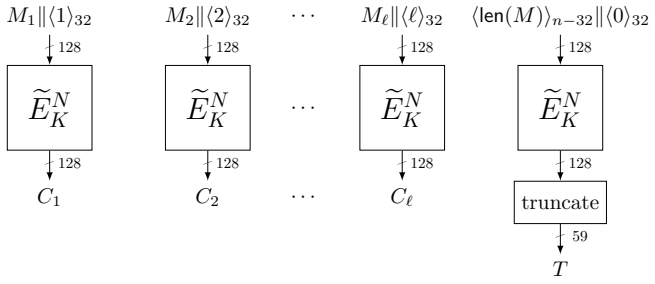
NWI-IMC061 – Applied Cryptography
Personalized Appendix, Academic Year 2021–2022
Sequence Number: 18

Appendix to Question 1

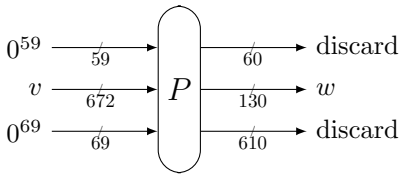
Your question will be about EWPC.
The article can be found at `https://eprint.iacr.org/2015/1049.pdf` (ignore SCT).

Appendix to Question 2

Consider the following parameters: $k = 128$, $t = 96$, $n = 128$, $a = 32$, and $b = 59$. CrAp is depicted below:



Appendix to Question 3



(The personalized appendix continues on the next page!)

Appendix to Question 4

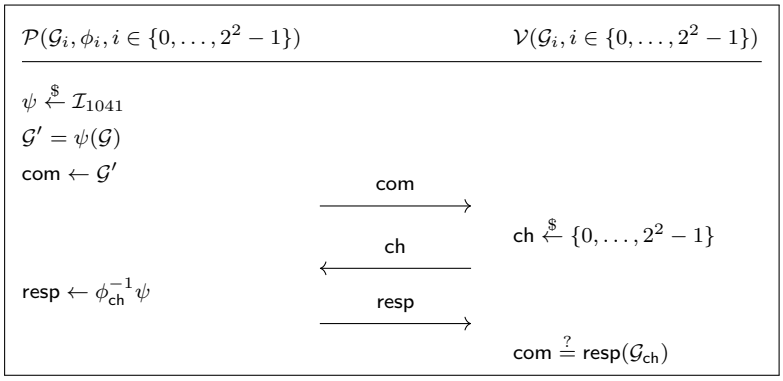
Your question will be about NTS-KEM.
The article can be found at `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/submissions/NTS-KEM-Round2.zip`.
The document you need to read within the zip file has path `NTSKEM_noKATS\NTSKEM\Supporting_Documentation\nts-kem.pdf`.

Appendix to Question 5

The CGI2 problem is defined as follows.

Let $\mathcal{G}$ be a graph given by the polynomial $\Gamma = \sum_{1 \le i \le j \le 1041} \alpha_{i,j} x_i x_j$, and let $\mathcal{I}_{1041}$ be the set of isomorphisms on graphs of size 1041.
Let $\mathcal{G}_0, \mathcal{G}_1, \ldots, \mathcal{G}_{2^2-1}$ be 2^2 graphs isomorphic to $\mathcal{G}$, i.e., for each $\mathcal{G}_i$, $i \in \{0, \ldots, 2^2 - 1\}$ there exists an isomorphism $\phi_i \in \mathcal{I}_{1041}$ such that $\mathcal{G}_i = \phi_i(\mathcal{G})$.
Find an isomorphism $\phi^* \in \mathcal{I}_{1041}$ such that $\mathcal{G}_a = \phi^*(\mathcal{G}_b)$ for some $a \neq b$, where $a, b \in \{0, \ldots, 2^2 - 1\}$.

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



The remaining parameters used in your personalized version of the assignment are $\lambda = 192$, $k = 27$.