US 20230231835A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2023/0231835 A1

Kuang et al. (43) Pub. Date: Jul. 20, 2023

(54) **QUANTUM-SAFE CRYPTOGRAPHIC METHODS AND SYSTEMS**

(71) Applicant: **Quantropi Inc.**, Ottawa (CA)

(72) Inventors: **Randy Kuang**, Ottawa (CA); **Maria Perepechaenko**, Ottawa (CA)

(73) Assignee: **Quantropi Inc.**, Ottawa (CA)

(21) Appl. No.: **18/186,130**

(22) Filed: **Mar. 17, 2023**

Related U.S. Application Data

(60) Division of application No. 17/691,295, filed on Mar. 10, 2022, now Pat. No. 11,641,347, which is a continuation-in-part of application No. PCT/CA2021/050319, filed on Mar. 10, 2021.

(60) Provisional application No. 63/286,195, filed on Dec. 6, 2021, now abandoned, provisional application No. 63/252,292, filed on Oct. 5, 2021, provisional application No. 63/235,457, filed on Aug. 20, 2021, provisional application No. 63/214,511, filed on Jun. 24, 2021.

Publication Classification

(51) **Int. Cl.**

H04L 9/40	(2022.01)
H04L 9/32	(2006.01)
H04L 9/06	(2006.01)
H04L 9/30	(2006.01)
H04L 9/08	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 63/0442*** (2013.01); ***H04L 9/3247*** (2013.01); ***H04L 9/0618*** (2013.01); ***H04L 9/3026*** (2013.01); ***H04L 9/0825*** (2013.01); ***H04L 9/3218*** (2013.01); *H04L 2209/08* (2013.01)

(57) **ABSTRACT**

Cryptographic methods and systems for key exchange, digital signature and zero-knowledge proof. In the digital signature scenario, there is provided a method of signing a digital document, comprising: obtaining a private cryptographic key associated with the signer; obtaining a digital asset from the digital document; selecting a base data element; computing a plurality of signature data elements from (i) the digital asset, (ii) the base data element and (iii) the private cryptographic key; and transmitting the digital document and the plurality of signature data elements to a recipient over a data network. Provenance of the digital document is confirmable by the recipient carrying out a predefined computation involving the digital document, the signature data elements, a plurality of noise variables and a public cryptographic key corresponding to the private cryptographic key associated with the signer. In the zero-knowledge proof scenario, the digital asset plays the role of a challenge data element.