Symmetric encryption

Dongles with hardware algorithms operate according to the following general scheme: a block of data is sent from the protected application to the dongle (question to dongle), this sequence of data is then converted (encrypted or decrypted) by the dongle using the symmetrical hardware algorithm. This way, we get the dongle answer to be sent to the protected application.

More often, while working on an application, a protection system developer creates a few possible questions/answers, which are used during a short timeframe. This significantly simplifies the task of building table emulators, since it is this short timeframe that is required to track all questions and answers. This is one of the most frequent mistakes in developing a protection system.

To ensure effective fight against table emulators the number of various questions and answers should be as big as possible and the time when they will be used should span months.

GSII64 (key length of 128 or 256 bits) and AES (key length of 128 bits) algorithms implemented in Guardant dongles symmetrically encrypt and decrypt information inside the dongle. This allows to significantly enhance the capabilities of Guardant dongles and increase the tamperproofness of the protected application by the means of having data for encryption dynamically changed.