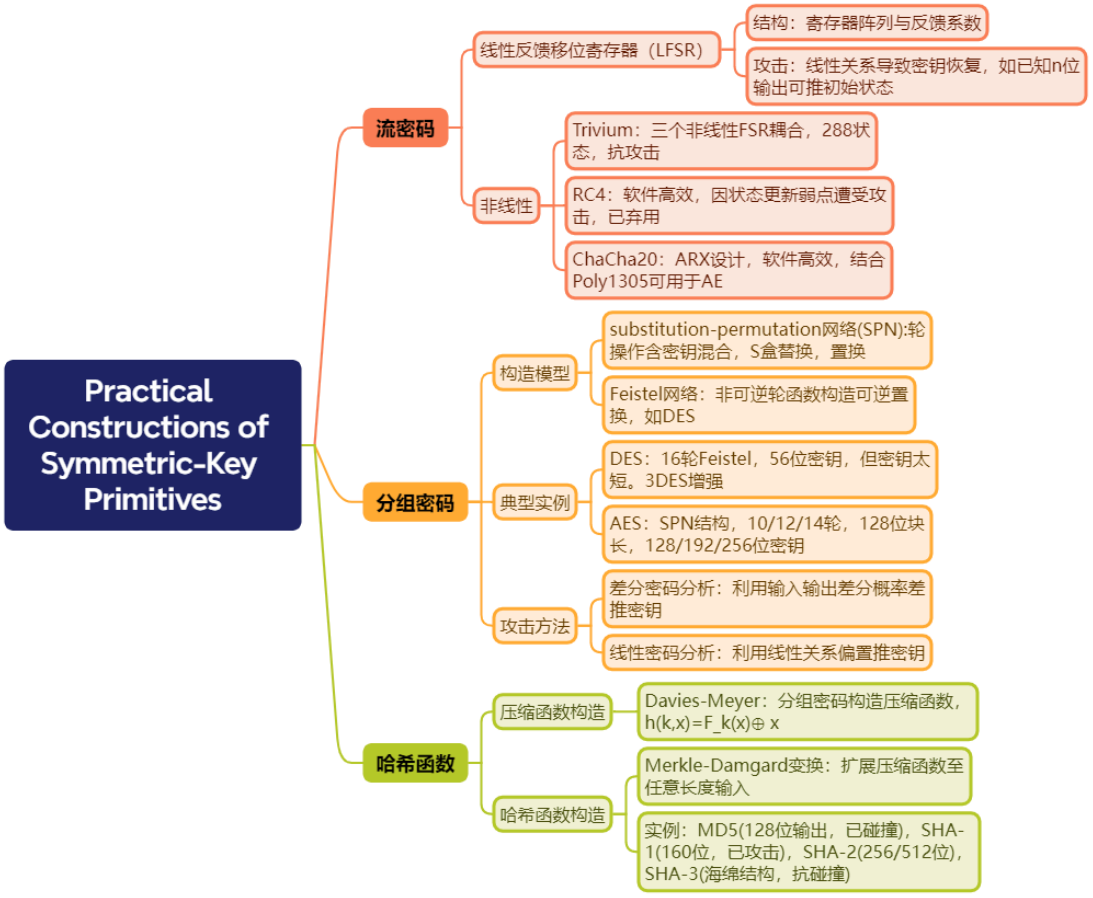
一段话总结

文档聚焦对称密钥原语的实际构造，涵盖**流密码**（如基于线性反馈移位寄存器的Trivium、曾广泛使用但现因弱点被弃用的RC4、软件高效的ChaCha20）、**分组密码**（包括 substitution-permutation 网络、Feistel 网络，以及典型实例DES和AES）、**哈希函数**（如通过Merkle–Damgård变换构造的MD5、SHA-1/2及新的SHA-3）。文中阐述各构造的设计原理、安全特性及实际攻击案例，强调如AES因128位块长和128/192/256位密钥长度较DES（56位密钥、64位块长）更安全，而哈希函数需应对生日攻击等挑战，构造时需考虑碰撞抗性等核心要求。

思维导图



详细总结

一、流密码

1. 线性反馈移位寄存器(LFSR) - 结构：n个寄存器与反馈系数，状态更新时右移，左寄存器为当前状态位异或和，输出右寄存器位。 - 安全性：最大长度LFSR可循环2^n-1非零状态，但线性关系致攻击，如n位输出暴露初始状态，2n位输出推反馈系数。

2. 非线性流密码 - Trivium：三耦合非线性FSR（93/84/111位），288位状态，Init加载80位密钥与IV，运行4×288轮初始化，无优于穷举攻击。 - RC4：状态为256字节数组S及i,j，Init初始化S并打乱，Next生成字节，因状态更新偏差致碰撞，如第二字节偏0，WEP中IV使用不当致密钥恢复。 - ChaCha20：ARX设计，核心512位置换P，构造伪随机函数F，流密码输出F(IV||计数器)，软件高效，用于TLS。

二、分组密码

1. 构造模型　- substitution-permutation网络(SPN)：轮操作含密钥混合、S盒替换、线性置换，如AES，需多轮达雪崩效应，1位输入变致多轮后全位影响。　- Feistel网络：分左右半块，轮函数f非可逆，输出左半块为原右半块，右半块为原左半块异或f(右半块)，可 invertible，如DES。

2. 典型实例　- DES：16轮Feistel，64位块长，56位密钥，轮函数含扩展、S盒、置换，因56位密钥短，穷举攻击可行（2^{56}次，现26小时破解），3DES用两或三密钥增强。　- AES：SPN结构，128位块长，128/192/256位密钥，轮数10/12/14，轮操作含字节替换、行移位、列混合、密钥加，无实质攻击，安全。

3. 攻击方法　- 差分密码分析：找输入输出差分对，如SPN中输入差Δx致输出差Δy概率超随机，推密钥位。　- 线性密码分析：找输入、输出、密钥线性关系，如DES需2^{43}已知明文。

三、哈希函数

1. 压缩函数构造　- Davies–Meyer：块密码F构造$h(k,x)=F_k(x)\oplus x$，理想 cipher 模型下抗碰撞，q次查询碰撞概率≤$q^2/2^{\ell}$。

2. 哈希函数构造　- Merkle–Damgård变换：压缩函数扩展至任意长输入，如MD5（128位，2004年现碰撞）、SHA-1（160位，2017年现碰撞）、SHA-2（256/512位）。　- 海绵构造与SHA-3：用1600位置换P，吸收与挤压阶段，抗碰撞，q次查询概率≤$q^2/2^v + q(q+1)/2^c$。

3. 攻击　- 生日攻击：输出ℓ位时，$2^{\ell/2}$次操作找碰撞，故输出需≥2n位抗2^n次攻击。

| 密码类型 | 实例 | 密钥长度 | 块长度 | 安全现状 |

| 流密码 | ChaCha20 | 256位 | - | 安全，软件高效 |

| 分组密码 | DES | 56位 | 64位 | 不安全，因密钥短 |

| 分组密码 | AES | 128/192/256位 | 128位 | 安全，广泛使用 |

| 哈希函数 | SHA-256 | - | - | 安全，推荐使用 |

关键问题

1. 流密码与分组密码的核心区别是什么?

答案：流密码逐位/字节生成密钥流，与明文异或加密，如RC4；分组密码将明文分块，块长固定，如AES分128位块加密。流密码可实时加密，分组密码需块对齐，且流密码状态更新影响后续输出，分组密码各块独立（如ECB模式）或关联（如CBC模式）。

2. AES相比DES在安全性和设计上有哪些改进?

答案：AES密钥长度128/192/256位，DES仅56位，抗穷举攻击；块长128位，DES64位，减少IV重复风险。设计上AES用SPN，轮数依密钥长10-14轮，S盒非线性强，扩散快；DES是Feistel，16轮，S盒设计抗差分攻击，但密钥短。

3. 哈希函数的碰撞攻击原理是什么？为何SHA-1比MD5更安全?

答案：碰撞攻击基于生日悖论，输出ℓ位时，$2^{\ell/2}$次操作找碰撞。MD5输出128位，理论碰撞需2^{64}次，2004年现实际碰撞；SHA-1输出160位，理论需2^{80}次，2017年用2^{63}次找到碰撞，因输出更长，碰撞难度更高，故曾比MD5安全，但现也不安全，需用SHA-2/3。