

Mathematical Security Proofs for Dynamic Multi-Primitive Cryptographic Hopping Protocol (DMP-CHP) (also referred to as DLHP)

Technical Specification Supplement

January 26, 2026

Abstract

This document provides formal mathematical arguments supporting the security goals of the Dynamic Multi-Primitive Cryptographic Hopping Protocol (DMP-CHP), also referred to herein as DLHP, focusing on (i) Holographic Entropy Dispersion (HED), (ii) orthogonal security under poly-algorithmic encryption, and (iii) unpredictability of the hopping schedule.

1 Holographic Entropy Dispersion (HED)

1.1 Preliminaries

Let \mathcal{M} be the message space and \mathcal{S} be the share space. The system utilizes a (k, n) threshold secret sharing scheme (e.g., Shamir's Secret Sharing over a finite field \mathbb{F}_q).

Definition 1 (Holographic Fragmentation). *A message $m \in \mathcal{M}$ is divided into n shares $\{s_1, s_2, \dots, s_n\}$ such that:*

1. **Reconstruction:** Any subset of k shares can reconstruct m .

2. **Secrecy:** Any subset of fewer than k shares reveals no information about m .

Each share s_i is subsequently encrypted using a distinct cryptographic algorithm $\mathcal{E}_i \in \Lambda$, where Λ is the Orthogonality Library.

1.2 Information-Theoretic Security Proof

Theorem 1 (Perfect Secrecy of Sub-Threshold Fragments). *Let S be the random variable representing the secret message and let $V_T = \{s_{i_1}, s_{i_2}, \dots, s_{i_t}\}$ be a set of $t < k$ shares intercepted by an adversary. Then:*

$$H(S | V_T) = H(S)$$

where $H(\cdot)$ denotes Shannon entropy.

Proof. Consider Shamir's scheme where the secret $S = a_0$ is the constant term of a random polynomial $P(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1}$ of degree $k - 1$ over \mathbb{F}_q , with coefficients a_1, \dots, a_{k-1} chosen uniformly at random.

A set of t shares corresponds to t points (x_j, y_j) where $y_j = P(x_j)$. For any candidate secret $s' \in \mathbb{F}_q$ and any set of $t < k$ shares, there exists a unique polynomial $P'(x)$ of degree $k - 1$ such that $P'(0) = s'$ and $P'(x_j) = y_j$ for all $j \in \{1, \dots, t\}$.

Since the remaining $k - 1 - t$ coefficients are free variables, there are exactly q^{k-1-t} polynomials consistent with the shares and the candidate secret. This count is independent of the value of s' . Therefore, for any observation of $t < k$ shares, every possible secret s' is equally likely.

$$\Pr[S = s | V_T = v] = \Pr[S = s]$$

$$H(S | V_T) = H(S)$$

Thus, the shares provide zero mutual information about the secret S . □

2 Orthogonal Security Analysis

2.1 Assumptions

Let $\Lambda = \{\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_N\}$ be a set of cryptographic algorithms. We define $\text{Hard}(\mathcal{A}_i)$ as the underlying mathematical problem for algorithm \mathcal{A}_i (e.g., SIS, LWE, MQ, Code-Decoding).

Definition 2 (ϵ -Orthogonality (advantage form)). *Two algorithms \mathcal{A}_i and \mathcal{A}_j are ϵ -orthogonal if access to efficient auxiliary information or solver capabilities for $\text{Hard}(\mathcal{A}_i)$ does not increase a polynomial-time adversary's advantage in solving $\text{Hard}(\mathcal{A}_j)$ by more than ϵ . Formally, for any PPT adversary \mathcal{B} ,*

$$\text{Adv}_{\mathcal{B}}(\text{Hard}(\mathcal{A}_j) \mid \text{Aux}_{\mathcal{A}_i}) \leq \text{Adv}_{\mathcal{B}}(\text{Hard}(\mathcal{A}_j)) + \epsilon,$$

where ϵ is negligible in the security parameter and $\text{Aux}_{\mathcal{A}_i}$ denotes auxiliary information derivable from running efficient solvers or side-information about $\text{Hard}(\mathcal{A}_i)$.

2.2 Joint Security of Holographic Session

Theorem 2 (Composite Hardness). *For a (k, n) HED session, let E_i be the event that an adversary successfully breaks algorithm \mathcal{A}_i . Assuming ϵ -orthogonality between all pairs in Λ , the probability of compromising the payload $P_{\text{compromise}}$ is:*

$$P_{\text{compromise}} \leq \sum_{\substack{T \subseteq \{1, \dots, n\} \\ |T|=k}} \left(\prod_{j \in T} \Pr[E_j] \right) + \delta$$

where δ is a negligible term representing higher-order correlations.

Proof. To recover the payload, the adversary must obtain k valid shares. Let S_i be the share protected by \mathcal{A}_i . Recovering S_i requires event E_i . The adversary succeeds if they break any subset of k algorithms.

Under the assumption of pairwise ϵ -orthogonality (as defined above), the dependence between events E_i and E_j is bounded: knowledge or solver capabilities for one gives at most negligible extra advantage for the other, up to ϵ terms. We therefore treat the joint success probability for a chosen subset T of size k as approximately the product of individual success probabilities, with a small residual term capturing higher-order correlations.

Let $p_i = \Pr[E_i]$. Then, for any subset T of size k an upper bound on the adversary's success probability is:

$$\Pr \left[\bigcap_{j \in T} E_j \right] \leq \prod_{j \in T} p_j + \delta_T,$$

where δ_T captures higher-order correlations and is expected negligible when ϵ is negligible. Summing over all $\binom{n}{k}$ subsets yields the composite bound in the theorem statement, with the global residual denoted δ .

If $p_i \approx 2^{-\lambda}$ for all i , the dominant term scales like $2^{-k\lambda}$, i.e., the effective security parameter grows approximately linearly with k under the independence approximation.

The bound is conservative: if algorithms share substantial structure (e.g., all lattice-based with correlated parameters), ϵ and δ may be non-negligible, and the product approximation would no longer hold. Thus orthogonality and diversity in hard problems are essential to the claimed scaling. \square

3 Hopping Schedule Unpredictability

3.1 Schedule Generation

The schedule is generated via a function $F(K, t, \eta)$, where K is a master secret (e.g., K_{session}), t is the time/index (or packet sequence identifier), and η is auxiliary entropy.

Definition 3 (PUF-Bound PRF). *Let $PUF(c)$ be a physical unclonable function response to challenge c . The hopping key is $K_{\text{hop}} = HKDF(K_{\text{session}}, PUF(\text{nonce}))$. The schedule at step i is $A_i = \mathcal{H}(K_{\text{hop}} \parallel i) \bmod |\Lambda|$.*

Theorem 3 (Future Unpredictability). *If $PUF(\cdot)$ has min-entropy γ and \mathcal{H} is modeled as a Random Oracle, then for an adversary \mathcal{B} with view of previous algorithms $\{A_0, \dots, A_{t-1}\}$ but without physical access to the device:*

$$\Pr[\mathcal{B} \text{ predicts } A_t] \leq \frac{1}{|\Lambda|} + negl(\lambda)$$

Proof. The output A_i depends on K_{hop} . Access to $\{A_0, \dots, A_{t-1}\}$ gives information about K_{hop} only if \mathcal{H} can be inverted. Even if K_{session} is compromised (e.g., memory dump), K_{hop} remains unknown because $PUF(\text{nonce})$ cannot be computed without the physical hardware instance. Assuming the PUF response has sufficient entropy γ , the conditional entropy $H(K_{\text{hop}} | K_{\text{session}}) \approx \gamma$. Therefore, the sequence $\{A_i\}$ remains pseudo-random to any observer lacking the physical device. \square

4 Federated Mutation Function

The schedule mutation rule is defined as:

$$S_{t+1} = \mathcal{G}(S_t, \theta_{\text{threat}}, \mathcal{E}_{\text{env}})$$

where \mathcal{G} is the evolution function derived from the Federated Reinforcement Learning agent.

Let the loss function for the RL agent be:

$$\mathcal{L}(\pi) = \mathbb{E}_{\tau \sim \pi} \left[\sum_{t=0}^T \gamma^t (R_{\text{security}}(s_t, a_t) - \lambda C_{\text{bandwidth}}(s_t, a_t)) \right]$$

By optimizing this objective across M nodes without sharing raw trajectories τ , the system converges to a global policy π^* that maximizes security while minimizing bandwidth overhead.