Getting Answers of Hardware Algorithms

In order to use the dongle hardware algorithms, you need to know the sequence that the algorithm will return in response to the input question. Then this sequence (algorithm's answer) can be used for complicating the protection system logic.

GrdUtil.exe provides a user-friendly service for getting answers of hardware algorithms. The utility calls the selected algorithm and gets its answers to be saved in a special report file.

Important information

If the algorithm for which the report is generated has not yet been recorded into dongle memory, or its properties and/or determinant have been changed in the process of editing the mask, execute command **Dongle | Write into dongle** before generating the report

In order to get an array of answers from an algorithm, select it from the list and execute the menu command **Dongle | Generate algorithm report:**
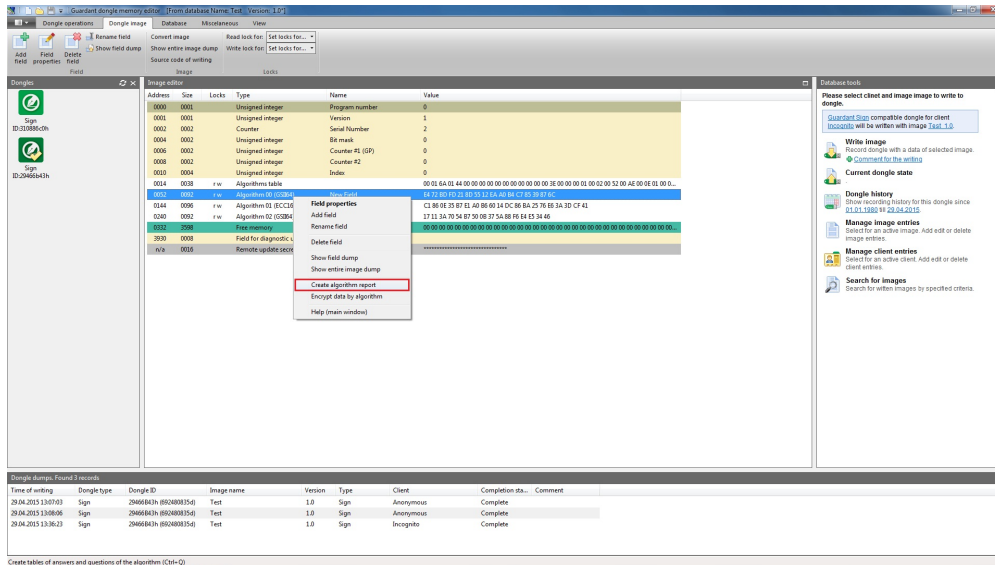
In the dialog box that will appear specify the number of questions to the algorithm, required programming language and report form. Additionally for GSII64 type algorithms specify the question size as well as method and mode of encryption.

Questions to the algorithm are represented as sequences of random numbers.

Number of questions

In the **Number of questions** field, specify the number of calls *GrdTransform* function to the algorithm (in the selected number representation).

For each call (question) the algorithm will generate a response sequence with the length equal to the length of the question.

Programming language

Using **Programming language** dropdown list select the language which syntax rules will be applied to generating the report file.

Available options: C/C++, Pascal/Delphi, Assembler.

Report form

Questions and received algorithm answers are saved in the report file as one or two arrays. Select a report form using the dropdown list.

Report form	Description
1 array	A question and answer of the algorithm form a sequence of array elements. The number of array elements equals the doubled number of questions
2 array	Algorithm questions form the first array of elements and respective answers – the second. The number of elements of each array equals the number of questions

Additional parameters for symmetric algorithms

Size of GrdTransform question

In this case the size of the question (**Question size** field) stands for the maximum size of GrdTransform input data, which this operation can process at once (compare to **Size of question to algorithm**).

For unidirectional hardware algorithms the question length for GrdTransform is a fixed value unlike GSII64 (AES) type algorithms, which can receive blocks of various sizes from GrdTransform:

Symmetric algorithm operating modes	Question size of GrdTransform, bytes
ECB and CBC	Number, multiple of 8. Maximum value - 248
CFB and OFB	Random number not exceeding 255

Set the question size in the field (value by default – 8 bytes).

Transform mode

AES and GSII64 type algorithms are symmetric: encryption of GSII64 algorithm question into its answer is reversible.

Select the direction for conversion (encryption or decryption) from the dropdown list.

Transform method

AES and GSII64 type algorithms have 4 operating modes different by their properties and purposes. GSII64 algorithm is described in details in Chapter **Hardware Algorithms.**

Select a method of encryption using the dropdown list.

Initialization vector

Clicking **[Init. vector]** button launches a hexadecimal editor serving for setting the initialization vector value:
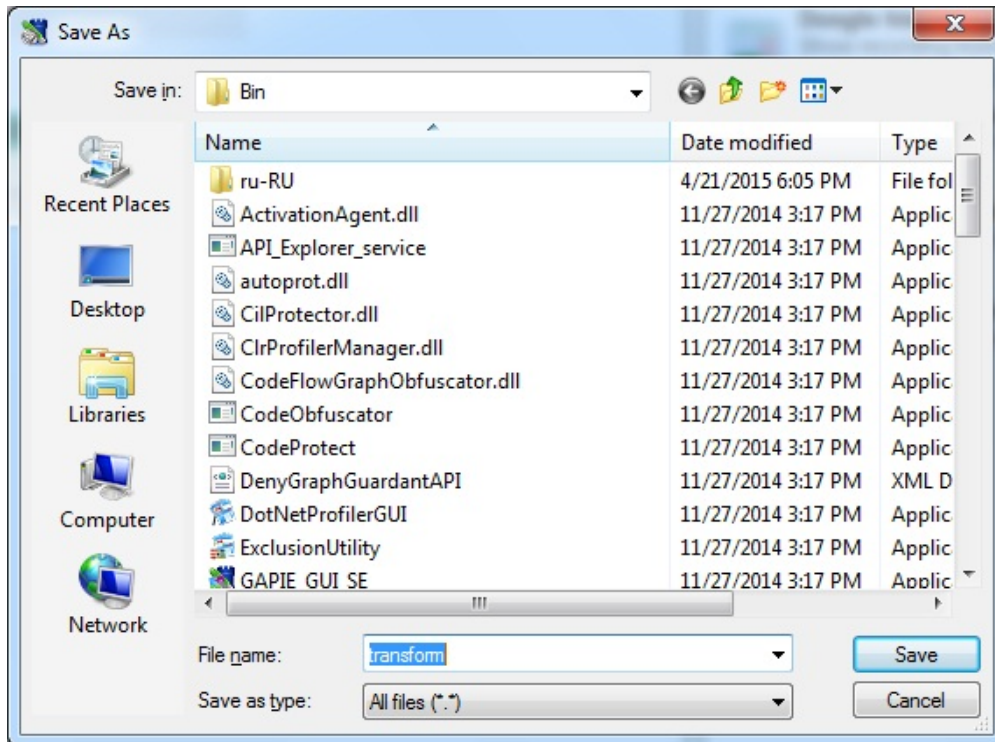
Initialization vector dialog box control elements:

Interface element	Description of purpose
Hexadecimal editor window	Allows to enter initialization vector value
[Load] button	Loads dump from *.dmp file
[Save] button	Saves dump into *.dmp file
OEM flag	Selects Windows/DOS encoding. Windows (ANSI) encoding is used by default – OEM option is off.

Dependence of operating modes of symmetric algorithms on the initialization vector:

Symmetric algorithm operating modes	Dependence on the initialization vector
ECB	None
CBC and OFB	Depend on the initialization vector. The same initialization vector must be used for information encryption. Otherwise the data will be decrypted incorrectly
CFB	Depends on the initialization vector. The same initialization vector must be used for information encryption. Otherwise the first 8 bytes of data will be decrypted incorrectly

Generating report

Clicking [Create report] button launches a standard system dialog box for saving file (filename by default: *Transform.rep).*

After this the report generation starts. Using GrdTransform operation GrdUtil.exe calls the selected algorithm in the dongle, receives answers of this algorithm and saves them in a report file.

The progress bar indicates the process of report generation completion.

Using report data

Arrays written into report file are used in the protected application.

An array of questions is stored in the body of application and is used for further accessing the dongle (it is strongly recommended to keep it in the encrypted form).

An array of answers shouldn't be stored in the application; otherwise the level of protection cannot be appropriate. Any important data used by the application can be encrypted using this array (for example, you can use the software symmetric encryption with the array of answers as the password).