Q1 (100 points): ICRDB Design

(a) (30 points) After read the document of the Integrity-Coded Relational Database (ICRDB), please itemize all your findings of the ICRDB, which may include any incorrectness, any un-considered case, and any different approach that might be better than the approach in the document, etc. In other words, you can include any thought that might help improving the design of ICRDB.

(b) (70 points) In the document, I described how to convert standard SQL queries to modified SQL queries in an ad hoc style. There is a need to have a pseudocode-like query converting algorithm(s) that covers all cases. Please do your best to design such algorithm(s).

Q2 (50 points): P2P Email Encryption

In the document I posted on the class website, I described a possible identity-based group key agreement protocol that may be used to implement the P2P email encryption. What do you think about this protocol? That is

(a) Is this protocol correct?
(b) From your opinion, is this protocol efficient?
(c) Is there any security vulnerability of the protocol?
(d) Any other thought you have about this protocol.