

Name of the proposed cryptosystem:	CRYSTALS-DILITHIUM
Principal submitter:	Vadim Lyubashevsky IBM Research – Zurich Saumerstraße 4 8803 Ruschlikon Switzerland email: vadim.lyubash@gmail.com phone: +41792465983
Auxiliary submitters:	Shi Bai Léo Ducas Eike Kiltz Tancrède Lepoint Peter Schwabe Gregor Seiler Damien Stehlé
Inventors of the cryptosystem	The submitters. Based on a large collection of previous work, most importantly by Vadim Lyubashevsky, Tim Güneysu, Thomas Pöppelmann, Shi Bai, and Steven Galbraith
Owner of the cryptosystem	None (dedicated to the public domain)
Alternative point of contact:	Gregor Seiler IBM Research – Zurich Saumerstraße 4 8803 Ruschlikon Switzerland email: gseiler@inf.ethz.ch phone: +41792465983

N. Linz

Oct. 1, 2020
Ruschlikon, Switzerland