Cryptonote over Ring-LWE

ADK Developer

August 13, 2018

The equations below were a draft inspired by "Unlinkable payments" and "One-time ring signatures" in Cryptonote(https://cryptonote.org/v
over Ring-LWE, which is one of Post-Quantum cryptgraphy.
Does it make sense?
Or please let me know if there already exists simillar or better idea in some papers etc.

1 Unlinkable Payments

Setup: Select $A \in R_q$

1. Bob makes a private key $s_A, s_B \in R_q$ and its public key $P_A = As_A + e_A$,$P_B = As_B + e_B$, $e_A, e_B \in \chi$.
2. Alice makes an ephemeral private key $r \in R_q$ and one time public key $P_{epm} = Ar + e_1$, $e_1 \in \chi$.
3. Alice does key exchange by NewHope(https://eprint.iacr.org/2015/1092.pdf) etc with Bob's public key P_A and get $K \in R_q$
4. Alice computes one time public key $P = AH_s(K) + P_B$.
5. Alice sets P and P_{epm} as a destination key in a transaction.
6. Bob does key exchange with P_{epm} and gets K.
7. Bob computes $P = AH_s(K) + P_B = A(H_s(K) + s_B) + e_B$ and its private key $H_s(K) + s_B$.

2 One-time ring signatures

Setup: Select $A \in R_q$

1. The signer picks a random secret key $x \in R_q$ and computes public key $P = Ax + e$ and the key image $I = H_p(P)x + e$.
2. He picks a random $\{q_i | i = 0...n\}$, $\{w_i | i = 0...n\}$ and $\{e_i | i = 0...n\}$ and applies the following transformations:
   $L_s = Aq_s + e_s$
   $L_i = Aq_i + e_i + w_i P_i \ (i \neq s)$
   $R_s = H_p(P)q_s + e_s$
   $R_i = H_p(P_i)q_i + e_i + w_i I \ (i \neq s)$
3. He gets a non-interactive challenge: $c = H_s(m, L_1, ...L_n, R_1, ...R_n)$
4. He computes the response:
   $c_i = w_i \ (i \neq s)$
   $c_s = c - \Sigma_{i=0}^{n} c_i$
   $r_i = q_i \ (i \neq s)$
   $r_s = q_s - c_s x \bmod l$
   $t_i = e_i \ (i \neq s)$
   $t_s = e_s - c_s e \bmod l$
   The signature is $\sigma = (I, c_1...c_n, r_1...r_n, t_1...t_n)$
5. The verifier checks the signature by:
   $L'_i = Ar_i + t_i + c_i P_i$
   $R'_i = H_p(P_i)r_i + t_i + c_i I$
   and $\Sigma_{i=0}^{n} c_i = ?H_s(m, L'_1, ...L'_n, R'_1, ...R'_n)$