF
Computation cost	Select k PUF responses	$1\cdot\text{Hash}+1\cdot\text{PUF}$	$2\cdot\text{Hash}$	$3\cdot\text{Hash}+2\cdot\text{PUF}$
Storage cost	$\mathcal{O}(\lvert M\rvert\cdot\lvert k\rvert\cdot L_{\text{PUF}})$	$\mathcal{O}(L_{\text{hash}})$	$\mathcal{O}(\lvert N\rvert\cdot L_{\text{PUF}})$	$\mathcal{O}(L_{\text{hash}})$
Communication cost	$\mathcal{O}(\lvert k\rvert\cdot L_{\text{PUF}})$	$\mathcal{O}(L_{\text{hash}})$	$\mathcal{O}(L_{\text{hash}})$	$\mathcal{O}(L_{\text{hash}})$
Provably secure	No	Yes	No	Yes

5　PUF-MAC 算法分析与比较

PUF-MAC 具有对称的算法结构, 仅需 Hash 函数与 PUF 作为算法组件, 且仅涉及 $\oplus$, || 等运算, 因此可被轻量实现以用于物联网终端等资源受限平台.

5.1　基于 PUF 的 MAC 算法间的对比

与其他基于 PUF 设计的 MAC 算法进行对比, 结果如表 1 所示. 在存储与通信开销上, 本方案与文献 [35] 要优于文献 [34,36], 且方案 [35] 的计算开销更小, 但该方案要求 tag 由同一方完成生成和

表 2 不同 MAC 算法的对比

Table 2 Comparison of different MACs

Scheme	HMAC [1]	CBC-MAC [2]	GMAC [13]	PMAC [14]	PUF-MAC
Primitives Used	Hash	Block cipher	Galois field	Block cipher gray code	Hash, PUF
Basic operations	$\|\|$	$\oplus$	$\otimes$	$\oplus$, $\lll$, $\ggg$	$\oplus$, $\|\|$
Components	Hash	Symmetric encryption	$\otimes$	Symmetric encryption Gray code calculation	Hash PUF evaluation
Storage cost	$\mathcal{O}(L_{\text{key}})$	$\mathcal{O}(L_{\text{key}}+L_{\text{IV}})$	$\mathcal{O}(L_{\text{key}})$	$\mathcal{O}(L_{\text{key}}+L_{\text{gray}})$	$\mathcal{O}(L_{\text{hash}})$
Communication cost	$\mathcal{O}(L_{\text{hash}})$	$\mathcal{O}(L_{\text{enc}})$	$\mathcal{O}(L_{\text{GF}(2^n)})$	$\mathcal{O}(L_{\text{enc}})$	$\mathcal{O}(L_{\text{hash}})$
Key needs secure storage	Yes	Yes	Yes	Yes	No

验证, 即无法应用于不同实体间的通信, 实用性较差. 在计算开销上, 虽然本方案需要更多的 Hash 与 PUF 操作次数, 但 Hash 的计算与 PUF 响应的生成均为轻量运算, 整体开销依然较小. 方案 [34, 36] 在通信前双方需预生成并存储一 PUF 响应数据库, 这会造成巨大的通信与存储负担, 从而影响方案的可持续性且不利于多用户的扩展.

综上, 本文的 PUF-MAC 算法能实现不同实体间的消息认证, 拥有更均衡的性能表现并具有完整的安全性证明; 同时, 本方案无需预先生成大量的 PUF 响应, 方便部署在物联网等分布式系统中, 有较好的实用性和可扩展性, 能满足实际中的认证需求.

5.2 与传统 MAC 算法的对比

比较 PUF-MAC 与传统 MAC 算法, 结果如表 2 所示. 其中, $||, \oplus, \otimes$ 分别表示比特串的连接、按位异或和有限域乘法运算; $\lll, \ggg$ 分别表示比特串的左右移位运算. 由表 2 可知, PUF-MAC 所用部件与基本运算都较为轻量, 存储与通信开销和传统 MAC 算法相近, 但能实现运行时敏感数据的保护. PUF-MAC 中的 Hash 函数与 PUF 可根据应用需求与行业标准进行替换, 具有良好的兼容性.

PUF-MAC 中 PUF 的引入使攻击者实施物理攻击时仅能获取存储器中的静态数据, 而无法通过重新运行设备或调用 PUF 等手段还原运算时的秘密参数, 这有效解决了传统 MAC 算法中的密钥管理问题. 如果将 PUF-MAC 的 KeyGen 用于生成传统算法的密钥, 虽然一定程度上能解决应用时的密钥安全存储问题, 但仍会面临使用长期密钥带来的安全风险. 因此, PUF-MAC 在解决实际环境中密钥管理问题的同时, 还能给出较为轻量且安全的构造.

6 总结

本文针对传统 MAC 算法在应用时的密钥管理问题, 提出了一种基于物理不可克隆函数的 MAC 算法, 该算法可处理任意长度的消息, 而且仅需 PUF 与 Hash 作为算法组件, 易于实现且结构轻量. 本文分别基于理想 PUF 与非理想 PUF 给出了算法流程, 而且证明了 PUF-MAC 算法在标准模型下的 EUF-CMA 安全性, 并将其归约到了 PUF 的 EUF-CMA 安全性与 Hash 的弱抗碰撞性. 同时, 本文基于 PUF-MAC 设计了一种可用于算法本身的密钥协商方案, 能在不安全环境中在线实现密钥更新且满足前后向安全性. 此外, 本文还基于该算法给出了一种身份认证协议, 可用于对等实体间的认证, 体现了 PUF-MAC 良好的实用性.

本文提供了 PUF-MAC 算法及其应用的理论分析, 在实现时应选取具有足够安全强度的轻量级

PUF 与 Hash 函数. 在后续研究中, 可对现有 PUF-MAC 算法的组成进行优化, 使其更加轻量; 多用户情景下 PUF-MAC 的设计与应用, 以及后量子可证明安全的 MAC 算法也是值得关注的方向.

参考文献

1 Bellare M, Canetti R, Krawczyk H. Keying hash functions for message authentication. In: Advances in Cryptology - CRYPTO'96. Berlin: Springer, 1996. 1–15

2 National Institute of Standards and Technology (NIST). Computer Data Authentication. Federal Information Processing Standard (FIPS) 113 (Withdrawn). 1985. https://csrc.nist.gov/publications/detail/fips/113/archive/1985-05-30

3 Krawczyk H, Bellare M, Canetti R. HMAC: keyed-hashing for message authentication. RFC 2104, 1997. doi: 10.17487/RFC2104

4 National Institute of Standards and Technology (NIST). The Keyed-Hash Message Authentication Code (HMAC). Federal Information Processing Standard (FIPS) 198-1. 2008. https://csrc.nist.gov/publications/detail/fips/198/1/final

5 Xie J, Sun W, Gu D, et al. Research on differential power analysis of HMAC-SM3. In: Proceedings of 2015 International Conference on Computer Science and Intelligent Communication, 2015. 103–106

6 Fouque P-A, Leurent G, Réal D, et al. Practical electromagnetic template attack on HMAC. In: Cryptographic Hardware and Embedded Systems-CHES 2009. Berlin: Springer, 2009. 66–80

7 Pappu R. Physical one-way functions. Dissertation for Ph.D. Degree. Massachusetts: Massachusetts Institute of Technology, 2002

8 Holcomb D E, Fu K. Bitline PUF: building native challenge-response PUF capability into any SRAM. In: Advanced Information Systems Engineering. Berlin: Springer, 2014. 510–526

9 Hesselbarth R, Wilde F, Gu C, et al. Large scale RO PUF analysis over slice type, evaluation time and temperature on 28 nm Xilinx FPGAs. In: Proceedings of IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, 2018. 126–133

10 Jouini Z C, Danger J-L, Bossuet L. Performance evaluation of physically unclonable function by delay statistics. In: Proceedings of IEEE 9th International New Circuits and systems conference, 2011. 482–485

11 National Institute of Standards and Technology (NIST). Recommendation for Block Cipher Modes of Operation: The CMAC Mode for authentication. SP 800-38B (Withdrawn). 2005. https://csrc.nist.gov/publications/detail/sp/800-38b/archive/2005-05-01

12 Bellare M, Guérin R, Rogaway P. XOR MACs: new methods for message authentication using finite pseudorandom functions. In: Advances in Cryptology - CRYPTO' 95. Berlin: Springer, 1995. 15–28

13 Dworkin M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication (SP) 800-38D. 2007

14 Black J, Rogaway P. A block-cipher mode of operation for parallelizable message authentication. In: Advances in Cryptology - EUROCRYPT 2002. Berlin: Springer, 2002. 384–397

15 Boneh D, Zhandry M. Quantum-secure message authentication codes. In: Advances in Cryptology - EUROCRYPT 2013. Berlin: Springer, 2013. 592–608

16 Armknecht F, Moriyama D, Sadeghi A R, et al. Towards a unified security model for physically unclonable functions. In: Proceedings of 2016 Cryptographers' Track at the RSA Conference. Cham: Springer, 2016. 271–287

17 Brzuska C, Fischlin M, Schröder H, et al. Physically unclonable functions in the universal composition framework. In: Proceedings of 2011 Annual Cryptology Conference. Berlin: Springer, 2011. 51–70

18 Badrinarayanan S, Khurana D, Ostrovsky R, et al. Unconditional UC-secure computation with (stronger-malicious) PUFs. In: Proceedings of 2017 Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer, 2017. 382–411

19 Delvaux J. Security analysis of PUF-based key generation and entity authentication. Dissertation for Ph.D. Degree. Leuven: Ku Leuven, 2017

20 Chatterjee U, Govindan V, Sadhukhan R, et al. Building PUF based authentication and key exchange protocol for IoT without explicit CRPs in verifier database. IEEE Trans Dependable Secure Comput, 2019, 16: 424–437

21 Chuang Y H, Lei C L. PUF based authenticated key exchange protocol for IoT without verifiers and explicit CRPs. IEEE Access, 2021, 9: 112733

22 Nimmy K, Sankaran S, Achuthan K. A novel lightweight PUF based authentication protocol for IoT without explicit CRPs in verifier database. J Ambient Intell Human Comput, 2021. doi: 10.1007/s12652-021-03421-4

23 Mahalat M H, Saha S, Mondal A, et al. A PUF based light weight protocol for secure WiFi authentication of IoT devices. In: Proceedings of 2018 International Symposium on Embedded Computing and System Design (ISED), Cochin, 2018. 183–187

24 Gope P, Lee J, Quek T Q S. Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions. IEEE Trans Inform Forensic Secur, 2018, 13: 2831–2843

25 Chaterjee U, Mukhopadhyay D, Chakraborty R S. 3PAA: a private PUF protocol for anonymous authentication. IEEE Trans Inform Forensic Secur, 2021, 16: 756–769

26 Alladi T, Naren T, Bansal G, et al. SecAuthUAV: a novel authentication scheme for UAV-ground station and UAV-UAV communication. IEEE Trans Veh Technol, 2020, 69: 15068–15077

27 Nyangaresi V O, Petrovic N. Efficient PUF based authentication protocol for Internet of drones. In: Proceedings of 2021 International Telecommunications Conference (ITC-Egypt), Alexandria, 2021. 1–4

28 Jiang Q, Zhang X, Zhang N, et al. Three-factor authentication protocol using physical unclonable function for IoV. Comput Commun, 2021, 173: 45–55

29 Renault É, Mühlethaler P, Boumerdassi S. Communication security in VANETs based on the physical unclonable function. In: Proceedings of 2021 IEEE International Conference on Communications (ICC), Montreal, 2021. 1–6

30 Falcone A, Felicetti C, Garro A, et al. PUF-based smart tags for supply chain management. In: Proceedings of the 16th International Conference on Availability, Reliability and Security. New York: ACM, 2021. 1–7

31 Qureshi M A, Munir A. PUF-RAKE: a PUF-based robust and lightweight authentication and key establishment protocol. IEEE Trans Dependable Secure Comput, 2021. doi: 10.1109/TDSC.2021.3059454

32 Mall P, Amin R. EuDaimon: PUF-based robust and lightweight authenticated session key establishment protocol for IoT-enabled smart society. IEEE Syst J, 2021. doi: 10.1109/JSYST.2021.3101201

33 Mahmood K, Shamshad S, Rana M, et al. PUF enable lightweight key-exchange and mutual authentication protocol for multi-server based D2D communication. J Inf Security Appl, 2021, 61: 102900

34 Bolotnyy L, Robins G. Physically unclonable function-based security and privacy in RFID systems. In: Proceedings of the 5th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'07). White Plains: IEEE, 2007. 211–220

35 Resende A, Aranha D. PUF-based authenticated encryption. 2013. https://www.researchgate.net/publication/292322269_PUF-based_authenticated_encryption. [Access Date: 2021-07-10]

36 Zheng Y, Zhao X, Sato T, et al. Ed-PUF: event-driven physical unclonable function for camera authentication in reactive monitoring system. IEEE Trans Inform Forensic Secur, 2020, 15: 2824–2839

37 Jung S W, Jung S. HRP: a HMAC-based RFID mutual authentication protocol using PUF. In: Proceedings of the International Conference on Information Networking 2013 (ICOIN), 2013. 578–582

38 Tuyls P, Schrijen G-J, Škorić B, et al. Read-proof hardware from protective coatings. In: Cryptographic Hardware and Embedded Systems - CHES 2006. Berlin: Springer, 2006. 369–383

39 Ruhrmair U, van Dijk M. PUFs in security protocols: attack models and security evaluations. In: Proceedings of 2013 IEEE Symposium on Security and Privacy. Berkeley: IEEE, 2013. 286–300

A PUF-based provably secure message authentication algorithm and application

Xiaolin ZHANG & Dawu GU*

School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240*, China*

* Corresponding author. E-mail: dwgu@sjtu.edu.cn

Abstract Message authentication code (MAC), widely used in all kinds of information systems, is a symmetric cryptographic algorithm that checks message integrity and source authenticity. However, when the devices running MAC face physical invasion, the attacker can extract the keys inside and generate valid tags by directly reading the memory or adjusting the circuits. In this paper, we propose PUF-MAC, a new MAC algorithm based on the physically unclonable function (PUF), which is constructed from the hash function and PUF. The PUF is a kind of data mapping entity with unclonable internal structures and unpredictable outputs. The difference between mappings preserved by PUF entities originates from minor variations in the physical environment during production. The communicating parties can apply the PUF to form the shared secret key. Under the standard security model, this paper inductively proves that PUF-MAC satisfies the existential unforgeability under a chosen message attack, and the EUF-CMA security of PUF-MAC relies on the (weak) collision resistance of hash and the EUF-CMA security of PUF. Additionally, this paper recasts PUF-MAC into a key agreement protocol with forward/backward security, along with a bilateral authentication protocol by which its practicability is indicated. A comparison with other MAC reveals that PUF-MAC is indeed lightweight and easy to deploy, and PUF-MAC requires no pre-established PUF responses. The involvement of the PUF allows an attacker to forge a valid tag even after retrieving the key, thereby ensuring communication security.

Keywords MAC, key management, PUF, authentication