From: Alperin-Sheriff, Jacob (Fed)
To: Liu, Yi-Kai (Fed)
Subject: Re: Ramstake Attack
Date: Tuesday, October 17, 2017 5:06:42 PM

The point is that, with (enough to for our purposes consider it broken) probability, it can be solved using LLL in dimension 4.

Specifically, consider that you're given F and G in the RDH problem, and you're trying to find the unknown y_1 and y_2.

Consider the representation of y_1 and y_2

y_1 = 2^{3*pi/8} * u + v,

y_2 = 2^(3*pi/8)*w + x

where u,v, w, x are all of absolute value less than 2^{3*pi/8}. This representation must obviously exist.

If, in fact, there is a representation of y_1 and y_2 as above where
u,v,w,x are all of absolute value (several times less than) 2^{pi/4}, then [u,v,w,x] will almost certainly be the shortest vector (by several times) in the lattice consisting of solutions to

G*2^{3*pi/8}*u + G*v + 2^{3*pi/8}*w + x = F (mod p).

then LLL will output the [u,v,w,x] such that y_1 = 2^{3*pi/8} * u + v, y_2 = 2^(3*pi/8)*w + x

Based on the manner in which y_1 and y_2 are chosen, we have that with probability a little less (1/2) the first bit chosen is "good" (e.g. it doesn't result in u [or w] being too big), while for each of the other 22 bits we have that with probability a little less than 2/3 it doesn't result in u,v,w or x being too big.

Bottom line, we have that this probability is (1/2)*(2/3)^(22)) for each of them, so somewhat less ((1/2)*(2/3)^(22))^2 jointly, which is roughly 2^{-28}.

This is obviously rather low (but still enough to be BAD NEWS for the purposes of our standardization and security), but

the probability that for some a,b,c,d in [0,pi)

y_1 = 2^{a} * u + 2^{b}v,

y_2 = 2^(c)*w + 2^{d}x

and that [u,v,w,x] is (by several times) the shortest vector in the lattice consisting of solutions to

G*2^{a} u + G*2^{b}v + 2^{c}*w + 2^{d}x = F (mod p)

Should be significantly higher (but more annoying to calculate so I didn't do it.

Is this explanation clearer?

On 10/17/17, 4:46 PM, "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov> wrote:

Hi Jacob,

Wait, I have a stupid question... is it really a 2-dimensional lattice? I thought the Ramstake Diffie-Hellman problem reduces to a lattice problem in dimension ~ ceil(log_2(p)).

Your idea seems nice -- I guess the idea would be to reduce to a lattice problem in a higher dimension, e.g., where the dimension is twice as large...

Cheers,

--Yi-Kai

From: Alperin-Sheriff, Jacob (Fed)
Sent: Monday, October 16, 2017 12:18:07 PM
To: internal-pqc
Cc: Liu, Yi-Kai (Fed)
Subject: Ramstake Attack

I believe I have an attack on Ramstake that is far under 2^128 complexity. Instead of a 2-dimensional lattice where each vector [x,y] satisfies Gx+y=C (mod p), create a 4 dimensional lattice where each vector [w,x,y,z] satisfies Gw+G*2^{3*pi/8)*x + y+2^{3*pi/8)*z=C (mod p).

(Instead of always 2^{3*pi/8} multiples and 1 multiples of G and 1, you could also vary them somewhat. The key is that the sparseness can be easily exploited).

In this case, with probability a little less than ((1/2)*(2/3)^(22))^2 ~ 2^{-28} over the choice of the sparse bits used in the public key, the shortest vector (by a large enough amount to guarantee LLL finds it) [w,x,y,z] in this lattice will be the one such that a=2^{3*pi/8}x+w, b=2^{3*pi/8)*z+y, allowing us to recover the secret a, b (or a', b'). LLL will be somewhat expensive here (maybe 2^{36} ???) with the the one in fpLLL, but this appears well well under the minimum NIST allowed complexity.

(Note that one should be able to vary the choice of lattice somewhat, especially by using a slightly larger dimensional lattice [6 or 8, say] to get a much higher probability of success for any given public key)

—Jacob Alperin-Sheriff