[Pqc-forum] Implementation Issues

pqc-forum-bounces@nist.gov on behalf of Hars, Laszlo <Laszlo.Hars@boeing.com>

Wed 9/14/2016 3:05 PM

To: pqc-forum <pqc-forum@nist.gov>;

1 attachments (420 bytes)

ATT00001.txt;

Maybe NIST could consider another set of evaluation critera, resistance against traditional physical attacks. Something, along the line described below.

--- ---

Implementation issues – Traditional attacks

The algorithm has to have a reasonably complex implementation, which resists known (published) types of physical attacks, with documented exceptions. The document describing exceptions tells, in what type of environment the implementation works safely, and what kind of physical protection it may need. E.g. FIB probing or photo voltaic charge detection can be prevented by physical means, like chip covers, but preventing leaks of secrets by timing- or simple power analysis needs careful implementations.

A submission my state that their algorithm is intended only in physically protected environments, where side channel attacks are prevented by the physical protection.

Side channel attacks

Some of the following side channel attacks (maybe even more?) need to be mitigated by proper implementations:

- Timing, EM radiation, SPA, DPA (High-order, multivariate…) attacks

A potential family of protection measures may include

- Random masking schemes on keys or on the secret input – such that the masking and de-masking procedure is simple enough, such that they can be made of low leakage

Fault injection attacks

The algorithm should have implementations of reasonable complexity, which leak no secrets at a small number (e.g. < 4) of targeted faults.

--- ---

Laszlo Hars, PhD
Chief Crypto Architect
Boeing Secure Computing Solutions
5753 W. Las Positas Blvd.
Pleasanton, CA 94588-4084

Laszlo.Hars@boeing.com

Office: 925-398-7625
Cell: 303-990-3994