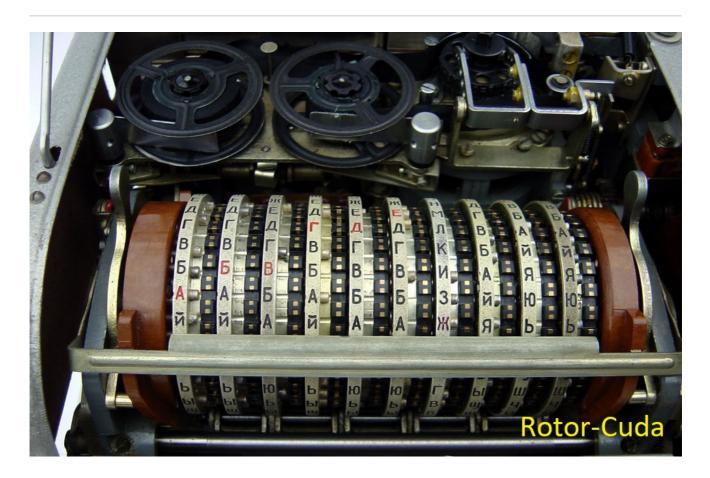


Rotor-Cuda v1.07



This is a modified version of KeyHunt v1.7. A lot of gratitude to all the developers whose

∷ README.md

Changes:

- Default Random 95% (252-256) bit + 5% (248-252) bit
- Random in a given bit range (1-256)
- Random between given bit ranges -n? -z?
- Time until the end of the search [years days hours minutes seconds] (max 300 years)
- Parameter -d 0 expert mode min. information (good for many GPUs)
- Automatic creation of Rotor-Cuda_START.bat with the specified cmd parameters
- Continuation of the search in the range, from the last checkpoint
- Ability to specify the time in minutes saving checkpoints
- Many small visual improvements

To search in a Range (CPUs)

- -t? how many cpu cores to use? (1-128 max)
- -n? save checkpoint every? minutes. (1-1000)
- If you do not specify -n? (search without continuing)
- After the Rotor-Cuda_Continue.bat file appears, you can continue from the last checkpoint.
- To continue correctly, do not change the parameters inside the bat file.
- IF YOU DO NOT NEED TO CONTINUE, DELETE THE Rotor-Cuda Continue.bat !!!
- If you start another range without deleting, a counter will be taken from the baht file and an incorrect continuation will start instead of searching.
- Example puzzle: Checkpoin recording every 2 minutes:

Random (CPUs)

- -t? how many cpu cores to use? (1-128 max)
- -r? How many billions values to update starting Private Keys? (1-100)
- -n? (1-256) bit. If you do not specify -n will be the default random 95% (252-256) bit + 5% (248-252) bit
- -z? (end random range must be greater than -n value) example: -n 63 -z 254
- Example: Random in the 253rd range:
- Random: Rotor-Cuda.exe -t 2 -m address --coin BTC -r 1
 1PWCx5fovoEaoBowAvF5k91m2Xat9bMgwb -n 253
- Example: Random between 125 and 254 bit range:
- Random: Rotor-Cuda.exe -t 2 -m address --coin BTC -r 1
 1PWCx5fovoEaoBowAvF5k91m2Xat9bMgwb -n 125 -z 254

- Random for search puzzle Example puzzle64:
- How to create databases and additional parameters

CPU Bitcoin Multi Address mode:

- Range: Rotor-Cuda.exe -t 1 -m addresses --coin BTC --range 1:1fffffffff -i puzzle_1_37_hash160_out_sorted.bin
- Random: Rotor-Cuda.exe -t 1 -m addresses --coin BTC -r 1 -i base160sorted.bin

CPU Bitcoin Single Addres mode:

- Range: Rotor-Cuda.exe -t 1 -m address --coin BTC --range 400000000:7fffffffff
 1PWCx5fovoEaoBowAvF5k91m2Xat9bMgwb
- Random: Rotor-Cuda.exe -t 1 -m address --coin BTC -r 1
 1PWCx5fovoEaoBowAvF5k91m2Xat9bMgwb

CPU ETHEREUM Multi Address mode:

- Range: Rotor-Cuda.exe -t 1 -m addresses --coin eth --range 1:1fffffffff -i puzzle_1_37_addresses_eth_sorted.bin
- Random: Rotor-Cuda.exe -t 1 -m addresses --coin eth -r 1 -i base160_eth_sorted.bin

CPU ETHEREUM Single Addres mode:

- Range: Rotor-Cuda.exe -t 1 -m address --coin eth --range 8000000:ffffffff 0xfda5c442e76a95f96c09782f1a15d3b58e32404f
- Random: Rotor-Cuda.exe -t 1 -m address --coin eth -r 1
 0xfda5c442e76a95f96c09782f1a15d3b58e32404f

CPU Public keys Multi X Points mode:

- Range: Rotor-Cuda.exe -t 1 -m xpoints --coin BTC --range 1:1fffffffff -i xpoints_1_37_out_sorted.bin
- Random: Rotor-Cuda.exe -t 1 -m xpoints --coin BTC -r 1 -i Pubkeys0.1up.bin

CPU Public key Single X Point mode:

- Range: Rotor-Cuda.exe -t 1 -m xpoint --coin BTC --range 8000000000:ffffffffffff
 a2efa402fd5268400c77c20e574ba86409ededee7c4020e4b9f0edbee53de0d4
- Random: Rotor-Cuda.exe -t 1 -m xpoint --coin BTC -r 1
 a2efa402fd5268400c77c20e574ba86409ededee7c4020e4b9f0edbee53de0d4

Example Range mode -n 2 (6 cores):

```
C:\Users\user>Rotor-Cuda.exe -t 6 -m addresses --coin BTC --range
1000000:fffffffffffff -i all.bin -n 2
```

Rotor-Cuda v1.05 (07.11.2021)

COMP MODE : COMPRESSED COIN TYPE : BITCOIN

SEARCH MODE : Multi Address

DEVICE : CPU
CPU THREAD : 6
SSE : YES
BTC HASH160s : all.bin
OUTPUT FILE : Found.txt

Loading : 100 %

Loaded : 23,908,481 Bitcoin addresses

Bloom at : 0000020CAF5ADE30

Version : 2.1
Entries : 47816962
Error : 0.0000010000
Bits : 1374985116
Bits/Elem : 28.755175

Bytes : 171873140 (163 MB)

Hash funcs : 20

Site : https://github.com/phrutis/Rotor-Cuda
Donate : bc1qh2mvnf5fujg93mwl8pe688yucaw9sflmwsukz9

Start Time : Sun Nov 7 23:46:43 2021

Global start : 1000000 (25 bit)

Global end : FFFFFFFFFF (52 bit) Global range : FFFFFFFFFF (52 bit)

Rotor info : Save checkpoints every 2 minutes. For continue range, run the bat file Rotor-Cuda_Continue.bat

CPU Core (1): 2AAAAAB7FFFFF -> 555555FFFFFE

Example continuation from Rotor-Cuda_Continue.bat

Rotor-Cuda v1.05 (07.11.2021)

COMP MODE : COMPRESSED COIN TYPE : BITCOIN

SEARCH MODE : Multi Address

DEVICE : CPU
CPU THREAD : 6
SSE : YES
BTC HASH160s : all.bin
OUTPUT FILE : Found.txt

Loading : 100 %

Loaded : 23,908,481 Bitcoin addresses

Bloom at : 000002331C2E9DB0

Version : 2.1
Entries : 47816962
Error : 0.0000010000
Bits : 1374985116
Bits/Elem : 28.755175

Bytes : 171873140 (163 MB)

Hash funcs : 20

Site : https://github.com/phrutis/Rotor-Cuda
Donate : bc1qh2mvnf5fujg93mwl8pe688yucaw9sflmwsukz9

Start Time : Sun Nov 7 23:56:05 2021

Rotor : Continuing search from BAT file. Checkpoint created: Sun Nov 7

23:54:13 2021

Global start : 1000000 (25 bit) Global end : FFFFFFFFFF (52 bit)

Global range : FFFFFFFFF (52 bit)

Rotor info : Continuation... Divide the remaining range FFFFF10DDD7F9 (52 bit)

into CPU 6 cores

Rotor info : Save checkpoints every 2 minutes. For continue range, run the bat file Rotor-Cuda_Continue.bat

CPU Core (2): 28B05C00 -> 2AAAAD3305BFF

CPU Core (1): 2AAAAD3305BFF -> 555557DB05BFE

CPU Core (3): 8000028305BFD -> AAAAAD2B05BFC

CPU Core (4): 555557DB05BFE -> 8000028305BFD

CPU Core (5): AAAAAD2B05BFC -> D55557D305BFB

CPU Core (6): D55557D305BFB -> FFFFFFFFFFFF

[00:00:12] [F033463D] [F: 0] [Y:015 D:351] [C: 0.000091 %] [CPU 6: 8.95 Mk/s]

[T: 4,108,218,368]

Example Random mode use -n 253 -z 254 (6 cores):

C:\Users\user>Rotor-Cuda.exe -t 6 -m addresses --coin BTC -i all.bin -r 1 -n 253 - z 254

Rotor-Cuda v1.05 (07.11.2021)

COMP MODE : COMPRESSED COIN TYPE : BITCOIN

SEARCH MODE : Multi Address

DEVICE : CPU
CPU THREAD : 6
SSE : YES
BTC HASH160s : all.bin
OUTPUT FILE : Found.txt

Loading : 100 %

Loaded : 23,908,481 Bitcoin addresses

Bloom at : 000001AA32D29D80

Version : 2.1
Entries : 47816962
Error : 0.0000010000
Bits : 1374985116
Bits/Elem : 28.755175

Bytes : 171873140 (163 MB)

Hash funcs : 20

Site : https://github.com/phrutis/Rotor-Cuda
Donate : bc1qh2mvnf5fujg93mwl8pe688yucaw9sflmwsukz9

Start Time : Sun Nov 7 23:58:07 2021

ROTOR Random : Private keys random 253 <~> 254 (bit)

Base Key : Randomly changes 6 Private keys every 1,000,000,000 on the

counter

[00:00:27] [R: 0]

[11969326AD87F607FEABE042E9CE70552742E0C0830BF138368058C87963E138] [F: 0] [CPU 6: 9.07 Mk/s] [T: 250,746,880]

To search in a Range Add parameters (GPUs)

- -n? save checkpoint every? minutes. (1-10000)
- If you do not specify -n? (search without continuing)
- After the Rotor-Cuda_Continue.bat file appears, you can continue from the last checkpoint.
- To continue correctly, do not change the parameters inside the file.
- If you do not need to continue, DELETE the Rotor-Cuda_Continue.bat !!!

For Random use - r 100 (GPUs)

- -r? How many billions to update 65535 starting Private Keys? (1-100000) Recommended every 5-15 minutes. (-n 100)
- -n? (1-256) bit. If you do not specify -n will be the default 95% (252-256) bit + 5% (248-252) bit
- -z? (end random range must be greater than -n value) example: -n 252 -z 256
- Random for search puzzle64 example:
- If you know that your parameters are correct, use the expert mode -d 0 If you are using many GPUs use -d 0 for convenience
- If your GPU is weaker than RTX 1080 or the driver crashes. Remove --gpux 256,256 from the row the grid will be auto-assigned.
- How to create databases and additional parameters

GPU Bitcoin Multi Address mode:

- Range: Rotor-Cuda.exe -g --gpui 0 --gpux 256,256 -m addresses --coin BTC --range
 1:1fffffffff -i puzzle_1_37_hash160_out_sorted.bin
- Random: Rotor-Cuda.exe -g --gpui 0 --gpux 256,256 -m addresses --coin BTC -r 250 -i base160sorted.bin

GPU Bitcoin Single Addres mode:

- Range: Rotor-Cuda.exe -g --gpui 0 --gpux 256,256 -m address --coin BTC --range 40000000:7ffffffff 1PWCx5fovoEaoBowAvF5k91m2Xat9bMgwb
- Random: Rotor-Cuda.exe -g --gpui 0 --gpux 256,256 -m address --coin BTC -r 250
 1PWCx5fovoEaoBowAvF5k91m2Xat9bMgwb

GPU ETHEREUM Multi Address mode:

- Range: Rotor-Cuda.exe -g --gpui 0 --gpux 256,256 -m addresses --coin eth --range 1:1ffffffff -i puzzle_1_37_addresses_eth_sorted.bin
- Random: Rotor-Cuda.exe -g --gpui 0 --gpux 256,256 -m addresses --coin eth -r 250
 -i base160_eth_sorted.bin

GPU ETHEREUM Single Addres mode:

- Range: Rotor-Cuda.exe -g --gpui 0 --gpux 256,256 -m address --coin eth --range 8000000:fffffff 0xfda5c442e76a95f96c09782f1a15d3b58e32404f
- Random: Rotor-Cuda.exe -g --gpui 0 --gpux 256,256 -m address --coin eth -r 250 0xfda5c442e76a95f96c09782f1a15d3b58e32404f

GPU Public key Multi X Points mode:

- Range: Rotor-Cuda.exe -g --gpui 0 --gpux 256,256 -m xpoints --coin BTC --range 1:1fffffffff -i xpoints_1_37_out_sorted.bin
- Random: Rotor-Cuda.exe -g --gpui 0 --gpux 256,256 -m xpoints --coin BTC -r 250 -i Pubkeys1up.bin

GPU Public key Single X Point mode Puzzle120 example:

- How to create databases and additional parameters

Example Range mode and -n 2:

```
C:\Users\user>Rotor-Cuda.exe -g --gpui 0 --gpux 256,256 -m xpoint --coin BTC --
range 800000000:ffffffffff
a2efa402fd5268400c77c20e574ba86409ededee7c4020e4b9f0edbee53de0d4 -n 2
 Rotor-Cuda v1.05 (07.11.2021)
 COMP MODE
            : COMPRESSED
 COIN TYPE : BITCOIN
 SEARCH MODE : Single X Point
            : GPU
 DEVICE
 CPU THREAD : 0
 GPU IDS
            : 0
 GPU GRIDSIZE: 256x256
             : NO
 SSE
 BTC XPOINT : a2efa402fd5268400c77c20e574ba86409ededee7c4020e4b9f0edbee53de0d4
 OUTPUT FILE : Found.txt
 Start Time : Sun Nov 7 23:59:13 2021
 Global start: 8000000000 (40 bit)
 Global end : FFFFFFFF (40 bit)
 Global range: 7FFFFFFFF (39 bit)
 GPU
             : GPU #0 NVIDIA GeForce RTX 2070 (36x64 cores) Grid(256x256)
            : Save checkpoints every 2 minutes. For continue range, run the bat
 Rotor info
file Rotor-Cuda_Continue.bat
            : Divide the range 7FFFFFFFF (39 bit) into GPU 65536 threads
 Thread 00000 : 8000000000 -> 80007FFFF
 Thread 00001 : 80007FFFFF -> 8000FFFFFE
 Thread 00002 : 8000FFFFFE -> 80017FFFFD
 Thread 00003 : 80017FFFFD -> 8001FFFFFC
 Thread 65534 : FFFEFF0002 -> FFFF7F0001
 Thread 65535 : FFFF7F0001 -> FFFFFF0000
 Thread 65536 : FFFFFF0000 -> 100007EFFFF
 [00:02:49] [C99473A60C] [F: 0] [00:02:04] [C: 57.543945 %] [GPU: 1.87 Gk/s] [T:
316,351,184,896]
______
 PubAddress: 1EeAxcprB2PpCnr34VfZdFrkUWuxyiNEFv
 Priv (WIF): p2pkh:KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qYjgd9aFJuCJDo5F6Jm7
 Priv (HEX): E9AE4933D6
 PubK (HEX): 03A2EFA402FD5268400C77C20E574BA86409EDEDEE7C4020E4B9F0EDBEE53DE0D4
______
 [00:02:50] [CA042FDBBD] [F: 1] [00:02:03] [C: 57.885742 %] [GPU: 1.87 Gk/s] [T:
318,230,233,088]
```

BYE

Continuation (example above) from last checkpoint run Rotor-Cuda Continue.bat

```
C:\Users\user>Rotor-Cuda.exe -g --gpui 0 --gpux 256,256 -m xpoint --coin BTC --
range 800000000:fffffffff
a2efa402fd5268400c77c20e574ba86409ededee7c4020e4b9f0edbee53de0d4 -n 2
 Rotor-Cuda v1.05 (07.11.2021)
 COMP MODE : COMPRESSED
 COIN TYPE
             : BITCOIN
 SEARCH MODE : Single X Point
          : GPU
 DEVICE
 CPU THREAD : 0
 GPU IDS
          : 0
 GPU GRIDSIZE: 256x256
 SSE
             : NO
 BTC XPOINT : a2efa402fd5268400c77c20e574ba86409ededee7c4020e4b9f0edbee53de0d4
 OUTPUT FILE : Found.txt
 Start Time : Mon Nov 8 00:03:13 2021
 Rotor : Continuing search from BAT file. Checkpoint created: Mon Nov 8
00:01:06 2021
 Global start: 8000000000 (40 bit)
 Global end : FFFFFFFF (40 bit)
 Global range: 7FFFFFFFF (39 bit)
 GPU
             : GPU #0 NVIDIA GeForce RTX 2070 (36x64 cores) Grid(256x256)
             : Save checkpoints every 2 minutes. For continue range, run the bat
 Rotor info
file Rotor-Cuda_Continue.bat
 Rotor info
            : Continuation... Divide the remaining range 4FAFFEFFFF (39 bit)
into GPU 65536 threads
 Thread 00000 : 8000305000 -> 80007FFFFF
 Thread 00001: 8000B04FFF -> 8000FFFFFE
 Thread 00002 : 8001304FFE -> 80017FFFFD
 Thread 00003 : 8001B04FFD -> 8001FFFFFC
 Thread 65534 : FFFF2F5002 -> FFFF7F0001
 Thread 65535 : FFFFAF5001 -> FFFFFF0000
 Thread 65536 : 100002F5000 -> 100007EFFFF
 [00:00:56] [C54475752E] [F: 0] [00:02:03] [C: 57.714844 %] [GPU: 1.87 Gk/s] [T:
317,290,708,992]
______
 PubAddress: 1EeAxcprB2PpCnr34VfZdFrkUWuxyiNEFv
 Priv (WIF): p2pkh:KwDiBf89QgGbjEhKnhXJuH7LrciVrZi3qYjgd9aFJuCJDo5F6Jm7
```

https://github.com/phrutis/Rotor-Cuda/

```
Priv (HEX): E9AE4933D6
```

PubK (HEX): 03A2EFA402FD5268400C77C20E574BA86409EDEDEE7C4020E4B9F0EDBEE53DE0D4

[00:00:57] [C5B436553B] [F: 1] [00:02:02] [C: 58.056641 %] [GPU: 1.87 Gk/s] [T:

319, 169, 757, 184]

C:\Users\user>goto :loop

Example Random mode use -n 63 -z 64:

C:\Users\user>Rotor-Cuda.exe -g --gpui 0 --gpux 256,256 -m xpoint --coin BTC -r 50 a2efa402fd5268400c77c20e574ba86409ededee7c4020e4b9f0edbee53de0d4 -n 63 -z 64

Rotor-Cuda v1.05 (07.11.2021)

: COMPRESSED COMP MODE COIN TYPE : BITCOIN

SEARCH MODE : Single X Point

DEVICE : GPU CPU THREAD : 0 **GPU IDS**

GPU GRIDSIZE: 256x256 : NO SSE

BTC XPOINT : a2efa402fd5268400c77c20e574ba86409ededee7c4020e4b9f0edbee53de0d4

OUTPUT FILE : Found.txt

Start Time : Mon Nov 8 00:05:07 2021

: GPU #0 NVIDIA GeForce RTX 2070 (36x64 cores) Grid(256x256) **GPU**

ROTOR Random : Private keys random 63 (bit) <~> 64 (bit)

Base Key : Randomly changes 65536 start Private keys every 50,000,000,000 on

the counter

[00:00:30] [R: 1] [2B86D4E372BDBA32] [F: 0] [GPU: 1.52 Gk/s] [T: 56,371,445,760]

Example Random --range

Rotor-Cuda.exe -g --gpui 0 --gpux 256,256 -m xpoints --coin BTC -r 100 --range 777777777:8888888888 -i Pub01.bin

Rotor-Cuda v1.05 (07.11.2021)

COMP MODE : COMPRESSED : BITCOIN COIN TYPE

SEARCH MODE : Multi X Points

DEVICE : GPU CPU THREAD : 0

10/3/22, 3:08 PM

GPU IDS : 0

GPU GRIDSIZE : 256x256 SSE : NO

BTC XPOINTS : Pub01.bin
OUTPUT FILE : Found.txt

Loading : 100 %

Loaded : 243,734 Bitcoin xpoints

Bloom at : 00000277E60E9E50

Version : 2.1 Entries : 487468

Error : 0.0000010000 Bits : 14017227 Bits/Elem : 28.755175 Bytes : 1752154 (1 MB)

Hash funcs : 20

Site : https://github.com/phrutis/Rotor-Cuda

Donate : bc1qh2mvnf5fujg93mwl8pe688yucaw9sflmwsukz9

Start Time : Mon Nov 8 00:06:12 2021

GPU : GPU #0 NVIDIA GeForce RTX 2070 (36x64 cores) Grid(256x256)

Base Key : Randomly changes 65536 start Private keys every 100,000,000,000

on the counter

ROTOR Random : Min 39 (bit) 777777777 ROTOR Random : Max 40 (bit) 8888888888

[00:01:19] [R: 1] [7FDFF2058C] [F: 0] [GPU: 1.12 Gk/s] [T: 104,555,610,112]

Example for multiple GPUs range search parameter -d 0

C:\Users\user>Rotor-Cuda.exe -g --gpui 0 --gpux 256,256 -m address --coin eth --range 1:1fffffffffffffff -d 0 0xfda5c442e76a95f96c09782f1a15d3b58e32404f

Rotor-Cuda v1.05 (07.11.2021)

COIN TYPE : ETHEREUM

SEARCH MODE : Single Address

DEVICE : GPU
CPU THREAD : 0
GPU IDS : 0

GPU GRIDSIZE : 256x256 SSE : NO

ETH ADDRESS : 0xfda5c442e76a95f96c09782f1a15d3b58e32404f

OUTPUT FILE : Found.txt

Start Time : Mon Nov 8 00:08:26 2021

```
GPU : GPU #0 NVIDIA GeForce RTX 2070 (36x64 cores) Grid(256x256) [00:00:42] [F: 0] [Y:156 D:015] [C: 0.000001 %] [GPU: 468.58 Mk/s] [T: 20,266,876,928]
```

Building

Windows

- Microsoft Visual Studio Community 2019
- CUDA version 10.22

For RTX 3060, 3070, 3080, 3090, A5000, A6000, A100

- Use CUDA 11.7
- Rename this file (remove 30xx) from the name and replace the file in the project

For RTX 2060, 2070, 2080

- Use CUDA 11.7
- Rename this file (remove 20xx) from the name and replace the file in the project

License

Rotor-Cuda is licensed under GPLv3.

Donation

BTC: bc1qh2mvnf5fujg93mwl8pe688yucaw9sflmwsukz9

Disclaimer

ALL THE CODES, PROGRAM AND INFORMATION ARE FOR EDUCATIONAL PURPOSES ONLY. USE IT AT YOUR OWN RISK. THE DEVELOPER WILL NOT BE RESPONSIBLE FOR ANY LOSS, DAMAGE OR CLAIM ARISING FROM USING THIS PROGRAM.

Releases 8



+ 7 releases