MAKWA, a submission to the Password Hashing Competition

This is the MAKWA submission package for the Password Hashing Competition. The package contains the following files and directories:

- **makwa-cover.pdf**: this document.
- **makwa-spec.pdf**: the formal specification of MAKWA; that document also includes the security analysis, some additional implementation considerations, and a detailed test vector.
- **c**/: a directory containing the C reference implementation.
- **java**/: a directory containing the Java reference implementation.
- **kat.txt**: the Known-Answer Tests. Both the C and Java implementations contain a tool to generate that file.
- **README.txt**: a introductory documentation, which contains in particular a quick start guide to the C and Java API.

MAKWA was designed by Thomas Pornin <pornin@bolet.org>.

I am not aware of any existing or pending patent application purporting to cover MAKWA implementation or usage, in all or in parts; I do not intend to file any such patent. MAKWA is and will remain available worldwide on a royalty-free basis; this applies to both the scheme itself, and the reference implementations in C and Java languages.

There is no intentional weakness in the design of MAKWA. Since MAKWA uses as parameter a big composite modulus, knowledge of the prime factors of that modulus allows for reverting the hashing process. This is a *feature* and not a backdoor; each deployment of MAKWA should use its own modulus, and a tool for the generation thereof is provided. In that respect, MAKWA uses a public/private key pair and is similar to, say, RSA. Private key usage is optional; hence, a “no-secret” usage is also possible.

Thomas Pornin, February 22, 2014.