From: Rainer Urian <rainer.urian@googlemail.com> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum <pqc-forum@list.nist.gov>
CC: raphael.schermann@student.tugraz.at
Subject: [pqc-forum] Classic McEliece Key Generation on RAM constrained devices
Date: Monday, November 21, 2022 11:34:59 AM ET

Hello,

we have just published the preprint: "Classic McEliece Key Generation on RAM constrained devices” on https://eprint.iacr.org/2022/1613

Abstract:
Classic McEliece is a code based encryption scheme and candidate of the NIST post quantum contest. Implementing Classic McEliece on smart card chips is a challenge, because those chips have only a very limited amount of RAM.

Decryption is not an issue because the cryptogram size is short and the decryption algorithm can be implemented using very few RAM. However key generation is a concern, because a large binary matrix must be inverted.

In this paper, we show how key generation can be done on smart card chips with very little RAM resources.

This is accomplished by modifying the key generation algorithm and splitting it in a security critical part and a non security critical part.

The security critical part can be implemented on the smart card controller. The non critical part contains the matrix inversion and will be done on a connected host.

Best regards,
Rainer

From: Tung Chou <blueprint@crypto.tw> via pqc-forum@list.nist.gov
To: Rainer Urian <rainer.urian@googlemail.com>, pqc-forum <pqc-forum@list.nist.gov>
CC: raphael.schermann@student.tugraz.at, D. J. Bernstein <djb@cr.yp.to>, Tanja Lange <tanja@hyperelliptic.org>, Ming-Shing Chen <mschen@crypto.tw>
Subject: Re: [pqc-forum] Classic McEliece Key Generation on RAM constrained devices
Date: Tuesday, November 22, 2022 09:09:49 AM ET

Hi Rainer,

We (code by Ming-Shing Chen and me, ideas with Daniel J. Bernstein and Tanja Lange)

independently developed an efficient outsourcing mechanism for Classic McEliece key

generation. The paper is not ready yet, but working code is available here:

https://github.com/devillegna/McOutsourcing

Best regards,

Tung Chou