中国移动专利申请
检索报告

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
申报单位	研究院
检索人	许达、xudayj@chinamobile.com、+86-13521894156
检索日期	2026.01.26
关联项目	_____（待填写）

与量子计算的关联说明：

本发明面向后量子威胁背景下的长期安全通信需求。量子计算机成熟后可利用Shor算法对RSA/ECC等传统公钥算法造成实质性威胁，同时后量子算法族仍处于持续公开分析演进阶段，存在未来被削弱的可能。本发明提出DMHP动态多原语密码跳频协议，在会话内按时间/序号对不同数学困难问题类别（如格、编码、哈希等）的密码算法与密钥上下文进行跳频，并可选结合多路径传输分散与阈值分片（全息熵分散，HED），以降低“现在存储、未来解密（SNDL）”攻击收益并提升对算法不确定性的韧性。

一、使用的中文与外文检索关键词

中文检索关键词： (1) 密码跳频, 动态算法切换, 密码敏捷 (2) 后量子密码, 抗量子攻击, SNDL（现在存储未来解密） (3) 正交安全, 硬问题类别, 算法多样性约束 (4) 多路径传输分散, MPTCP, QUIC多路 (5) 阈值分片, Shamir秘密共享, 纠删码, 全息熵分散

（补充同义/检索友好词：会话内密钥更新/频繁rekey、记录层/包级重密钥、无状态派生、乱序解密、过渡窗口/密钥回滚窗口、密码多样性/多假设安全、信息分散算法IDA）

外文检索关键词： (1) cryptographic hopping, algorithm rotation, crypto agility (2) post-quantum cryptography, quantum-resistant, store now decrypt later (3) orthogonal security, hard-problem class, algorithm diversity (4) multipath transport dispersion, MPTCP, multipath QUIC (5) threshold splitting, secret sharing, erasure coding

（补充同义/检索友好词：intra-session key update, frequent rekeying, per-record rekey, record layer key update, stateless key derivation, out-of-order decryption, key rollover window, overlap window, cryptographic diversity, multi-assumption security, heterogeneous cryptography, information dispersal algorithm (IDA)）

二、检索策略与检索式示例（可复现说明）

说明：以下为本发明主题的可复现检索策略框架与典型布尔检索式示例，可按实际使用的数据库/平台对字段语法（TI/AB/CL等）做等价替换。

- **检索对象：**专利文献与非专利文献（标准/草案/论文）。
- **检索字段：**标题（TI）、摘要（AB）、权利要求（CL）及全文（FT）分层检索；优先在TI/AB/CL中做主筛。
- **时间范围：**2000–2026（覆盖后量子迁移与现代传输协议演进阶段）。
- **主题分组：**（G1）会话内算法/密钥动态切换；（G2）无状态派生与乱序容忍；（G3）多算法多样性/多假设；（G4）阈值分片/信息分散；（G5）多路径/路径多样性。

英文检索式示例（可组合）：

- (TI/AB/CL: ("crypto agility" OR "algorithm rotation" OR "cipher suite rotation" OR "cryptographic hopping" OR "continuous rekey" OR "frequent rekey" OR "intra-session key update" OR "per-record rekey"))
- AND (TI/AB/CL: (packet OR record OR "sequence number" OR "packet number" OR nonce))
- (TI/AB/CL: ("stateless key derivation" OR "key derivation" AND ("sequence number" OR "packet number") OR "out-of-order" OR "out of order"))
- (TI/AB/CL: ("key rollover" OR "overlap window" OR "grace period" OR "dual decrypt" OR "dual decryption"))
- (TI/AB/CL: ("cryptographic diversity" OR "multi-assumption" OR "heterogeneous cryptography" OR "N-version"))

- (TI/AB/CL: (”secret sharing” OR threshold OR ”information dispersal” OR ”IDA” OR ”erasure coding”))
- (TI/AB/CL: (multipath OR MPTCP OR ”multipath QUIC” OR ”path diversity” OR ”traffic splitting”))

中文检索式示例（可组合）：

- （标题/摘要/权利要求：(”密码敏捷” OR ”算法轮换” OR ”动态算法切换” OR ”会话内密钥更新” OR ”频繁重密钥” OR ”记录层密钥更新” OR ”按包重密钥” OR ”密码跳频”)）
- AND（标题/摘要/权利要求：(序号 OR 记录号 OR 包号 OR nonce OR ”乱序” OR ”无状态” OR ”派生”))
- （标题/摘要/权利要求：(”阈值” OR ”秘密共享” OR ”信息分散” OR ”纠删码”)）
- （标题/摘要/权利要求：(”多路径” OR MPTCP OR QUIC OR ”路径多样性” OR ”分流”)）

三、相关文献条目

编号	相关度类别	文献信息 (标题/来源/作者/日期)
1	A (相关基础)	**RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3** 来源：IETF Standards Track 作者：Rescorla, E. 日期：2018 证据位置：Section 4.1.1 (Cipher Suite Negotiation) - 现有技术中的会话级协商机制
5	A (更贴近：会话内rekey)	**RFC 8446: TLS 1.3 Key Update mechanism**

		来源：IETF Standards Track 作者：Rescorla, E. 日期：2018 证据位置：Section 4.6.3 (Key Update) - 会话期间更新流量密钥（但仍为同一套件体制，非算法跳频）
2	A (相关基础)	**draft-ietf-tls-hybrid-design: Post-Quantum Hybrid TLS** 来源：IETF Draft 作者：Stebila, D. et al. 日期：2024 证据位置：Whole Document - 现有技术中混合后量子算法的静态组合方案
6	Y (更贴近：QUIC记录/包号)	**RFC 9001: Using TLS to Secure QUIC** 来源：IETF Standards Track 作者：Thomson, M., Turner, S. 日期：2021 证据位置：Packet Number/Key Phase相关章节 - 基于包号与密钥阶段的密钥派生与更新（但不涉及跨困难类别的正交约束）
3	Y (相关技术)	**The Spread Spectrum Concept** 来源：IEEE Transactions on Communications 作者：Scholtz, R.A. 日期：1977 证据位置：Abstract & Introduction - 频率跳变通信（FHSS）的基本原理（本发明借鉴思想）

7	Y (更贴近：多路径基础)	**RFC 8684: Multipath TCP (MPTCP) Protocol** 来源：IETF Standards Track 作者：Ford, A. et al. 日期：2020 证据位置：Whole Document - 多路径传输用于可靠性/吞吐（本发明在此基础上引入安全分散联动）
4	Y (相关技术)	**Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure** 来源：John Wiley & Sons 作者：Housley, R. & Polk, T. 日期：2001 证据位置：Chapter on Algorithm Maintenance - 传统的长期算法迁移策略（与本发明动态跳变对比）
8	Y (更贴近：密码敏捷框架)	**RFC 7696: Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms** 来源：IETF Informational 作者：Housley, R., et al. 日期：2015 证据位置：全文（概念与建议）- 讨论算法敏捷的设计原则与MTI算法选择，但未给出会话内细粒度算法跳频/正交约束/无状态派生机制

四、分析评述

（一）本申请方案的必要技术特征拆分（用于对照）

为便于与现有技术逐项比对，将本申请方案的关键必要技术特征拆分如下（编号仅用于检索与评述）：

- **F1 会话内动态跳频：**同一会话内，按时间片/序号/记录号等粒度对密码原语（算法/参数族）进行动态切换。
- **F2 确定性无状态派生：**接收端仅依据SeqID（或时间片）与会话种子即可独立派生当前单元的算法索引与密钥材料，容忍乱序/丢包。
- **F3 正交安全约束：**为算法配置困难问题类别元数据，并对相邻单元施加“类别距离$\geq d_{\min}$”之约束，避免在同一困难类别内循环。
- **F4 过渡重叠窗口：**在切换点提供重叠窗口与双解码策略，以提升工程落地可用性。
- **F5 可选HED阈值分片：**对载荷进行(k,n)阈值分片/纠删码分散，重构需至少k份额。
- **F6 可选MPTD多路径分散：**将不同单元/分片分散至不同物理路径或子流，提高捕获与重构难度。

（二）与主要现有技术方案的对比分析

基于检索到的相关文献（编号1-4），下表总结了现有通用技术路线与本申请方案的对比差异。

对照对象	覆盖特征	差异要点（本申请的技术贡献）
算法协商/密码敏捷（如文献1、5、8）	通常覆盖F1（粗粒度）	现有标准（如TLS 1.3）通常在握手/版本升级阶段确定算法；虽支持Key Update（文献5）实现会话内rekey，但**仍缺少会话内跨算法原语的细粒度跳频**与F3“正交类别距离”约束；F2无状态派生也未必具备。

后量子标准化/迁移（如文献2）	可能覆盖“PQC替换/混合”	往往聚焦“选择某一PQC算法族并替换”，**缺少跨困难类别的动态轮换与可度量约束（F3）**；对SNDL收益削弱通常不以“碎片化跳频+阈值分散”方式实现。
SNDL威胁分析（一般理论）	提供威胁动机	现有研究多为风险分析或建议性结论，**缺少可执行的会话内跳频与分散机制（F1/F5/F6）**以及工程同步策略（F4）。
多路径传输（如MPTCP等文献7）	覆盖F6（传输侧）	多路径协议的核心目标一般为吞吐/可靠性；**缺少与算法跳频/阈值分片联动的“算法-路径交叉分散”**整体框架（F1+F5+F6联动）。

（三）最接近现有技术、差异特征与技术效果（审查口径化表述建议）

1. 最接近现有技术的确定： 从工程实现形态看，文献1与文献5（TLS 1.3及其Key Update机制）与文献6（QUIC采用TLS保护并引入基于包号/密钥阶段的派生与更新）均属于”**在会话期间进行密钥更新/密钥派生**”路线，与本申请的”按序号/时间片驱动的记录/包级保护”较为接近，可作为最接近现有技术族进行对比。

2. 相对于最接近现有技术的主要差异特征： 与上述现有技术相比，本申请至少具有如下差异特征组合（对应前述F1–F4为核心）：

- **差异D1（对应F1）：**在同一会话内进行**跨密码原语/算法族的动态跳频**，而不仅是同一算法套件下的密钥更新；
- **差异D2（对应F2）：**以SeqID（或时间片）为输入，实现**确定性无状态派生**得到“算法索引+每单元密钥材料”，从而天然支持丢包/乱序；
- **差异D3（对应F3）：**引入困难问题类别（HPC）与类别距离约束$\geq d_{\min}$，实现**可度量的正交安全轮换规则**；
- **差异D4（对应F4）：**在切换点提供过渡重叠窗口与双解码策略，以在真实网络抖动/时延条件下保持可用性。

3. 由差异特征产生的技术问题与技术效果：

- 通过D1+D3，将连续数据保护的数学假设基础进行跨类别切换，解决”单一算法/同类数学假设被削弱后导致**连续失守**”的问题，技术效果为：**降低单点突破的连续影响范围**；

- 通过D2，在记录/包级场景中无需依赖严格前序状态即可定位算法与密钥上下文，解决“丢包/乱序条件下会话内频繁更新导致**解密同步困难**”的问题，技术效果为：**提高乱序容忍与并行处理能力**；

- 通过D4，解决“切换点时钟漂移/网络抖动导致**阶段性可用性下降**”的问题，技术效果为：**在不牺牲核心安全策略的前提下提升工程可用性**；

- 上述效果共同作用，降低SNDL攻击的”批量采集、未来统一解密”的价值密度，技术效果为：**提高长期保密的攻击成本与不确定性**。

4. 非显而易见性说明（组合并非简单拼接）：即使现有技术已公开”会话内rekey/密钥更新”（文献5）以及”基于包号/阶段的密钥派生与更新”（文献6），本申请的D1–D4组合仍非显而易见，原因在于：

- 将“算法级跳频”（D1）引入记录/包级保护后，必须与无状态派生（D2）和过渡窗口（D4）共同设计，否则在乱序与重传条件下会出现解密失败率上升、重放检测与密钥更新一致性冲突等工程问题；

- 现有的“算法敏捷”指导（文献8）多为版本级/策略级治理建议，**未给出可度量的困难类别距离约束（D3）**以及与记录/包级无状态派生联动的可执行机制；

- D3的“类别距离$\geq d_{\min}$”使算法多样性从“可配置”提升为“可度量、可审计、可强制执行”的规则体系，属于机制层面的实质改进，而非简单列举多算法。

（四）工程挑战与风险点（审查/落地的防御性说明建议）

为提升本申请文本在审查阶段的可实施性评价，并为后续说明书实施例补充提供依据，建议在检索报告中明确以下工程挑战与对应的防御性设计要点（不改变核心创造性结论，仅用于“可实施性/可信实现”论证）：

- **E1 不同PQC算法的密文尺寸差异与MTU碎片化风险：** 由于算法库可能包含格类、编码类、哈希基等不同PQC原语，其密文/封装输出长度存在显著差异。若按包/记录级跳频，输出包长可能随算法切换发生抖动，带来（i）网络层MTU碎片

化、额外重传与性能下降；（ii）攻击者通过包长度统计推断当前算法类别的**侧信道**风险。 **防御性建议：**在具体实施方式中引入**流量整形/自适应填充**模块：设定目标传输单元长度L_{target}（可取算法库中最大输出长度加冗余量），对短密文追加随机填充，使链路层观测到的包长呈现恒定或伪随机分布，从而同时减轻碎片化与"算法指纹"泄露。

- **E4 接收端状态同步与DoS攻击风险：** 虽然F2采用无状态派生，但若攻击者注入大量无效大序号包，可能诱发接收端执行高消耗的PQC解密。 **防御性建议：**引入**低成本预过滤机制：**在PQC解密前，基于轻量级对称MAC或Bloom Filter对SeqID的有效性及窗口范围进行预校验，快速丢弃非法流量，保护接收端计算资源。

- **E2 会话主密钥（MasterSecret）的前向安全性（PFS）与回溯风险：** 若会话期间MasterSecret保持静态，则在攻击者于时刻T获取会话主密钥的极端场景下，可能存在对历史数据的回溯解密风险（取决于派生链路与实现细节）。 **防御性建议：**在实现例中加入**棘轮/迭代更新**机制：每隔N个受保护单元或每个时间周期，执行$\text{MasterSecret}_{i+1} = \text{KDF}(\text{MasterSecret}_i, \text{"}ratchet\text{"})$并安全擦除旧值。该机制与F2无状态派生可并存：接收端在可配置窗口内保留少量近邻状态（例如最近w个棘轮点的种子）用于追赶与乱序容忍。

- **E3 算法库协商、实现体积与启动时延：** 若算法库覆盖多个困难问题类别，移动端/IoT设备可能面临代码体积、内存与初始化开销。 **防御性建议：**可将算法库拆分为"必选最小集（MTI-like）+可选扩展集"，握手阶段协商可用集合ID；并允许以"类别级"协商（仅协商HPC类别与版本）降低协商长度，具体算法索引由KDF在集合内部确定。

1. 与"算法协商与密码敏捷"相关公开资料的对比： 传统协议通常在握手阶段确定并锁定单一（或少量）算法套件，在会话期间长时间复用。其弱点在于算法与实现风险集中、容易被SNDL批量采集并等待未来突破。本发明的DLHP在会话内细粒度跳频，降低任一算法长期暴露的价值，且可在不重建会话的前提下完成动态切换。

2. 与"后量子标准化与单算法迁移"相关公开资料的对比： 单一PQC算法替换可提升抗量子能力，但无法消除算法族在未来被削弱的不确定性。本发明通过"硬问题类别正交约束"，在结构化格、编码理论、哈希基等类别间切换，形成可度量的多样性防线。

3. 与SNDL威胁分析相关公开资料的对比： SNDL核心在于长期保存密文等待未来大规模算力/新攻击。本发明通过微碎片化（按包/按块/按分片）减少单一算法保护

的连续数据规模，并可选通过阈值分片（HED）将重构门槛提升为“至少解出k个份额”。

4. 与多路径传输协议相关公开资料的对比： 多路径协议通常解决吞吐/可靠性或抗链路故障问题。本发明将多路径与算法跳频结合，形成“空间正交”：攻击者需要同时捕获多条物理路径并跨多个算法类别破译，显著提高完整会话重构难度。

五、检索结论

基于当前对包括RFC标准、IETF草案及经典扩频理论等文献的初步检索与分析，结论如下：

未发现单一公开文本同时覆盖本申请的“会话内动态跳频（F1）”、“确定性无状态派生（F2）”、“正交安全约束（F3）”与“过渡重叠窗口（F4）”等核心特征。

现有技术主要存在以下局限：

- 握手阶段算法协商/迁移（密码敏捷），但缺少会话内细粒度跳频与工程可用的过渡机制（F1/F4）；
- 基于单一PQC算法族的替换或混合，但缺少跨困难类别的“正交安全约束”与可度量的多样性策略（F3）；
- 多路径传输以性能/可靠性为主，缺少与算法跳频及阈值分片联动的安全分散框架（F6与F1/F5联动）。

综上所述，本申请提出的DMHP协议在会话内细粒度跳频、正交安全约束及无状态容错机制等方面具有实质性的改进，具备较好的新颖性与创造性前景。进一步地，从工程实现与安全机制耦合角度看：

- **F2（无状态派生/乱序容忍）与F4（过渡重叠窗口/双解码）并非简单拼接：**其需要在允许乱序和重传的网络条件下同时满足解密成功率、重放检测与密钥更新一致性，属于记录层/包级密钥更新的工程约束体系；
- **F3（困难问题类别距离约束）区别于一般“支持多算法/可配置”的密码敏捷：**本申请提供可度量的“类别距离$\geq d_{\min}$”选择规则，使连续受保护单元跨数学假设类别进行轮换，从而降低同类突破造成连续失守的风险。

建议：后续审查中可围绕“会话内频繁rekey/记录层动态切换/阈值分片重构/多路径安全传输结合”等主题进一步扩展检索，以排除相关性较低的组合干扰。