NIST Post-Quantum Cryptography Submission Cover Sheet

Name of the proposed cryptosystem

The Picnic Signature Algorithm

(Round 2 update)

Principal Submitter:

Greg Zaverucha, Microsoft

gregz@microsoft.com

+1 (425) 421-3271

1 Microsoft Way, Redmond WA, 98052

Auxiliary Submitters:

Melissa Chase

David Derler

Steven Goldfeder

Jonathan Katz

Vladimir Kolesnikov

Claudio Orlandi

Sebastian Ramacher

Christian Rechberger

Daniel Slamanig

Xiao Wang

Inventors(s)/Owners(s)/Developer(s) of the crypto system:

All listed submitters

Software contributions from Alexander Grass, Angela Promitzer and Daniel Kales

Backup point of contact:

Daniel Slamanig, AIT Austrian Institute of Technology

Donau-City-Strasse 1, 1220 Vienna, Austria

daniel.slamanig@ait.ac.at

+43 664 88256147

Signature

Greg Zaverucha

3/4/2019