

The PEACE Protocol¹

A protocol for decentralized encrypted data exchange.

Logical Mechanism LLC²

October 22, 2025

¹This project was funded in Fund 14 of Project Catalyst.

²Contact: support@logicalmechanism.io

Contents

1	Abstract	1
	Bibliography	1

1 Abstract

Test Citation [1]

Inline sanity: let $x \in \mathbb{Z}_q$, $u \in \mathbf{G}_1$, $Q \in \mathbf{G}_2$, and $E = mc^2$.

$$c = \text{AEAD}_k(m; \text{nonce}, \text{ad}). \quad (1.1)$$

As in (1.1), we encrypt with key k derived via HKDF:

$$\begin{aligned} \text{ikm} &= H(\text{ECDH}(u, \text{pk}_B)), \\ k &= \text{HKDF}(\text{salt}, \text{ikm}, \text{“PEACE-AES-GCM”, } 32). \end{aligned} \quad (1.2)$$

$$\text{Dec}_k(c) = \begin{cases} m, & \text{if } \text{AEAD_Dec}_k(c; \text{nonce}, \text{ad}) \text{ verifies,} \\ \perp, & \text{otherwise.} \end{cases}$$

$$M = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \|u\|_2 \leq 1, \quad \Pr[\text{forge}] \leq 2^{-\lambda}.$$

$$S(n) = \sum_{i=1}^n i = \frac{n(n+1)}{2}, \quad \int_0^1 x^2 dx = \frac{1}{3}.$$

Bibliography

- [1] C.-P. Schnorr, “Efficient signature generation by smart cards,” *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, 1991, doi: [10.1007/BF00196725](https://doi.org/10.1007/BF00196725).