

Cover Sheet
(Post-Quantum Cryptography Standardization Process)

Name of proposed cryptosystem: MQDSS

Principal submitter:
Simona Samardjiska
Radboud University
✉ simonas@cs.ru.nl
☎ +31 629 779 449
✉ Digital Security Group, Radboud University,
Toernooiveld 212, 6525 EC Nijmegen,
The Netherlands

Auxiliary submitters:
Ming-Shing Chen
Andreas Hülsing
Joost Rijneveld
Peter Schwabe

Inventors of the cryptosystem:
Ming-Shing Chen, Harunaga Hiwatari,
Andreas Hülsing, Joost Rijneveld,
Koichi Sakumoto, Simona Samardjiska,
Peter Schwabe and Taizo Shirai;
(also based on a large collection of previous
work, most importantly by A. Fiat and A.
Shamir, D. Pointcheval and J. Stern)

Owners of the cryptosystem: The inventors

signed:
Simona Samardjiska

Alternative point of contact:
Peter Schwabe
Radboud University
✉ peter@cryptojedi.org
☎ +31 243 653 456
✉ Digital Security Group, Radboud University,
Toernooiveld 212, 6525 EC Nijmegen,
The Netherlands