Framework for Quantum Identity Wallets

Javaid Iqbal Zahid
Toronto Metropolitan University
Toronto, Canada
Email: javaid.iqbal@torontomu.ca

Alex Ferworn
Toronto Metropolitan University
Toronto, Canada
Email: aferworn@torontomu.ca

Fatima Hussain
Toronto Metropolitan University
Toronto, Canada
Email: fatima.hussain@torontomu.ca

***Abstract*—Self-Sovereign Identity (SSI) is a relatively new framework for authentication of entities on the Internet. It is based on distributed peer-to-peer networking, a departure from centralized and federated identity management systems currently in practice. Security of SSI, as well as any information exchange using Internet, is based on Public-key cryptography,for example, Rivest-Shamir-Adleman (RSA) algorithm. Emerging Quantum Computing is a threat to public-key cryptography and needs to be upgraded either using post-quantum cryptography or using the principles of quantum computing. In this research, we propose a quantum digital identity storage framework in the form of "quantum digital wallets", using quantum cryptography approach that will be secure from attacks by quantum computers.**
Keywords: Self-Sovereign Identity, Digital Wallet, Verifiable Credentials, Public-key Cryptography, Quantum Cryptography, RSA, Peer-to-Peer Network.

I. Introduction

Digital wallet, an important component of Self-Sovereign Identity (SSI), is a kind of secure storage system along with an agent that facilitates messaging and communication protocols between peers [1]. Digital wallet can contain information belonging to and controlled by its user. The user information might contain, decentralized identifiers, verifiable credentials, digital copies of passports, driving licenses, birth certificates, diplomas, business cards, vaccination certificate/tokens, resumes, biographical information, usernames, passwords, or any other information of interest that a user might like to keep it in the wallet. Digital wallet is designed based on the principles of portability and openness by default, consent-driven, privacy-by-design, and security-by-design. The architecture of digital wallet is based on two major components; Secure Storage and Agent. The functions of these components are shown in Figure 1.

Quantum computing exploits the principles of quantum mechanics to perform information processing and transmission of information. Quantum information processing is an exciting and new research area with numerous applications, including quantum key generation and distribution, quantum teleportation, quantum computing, quantum lithography, and quantum memories. Quantum computers are expected to outperform the existing classical computing as it exploits the quantum principles of linear superposition, entanglement, and quantum parallelism. Linear superposition, contrary to the classical bit where only two distinct values 0 or 1 are allowed, allows quantum bit, or qubit, to take all possible linearly combined values. Quantum parallelism allows a large number of operations in parallel, can process multiple inputs simultaneously

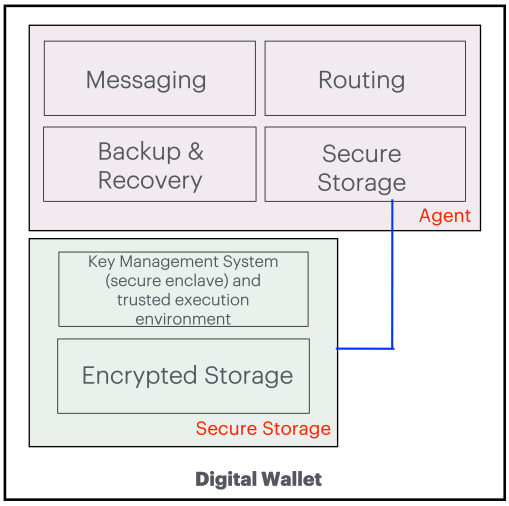

Fig. 1. Architecture of a Digital Wallet.

representing a major difference between classical and quantum [2]. Quantum technology is complex and multidisciplinary in nature, that requires expertise in physics, computer science, materials science, and other fields. We use quantum technology to design digital wallet.

In section II, we outline the objectives of the proposal, and in section III we describe the proposed framework. Finally, we conclude the paper in section IV.

II. Objective and Proposal

The primary objective of the proposed research on Quantum Digital Identity Wallet (QDIW) is to design an architecture and reference framework for promoting trusted digital identities for users to be in control of their own online transactions and presence. SSI and its digital wallet plays an important role to achieve self control. These wallets can be used for identification, authentication, and authorization services by various organizations. Driven by new technologies and standards in cryptography, distributed networks, cloud computing and smart phones, SSI is a paradigm shift for digital identity. The core of SSI security is based on classical public-key cryptosystems (like RSA) [3]. This is provably breakable when universal quantum computing is available [4]. Therefore, it is necessary to direct our research to design quantum digital identity wallet (QDIW) as a preamptive trustworthy service. It will facilitate the creation of encrypted containers or "identity

 ISBN: 978-1-68558-206-7

wallets". It is the right time to rethink the design of SSI schemes based on quantum computing. This will ensure a quantum-resistant SSI.

Specific objectives of this research proposal are as follows:

1) Explore and examine proposals, on digital identity wallet (if any) from national or international standards bodies, and draw operational and technical requirements/specifications for implementation of digital wallet using quantum technologies.
2) Develop architectural framework with use cases for prototyping the QDIW that will help is achieving following goals:
   a) Provide consumers with a WDIW that complies with the human rights principles of preserving people's privacy and control over their information.
   b) Counter Cyber Security threats using trusted and secure QDIW.

III. Proposed Quantum Identity Frame work

We intend to develop a set of algorithms that can take advantage of the unique properties of quantum systems to achieve high-security protection using the wallet concept. Essentially, the sequence of our objectives is as follows:

- Create a structure of digital identity
- Convert the structure into classical information bits
- Map the classical information bits into quantum bit (qubits)
- Develop a process (a quantum algorithm) to encrypt and sign this quantum digital identity
- Develop a procedure to securely share the quantum bits (teleportation) between two communicating parties over classical and quantum channels, while maintaining suitable authentication process.

A. Implementation and Test Bed

In table 1, we outline the project activities, milestones, deliverables, and timeline for the project. The software implementation of the quantum digital wallet is based on Python and Qiskit (IBM). The implementation consist of a *class Wallet* with few instance variables related to some personal attributes of people. Objects of *Wallet* are created, sample from the attributes is selected, and is converted to binary format. This binary information is mapped to quantum bits (qubits) in an initialization process. Further processing of qubits is performed to show the possibility of having secure storage using functions, such as; shifting, transposing, encryption and hashing. Some algebraic processing (inner product, outer product, tensor product, finding density matrix, decimal-to-binary, binary-to-decimal conversion, random quantum state generation, calculation of Shannon entropy, and Linear entropy) would also be needed. The process is shown in Figure 2.

TABLE I
Detailed Research Plan

Objectives	Description
Literature Review on SSI	Comprehensive review of existing literature on SSI schemes (strengths and weakness), and quantum computing.
Identification and Evaluation of Relevant Technologies	Process of selecting relevant and suitable quantum computing, quantum communication, and quantum cryptography approaches to implement SSI.
Development of a Proof of Concepts (PoC)	Design and implement a prototype to prove the viability of designed SSI architecture.
Analysis of Results from PoC	Analysis of effectiveness of our architecture based on the results obtained from PoC.
Assessment of Social Impact	Assessment of the impact of technology on data privacy, protection of individual rights, and other consequences.

Fig. 2. Quantum Information Processing.

IV. Conclusion

Quantum algorithms hold great promise for solving complex problems, however, many technical and practical challenges need to be overcome before they can be widely adopted. Implementation of quantum algorithms is difficult because of the fragility of quantum systems as quantum hardware and software is still in its early stages of development and is not yet scalable or fault-tolerant enough for practical applications. Furthermore, qubits are highly sensitive to their environment and can easily become de-cohered, resulting in errors and loss of quantum information. Quantum algorithms also require significant expertise in both quantum mechanics and computer science, which is also not very common.

References

[1] A. Preukschat and D. Reed, *Self-Sovereign Identity*. Manning Publishing Co., 2021.
[2] M. A. Nielsen and I. L. Chuang, *Quantum Computing and Quantum Information*. Cambridge University Press, 2010.
[3] A. S. R. L. Rivest and L. Adleman, "A method for obtaining digital signatures and public key cryptosystem," in *Communications of the ACM*, vol. 21, no. 2, 1978, pp. 120–126.
[4] P. W. Shor, "Polynomial-time algorithm for prime factorization and discrete logarithms on a quantum computer," in *SIAM Journal on Computing*, vol. 26, no. 5, October 1997, pp. 1484–1509.