Empowering Web3 Wallets with Multi-Party Computation (MPC)

The security of digital assets – which includes sensitive information, financial data, intellectual property and other valuable assets - is of utmost importance in today's technology-driven world. As technology has advanced, so have the methods used by cybercriminals to gain unauthorised access to digital assets.

Multi-party computation (MPC) is a cryptographic technique that allows multiple parties to jointly compute a function on their private inputs without revealing their inputs to each other. The result is returned to each party without revealing any private data.

In traditional computation models, data must be centralised to be processed, making it vulnerable to attacks or unauthorised access. MPC, on the other hand, allows data processing in a distributed manner while preserving data privacy. The risk of data being stolen or compromised is greatly reduced, as there is no central data repository that external or internal actors can target. This explains why MPC is a blockchain-agnostic solution that offers increased security and protection for digital assets while remaining accessible. Also, MPC has a wide range of use cases across different industries and applications such as web3 gaming, decentralised finance (DeFi), Decentralised Autonomous Organisations (DAOs), and more.

During this interactive workshop, we will discuss cryptographic building blocks such as digital signatures, and various threshold signature schemes actively deployed today. We will also compare MPC wallets against existing wallet approaches such as multi-signature and smart wallets. Participants will be guided step-by-step on the inner workings of an MPC wallet and interact with it via a sample decentralised application (dApp).

References:

- Article: A short introduction to Multi-party Computation (MPC) [MPC Alliance org]
- Video: Introduction to Secure MPC for data security [MPC Alliance org]

Objectives

A. Knowledge and Understanding (Theory Component)

At the end of this course, participants should be able to:

- Explain the fundamental capabilities and applications of threshold signature schemes/MPC
- Understand the security and privacy implications of MPC wallets for web3
- Analyse the real-world use cases of MPC wallets in web3 in the context of different custody models.
- Assess web3 wallets to compare and contrast alternative solutions like multi-signature wallets and smart contract wallets.

B. Key Skills (Practical Component)

At the end of this course, participants should be able to:

- Design decentralised applications (or dApp) on Ethereum that builds on MPC wallets.
- Adhere to security best practices for MPC wallet-enabled dApps.

SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Topics

Time	Agenda
Day 1	
09:30 – 09:40	Course Overview
09:40 – 10:00	Introduction of Bolt Labs: Mission & Vision
10:00 – 11:00	Introduction [1 Hour] - What are Hash Functions and Digital Signatures? - Introduction to Threshold Signature Schemes (TSS), Multi-signature Schemes, and Aggregate Signatures - How does TSS work with Multi-Party Computation (MPC)?
11:00 – 11:15	Break

11:15 – 12:15	Deeper Dive into Threshold Signatures Schemes in practice [1 hour]
	- Building blocks of TSS
	  ○ Secret sharing, Commitments, ZK proofs, and Paillier encryption.
	- Applications of TSS
	  ○ How TSS enables different custody models for digital assets
	  ○ Capabilities, Strengths and weaknesses of TSS in blockchains
	- Q&A

12:15 – 13:15	Lunch
13:15 – 15:15	An overview of web3 development on Ethereum [2 hours] - What is web3? Compare web2 & web3, properties and limitations. - Basics of Ethereum Accounts and Smart Contracts/dApps. - Discuss tokenisation and ERC standards. - Future of Ethereum: upgrades like Ethereum 2.0 and impact on Web3, account abstraction, etc. Exercise: Software installation of hardhat development environment, develop a basic smart contract, and deploy it to the Ethereum test network.
15:15 – 15:30	Tea Break
15:30 – 16:30	Deeper dive into web3 wallets [1 hour] - Applications: Fungible Tokens, NFTs, DeFi, etc. - Wallet types in practice: ○ Multi-sig vs Smart wallets vs MPC wallets - Advantages and disadvantages of each wallet type - Learn more about MetaMask
Day 2	
09:30 – 09:45	Review from Day 1

09:45 – 10:45	MPC wallets and implications for web3 [1 hour]
	- How do MPC wallets work?
	  ○ Building blocks to achieve security and defence-in-depth
	  ○ Possible deployments and challenges to adoption
	- Use cases

10:45 – 11:45	Case Study – Walkthrough [1 hour] - Build your decentralised app on top of MetaMask using MPC wallets to approve transactions, etc.
11:45 – 12:30	Panel Discussion: "**From Distributing Trust to Distributing Responsibility: MPC Wallet for Digital Assets**" by Dr Ayo Akinyele, Prof David Lee Kuo Chuen, & Shawn Lim
12:30	Lunch

Requirements

For instances:

- Attendees should be excited about mathematics, cryptography, and their applications.
- Attendees have to bring along their own laptop and writing material and be prepared to participate in several practical exercise sessions and case studies
- We may advise attendees to install the relevant software on their machines prior to the course. (Installation guides will be provided before the course.) Time for software installation help is included on the first day.

Duration: 1.5 days

Venue: Singapore University of Social Sciences (SUSS), Blk C

Trainer's Profile

Dr J. Ayo Akinyele
CEO of Bolt Labs

Ayo received a PhD in Computer Science in 2013 from Johns Hopkins University specialising in cryptographic engineering. He is the CEO and co-founder at Bolt Labs — a mission-driven tech startup with deep expertise in designing privacy-enhancing technologies via zero-knowledge proofs and multi-party computation (MPC) techniques.

Ayo leads a fantastic team of cryptographers and engineers building usable, secure, and scalable infrastructure to securely store digital assets while preventing theft and misuse. In particular, Bolt's web3-centric infrastructure enables secure MPC-powered wallets for digital assets in gaming and beyond.

Before Bolt, Ayo co-founded YeleTech Security, a consulting firm specialising in performing security audits for various smart contract and blockchain projects. In particular, YeleTech has audited software for Handshake and Bitcoin Core in addition to open-source cryptographic libraries like bcrypto, libsodium, OpenVPN, and many others.