Appendix to Question 1

Your question will be about EWCDM.
The article can be found at `https://eprint.iacr.org/2016/525.pdf`.

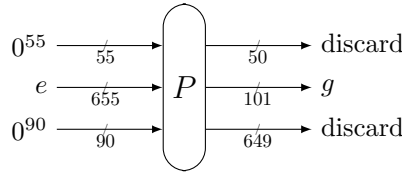## Appendix to Question 2

Consider the following parameters: $k = 128$, $t = 96$, $n = 128$, $a = 26$, and $b = 62$. CrAp is depicted below:
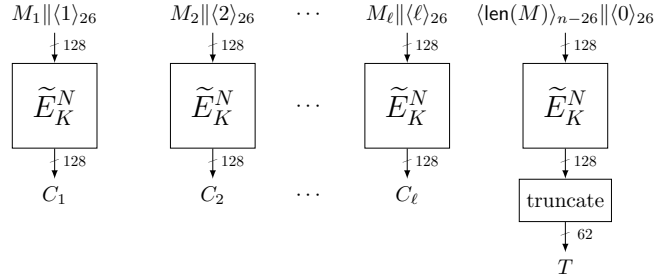
Appendix to Question 3

(The personalized appendix continues on the next page!)

Appendix to Question 4

Your question will be about LEDACrypt.
The article can be found at `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-C`
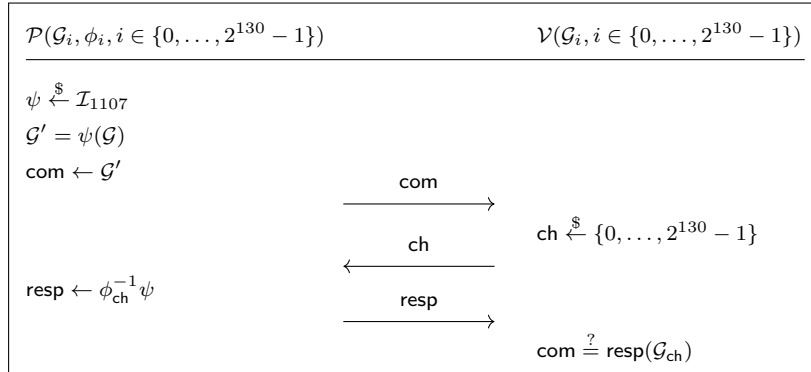`ryptography/documents/round-2/submissions/LEDAcrypt-Round2.zip`.
The document you need to read within the zip file has path `LEDAcrypt_NOKATS\LEDAcrypt_sub`
`mission\Supporting_Documentation\specification_LEDAcrypt.pdf`.

Appendix to Question 5

The CGI2 problem is defined as follows.

Let $\mathcal{G}$ be a graph given by the polynomial $\Gamma = \sum_{1 \leq i \leq j \leq 1107} \alpha_{i,j} x_i x_j$, and let $\mathcal{I}_{1107}$ be the set of isomorphisms on graphs of size 1107.

Let $\mathcal{G}_0, \mathcal{G}_1, \ldots, \mathcal{G}_{2^{130}-1}$ be 2^{130} graphs isomorphic to $\mathcal{G}$, i.e., for each $\mathcal{G}_i$, $i \in \{0, \ldots, 2^{130} - 1\}$ there exists an isomorphism $\phi_i \in \mathcal{I}_{1107}$ such that $\mathcal{G}_i = \phi_i(\mathcal{G})$.

Find an isomorphism $\phi^* \in \mathcal{I}_{1107}$ such that $\mathcal{G}_a = \phi^*(\mathcal{G}_b)$ for some $a \neq b$, where $a, b \in \{0, \ldots, 2^{130} - 1\}$.

The protocol $\mathsf{ID}_{\mathrm{CGI2}}$ is given below.

$\mathcal{P}(\mathcal{G}_i, \phi_i, i \in \{0, \ldots, 2^{130} - 1\})$	$\mathcal{V}(\mathcal{G}_i, i \in \{0, \ldots, 2^{130} - 1\})$
$\psi \xleftarrow{\$} \mathcal{I}_{1107}$	
$\mathcal{G}' = \psi(\mathcal{G})$	
$\mathsf{com} \leftarrow \mathcal{G}'$	
$\xrightarrow{\quad \mathsf{com} \quad}$	
	$\mathsf{ch} \xleftarrow{\$} \{0, \ldots, 2^{130} - 1\}$
$\xleftarrow{\quad \mathsf{ch} \quad}$	
$\mathsf{resp} \leftarrow \phi_{\mathsf{ch}}^{-1} \psi$	
$\xrightarrow{\quad \mathsf{resp} \quad}$	
	$\mathsf{com} \stackrel{?}{=} \mathsf{resp}(\mathcal{G}_{\mathsf{ch}})$

The remaining parameters used in your personalized version of the assignment are $\lambda = 192$, $k = 36$.