**Diffie–Hellman (DH) 与 MITM 防御**

1. [Preventing Man-In-The-Middle Attack in Diffie-Hellman Key Exchange Protocol](https://www.researchgate.net/publication/280722113_Preventing_Man-In-The-Middle_Attack_in_Diffie-Hellman_Key_Exchange_Protocol)

Aqeel Sahi, David Lai (2015)

论文详细分析了传统 Diffie–Hellman 密钥交换的漏洞：由于没有身份验证机制，攻击者可在双方中间伪造公钥，从而中间人拦截并解密通信。作者提出使用基于伪随机序列生成器（如 Geffe Generator）的改进 DH 模型，通过增加不可预测性和认证标签，使密钥生成过程更安全。可引用其对传统 DH 不安全性的解释和防御思路作为“MITM 问题提出”与“增强密钥随机性”的论据。

2. [An Improved Diffie-Hellman Scheme for Mitigating a MITM Attack](https://www.ijisrt.com/assets/upload/files/IJISRT24APR2479.pdf)

IJISRT (2024)

该研究在传统 DH 协议中加入双向认证步骤：在密钥交换时使用时间戳、数字签名与随机质询，验证通信双方身份。文中指出这种方法可防止攻击者伪造身份并进行 MITM 攻击。适合引用为“利用时间同步与身份验证机制抵御 MITM”的现代化改进方案。

3. [Diffie-Hellman in the Air: A Link Layer Approach for In-Band Wireless Pairing](https://arxiv.org/abs/1901.09520)

Wenlong Shen et al. (2019)

提出一种用于无线通信的 DH 安全方案，通过检测信号碰撞、重放延迟等物理层特征判断是否存在 MITM 攻击者。文章展示了物理层信息如何补充传统加密层，成为一种“跨层防御”。可在论文中用作“实际系统层实现防御”的示例。

4. [Detecting Man-in-the-Middle Attacks on Ephemeral Diffie–Hellman (ZRTP / RFC6189)](https://datatracker.ietf.org/doc/html/rfc6189)

Phil Zimmermann 等（IETF 标准, 2011）

介绍 ZRTP 协议如何通过短认证字符串（SAS）在通话双方通过语音确认时验证密钥一致性，从而有效检测 MITM。该方法不依赖 PKI，具有较强的实用性。适合引用在“基于用户交互的 MITM 检测方案”部分。

5. [A Survey on Man-in-the-Middle Attacks and Their Countermeasures](https://ieeexplore.ieee.org/document/9059025)

Shubhankar Kumar et al. (2020)

全面总结了 MITM 攻击在不同层（网络层、TLS、DH、Wi-Fi 等）的变体和防御措施，包括 PKI 签名、密钥认证、PAKE、加盐机制等。可作为“MITM 攻击分类与综合防御框架”的理论支撑文献。

6. [Cryptographic Advancements Enabled by Diffie–Hellman](https://www.isaca.org/resources/isaca-journal/issues/2024/volume-3/cryptographic-advancements-enabled-by-diffie-hellman)

ISACA Journal, Vol.3 (2024)

文章概述了 DH 协议在现代加密体系（如 TLS、IPSec、PGP）中的应用，并指出“缺乏认证”的风险是 MITM 的根源之一。可用作引言或背景，说明“为什么 DH 在安全协议中必须结合认证机制”。

**RSA 与 Factorization Attack 防御**

1. [Twenty Years of Attacks on the RSA Cryptosystem](https://crypto.stanford.edu/~dabo/papers/RSA-survey.pdf)

Dan Boneh (1999)

经典综述，详细回顾了 RSA 的攻击手段，包括因式分解、低加密指数攻击、共模攻击、时序攻击等。指出因式分解是 RSA 安全的核心风险。可用作“RSA 攻击历史与背景介绍”的权威引用。

2. [Survey of RSA Vulnerabilities](https://www.mdpi.com/2297-8747/25/4/63)

Overmars et al. (2020)

文章系统地总结了 RSA 的结构性弱点，包括：

• 素数生成不随机导致模数易被分解；

• 小公钥指数引起的消息重构攻击；

• 多设备重复素数导致的共因子攻击。

可直接引用到“RSA 因式分解攻击与弱密钥风险”章节。

3. [Cryptoanalysis of RSA variants with special structure of RSA primes](https://arxiv.org/abs/2403.06184)

Haseeb Anwar et al. (2024)

研究了当 RSA 的素数具有某种数学结构（如接近幂次或存在小差距）时，攻击者可利用数论方法快速分解模数。强调必须避免“特殊形式素数”的密钥生成。可用于讨论“改进密钥生成算法”的部分。

4. [An Efficient All-to-All GCD Algorithm for Low Entropy RSA Key Factorization](https://arxiv.org/abs/2405.03166)

Andrew Pelofske (2024)

论文提出一种基于批量 GCD 的算法，可以从大量 RSA 公钥中检测出共享素数的弱密钥。适合引用为“现代 RSA 因式分解技术”实例，并指出“低熵 RNG”是主要原因。

5. [Practical Factorization of Widely Used RSA Moduli (ROCA Attack)](https://crocs.fi.muni.cz/_media/public/papers/nemec_roca_ccs17_preprint.pdf)

Matej Nemec et al. (2017, ACM CCS)

介绍了 ROCA 攻击：某厂商使用特定算法生成 RSA 素数，导致模数可被部分恢复。文中展示了数百万真实设备（如 TPM、智能卡）受影响的实例。适合用作“现实案例”说明因式分解风险。

6. [Microarchitectural Side-Channel Vulnerabilities and Countermeasures: A Survey](https://dl.acm.org/doi/10.1145/3446370)

Ashish Venkat et al. (2021)

探讨侧信道攻击（如缓存、分支预测、功耗分析）如何间接帮助攻击者推导 RSA 密钥，从而简化因式分解。文章还介绍了常数时间运算、随机掩蔽、硬件隔离等防御技术。可用于“RSA 实现层安全强化”章节。