The PEACE Protocol[1]

A protocol for decentralized encrypted data exchange.

Logical Mechanism LLC[2]

October 20, 2025

[1]This project was funded in Fund 14 of Project Catalyst.
[2]Contact: support@logicalmechanism.io

Contents

1 Abstract

Test Citation [1]

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

$$c \;=\; \mathrm{AEAD}_k(m;\ \mathsf{nonce},\ \mathsf{ad}). \tag{1.1}$$

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

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

$$\mathrm{Dec}_k(c) \;=\; \begin{cases} m, & \text{if AEAD\_Dec}_k(c;\ \mathsf{nonce},\ \mathsf{ad}) \text{ verifies},\\ \bot, & \text{otherwise.} \end{cases}$$

$$M \;=\; \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \|u\|_2 \le 1, \qquad \Pr[\mathrm{forge}] \le 2^{-\lambda}.$$

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

Bibliography

[1] C.-P. Schnorr, “Efficient signature generation by smart cards,” in *Journal of cryptology*, 1991, pp. 161–174. doi: 10.1007/BF00196725.