On the security of REDOG

Alex Pellegrini

Eindhoven University of Technology

July 16, 2023

with Tanja Lange and Alberto Ravagnani

Codes in the rank metric

Let $\{\alpha_1, \dots, \alpha_m\}$ a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.
Write $x \in \mathbb{F}_{q^m}$ as $x = \sum_{i=1}^m X_i \alpha_i$, $X_i \in \mathbb{F}_q$.
So x can be represented as $(X_1, \dots, X_m) \in \mathbb{F}_q^m$.
Extend to $v = (v_1, \dots, v_n) \in \mathbb{F}_{q^m}^n$ as the map $Mat : \mathbb{F}_{q^m}^n \to \mathbb{F}_q^{m \times n}$ defined by:

$$v \mapsto \begin{bmatrix} V_{11}, & V_{21} & \dots & V_{n1} \\ V_{12}, & V_{22} & \dots & V_{n2} \\ \vdots & \vdots & \dots & \vdots \\ V_{1m}, & V_{2m} & \dots & V_{nm} \end{bmatrix}$$

The **rank weight** of v is then $wt_R(v) := rk_q(Mat(v))$.
The **rank distance** between $v, w \in \mathbb{F}_{q^m}^n$ is $d_R := wt_R(v - w)$.

Codes in the rank metric

A rank metric $[n, k, d]$-code C is a k-dimensional $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}_{q^m}^n$ with **minimum distance**

$$d := \min_{a,b \in C, a \neq b} d_R(a, b)$$

and **correction capability** $\lfloor (d-1)/2 \rfloor$.
G is a **generator matrix** of C if its rows span C.
H is a **parity check matrix** of C if its rows span the right-kernel of G.
A very well known class of rank metric codes are **Gabidulin codes**, which have $d = n - k + 1$ and can be efficiently decoded up to $\lfloor (d-1)/2 \rfloor$ errors.

REDOG Specification

- **Setup**: integers $(\ell, m, n, k, r, t, \lambda)$, with $\ell < n$ and $\lambda t \leq r \leq \lfloor (n-k)/2 \rfloor$.
- **Keygen:**
  - $H = (H_1 \mid H_2)$, $H_2 \in GL_{n-k}(\mathbb{F}_{q^m})$, a parity check matrix of a $[2n-k, n]$ Gabidulin code, with decoder Φ correcting $r = \lfloor (n-k)/2 \rfloor$ errors.
  - $HF : \mathbb{F}_{q^m}^{2n-k} \to \mathbb{F}_{q^m}^{\ell}$ hash function.
  - Full rank $M \in \mathbb{F}_{q^m}^{\ell \times n}$ and isometry $P \in \mathbb{F}_{q^m}^{n \times n}$ (wrt. the rank metric).
  - λ-dimensional subspace $\Lambda \subset \mathbb{F}_{q^m}$ and $S^{-1} \in GL_{n-k}(\Lambda)$.
  - **Public**: $pk = \left(M, F = MP^{-1} H_1^T \left(H_2^T\right)^{-1} S \right)$
  - **Secret**: $sk = (P, H, S, \Phi)$.

REDOG Specification - cont'd

RECALL: $pk = \left(M, F = MP^{-1}H_1^T\left(H_2^T\right)^{-1}S\right)$ and $sk = (P, H, S, \Phi)$.

- **Encrypt**$(m \in \mathbb{F}_{q^m}^{\ell}, pk)$
  - generate uniformly random $e = (e_1, e_2) \in \mathbb{F}_{q^m}^{2n-k}$ with $wt_R(e) = t$ $e_1 \in \mathbb{F}_{q^m}^{n}$ and $e_2 \in \mathbb{F}_{q^m}^{n-k}$.
  - Compute $m' = m + HF(e)$.
  - **Send** $c_1 = m'M + e_1$ and $c_2 = m'F + e_2$.
- **Decrypt**$((c_1, c_2), sk)$
  - Compute $c' = c_1P^{-1}H_1^T - c_2S^{-1}H_2^T$.
  - Decode $\Phi(c')$ to obtain $e' = (e_1P^{-1}, -e_2S^{-1})$ and recover $e = (e_1, e_2)$.
  - Solve $m'M = c_1 - e_1$.
  - **Output** $m = m' - HF(e)$.

Incorrectness of REDOG's decryption

Lemma

Let V be a t-dimensional subspace of $\mathbb{F}_q^m$ and let $S \in V^s$ be a uniformly random s-tuple of elements of V. The probability that $\langle S_i \mid i \in \{1, \dots s\} \rangle = V$ is at least

$$1 - \sum_{i=0}^{t-1} \begin{bmatrix} t \\ i \end{bmatrix}_q (q^{-t+i})^s.$$

Proposition

Let (n, k, m, q, t, λ) be any set of parameters proposed for REDOG. If $e = (e_1, e_2) \in \mathbb{F}_{q^m}^{2n-k}$ with $e_1 \in \mathbb{F}_{q^m}^n$ and $e_2 \mathbb{F}_{q^m}^{n-k}$ is a uniformly random error with $wt_R(e) = t$, then $wt_R(e_1) = wt_R(e_2) = t$ with probability ~ 1.

Incorrectness of REDOG's decryption - cont'd

RECALL: $e' = (e_1 P^{-1}, -e_2 S^{-1})$.

Theorem

$wt_R(e') > \lambda t = r = \lfloor (n-k)/2 \rfloor$ with probability ~ 1.[1]

Sketch of Proof

By Proposition we can prove that, with probability ~ 1:

- $wt_R(e_1 P^{-1}) = wt_R(e_1) = t$ since P is isometry.
- $wt_R(-e_2 S^{-1}) = \lambda t$.
- $\langle Mat(e_1 P^{-1}) \rangle \not\subset \langle Mat(-e_2 S^{-1}) \rangle$.

So $wt_R(e') \geq wt_R(-e_2 S^{-1}) + 1 = \lambda t + 1$. $\square$

Remark

Φ decrypts correctly when $wt_R(e') \leq r = \lfloor (n-k)/2 \rfloor$.

Theorem above shows that REDOG's decryption is **incorrect** and the system is likely vulnerable to **reaction attacks**.

[1] Support Sage code at this URL

Breaking REDOG's implementation

One way to get around Theorem is to build errors as follows:

Algorithm

1. Pick $\beta_1, \ldots, \beta_t \in \mathbb{F}_{q^m}$ being $\mathbb{F}_q$-linearly independent.
2. Pick random $\pi \in Sym(2n-k)$.
3. Set $e_{init} = (\beta_1, \ldots, \beta_t, 0, \ldots, 0) \in \mathbb{F}_{q^m}^{2n-k}$
4. **Output**: $e = \pi(e_{init})$.

Error vectors in REDOG's implementation are generated in an equivalent way to Algorithm. Indeed, $wt_R(e') = (e_1^{P^{-1}}, -e_2 S^{-1}) \leq \lambda t$ and can be decoded.

Remark

Algorithm above produces an error vector e such that $wt_H(e) = wt_R(e) = t$. (!!!)

The attack on REDOG's implementation

RECALL: $pk = (pk_1, pk_2) = \left(M, F = MP^{-1}H_1^T \left(H_2^T\right)^{-1} S\right)$.

Idea:

- View $N = (pk_1 \mid pk_2)$ as the generator matrix of a random linear $[2n-k, \ell]$-code C' over $\mathbb{F}_{q^m}$ in the **Hamming metric**.
- Error vectors e with $wt_H(e) = t$ are generated by Algorithm.
- Use Information Set Decoding technique (Prange) to decode in C'.

Running the attack[2] in Sagemath 9.5 on a Linux Mint virtual machine we broke the KAT ciphertexts for all the proposed parameters.

Security parameter	Time (sec.)
128	~ 8
192	~ 82
256	~ 232

[2] Support Sage code at this URL

General rank metric attack costs recomputed

We believe that attacks costs have been computed incorrectly in REDOG's specification.
During transmission, an error vector of rank weight t is added to the ciphertext, but in the costs computation the value r is used instead.
For example, parameters for 128 bits security, produce:

Attack	Old cost	New cost
AGHT	2^{257}	2^{53}
GRSH	2^{147}	2^{34}
MMJ	2^{416}	2^{134}

REDOG's keys are quite large compared to other rank metric code based systems. Increasing the keys to overcome these attacks would make it impractical.

Conclusions

- REDOG's decryption is incorrect, likely exposing it to reaction attacks and causing a weak choice in the current implementation to achieve correctness.
- Efficient message recovery attack on REDOG's implementation.
- We believe attacks costs have been wrongly computed.

Thank you for your attention!