Rainbow - Algorithm Specification and Documentation

The 2nd Round Proposal

Changes to the first round submission

We applied the following changes to our submission.

1. **Improvements on Key Generation Process**:

   We improved the key generation algorithm for the original Rainbow scheme as submitted in our first round proposal.

   In order to speed up the key generation process of Rainbow, we switched from computing the public key by interpolation to computing the public key using matrix products.
   Firstly, we restrict to homogeneous maps $\mathcal{S}$, $\mathcal{F}$ and $\mathcal{T}$. Note that this leads to a homogeneous public key $\mathcal{P}$. It is widely accepted that the complexity of direct attacks is determined only by the homogeneous part of highest degree. All other known attacks against Rainbow (see Section 8) explicitly use the (symmetric) matrices representing this homogeneous quadratic part. Therefore the security of Rainbow is not weakened by this modification.
   Secondly, we restrict the linear maps $\mathcal{S}$ and $\mathcal{T}$ to a special form. We use

$$\mathcal{S} = \begin{pmatrix} 1_{o_1 \times o_1} & S'_{o_1 \times o_2} \\ 0_{o_2 \times o_1} & 1_{o_2 \times o_2} \end{pmatrix}$$

   and

$$\mathcal{T} = \begin{pmatrix} 1_{v_1 \times v_1} & T^{(1)}_{v_1 \times o_1} & T^{(2)}_{v_1 \times o_2} \\ 0_{o_1 \times v_1} & 1_{o_1 \times o_1} & T^{(3)}_{o_1 \times o_2} \\ 0_{o_2 \times v_1} & 0_{o_2 \times o_1} & 1_{o_2 \times o_2} \end{pmatrix}.$$

   Since for every Rainbow public key $\mathcal{P}$ there exists a corresponding Rainbow private key $(\mathcal{S}, \mathcal{F}, \mathcal{T})$ with $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ and $\mathcal{S}$ and $\mathcal{T}$ being of the above form, the security of Rainbow is not weakened by this assumption. For a Rainbow scheme fulfilling these two conditions, we can perform the key generation process (both for the standard and modified variants which

we will discuss below) using a number of matrix products, which enables us to speed up the Rainbow key generation process drastically.

2. **Parameter Choice**:
   Compared to the 9 recommended parameter sets of the first round submission, we narrow them to three parameter sets, namely

   - **Ia**: $\mathbb{F}$=GF(16), $(v_1, o_1, o_2) = (32, 32, 32)$ for the NIST security categories I and II,
   - **IIIc**: $\mathbb{F}$= GF(256), $(v_1, o_1, o_2) = (68, 36, 36)$ for the NIST security categories III and IV and
   - **Vc**: $\mathbb{F}$=GF(256), $(v_1, o_1, o_2) = (92, 48, 48)$ for the NIST security categories V and VI.

3. **Key Size and Performance Trade-off Variants**:

   We propose two variants of Rainbow, which make a trade-off in key size and performance. The first one of these is denoted as "cyclic Rainbow" and allows us to reduce the public key size of the scheme by up to 70 % at a higher cost of signature verification. The second version (denoted as "compressed Rainbow") furthermore stores the private key in the form of a 512 bit seed, thus enabling us to store the private key easily on small devices at the cost of the efficiency of the signature generation process. By proposing these Rainbow variants we want to illustrate the flexibility of the Rainbow signature scheme.