IPSECME
Internet-Draft
Intended status: Standards Track
Expires: 31 August 2026

J. Li
M. Li
China Mobile

27 February 2026

Multi-Path Secret Sharing for QKD Key Relay in IP Networks
draft-li-ipsecme-qkd-multipath-secret-sharing-01

Abstract

Trusted relay is currently the most practical deployment model for Quantum Key Distribution (QKD) networks. However, trusted relay nodes pose inherent security vulnerabilities, as intermediate nodes can access the plaintext random number used to derive the end-to-end QKD key, leading to complete key exposure if any single relay node is compromised. To mitigate this risk, this document proposes a Multi-Path Secret Sharing (MPSS) mechanism for QKD key relay. The core idea is to split the random number into multiple shares using a threshold secret sharing scheme, distribute each share through independent QKD relay paths planned by the Key Management Plane (KMP), and reconstruct the complete random number only at the destination node. This mechanism transforms the security model from "all-or-nothing" to "threshold security". Notably, this mechanism leverages an extended IPv6 Destination Option Header (DOH) to carry key share-related metadata and utilizes Segment Routing over IPv6 (SRv6) to enforce strict path isolation.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 31 August 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

The integration of Quantum Key Distribution (QKD) with classical IP networks, specifically for securing IPsec tunnels, is an active area of standardization within the IETF.

However, a critical challenge remains in large-scale QKD networks: the reliance on Trusted Relay Nodes. In current deployments, if a QKD link exceeds the physical distance limit, keys are decrypted, stored, and re-encrypted at intermediate nodes. If any single trusted node is compromised (physically or logically), the end-to-end secrecy of the key is completely broken. Taking an operational "QKD

trunk line" as an example, 32 trusted relay nodes are distributed along a 2,000-kilometer path, and an attacker only needs to breach one node to undermine the end-to-end security of QKD.

This document proposes a Multi-Path Secret Sharing (MPSS) scheme to address this vulnerability. Instead of transmitting the raw key through a single path of trusted nodes, the scheme adopts a (t, n)-threshold secret sharing mechanism, splits the key material into n shares, and utilizes the physical isolation capability of network forwarding paths provided by Segment Routing over IPv6 (SRv6) [RFC8754] to transmit the shares simultaneously over n physically disjoint paths. The original key can only be reconstructed if the receiver successfully obtains at least t shares, ensuring that even if fewer than t nodes are compromised, the attacker cannot obtain any valid information about the key.

This mechanism can serve as a security enhancement layer for the QKD-IPsec integration architecture, effectively defending against insider threats and node compromise risks in the relay network. The scheme is designed to be compatible with the key management interfaces defined in [I-D.nagayama-ipsecme-ipsec-with-qkd] and supports various secret sharing algorithms.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997) and [RFC8174] (Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017).

1.2. Terminology

* QKD: Quantum Key Distribution.

* Trusted Node (TN): An intermediate node in a QKD network that temporarily holds the key material in plaintext during the relay process.

* Threshold Secret Sharing Scheme (SSS): A cryptographic method for distributing a secret among a group of participants, where the secret can only be reconstructed when a specific threshold number of shares are combined. Examples include Shamir’s Secret Sharing and Blakley’s scheme.

* (t, n)-Threshold Scheme: A scheme where the secret can be reconstructed only if at least t out of n shares are combined.

* SRv6: Segment Routing over IPv6.

* KMP: Key Management Plane, the logical entity responsible for coordinating QKD key generation, distribution, path calculation, and SRv6 policy enforcement.

* Disjoint Paths: Network paths that do not share any common intermediate nodes (node-disjoint) or links (link-disjoint).

* QKD-DOH: A proposed IPv6 Destination Option Header extension for carrying QKD share metadata.

2. Motivation

In traditional QKD relay networks, the security model assumes that all intermediate nodes are fully trusted. The key flow is typically: Alice --(QKD)--> TN_1 --(Classical)--> TN_2 --(...)--> Bob

If an attacker compromises TN_i, they can access the plaintext key material being relayed. As the network scales, the probability of at least one node being compromised increases, creating a significant bottleneck for high-security applications.

3. Proposed Architecture: MPSS over SRv6

3.1. Key Splitting and Share Generation

Upon generation of a QKD key seed R at the source node, the KMP invokes a Threshold Secret Sharing algorithm.

* Input: Seed R, Threshold t, Total Shares n, Algorithm Identifier.

* Output: Set of shares S_1, S_2, S_n.

* Property: Any subset of shares with size < t provides no information about R.

3.2. Multi-Path Enforcement via SRv6

To ensure that the compromise of intermediate nodes does not lead to key leakage, the n shares shall be forwarded through disjoint paths as much as possible. This document leveragesSRv6 to explicitly encode these paths in the packet header.

The source node constructs n IPv6 packets, each carrying one share S_i, and encapsulates information such as the sharing algorithm and share sequence number into the DOH header. Each share S_i is mapped to a different SRv6 Policy through the information in the DOH header. By utilizing the SRv6 Policy mechanism, the source can ensure:

1. No two paths share a common intermediate Trusted Node

2. Minimizing latency differences to facilitate timely reconstruction

3. Comprehensively considering parameters such as the link quality and trust level of quantum links

3.3. Key Reconstruction at the Destination

The destination node collects the incoming shares. Once t valid shares are received, the KMP reconstructs the original seed R using the corresponding inverse algorithm. The reconstructed seed is then processed to generate the final key, which is used for IPsec/IKEv2 as defined in [RFC8784] and [I-D.nagayama-ipsecme-ipsec-with-qkd].

4. Protocol Details

4.1. IPv6 Destination Option for QKD Metadata (QKD-DOH)

To carry necessary metadata without modifying the upper-layer protocol, this document defines a new IPv6 Destination Option, which is used to map SRv6 Policies and enable the receiver to identify the sharing algorithm and parameters required for reconstruction.

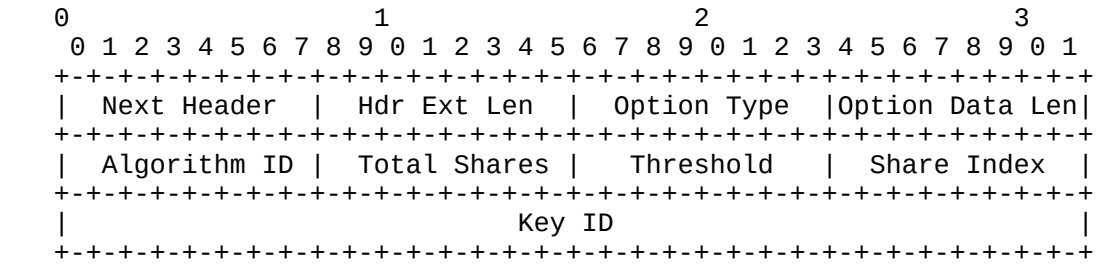

Figure 1: QKD-DOH

* Option Type: To be assigned by IANA (TBD)

* Option Data Format:

  - Key ID (4 bytes): Identifies the QKD session

- Share Index (1 byte): Indicates which share (1…n) this packet carries

- Total Shares (1 byte): Value n

- Threshold (1 byte): Value t

- Algorithm ID (1 byte): Identifies the secret sharing algorithm used (e.g., 0x01 for Shamir, 0x02 for Blakley, etc.), ensuring extensibility

This option is primarily processed by the source node and the destination node.

4.2. Integration with Key Management Plane (KMP)

The MPSS mechanism is transparent to the IPsec stack. The KMP interacts with the following modules:

1. QKD Quantum Layer: To fetch raw key seeds

2. SDN Controller/PCE: To compute n disjoint paths and generate SIDs

3. Application Layer (IPsec/IKE Daemon): To deliver the reconstructed key for use as a PPK, in accordance with [RFC8784]

The KMP is responsible for synchronizing the state of share transmission, negotiating the Algorithm ID during session setup, and triggering retransmission if fewer than t shares arrive within a timeout window.

5. Security Analysis

5.1. Traditional Single-Path Model

The random number R is transmitted through a single path, and any compromised intermediate node can obtain the plaintext R, leading to the complete exposure of Key_AB. The security risk is 1/N_node (N_node is the number of intermediate nodes in the path), and the attack success rate is 100% for a single node compromise.

5.2. MPSS Mechanism

R is split into N shares through (k, N) threshold secret sharing, and each share is transmitted through a completely non-overlapping path. An attacker needs to compromise at least k paths (i.e., at least one node in each of k paths) to obtain k valid shares and reconstruct R. The security improvement is reflected in two aspects:

* Threshold Security: The attack threshold is raised from "compromise 1 node" to "compromise k paths (at least k nodes)". For (2,3) configuration, the attacker needs to compromise at least 2 non-overlapping paths (2 nodes) to reconstruct R, and the attack success rate is significantly reduced.

* Isolation of Shares: Since the paths are completely non-overlapping, compromising a single node only exposes a single share, and the attacker cannot obtain any information about R from a single share (due to the perfect secrecy of the threshold secret sharing algorithm).

5.3. Quantitative Analysis

Assume that the probability of a single QKD node being compromised is P, and the MPSS mechanism uses (k, N) threshold sharing with completely non-overlapping paths (each path has m intermediate nodes). The probability of the attacker successfully reconstructing R is:

* $P_{MPSS} = C_N^k * (P^m)^k$

For the traditional single-path model (1 path, m nodes), the probability of successful attack is:

* $P_{Traditional} = 1 - (1-P)^m$

Example: If P=0.01 (1% compromise probability per node), m=3 (3 intermediate nodes per path), (k=2, N=3) for MPSS:

* $P_{MPSS} = C_3^2 * (0.01^3)^2 = 3 * 10^(-12)$

* $P_{Traditional} = 1 - (1-0.01)^3$ 0.0297

The attack success probability of MPSS is reduced by 9 orders of magnitude compared with the traditional model, which significantly improves security.

6. IANA Considerations

This document requests IANA to assign: 1. A new IPv6 Destination Option type under the "IPv6 Extension Header Types" registry for the QKD-DOH defined in Section 5.1. 2. A new "QKD Secret Sharing Algorithm IDs" registry to manage the Algorithm ID field, initially populated with: - 0x01: Shamir’s Secret Sharing - 0x02: Blakley’s Scheme - 0x03-0xFF: Unassigned / Experimental # Security Considerations TBD.

Acknowledgments

The authors would like to thank the following for their valuable contributions of this document: TBD

Normative References

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/rfc/rfc8200>.

[RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/rfc/rfc8754>.

[RFC8784] Fluhrer, S., Kampanakis, P., McGrew, D., and V. Smyslov, "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security", RFC 8784, DOI 10.17487/RFC8784, June 2020, <https://www.rfc-editor.org/rfc/rfc8784>.

[RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <https://www.rfc-editor.org/rfc/rfc8986>.

Authors' Addresses

Jinming Li
China Mobile
Email: lijinming1836@163.com

MengMeng Li
China Mobile
Email: limengmeng@chinamobile.com