pqsigRM Practical Key Recovery Provisional Outline

Pierre Briaud, Maxime Bros, Ray Perlner, Daniel Smith-Tone

Key Observation
(Confirmed Via Experiment Details to Follow)

- Observation: The hull is a subcode of:

$$\begin{pmatrix} G(r,m-2)\sigma_1^p & G(r,m-2)\sigma_1^p & G(r,m-2)\sigma_1^p & G(r,m-2)\sigma_1^p \\ 0 & G(r-1,m-2) & 0 & G(r-1,m-2) \\ 0 & 0 & G(r-1,m-2) & G(r-1,m-2) \\ 0 & 0 & 0 & 1 \ldots 1 \\ & \multicolumn{2}{c}{Single\ codeword\ from\ Dual\ Code} & \end{pmatrix}$$

- Top 3 rows are orthogonal to any vector consisting of the same 2^{m-2} bits repeated 4 times
- 4th row is orthogonal to any vector with even Hamming weight on the last 2^{m-2} bits
- Bottom row is orthogonal to half of all vectors
- Consequence: There are a lot of weight 8 codewords in the dual code of the hull!
  - These codewords have matching values on columns that are 2^{m-2} bits apart in the private key
  - Finding these codewords is cheap and reveals a lot of structure from the private key.

Observation 2

- Without the $k_{app} = 2$ random rows added to the public code, the hull has the following subcode:
$$\begin{pmatrix} 0 & G(r-1, m-2) & G(r-1, m-2) & 0 \end{pmatrix}$$
- Lots of weight 128 codewords in the above code
  - Only 4 times fewer with the appended rows
  - Confirmed Via Experiment

Attack in Detail Step 1: Find matched sets of 4

- Look for a weight-8 codeword in the dual of the hull
- Look for another weight-8 codeword with weight 4 outside the support of the 1st weight-8 codeword
  - The intersection is a matched set, as are the parts of each weight-8 codeword that don't intersect.
- Repeat until somewhere between 871 and 2048 matched sets are found
  - When enough matched sets have been found, can recover the dimension 1484 subcode which (unpermuted) repeats every 2048 bits
  - Confirmed via experiment. We used 1768 matched sets, but that's probably more than we needed
- Important note: There are two classes of matched sets
  - Class 0: The single codeword added to the private key from the Dual code has even weight when restricted to the matched set
  - Class 1: The single codeword added to the private key from the Dual code has odd weight when restricted to the matched set

Attack in Detail Step 2: Recover

$$(G(r,m-2) \quad G(r,m-2) \quad G(r,m-2) \quad G(r,m-2))$$

Using Chizov-Borodin https://eprint.iacr.org/2013/287

- Start with the subcode of the public code with all bits equal on matched sets; this should reveal all 2048 matched sets (i.e. all the sets of 4 identical columns in a generator matrix for this subcode)
- Apply (and remember) a permutation to get each matched set to columns $i, i + 2048, i + 4096, i + 6144$
- Restrict attention to the first 2048 columns: These should be a large subcode of $RM(6,11)$ up to permutation of the columns
- Adjoin the all 1s codeword and take the hull to get permuted $RM(4,11)$ – Is this the whole $RM(4,11)$ or is it 1 dimension smaller?
- Take the square code to get permuted RM(8,11)
- Take the dual code to get permuted RM (2,11) – note this has dimension only 67
- Look for a minimum weight (weight 512) codeword
- Look for another minimum weight codeword with weight 256 outside the support of the first codeword (The intersection should be in permuted RM(3,11), but not permuted RM(2,11))
- Get enough codewords from permuted RM(3,11) so we can compute permuted RM(3,11)* permuted RM(6,11) = permuted RM(9,11)
- Take the dual code to get permuted RM(1,11)

Step 2 continued

- Once you have permuted RM (1,11) take an 11 x 2048 matrix whose rows are linearly independent codewords with at least one zero (i.e. 1024 zeroes)
- Permute the columns of the matrix , if you take the columns as binary expansions of integers, they count monotonically from 0 to 2047, i.e. so the matrix looks like:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & & 1 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 0 & 1 & & 1 \end{pmatrix}$$

- Remember the permutation and apply it to the other 3 groups of 2048 columns

Step 3: Recover σ_1^p and: $(0 \quad G(r-1,m-2) \quad G(r-1,m-2) \quad 0)$

- Use modified ISD to look for minimum weight codewords from $(0 \quad G(5,11) \quad G(5,11) \quad 0)$ in the hull of the public code (see Observation 2)
  - Guess zeros in matched columns outside the support of a minimum weight codeword in $\left(G(5,11)\sigma_1^p \quad G(5,11)\sigma_1^p \quad G(5,11)\sigma_1^p \quad G(5,11)\sigma_1^p\right)$, which can be constructed using the information extracted in step 2
- Each codeword helps identify
  - Matched sets of 4 with two 1s (blocks 2 and 3) and two 0s (blocks 1 and 4)
  - Can easily use shared non-support to get minimum weight codeword in $(0 \quad 0 \quad G(r-1,m-2) \quad G(r-1,m-2))$ or $(0 \quad G(r-1,m-2) \quad 0 \quad G(r-1,m-2))$ from public code – thus identifying block 4, and partially separating blocks 2 and 3.
- Codewords with exactly 1 bit in each block outside the support of the minimum weight codeword from $\left(G(5,11)\sigma_1^p \quad G(5,11)\sigma_1^p \quad G(5,11)\sigma_1^p \quad G(5,11)\sigma_1^p\right)$ helps identify:
  - One of the bits moved by σ_1^p

Step 4: Recover σ_2^p and: $(0 \quad 0 \quad 0 \quad G(r-2, m-2))$

- Identify codewords from public code in $\begin{pmatrix} 0 & 0 & 0 & G(r-2,m-2)\sigma_2^p \end{pmatrix}$ by forcing columns identified as block 1, 2 or 3 to 0.
- Run Chizov-Borodin (i.e. the same process as step 2) to get a permuted version of $\begin{pmatrix} 0 & 0 & 0 & G(1,m-2)\sigma_2^p \end{pmatrix}$
- Rather than picking 11 linearly independent codewords from $\begin{pmatrix} 0 & 0 & 0 & G(1,m-2)\sigma_2^p \end{pmatrix}$ at random, aim for x0', x1', …x11' with maximum support overlap with x0,x1,x2…x11 in $(0 \quad 0 \quad 0 \quad G(1,m-2))$ as identified in step 3. The process to do this is basically ISD.
- If successful, the column permutation that recovers $\begin{pmatrix} 0 & 0 & 0 & G(1,m-2)\sigma_2^p \end{pmatrix}$ should differ from the one that recovers $(0 \quad 0 \quad 0 \quad G(1,m-2))$ at only 561 columns.