Analysis on Layered ROLLO-I

April 2023

Note that we used the same notations as in [2].

1 Key recovery attack

1.1 Instance

A ciphertext in Layered ROLLO-I is generated as follows.

$$\mathbf{c} = \Phi_2^{-1}(P_P P_{E,1} + P_H P_{E,2} \mod P^b),$$

where the vector $(\Phi_2^{-1}(P_{E,1}), \Phi_2^{-1}(P_{E,2})) \in \mathbb{F}_{q^m}^{2n}$ is of rank weight r.

Notice that the ciphertext $\mathbf{c}$ is a syndrome calculated by the parity check matrix

$$[\mathcal{I}(\Phi_2^{-1}(P_P, P^b)) \mid \mathcal{I}(\Phi_2^{-1}(P_H, P^b))]$$

of an $[2n, n]$ ideal code over $\mathbb{F}_{q^m}$. Thus we can apply combinatorial attacks to solve the IRSD problem or algebraic attacks to solve the RSD problem, with an error of rank weight r.

1.2 Combinatorial attack

The complexity of the combinatorial attack for an $[tn, n]$ ideal code over $\mathbb{F}_{q^m}$ is suggested in [3] as follows.

$$\mathcal{O}\left(((t-1)nm)^\omega q^{r\lceil \frac{m(n+1)}{tn} \rceil - m}\right).$$

The value for ω is suggested to be taken as $\omega = 2$ in [3], but we will also consider $\omega = 3$ to show that the parameters of Layered ROLLO-I fall considerably short of the security level in any cases. The costs of the combinatorial attacks are shown on the table below.

Security Level	q	n	m	r	t	Complexity: $\omega = 2$	Complexity: $\omega = 3$
128	2	74	67	3	2	2^{60}	2^{72}
192	2	86	79	4	2	2^{106}	2^{119}
256	2	106	97	5	2	2^{175}	2^{188}

1.3 Algebraic attack

Algebraic attacks consider the RSD instance and use a system of equations. If the system is solved, it can be said that a solution is found for the RSD instance.

The algebraic attack demonstrated in [1] considers two cases comparing the number of equations and those of variables. When the number of equations is greater than or equal to those of variables, it is called *an overdetermined case*. Otherwise, it is called *an underdetermined case*.

For an instance of the RSD problem with an $[n, k]$ code over $\mathbb{F}_{q^m}$ and an error vector with rank weight r, it is an overdetermined case if the inequality (1) is satisfied.

$$m\binom{n-k-1}{r} \geq \binom{n}{r}. \tag{1}$$

The complexity, in this case, is as follows.

$$\mathcal{O}\left(m\binom{n-k-1}{r}\binom{n}{r}^{\omega-1}\right). \tag{2}$$

For an overdetermined case, if we can find a nonzero p satisfying the inequality (3), it is called *a super-overdetermined case*.

$$m\binom{n-p-k-1}{r} \geq \binom{n-p}{r}. \tag{3}$$

For the maximal value of p satisfying (3), we can reduce the attack complexity (2) as follows.

$$\mathcal{O}\left(m\binom{n-p-k-1}{r}\binom{n-p}{r}^{\omega-1}\right).$$

Note that algebraic attacks can also be applied to Layered ROLLO-I, and we will apply the attack for an instance of an $[2n, n]$ code with an error of rank weight r. Since the proposed parameters of Layered ROLLO-I all satisfy

- $m\binom{n-1}{r} \geq \binom{2n}{r}$ and
- $m\binom{n-p-1}{r} \geq \binom{2n-p}{r}$ for $p \neq 0$,

we can apply the complexities below.

- Overdetermined case:

$$\mathcal{O}\left(m\binom{n-1}{r}\binom{2n}{r}^{\omega-1}\right)$$

- Super-overdetermined case:

$$\mathcal{O}\left(m\binom{n-p-1}{r}\binom{2n-p}{r}^{\omega-1}\right)$$

The calculated results are shown in the table below. We used $\omega = 2.81$ as suggested in [1].

Security Level	q	n	m	r	Over. Case	p	Super-over. Case
128	2	74	67	3	2^{56}	47	2^{49}
192	2	86	79	4	2^{73}	39	2^{66}
256	2	106	97	5	2^{90}	31	2^{86}

1.4 Structural attack

The complexity of a structural attack using the structure of BII-LRPC codes is suggested in [2] as follows.

$$S_S = \left(\frac{n}{b}\right)^2 m^3 q^{(b-1)m+d\lceil\frac{m}{2}\rceil-m-\frac{n}{b}}. \tag{4}$$

It seems that there is a typo in (4) because it is said in [2] that S_S will be the same to $S_{S_{ROLLO}}$ if $b = 1$, but it does not.

$$S_{S_{ROLLO}} = n^3 m^3 q^{d\lceil\frac{m}{2}\rceil-m-n}.$$

Thus we used the following complexity instead of (4), and obtained the cost of the attack in the table below.

$$S'_S = \left(\frac{n}{b}\right)^3 m^3 q^{(b-1)m+d\lceil\frac{m}{2}\rceil-m-\frac{n}{b}}.$$

Security Level	q	n	m	d	b	S'_S
128	2	74	67	2	2	2^{65}
192	2	86	79	3	2	2^{112}
256	2	106	97	3	2	2^{131}

As it can be seen in the table above, the proposed parameters by authors of [2] do not reach the security levels, respectively, by the attack claimed by themselves.

2 Conversion to ROLLO-I

The public key of Layered ROLLO-I consists of the following two polynomials:

$$\begin{aligned} P_P &= P_O\Psi(P_I) \bmod P^b, \\ P_H &= P_O\Psi(\mathbf{z}) + P_N P \bmod P^b, \end{aligned}$$

for a random degree-$(b-1)$ polynomial $P_I \in \mathbb{F}_{q^m}[X]/\langle P\rangle$, and degree-$n$ polynomials $P_O, P_N \in \mathbb{F}_{q^m}[X]/\langle P^b\rangle$. For decapsulation works, P_O has an inverse in $\mathbb{F}_{q^m}[X]/\langle P^b\rangle$, and P_I has an inverse in $\mathbb{F}_{q^m}[X]/\langle P\rangle$ (and so in $\mathbb{F}_{q^m}[X]\langle P^b\rangle$). Hence we can compute the following:

$$\begin{aligned} P_P^{-1}P_H \bmod P^b &= (P_O\Psi(P_I))^{-1}(P_O\Psi(\mathbf{z}) + P_N P) && \bmod P^b \\ &= \Psi(P_I)^{-1}\Psi(\mathbf{z}) + P_P^{-1}P_N P && \bmod P^b. \end{aligned}$$

Since P^b is a multiple of P, we can take $\bmod P$ to the equation above. Then, using $\Psi(\mathbf{z}) \bmod P = P_I\mathbf{x}^{-1}\mathbf{y} \bmod P$, we have the following equation:

$$\begin{aligned} \left[P_P^{-1}P_H \bmod P^b\right] \bmod P &= \left[\Psi(P_I)^{-1}\Psi(\mathbf{z}) + P_P^{-1}P_N P \bmod P^b\right] \bmod P \\ &= \Psi(P_I)^{-1}P_I\mathbf{x}^{-1}\mathbf{y} && \bmod P \\ &= \mathbf{x}^{-1}\mathbf{y} && \bmod P. \end{aligned}$$

Resultantly, the public key of Layered ROLLO-I is converted to a public key of ROLLO-I with parameter $[2n/b, n/b]$. Note that this conversion does not require any secret information.

Similarly, a ciphertext of Layered ROLLO-I can be converted to a ciphertext of ROLLO-I.

$$\begin{aligned} \left[P_P^{-1}\mathbf{c} \bmod P^b\right] \bmod P &= \left[P_P^{-1}(P_P P_{E,1} + P_H P_{E,2})\right] && \bmod P \\ &= \left[P_{E,1} + P_P^{-1}P_H P_{E,2} \bmod P^b\right] && \bmod P \\ &= P_{E,1} + \mathbf{x}^{-1}\mathbf{y}P_{E,2} && \bmod P \end{aligned}$$

In conclusion, (q, n, m, r, d, b)-Layered ROLLO-I can be converted to $(q, n/b, m, r, d)$-ROLLO- I.

References

[1] Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel. Algebraic attacks for solving the rank decoding and minrank problems without gröbner basis. 2020.

[2] Chanki Kim, Young-Sik Kim, and Jong-Seon No. New design of blockwise interleaved ideal low-rank parity-check codes for fast post-quantum cryptography. *IEEE Communications Letters*, 2023.

[3] Rollo. Rollo specification. *Available on [online], https://pqc-rollo.org/documentation.html*, 2020.