发明专利技术交底书

动态多原语密码跳频协议（DMHP）的安全通信系统及方法

中国移动通信有限公司研究院

2026 年 1 月 26 日

中国移动专利申请

技术交底书

公司编号	
发明名称	动态晶格跳跃协议（DLHP）的多原语密码跳频安全通信系统及方法
申报单位	研究院
申报类型	发明
发明人	许达
技术联系人	许达 (xudayj@chinamobile.com, +86-13521894156)
注意事项	1．技术联系人应为深入了解本申请提案技术方案的技术人员。 2．请按照集团公司提供的本技术交底书模板逐项填写。

一、 发明名称

动态多原语密码跳频协议（DMHP）的安全通信系统及方法

二、 技术领域

本发明涉及密码通信与网络安全技术领域，尤其涉及一种面向后量子威胁环境的**动态多原语（Multi-Primitive）密码跳频**安全通信协议、系统与方法。

与量子计算的关联说明：

量子计算机在成熟后可利用 Shor 算法对 RSA/ECC 等传统公钥密码体制构成实质性威胁，同时后量子密码（PQC）算法族仍处于持续分析演进阶段，存在算法被逐步削弱或出现新型攻击的风险。本发明通过在会话内对密码算法进行**时间维/序号维的动态跳变**，并在必要时引入**多路径传输分散**与**阈值分片（全息熵分散，HED）**，降低”现在存储、未来解密（SNDL）”攻击的价值，提升面对量子时代持续攻防演化的不确定性韧性。

关联项目：_____（待填写）

三、 术语与缩写（建议）

为避免全文表述歧义，本文对主要术语与缩写作如下统一约定：

术语/缩写	含义（本文口径）
DMHP	动态多原语密码跳频协议（Dynamic Multi-Primitive Hopping Protocol），泛指会话内按时间/序号对不同数学困难类别的密码原语与密钥上下文进行动态切换的协议机制。
Cryptographic Hopping	“密码跳频/密码跳变”，类比无线电跳频思想，将算法选择与密钥派生上下文作为随时间/序号演化的变量。
受保护单元	被加密与认证的最小保护粒度，可为数据包、记录（Record）或数据块（Block），具备可识别的SeqID或时间片标识。
SeqID	序号/记录号/包号等单调标识，用于无状态派生与重放检测窗口定位。
EpochID	可选的“纪元”标识，与SeqID构成$\langle \text{EpochID}, \text{SeqID} \rangle$联合计数器，用于回绕处理或策略推进。
KDF	密钥派生函数（Key Derivation Function），用于从MasterSecret与SeqID（或时间片）派生每单元算法索引与密钥材料。

AEAD	带认证的加密（Authenticated Encryption with Associated Data），或同等强度的“加密+完整性校验”组合。
AAD	附加认证数据（Associated Authenticated Data），建议至少包含SeqID/TimeSlotID、EpochID（若存在）与模式/版本标识，用于绑定上下文并降低重放/篡改风险。
HPC	硬问题类别（Hard Problem Class），用于对算法的数学基础进行分类标注（如格/编码/哈希基/同源等），供正交选择器执行类别距离约束。
HED	全息熵分散（Holographic Entropy Dispersion），本文指将载荷按(k,n)阈值进行分片（或纠删码分散）并分别保护、满足至少k份额方可重构的机制。
MPTD	多路径传输分散（Multi-Path Transport Dispersion），本文指将不同受保护单元或HED分片映射到不同物理链路/子流进行分散传输的机制。
SNDL	“现在存储、未来解密”（Store Now, Decrypt Later）攻击模型。

四、 现有技术的技术方案

4.1 加密通信与后量子迁移的现状

在现有安全通信协议（例如 TLS、IPsec、QUIC 等）中，通常在握手阶段确定单一（或少量）算法套件，并在会话期内固定使用。该模式在后量子迁移背景下存在如下特点：

- **单点算法风险集中**：一旦会话采用的某一公钥算法/对称算法出现弱点或实现漏洞，会话内大量数据可被同类攻击集中利用；
- **SNDL 攻击收益高**：攻击者可长期批量采集同一算法保护的数据，待未来出现突破（含量子计算可行）后统一解密；
- **算法替换成本高**：算法迁移往往需要重新协商或重建会话，可致时延上升与运维

复杂；

- **侧信道累积：**长期重复使用同一密钥/同一算法实现，会提高功耗/时间等侧信道信号的可观测性。

4.2 密码敏捷（Crypto Agility）与其不足

现有"密码敏捷"多数停留在**版本升级层面**（替换算法套件、参数更新），缺少会话内部的细粒度动态调整机制；部分"组合器（combiner）"方案将多个算法同时使用，带来开销上升且并未有效降低捕获与分析的整体收益。

五、 现有技术的缺点及本申请提案要解决的技术问题

现有技术主要存在以下缺陷与亟需解决的技术问题：

(1) **后量子不确定性下的长期保密缺口：**大量敏感通信可被"现在存储、未来解密（SNDL）"方式长期采集；即便采用单一PQC算法，也可能在未来出现结构性削弱而造成历史通信泄露。

(2) **会话内缺乏细粒度算法切换机制：**多数协议在会话期间固定算法套件，无法按时间片、按数据块甚至按数据包进行动态切换。

(3) **算法相关性风险未被系统性约束：**即便存在"算法轮换"，也可能在同一困难问题类别（如均为格）内切换，无法形成真正的"正交安全"。

(4) **传输捕获面过于集中：**单路径传输使攻击者只需捕获单一链路即可收集足够材料。

(5) **侧信道与实现漏洞的累积暴露：**长期使用同一实现会放大侧信道统计优势。

(6) **现有密码敏捷性的被动性与滞后性：**现有的敏捷机制通常是“发现漏洞-发布补丁-协商升级”的被动响应模式，缺乏在漏洞未知阶段的“主动防御（Moving Target Defense）”能力。

本发明旨在提出一种**动态多原语密码跳频协议（DMHP）**的安全通信系统及方法，使通信在会话内持续进行算法和密钥上下文的微重构，显著降低攻击者对单一算法与单一路径的依赖收益。

六、 本发明技术方案

本发明提供一种动态多原语密码跳频协议（DMHP）的安全通信系统及方法。系统以"类似无线电跳频"的思想为出发点，将**算法选择**与**密钥派生上下文**作为可随时间/序号动态演化的变量，并引入硬问题类别正交约束与可选的多路径分散与阈值分片机制。

6.1 系统总体架构

主要组成包括：

通信节点（DLHP Cognitive Node）：至少包括发送节点与接收节点，用于建立会话、生成跳频计划并对业务数据进行封装/解封装。

协议状态机：至少包括 INITIAL、HANDSHAKING、ACTIVE、TRANSITIONING、SUSPENDED、CLOSED、ERROR 等状态，用于管理会话建立、密钥更新与过渡窗口。

算法库与正交选择器（Orthogonal Algorithm Selector）：存储多种密码算法原语，且每一算法关联硬问题类别元数据（例如结构化格、非结构化格、编码理论、同源/同态类、哈希基等）。选择器依据预定义的"类别距离矩阵"执行选择，使相邻受保护单元尽可能来自不同困难问题类别。

同步与调度模块：支持基于时间（Macro）或基于序号（Nano）两类派生方式，并支持过渡重叠窗口以容忍时钟漂移与网络时延。

可选多路径传输分散模块（MPTD）：在存在多链路（如5G/Wi-Fi/卫星）时，将不同受保护单元映射到不同物理路径，实现空间维度的分散捕获难度提升。

可选全息熵分散模块（HED）：将载荷拆分为(k, n)阈值份额后分别采用不同算法加密，重构需至少k份额。

请参考**图 1**，其展示了DLHP节点的总体架构。

6.2 关键技术流程

6.2.1 会话建立与跳频种子协商

(1) **握手阶段（Handshaking）**：双方节点通过密钥封装机制（KEM）协商会话种子 MasterSecret；支持混合模式（Classical+PQC），例如 ECDH + Kyber；协商算法库标识、正交约束参数（如类别距离下限）、跳频调度模式（时间驱动/序号驱动）等。

(2) **跳频种子派生**：从 MasterSecret 和 SeqID（或时间戳）派生每个受保护单元的$(algorithm_index, per_unit_key_material)$。派生函数采用密钥派生函数（KDF），确保

单调序号下的确定性与无状态性。

6.2.2 无状态派生与乱序容忍

接收端仅需知道 SeqID（从数据包头部或记录号获取），即可独立计算该单元的算法索引与密钥材料，而无需严格依赖前序状态。这使得协议天然支持：

- **丢包容忍**：丢失中间包不影响后续包解密；
- **重传与乱序**：接收端可对任意到达的包独立解密；
- **并行处理**：多核或分布式解密节点可并行处理不同SeqID。

6.2.3 受保护单元（数据包/记录）的最小格式与AAD绑定（建议）

为便于工程实现与后续权利要求撰写，给出每个“受保护单元”（可为数据包、记录或数据块）的最小可实施封装格式示例：

- **明文/可见头部字段（示例）**： SeqID（或时间片TimeSlotID）、可选EpochID、调度模式标识（时间驱动/序号驱动）、算法库/版本标识（可选）、以及用于重放防护的窗口参数标识（可选）。
- **密文载荷**：业务载荷P经由当前跳频选定的算法原语（例如AEAD或“加密+完整性校验”的等价组合）处理得到密文C。
- **AAD绑定建议**：将SeqID（或TimeSlotID）、EpochID（若存在）、调度模式标识与算法集合/版本标识（若存在）作为附加认证数据（AAD）输入，以将密文与上下文绑定，降低重放、降级与篡改风险。

实现边界说明（建议写入交底以便后续权利要求支撑）：

- **防重放与接收窗口**：在允许乱序的同时，接收端可维护基于SeqID的滑动窗口与位图（或Bloom/哈希集合）用于重放检测。窗口大小可根据链路抖动与最大乱序深度配置。
- **SeqID回绕处理**：当SeqID为固定比特宽度（例如32/64位）时，可采用（i）禁止回绕并在接近上限前触发一次会话更新；或（ii）引入EpochID与SeqID组成联合计数器$\langle \text{EpochID}, \text{SeqID} \rangle$，回绕时Epoch自增并重新派生上下文。

- **AEAD/完整性校验：**对每个受保护单元建议使用带认证的加密（AEAD）或等价完整性机制，并将SeqID（或时间片）、模式标识等作为AAD输入，以绑定上下文并降低重放/篡改风险。

6.2.4 正交安全约束与类别距离度量

定义**硬问题类别（Hard Problem Class，HPC）**：例如 {Lattice-Structured, Lattice-Unstructure为每个算法A分配类别$C(A)$。

定义**类别距离**$d(C_1, C_2)$：例如，同一类别距离为0，不同主类别距离为1或更高。

距离矩阵配置示例（Distance Matrix Example）： 为确保正交性，系统维护如下距离矩阵示例（数值代表数学假设的差异度）：

- 格（Lattice） $\leftrightarrow$ 格（Lattice）：$d = 0.2$（同类，低差异）；
- 格（Lattice） $\leftrightarrow$ 编码（Code-based）：$d = 1.0$（完全正交）；
- 格（Lattice） $\leftrightarrow$ 哈希（Hash-based）：$d = 1.0$（完全正交）；
- 结构化格（Structured） $\leftrightarrow$ 非结构化格（Unstructured）：$d = 0.5$（中等差异）。

正交约束：对于相邻受保护单元i与$i+1$，要求

$$d(C(A_i), C(A_{i+1})) \geq d_{\min}$$

从而确保连续单元由不同数学基础保护，降低单一算法突破造成连续失守的风险。

6.2.5 过渡重叠窗口与双解码策略

在算法切换点，为避免时钟不同步或网络抖动导致的解密失败，定义过渡窗口W：

- 发送端在$t \in [T - \delta, T + \delta]$时，可选择旧算法或新算法加密（或同时发送两个版本）；
- 接收端在该窗口内尝试双解码，若一种失败则尝试另一种，从而保证工程可用性。

关于算法标识（algorithm_id）的可选承载方式：

- **明文标识方式：**algorithm_id以明文字段出现，便于快速定位解密算法；为避免泄露过多可区分信息，可对外仅暴露“类别标识/集合标识”，细粒度算法索引通过KDF内部确定。
- **受保护标识方式：**algorithm_id作为受保护元数据随密文一并认证（例如作为AEAD密文的一部分，或以密文头部封装）。接收端可通过“少量候选集试解码”或“类别到算法的确定性映射”实现定位。
- **零显式标识方式：**不显式传algorithm_id，双方仅依赖KDF(MasterSecret, SeqID)得到算法索引。该方式最小化侧信道与可区分特征，但要求收发双方算法库版本严格一致，并对版本迁移做好协商。

6.2.6 可选的全息熵分散（HED）

对载荷P，执行(k, n)秘密分享或纠删码：

$$P \to (S_1, S_2, \ldots, S_n), \quad k \leq n$$

每个分片S_i采用不同算法A_i加密为C_i。只有收集至少k个C_i并解密后才能重构P。

这使得即使攻击者在某一算法或某条路径成功，仍无法单独获取完整载荷。

6.2.7 可选的多路径传输分散（MPTD）

若通信节点具备多个物理接口（如5G蜂窝、Wi-Fi、卫星链路），将不同受保护单元或不同HED分片通过不同路径发送：

- 空间分散：攻击者需同时监控多条链路；
- 算法-路径交叉：例如A_1加密的单元走路径1，A_2加密的单元走路径2，增加捕获难度。

6.2.8 威胁感知与自适应跳频（可选）

集成威胁监测模块，实时收集：

- 网络延迟异常（可能意味着中间人攻击）；
- 错误率飙升（可能意味着算法弱化或侧信道探测）；

- 外部威胁情报（如新发现的算法漏洞）。

根据威胁级别动态调整：

- **跳频频率**：高威胁时缩短单元粒度（如从每100包切换一次改为每10包）；
- **算法权重**：降低可疑算法的选择概率；
- **诱饵流量（Chaffing）**：注入虚假流量增加分析难度。

七、 本发明拟保护的主要创新点

本发明主要包含以下关键创新点与拟保护点：

(1) **会话内多原语动态跳频机制**：在同一会话内，按时间片/数据块/数据包等粒度对加密算法或封装原语进行动态切换，无需频繁重建会话。

(2) **确定性无状态派生与乱序容忍**：以`SeqID`等单调标识作为派生输入，在接收端无需严格依赖前序状态即可计算当前受保护单元的算法与密钥上下文，从而容忍丢包、重传与乱序。

(3) **正交安全约束与距离度量**：定义硬问题类别及距离度量，对相邻受保护单元施加正交约束，降低同类突破造成连续失守的风险。

(4) **过渡重叠窗口与双解码策略**：在切换点提供重叠窗口W，在保证安全性的同时提升工程可用性。

(5) **全息熵分散（HED）的阈值重构机制（可选）**：对载荷进行(k, n)分片并分别采用不同算法保护，显著降低SNDL与单一算法突破的攻击收益。

(6) **多路径传输分散（MPTD）（可选）**：结合多链路或多子流将不同受保护单元分散传输，使攻击者需同时捕获多路径才能重构完整会话数据。

(7) **威胁感知与自适应跳频（可选）**：依据威胁指标动态调整跳频频率、算法权重与诱饵注入策略。

八、 本发明的优点

与现有技术相比，本发明具有以下显著优点：

(1) **显著降低SNDL收益**：通过微碎片化与会话内跳频，将大量历史数据分散到多个算法与多个密钥上下文，削弱"批量采集、统一解密"的性价比。

(2) **面对算法不确定性更具韧性**：即便某一算法族在未来被削弱，也仅影响部分受保护单元，降低系统性失守概率。

(3) **正交安全可配置可验证**：通过硬问题类别标注与距离约束，使"算法多样性"可度量、可执行、可审计。

(4) **工程可用性强**：无状态派生与过渡重叠窗口设计，使协议更适应存在丢包/乱序/抖动的真实网络环境部署。

(5) **可扩展的空间与阈值增强**：多路径分散与阈值分片机制可按场景打开或关闭，在不同成本/安全需求下提供可组合的增强。

九、 本发明可能的实现特征

本发明的实现通常包括以下可观测特征：

- **协议报头与元数据特征**：实现通常需包含算法标识`algorithm_id`、模式标识`mode_id`、序号`SeqID`、跳频索引/时间片等字段（可掩文或受保护的可解析形式），可用于识别跳频行为；
- **会话内算法切换痕迹**：抓包或日志可观察到相邻受保护单元的算法族类别在短时间内反复切换；
- **多路径分散行为（可选）**：多接口并行流量与"路径↔算法类别"映射的关联性；
- **阈值分片重构行为（可选）**：同一业务载荷对应多份额的并行传输、重构阈值与份额标识策略。
- **流量整形特征（可选）**：数据包长度呈现恒定或特定粒度分布（如填充至L_{max}），消除了因不同算法产生的自然密文长度抖动。

补充说明：为降低被动监听者利用明文元数据进行流量分类的能力，协议可选择将`mode_id`、`algorithm_id`、时间片标识等以“受保护元数据”或“隐式派生”方式承载；同时配合接收窗口与AAD绑定，可在允许乱序的前提下实现重放防护。

十、 附图说明

图 1：DLHP 节点总体架构图，展示算法库、正交选择器、同步调度模块、可选MPTD与HED模块的集成关系。

图 2：协议状态机转换图，展示从INITIAL到ACTIVE再到TRANSITIONING等状态的流转与触发条件。

图 3：无状态派生流程示意图，展示如何从(MasterSecret, SeqID)派生($algorithm\_index, per\_unit\_$

图 4：正交约束示例图，展示不同硬问题类别（格/编码/同源）之间的距离矩阵与相邻单元选择约束。

图 5：过渡重叠窗口时序图，展示旧算法与新算法在切换点的并行使用与双解码策略。

图 6（可选）：全息熵分散（HED）流程图，展示载荷分片、不同算法加密、阈值重构过程。

图 7（可选）：多路径传输分散（MPTD）拓扑图，展示不同受保护单元通过不同物理链路传输的空间分散策略。

十一、 具体实施方式

下面结合附图和具体实施例对本发明作进一步详细说明。应当理解，这些实施例仅用于说明本发明而不用于限制本发明的范围。

11.1 实施例1：基于序号的动态跳频通信

某企业内网需在两个数据中心之间建立后量子安全隧道。双方采用本发明的DLHP协议，具体流程如下：

步骤1：握手与种子协商

- 客户端与服务端通过混合KEM（ECDH+Kyber）协商MasterSecret；
- 协商算法库列表：包含 Kyber-512、NTRU-HRSS、Classic McEliece、SPHINCS+等；
- 协商正交约束：相邻单元算法类别距离≥ 1；
- 协商调度模式：基于SeqID派生（Nano模式）。

步骤2：业务数据传输

- 每个数据包携带SeqID（单调递增）；

- 发送端根据KDF(MasterSecret, SeqID)派生(alg_idx, key)，选择对应算法加密载荷；

- 接收端读取SeqID，同样派生(alg_idx, key)，执行解密。

步骤3：正交约束检查

协议栈在选择算法时，检查前一单元的类别C_{prev}，确保$d(C_{prev}, C_{curr}) \geq 1$，若不满足则跳过该算法重新选择。

效果：即使某一算法在未来被攻破，攻击者也仅能解密该算法保护的离散片段，无法连续重构完整会话。

11.2 实施例1a：作为现有协议栈记录层/隧道层的落地方式（示例）

本实施例说明DLHP在工程中的一种嵌入方式，便于后续产品化与权利要求抽象：

- **记录层嵌入（类似TLS/QUIC Record保护单元）：**将“受保护单元”定义为记录（Record）或数据包载荷（Payload）。每个记录携带SeqID（或记录号）作为不可回退的单调计数。发送端对每条记录独立派生(alg_idx, key)并执行AEAD；接收端按记录号乱序解密，并基于窗口防止重放。

- **隧道层嵌入（类似IPsec/自定义隧道封装）：**将IP数据报作为载荷P，外层封装头部携带⟨EpochID, SeqID⟩和可选的受保护元数据。可在链路切换或策略更新时推进Epoch，以实现快速密钥/算法上下文刷新。

通过上述嵌入方式，DLHP既可独立构成安全通道，也可作为现有安全协议的“内层保护模块”使用，从而覆盖更多部署形态。

11.3 实施例2：结合HED的阈值分片

某金融机构传输敏感交易数据，采用$(3, 5)$阈值方案：

- 将每笔交易载荷P分为5个分片$S_1, \ldots, S_5$，任意3个可重构；

- 每个分片采用不同算法加密：S_1用Kyber、S_2用NTRU、S_3用McEliece、S_4用SPHINCS+、S_5用混合；

- 分片通过不同路径发送（如部分走5G、部分走Wi-Fi）。

攻击者即使攻破Kyber并截获路径1的流量，也只能获得S_1，无法单独重构交易内容。

11.4 实施例3：威胁自适应调整

某物联网网关检测到异常延迟与高重传率，触发威胁分析器：

- 跳频频率从每100包提升到每10包；
- 降低可疑算法权重；
- 注入5%诱饵流量。

威胁缓解后恢复正常跳频策略，平衡性能与安全。

十二、 结束语

以上所述仅为本发明的较佳实施例而已，并不用于限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。