EchoPulse Private & Public Path Structure

1. Key Representation

In the EchoPulse Key Encapsulation Mechanism (KEM), both the private key (SK) and the public key (PK) are not represented as algebraic elements within a mathematical structure, but rather as ordered sequences of abstract symbols drawn from the finite symbol set $\Sigma=\{s0,s1,...,s255\}$. The private key SK is a sequence of l symbols, denoted as $SK=(\sigma1,\sigma2,...,\sigma l)$, and the public key PK is a sequence of l′ symbols, denoted as $PK=(\sigma1',\sigma2',...,\sigma l'')$. Both the private and public key paths originate from a common, fixed initial state $v0\in V$ within the state transition graph $G(V,E)$.

2. Private Path (SK)

The private key SK is a secret sequence of l symbols from Σ. When these symbols are applied sequentially as inputs to the transition function δ, starting from the initial state v0, they deterministically lead to a specific private state $vpriv\in V$:

$vpriv=\delta(\delta(...\delta(v0,\sigma1),\sigma2)...,\sigma l)$

The private key sequence SK must be chosen randomly from the space of all possible symbol sequences of length l, or it can be derived deterministically from a high-entropy master secret using a cryptographically secure key derivation function. The length l of the private key sequence is a security parameter and must be chosen such that the number of possible private paths is sufficiently large to resist brute-force attacks. Based on the path entropy model outlined in the "EchoPulse Key Derivation Model" specification, l should be at least 25 symbols to approach a 128-bit security level, considering the out-degree of the graph.

3. Public Path (PK)

The public key PK is a sequence of l′ symbols from Σ that, when applied sequentially as transitions starting from the same initial state v0, leads to a public state $vpub\in V$:

$vpub=\delta(\delta(...\delta(v0,\sigma1'),\sigma2')...,\sigma l'')$

The public key PK can be derived deterministically from the private key SK or generated independently from a separate public seed. If derived from SK, the derivation process must be a one-way function, ensuring that it is computationally infeasible to recover SK from PK. This derivation could involve pseudorandom expansion or a compression technique applied to SK followed by a deterministic transformation to generate a distinct symbol sequence PK of length l′. Alternatively, PK can be generated directly from a public seed using a deterministic algorithm that traverses the state graph from v0 to vpub. The length l′ of the public key sequence may differ from the length l of the private key sequence, depending on the chosen derivation method and optimization goals. Regardless of the derivation method, the mapping from the initial state v0 to the public state vpub via PK must be deterministic.

4. Security Separation

A crucial security requirement of the EchoPulse KEM is the unlinkability of the private key SK and the public key PK to any unauthorized party. Even if the method of deriving PK from SK is known, it must be computationally infeasible to reverse this process and recover SK given PK. This one-way property is essential to maintain the secrecy of the private key.

Furthermore, collisions in the public state vpub (i.e., different public key sequences leading to the same vpub) should not compromise the security of the private key path or the final shared secret. The design of the graph and the key derivation process should ensure that knowledge of vpub does not significantly reduce the entropy of the possible private key sequences leading to vpriv. The public exposure of PK should not reveal any substantial information about the sequence of symbols constituting SK.

5. Key Encoding Format

The private key SK, being a sequence of l symbols from Σ, can be directly encoded as an array of l bytes, where each byte represents a symbol. This straightforward encoding facilitates efficient storage and processing.

The public key PK, depending on its derivation, can be encoded in several ways. If it is a direct sequence of l′ symbols, it can also be stored as an array of l′ bytes. Alternatively, if PK is derived from a public seed and a deterministic derivation rule, the public key could be represented by the seed and a concise description of the derivation algorithm, potentially leading to a smaller encoded size. Compression techniques could also be applied to the symbol sequence of PK if storage size is a critical constraint.

The chosen encoding format for SK and PK has implications for their export, integration into hardware security modules, and use within cryptographic certificates. Standardized encoding formats would be necessary for interoperability.

6. Conclusion

The private key SK and the public key PK in the EchoPulse KEM are fundamentally represented as sequences of abstract symbols that define deterministic paths within the state transition graph, originating from a common initial state. The private key leads to a secret state, while the public key leads to a publicly known state. A secure derivation process ensures that the public key does not reveal information about the private key. The symbolic nature of the keys and the path-based structure contribute to the post-quantum security rationale of the scheme, while the encoding formats are designed for efficient storage and transmission.

Version 1.0 — Key Format & Symbolic Path Layer — EchoPulse Initiative