INTEGRATION OF POST-QUANTUM CRYPTOGRAPHY ALGORITHMS INTO HIGH-LEVEL PROTOCOLS

Interested?
Contact us NOW!
horizon2025@rosenpass.eu

Topic of the project

Our project focuses on post-quantum migration using protocol-level combiners.

We focus on three major project components:

- **Hybridization of existing applications and protocols** using Rosenpass key exchange.
- Adding capabilites such as **single-sided authentication**, using a **password-authenticated key exchange**, and **0-RTT** using advanced cryptography.
- Building an **engineering-focused** infrastructure for **formal verification** of cryptographic protocols using the Domino protocol verifier by Chris Brzuska.

Panels:

Fundamental **Research** Panel	Ethics & **Social** Impact Panel	Translation & **Business** Impact Panel

Call for integration partners (open source and industry) and panelists

We invite **major partners** to join our team, who are seeking **hybridization of their applications, protocols, standards, or products** using a **protocol-level combiner approach** through integration with the Rosenpass protocol.

We are also looking for **minor partners** interested in joining our **accompanying panels**. These panels will come together **once or twice per year** to act in an **advisory capacity.**

All results are meant to be published as open source, open science, or open standards.

We'd be happy to find potential partners **preferably** (but not exclusively) **from Southern and Eastern Europe**

with a particular interest in

- **open-source** and/or **open-science**
- positive, human-centered **social impact**
- serving **marginalized peoples** and **communities**

Scientific & Technical Leadership Team

Chris Brzuska
Aalto University

Tibor Jager
Wuppertal University

Karolin Varner
Rosenpass e.V.

Conceptual Approach

Vertical integration

Bringing together all relevant stakeholders (protocol designers, pen-and-paper cryptographic analysts, cryptography engineers, technological integrators/product builders, users) into **one comprehensive action team**

Fearless Cryptography

Building **engineering-focused proof assistants** for cryptographic protocols to enable agile, **continuous development** of cryptographic protocols

Protocol-level combiners

Post-quantum hybridization on the protocol level to provide **highly reusable protocol components**. Allowing third-party vendors to hybridize using their own key-exchange implementations for **improved crypto agility**

You can find the call for „Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols" in the **EU Funding & Tenders Portal**

Contact us at:
horizon2025@rosenpass.eu