

Name of the proposed cryptosystem: CRYSTALS-KYBER

Principal submitter:

Peter Schwabe
Radboud University
Toernooiveld 212
6525 EC Nijmegen
The Netherlands
email: peter@cryptojedi.org
phone: +31243653456

Auxiliary submitters:

Roberto Avanzi
Joppe Bos
Léo Ducas
Eike Kiltz
Tancrède Lepoint
Vadim Lyubashevsky
John M. Schanck
Gregor Seiler
Damien Stehlé

Inventors of the cryptosystem

The submitters;
based on a large collection of previous work,
most importantly by Oded Regev, Vadim
Lyubashevsky, Chris Peikert, Eiichiro Fu-
jisaki, and Tatsuaki Okamoto.

Owner of the cryptosystem

None (dedicated to the public domain)



Peter Schwabe

Alternative point of contact:

Vadim Lyubashevsky
IBM Research – Zurich
Saumerstraße 4
8803 Ruschlikon
Switzerland
email: vadim.lyubash@gmail.com
phone: +41792465983