Improved Private Information Download Protocol

In this paper, an improved private information download protocol will be proposed. The new protocol is more efficient than the well known NetWare version 4 protocol and the recently reported Perlman- Kaufman protocols. More importantly, in order to develop a generic protocol for private information download, no existence of secure trapdoor one-way function, i.e., public-key based encryption/ decryption, is assumed for the protocol construction.