Name of the proposed cryptosystem: NTRU

Principal submitter: John M. Schanck

Institute for Quantum Computing

University of Waterloo 200 University Avenue West Waterloo, ON N2L 3G1

Canada

email: jschanck@uwaterloo.ca phone: +1 519 888 4567 x39057

Auxiliary submitters: Cong Chen

> Oussama Danba Jeffrey Hoffstein Andreas Hülsing, Joost Rijneveld Tsunekazu Saito Peter Schwabe William Whyte Keita Xagawa Takashi Yamakawa Zhenfei Zhang

Inventors of the cryptosystem

NTRU was invented by Jeffrey Hoffstein, Jill

Pipher, and Joseph H. Silverman.

Owner of the cryptosystem

Im M. Sa

None (dedicated to the public domain)

John M. Schanck

Alternative point of contact: Peter Schwabe

> Radboud University Toernooiveld 212 6525 EC Nijmegen The Netherlands

email: peter@cryptojedi.org

phone: +31243653456