Baltazar Wallet: Secure Password Authentication on Web3 via OPAQUE

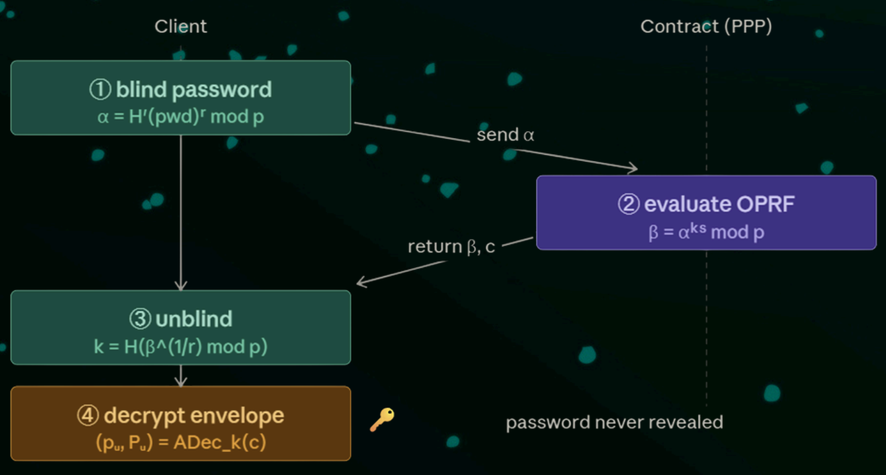
Author: Tomáš Krajčí Year: 2025 Supervisor: doc. Ing. Ivan Homoliak, Ph.D. Consultant: Ing. Samuel Olekšák

1. The Problem:

Passwords are a universal authentication method used worldwide across every digital service. Yet Web3 wallets force users to manage raw private keys or seed phrases, while hardware wallets require dedicated devices. Both are unfriendly towards new users. Public blockchains expose all state and impose no rate limit, making offline brute-force attacks against password-derived keys trivial. Our goal is to make Web3 wallets more usable for ordinary Web2 users while preserving security.

2. The Background / OPAQUE OPRF:

OPAQUE is a modern asymmetric Password-Authenticated Key Exchange (PAKE).
The server never learns the password, even if its storage is compromised.
Offline guessing is impossible.



3. The Idea:

4. The Architecture:

Balthazar consists of three components. The Client blinds the password locally; it never leaves the device. The Relay verifies the user's email identity and sponsors gas, so no prior cryptocurrency is needed, but it is fully untrusted and sees only the blinded input. The PPP Smart Contract, running in an Intel SGX enclave on Oasis Sapphire, holds the secret OPRF key, evaluates the blinded request, and returns the encrypted envelope; all computations remain confidential within the TEE.

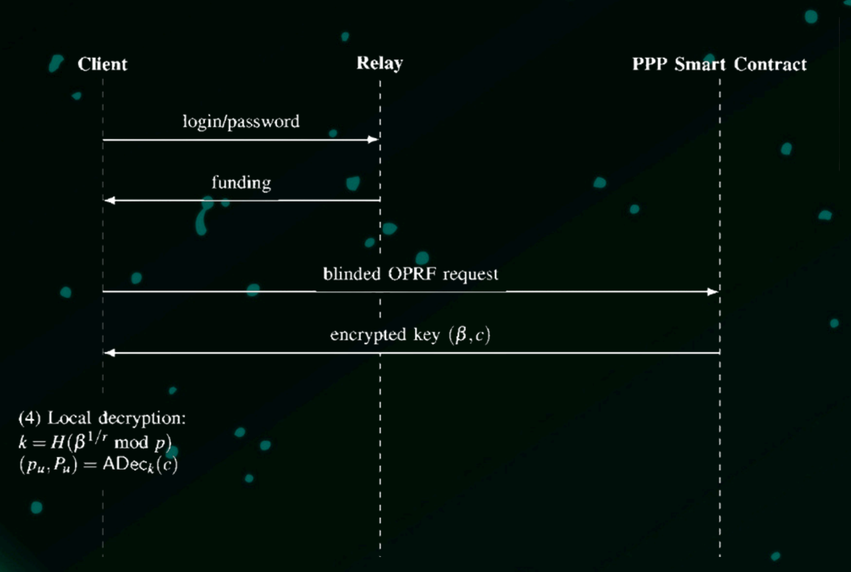


Fig. 1: System overview.
The client authenticates using a login and password.
The relay funds the ephemeral wallet and forwards requests to the PPP smart contract.
The encrypted key is returned to the client, which decrypts it locally.

5. Registration Flow:

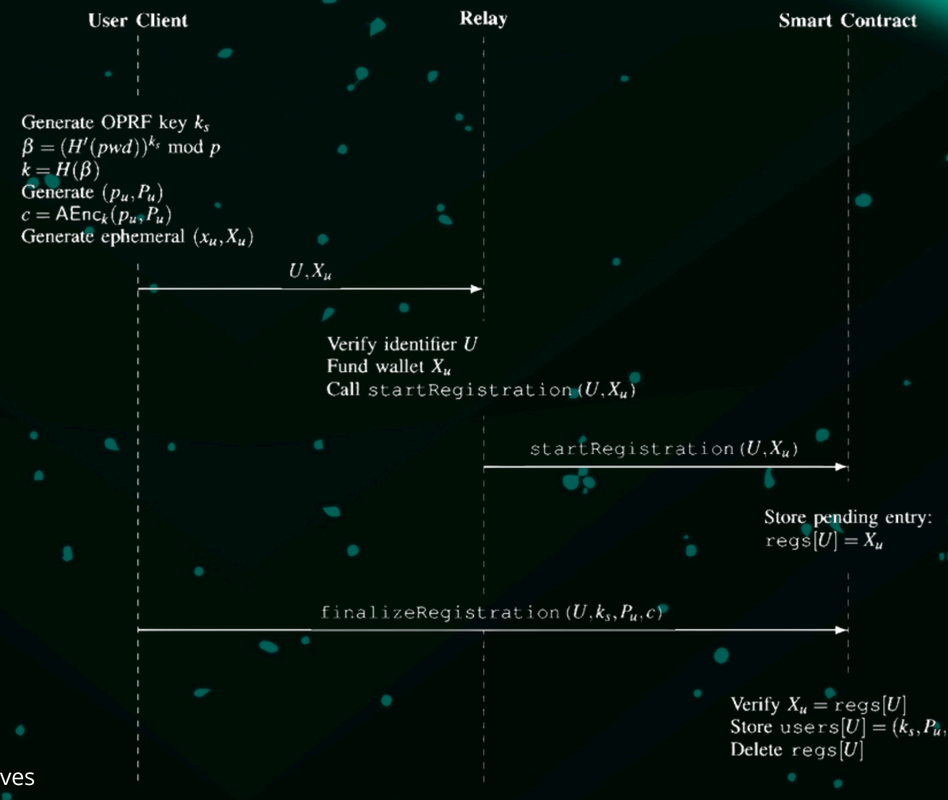
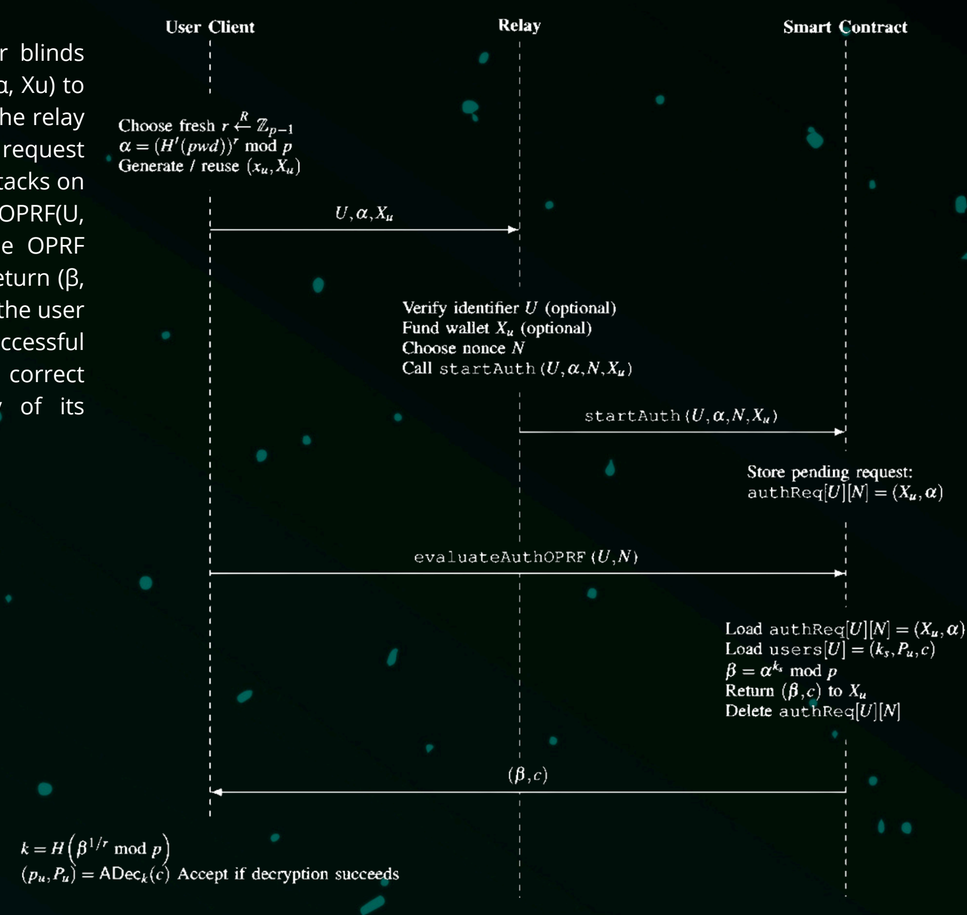


Fig. 2: Registration protocol.
The user derives the envelope encryption key locally using the OPAQUE OPRF, constructs the encrypted credential envelope c, and provisions the server-side OPRF key ks and public key Pu to the PPP contract. The relay only verifies identifiers and funds the ephemeral wallet used to pay for on-chain execution.
All sensitive values are stored confidentially inside the contract's TEEprotected state.

6. Authentication Flow:

Fig. 3: Authentication protocol. The user blinds the password input into α and sends (U, α, Xu) to the PPP contract (optionally via a relay). The relay submits startAuth to create a pending request that serves as a defense against replay attacks on the TEE. The user then calls evaluateAuthOPRF(U, N), causing the contract to evaluate the OPRF using the enclave-protected key ks and return (β, c). After unblinding β and recomputing k, the user decrypts the credential envelope. Successful decryption proves knowledge of the correct password without revealing it or any of its derivatives.



7. Evaluation:

All experiments were conducted on a local Oasis Sapphire testnet using a TypeScript client and Solidity smart contract with Hardhat tooling. The OPRF modular exponentiation runs via EVM precompile 0x05 inside the SGX enclave. A complete authentication requires ~496k gas (2048-bit) or ~300k gas (1024-bit), with every step completing in under 4.2 s, which is a latency acceptable for real-world login flows. One-time registration costs ~275k gas total.

Tab. 1: Gas Cost and Latency of Core Operations

Operation	Gas Cost (avg) 2048-bit	Gas Cost (avg) 1024-bit	Latency	Notes
startRegistration	~111,000	~111,000	<4023 ms	Store eph. X_u
finalizeRegistration	~164,000	~164,000	<4102 ms	Write k_s, P_u, c
startAuth	~338,000	~213,000	<4059 ms	Store α, N
evaluateAuthOPRF	~158,000	~87,000	<4115 ms	OPRF modexp + return

8. Conclusion:

Balthazar demonstrates that password-based blockchain wallets, which were long considered incompatible with public blockchains, are now both secure and practical when combined with Privacy-Preserving Smart Contract Platforms.

Main Takeaways:
- Password never leaves the device
- Every auth attempt is on-chain — rate limits enforced
- Resistance to offline attacks and server compromise
- Compatible with standard Ethereum tooling
- 1+1 wallet: password + enclave key, neither alone sufficient

References:

- Bonneau et al. The Quest to Replace Passwords. IEEE S&P, 2012.
- Jarecki, Krawczyk, Xu. OPAQUE: An Asymmetric PAKE Protocol. EUROCRYPT, 2018.
- Bourdrez et al. The OPAQUE aPAKE Protocol. RFC 9807, IRTF CFRG, 2025.Szalachowski.
- Password-Authenticated Decentralized Identities. arXiv, 2020.
- Oasis Protocol Foundation. Oasis Sapphire: Confidential EVM. 2022.
- Costan, Devadas. Intel SGX Explained. IACR ePrint, 2016.

Excel@FIT 2026

BRNO UNIVERSITY OF TECHNOLOGY FACULTY OF INFORMATION TECHNOLOGY