From: Perlner, Ray (Fed)
To: (b) (6) ; Petzoldt, Albrecht R. (IntlAssoc)
Subject: RE: SAC
Date: Monday, August 28, 2017 10:11:00 AM

When we analyze breakeven points, we should also note that linear algebra search can be slowed down a lot by using slightly fewer variables (is projected ABC the right name for this?). For example, if we use sxs matrices for A,B, and C, we can solve for s^2 plaintext variables. However, if we limit the number of plaintext variables to s^2-s the cost of linear algebra search is q^(3s+1) instead of q^(s+2): Either the linear algebra search proceeds by guessing 3 vectors sharing a row and a column band kernel, in which case we need less than full rank for both a random 2sx 3s and a random 3s x s matrix, thus requiring a cost of q^(s+1)*q^(2s+2), or we choose 2 vectors (in which case the probability they share a band kernel is still q^-(s+2), but we only have 2s^2 -2s linear constraints on the 2s^2 t variables, so we need to search through a 2s-dimensional space to find the correct answer resulting in a cost of q^(2s-1)*q^(s+2).) Using fewer variables makes the algebraic attack easier, but it might be a net win, if we can use a smaller value for q, use a rectangular scheme to avoid decryption failures etc..

From: Daniel Smith (b) (6)
Sent: Wednesday, August 23, 2017 10:00 AM
To: Petzoldt, Albrecht R. (IntlAssoc) <albrecht.petzoldt@nist.gov>
Cc: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: SAC

Hi, Albrecht,

Thanks for letting me know. I wouldn't worry too much about the lack of questions at SAC. The crowd who publish there typically have a different focus, though this year everything was post-quantum. I still expect that the publication will get some attention from the Japanese and Chinese communities, though.

I want to try to work with you and Ray on finding break even points for the linear algebra MinRank attack, the KS attack, and the minors modeling attack for various systems (in particular for ABC). I think that it would be interesting to fix the number of rows and columns for the rectangular ABC scheme and determine which is the best rank attack for each q. I think that we have found some parameters for which the linear algebra search is faster than the algebraic attack. I think that this should never be the case for either KS or minors. Still, knowing break-even points is interesting and will prove to the French team that minors is not always the best. In fact, for ZHFE, I think that even KS always beats minors. That would be good to study, too.

Cheers,
Daniel

On Mon, Aug 21, 2017 at 8:19 AM, Petzoldt, Albrecht R. (IntlAssoc) <albrecht.petzoldt@nist.gov> wrote:

> Hi Daniel,

Unfortunately I couldn't access my NIST emails from Canada, so I read your mail just now.

There was a panel discussion on post quantum cryptography on Wednesday, but the NIST process was not mentioned at all. Instead they discussed about the question when a quantum computer able to break RSA 2048 will be build (and if RSA 2048 will be broken by classical algorithms sooner). A second topic was which of the lattice key exchange protocols is most promising.

The talk on Friday was ok. However, there were no questions or comments at all.

Best regards,
Albrecht

From: Daniel Smith (b) (6)
Sent: Wednesday, August 16, 2017 10:09 PM
To: Petzoldt, Albrecht R. (IntlAssoc) <albrecht.petzoldt@nist.gov>
Subject: SAC

Hi, Albrecht,

How was the Q&A session today at SAC? I'm curious if there were any particularly interesting issues that came up; in particular, I'm curious if there were any interesting critiques of NIST's process so far. I'm always interested in ways we can improve.

Good luck with your presentation on Friday!

Cheers,
Daniel