

1. What does these codes do?

The “SPECK_Related_Key_Diff.cpp” source code finds a related-key differential characteristic of 10 rounds SPECK32/64. This characteristic is shown in Table 8.

The “Find_Weak_Key.cpp” source code finds a pair of weak keys based on Table 8 for SPECK32/64.

1.1 Notations:

The notations are used in the source codes are shown in Figure 1:

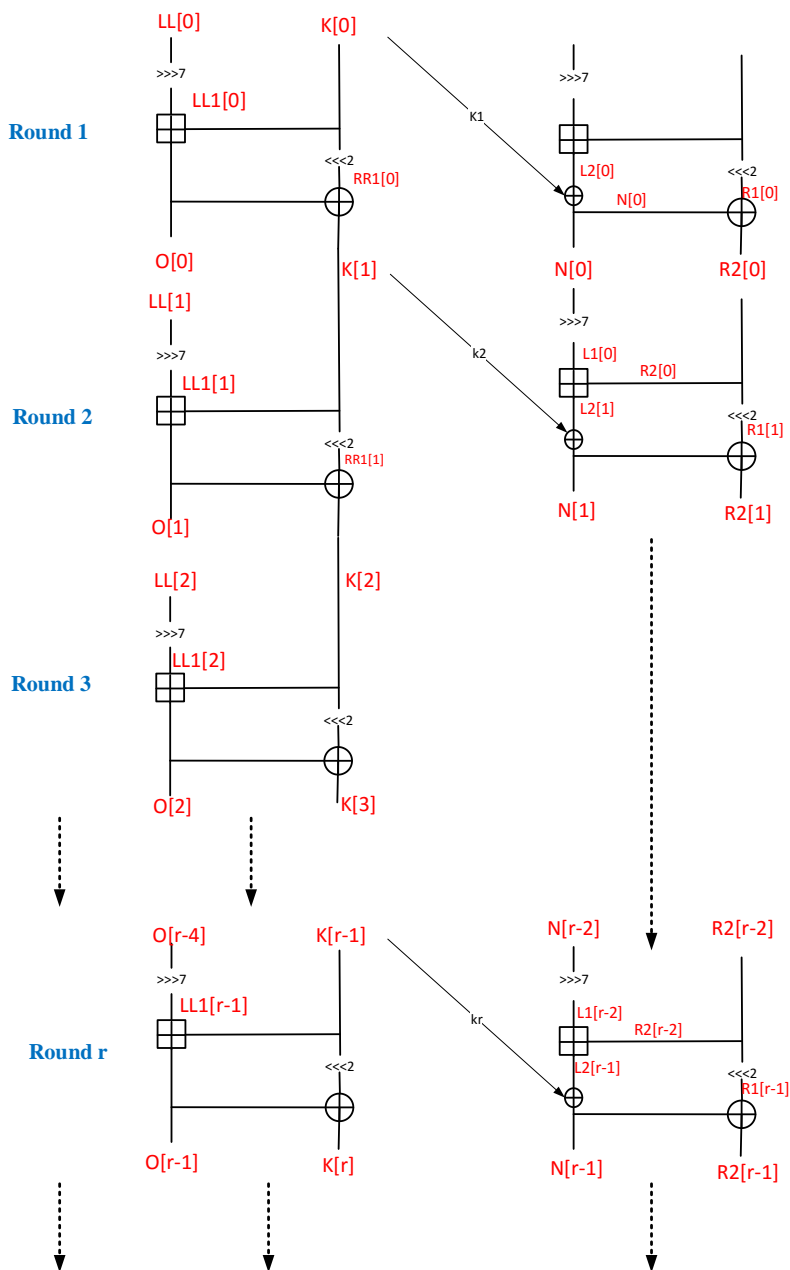


Figure 1. Notations that are used in the source codes

2. How to get up and running with Gurobi in Microsoft Visual Studio

The following steps demonstrate how to achieve this for a mixed integer programming problem:

2.1. Install & Licence Gurobi

Run the Gurobi installer file (get in from <http://www.gurobi.com/>). At the time of writing our code, we installed 64-bit version of Gurobi 8.0.1.

2.2. Create a new Visual Studio project

We are using the Visual Studio 2017, though Gurobi should be suitable for version 2015 as well. To keep things simple, open Visual Studio C++ project.

3. Set the additional include directories

Before writing any code, set the Visual Studio project dependencies, starting with the additional include files it will need.

Right-click your project folder and select properties. In the dialog that appears, select C/C++ > General > Additional Include Directories. Set this value according to how you installed Gurobi. In our installation the include files are located in the folder 'C:\gurobi752\win64\include'.

4. Set the library dependencies

Right-click your project folder and select properties. In the dialog that appears, select Linker > General > Additional Library Directories. Set the directory to the location of where your Gurobi library files are located. In our installation this location is C:\gurobi752\win64\lib

In the same dialog, select the Linker > Input tab and set the variables needed for the Additional Dependencies. For Visual Studio 2017 and this version 8.0.1 of Gurobi the additional dependencies needed are :

gurobi_c++mdd2017.lib

gurobi80.lib

Once these are set click OK.