From: Moody, Dustin (Fed)
To: (b) (6)
Subject: RE: Security Notes
Date: Thursday, December 14, 2017 3:15:00 PM

Thanks – have you uploaded them yet?

From: Daniel Smith (b) (6)
Sent: Thursday, December 14, 2017 3:12 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Security Notes

Hi, Dustin,

Here are the security notes I have on the schemes for which I think I have a working attack on some parameter sets. I placed these in the checklists, since that's a good place to keep them.

DAGS: In reference to sharing keys of length at least 256 bits: I guess this is interpretation, but the suggested parameters only provide 160 or 192 bits of entropy. Technically, one can share a key of length 256 bits, but trivially with any algorithm I can share a key of arbitrary length by computing H(m),H^2(m),… This certainly doesn't provide the amount of entropy I would want for claiming to establish "shared keys of length at least 256 bits." On that note, I can break the 256-bit classical security level scheme right now.

DME: In reference to the presence of security arguments: I am skeptical on the algebraic attack security claims. They don't seem to consider field equations. I'm not too sure about this. The public key appears to consist of a system of 6 equations in 6 variables with 64 monomials of high degree. The authors mention algebraic attacks over F2, but they don't mention that there necessarily is a solution over F2, so that one can add field equations x_i^2+x_i. This reduces the degree of all monomials to at most 4 (which they did mention). I checked the arithmetic and this indicates that the degree of regularity (and likely the solving degree) are around 18, way less than q=2^24 as they claim. So their claims are wrong. This still does not break the 128-bit scheme, but it does break the 256-bit parameters. The complexity is about 2^205. Also, they mention that since anyone can recover the exponential maps that they can be made public to improve EFFICIENCY. This can't be true unless the entire private key is made public. The contributors clearly haven't thought through the science…

KERUS: In reference to providing copies of references: Vacuously they do provide references... by which I mean, I seriously doubt that there exist references to provide so they have provided all of them. I'll provide an additional cryptanalysis on behalf of the submitters, since they couldn't do their own job. In pass one, the matrices T1=YA, and T2=BY^-1X are sent openly. In pass two, the matrices T3=DYAC^-1 and T4=CBY^-1XH are sent openly. In pass three, the matrix T5=DXH is sent openly. Since A and B are centro-symmetric, the product P=A^-1B^-1 is as well. Notice that P satisfies the linear equation T3PT4=T5 by the commutativity property of centro-symmetric matrices. So we can solve for P. Then T1PT2=X, the shared "secret." The scheme is totally bogus.

I'll upload the 10 I've completed so far.

Cheers,
Daniel