National Research Council of Italy

DEEPSEC

BITLOCKER MEETS GPUS

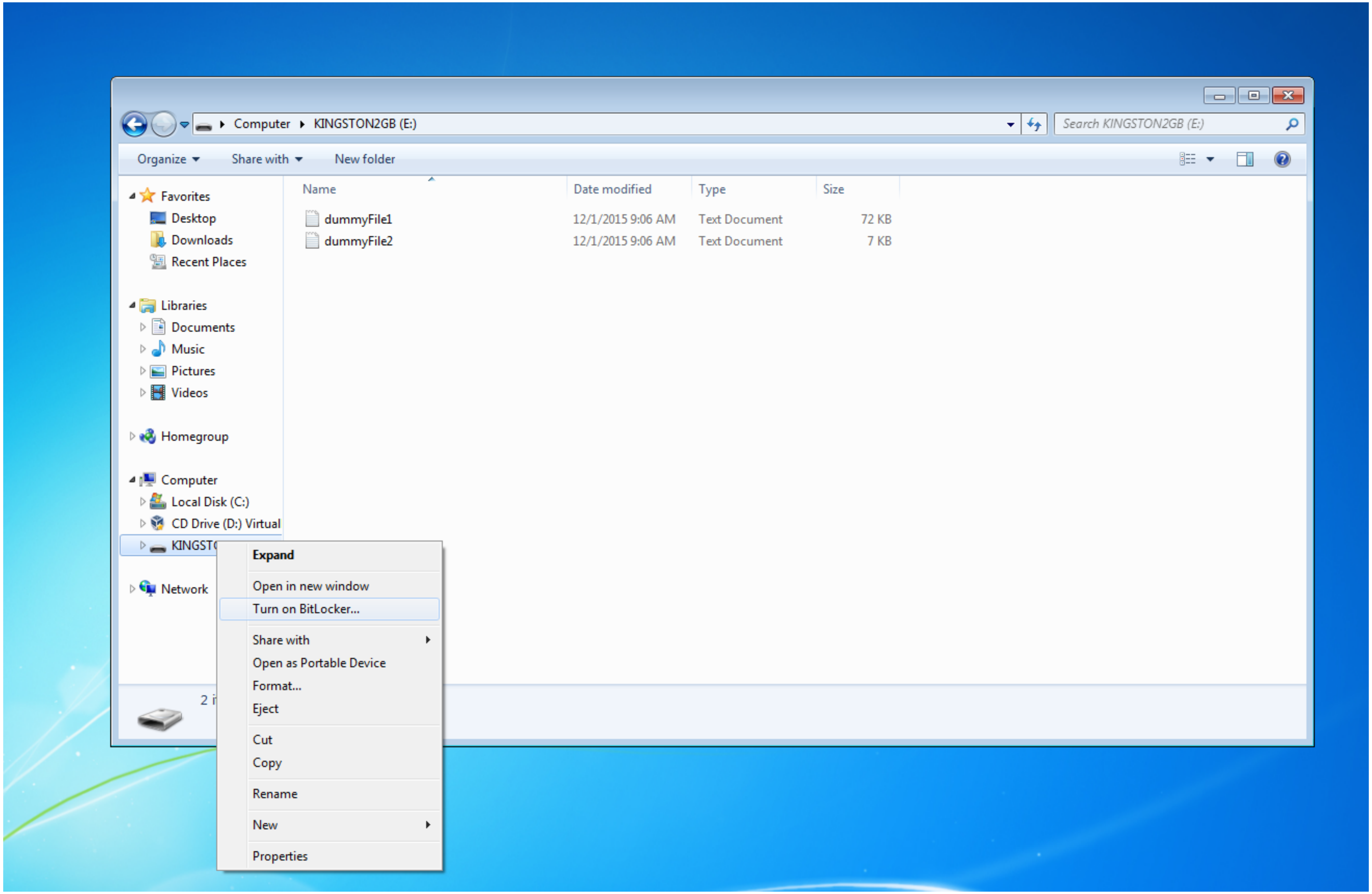
BITCRACKER

Elena Agostini, Massimo Bernaschi

BITLOCKER

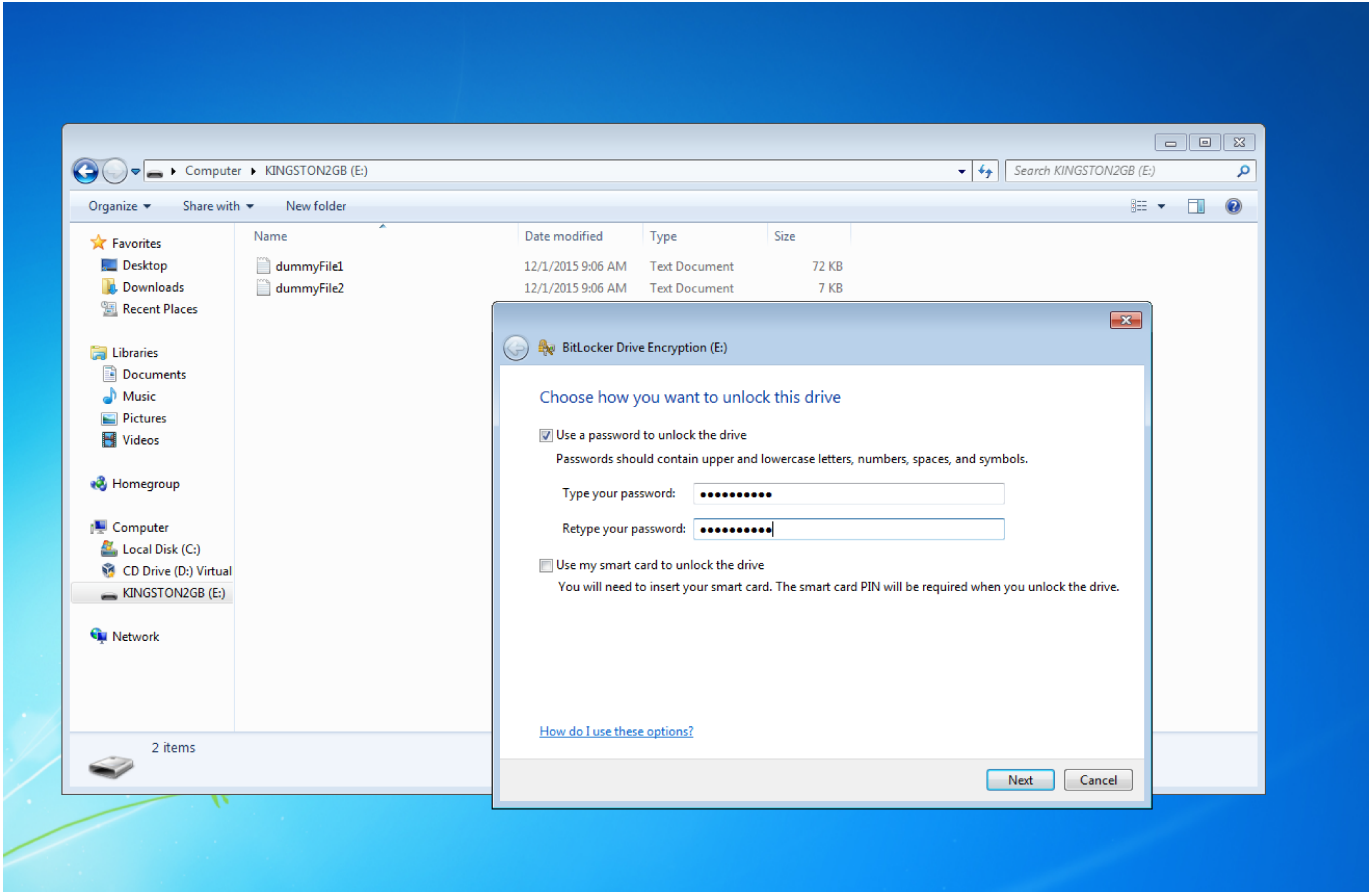
- Windows Vista, 7, 8.1 and 10 encryption feature (Ultimate, Pro, Enterprise, etc..)
- It encrypts several types of memory units like internal HD (native BitLocker) or removable devices (BitLocker To Go) like USB, SD cards, etc..
- Several authentication methods to encrypt (decrypt) memory devices:
  - TPM (Trusted Platform Module), TPM + PIN, etc..
  - Smart Card
  - Recovery Key
  - **User Password**

BITLOCKER PASSWORD METHOD: ENCRYPTION, STEP 1



Name	Date modified	Type	Size
dummyFile1	12/1/2015 9:06 AM	Text Document	72 KB
dummyFile2	12/1/2015 9:06 AM	Text Document	7 KB

BITLOCKER PASSWORD METHOD: ENCRYPTION, STEP 2



BitLocker Drive Encryption (E:)

Choose how you want to unlock this drive

☑ Use a password to unlock the drive

Passwords should contain upper and lowercase letters, numbers, spaces, and symbols.

Type your password: ●●●●●●●●●●●

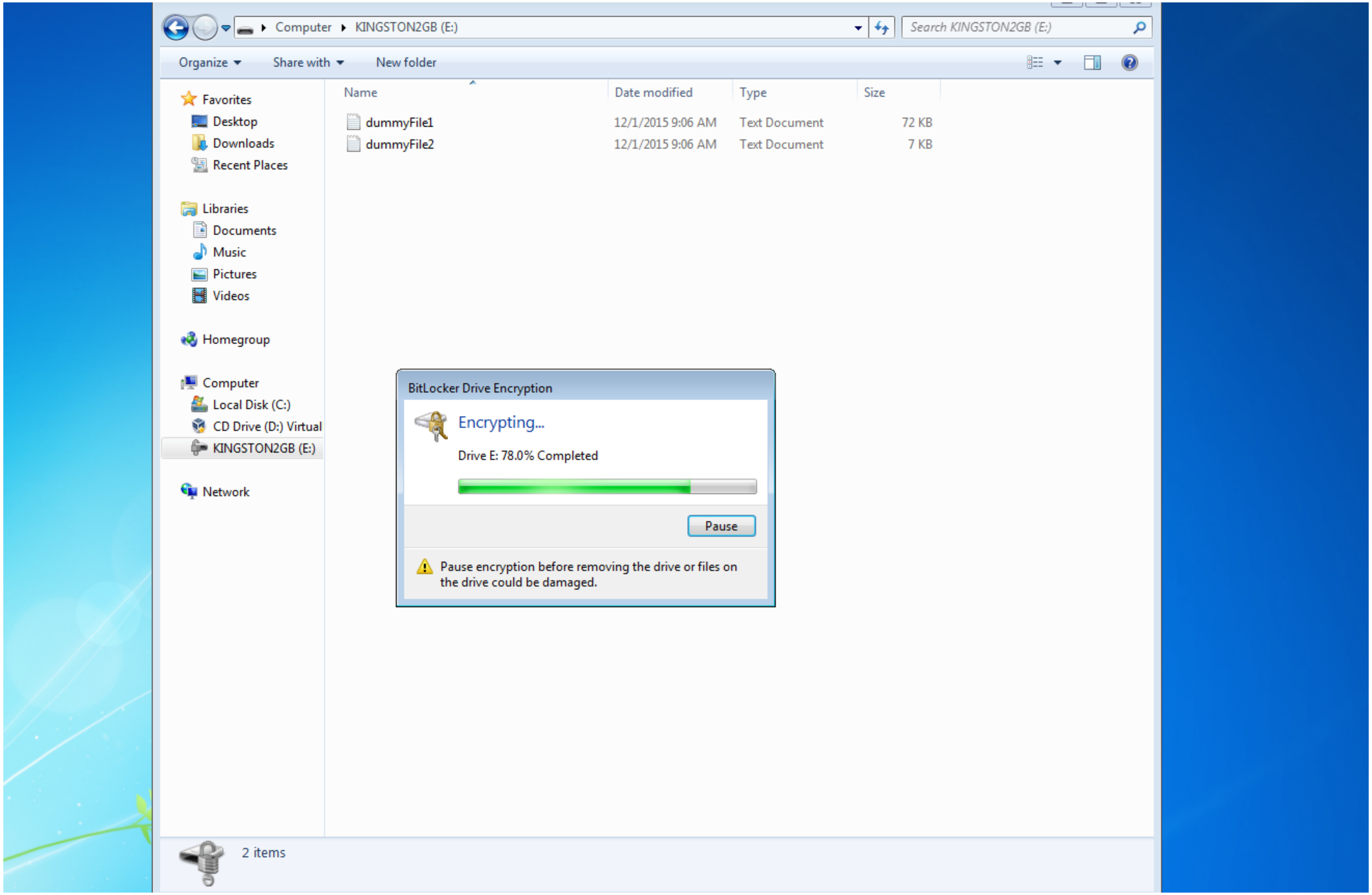
Retype your password: ●●●●●●●●●●●

□ Use my smart card to unlock the drive

You will need to insert your smart card. The smart card PIN will be required when you unlock the drive.

How do I use these options?

BITLOCKER PASSWORD METHOD: ENCRYPTION, STEP 3



Name	Date modified	Type	Size
dummyFile1	12/1/2015 9:06 AM	Text Document	72 KB
dummyFile2	12/1/2015 9:06 AM	Text Document	7 KB

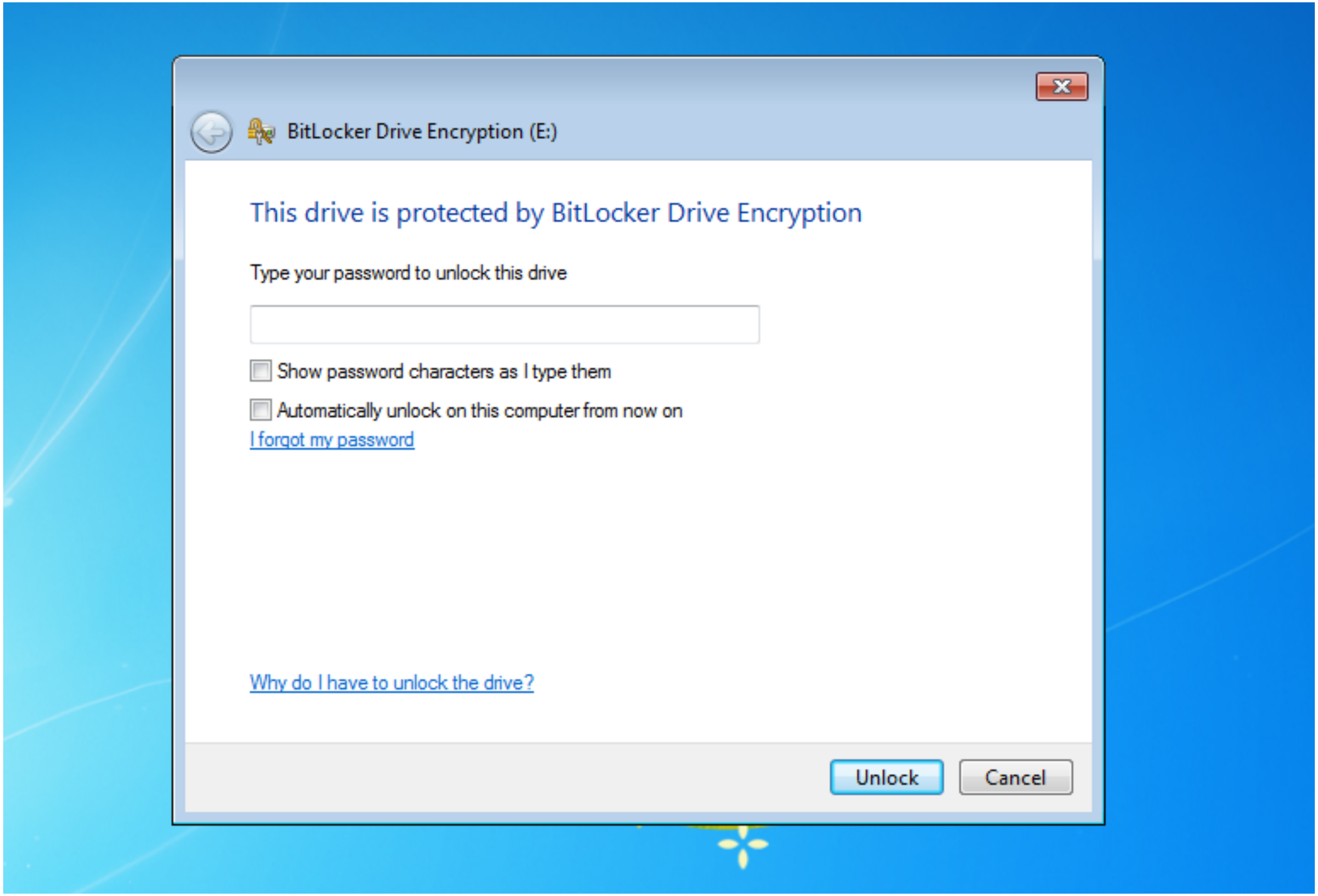
BitLocker Drive Encryption

Encrypting...

Drive E: 78.0% Completed

Pause encryption before removing the drive or files on the drive could be damaged.

BITLOCKER PASSWORD METHOD: DECRYPTION



BitLocker Drive Encryption (E:)

This drive is protected by BitLocker Drive Encryption

Type your password to unlock this drive

□ Show password characters as I type them

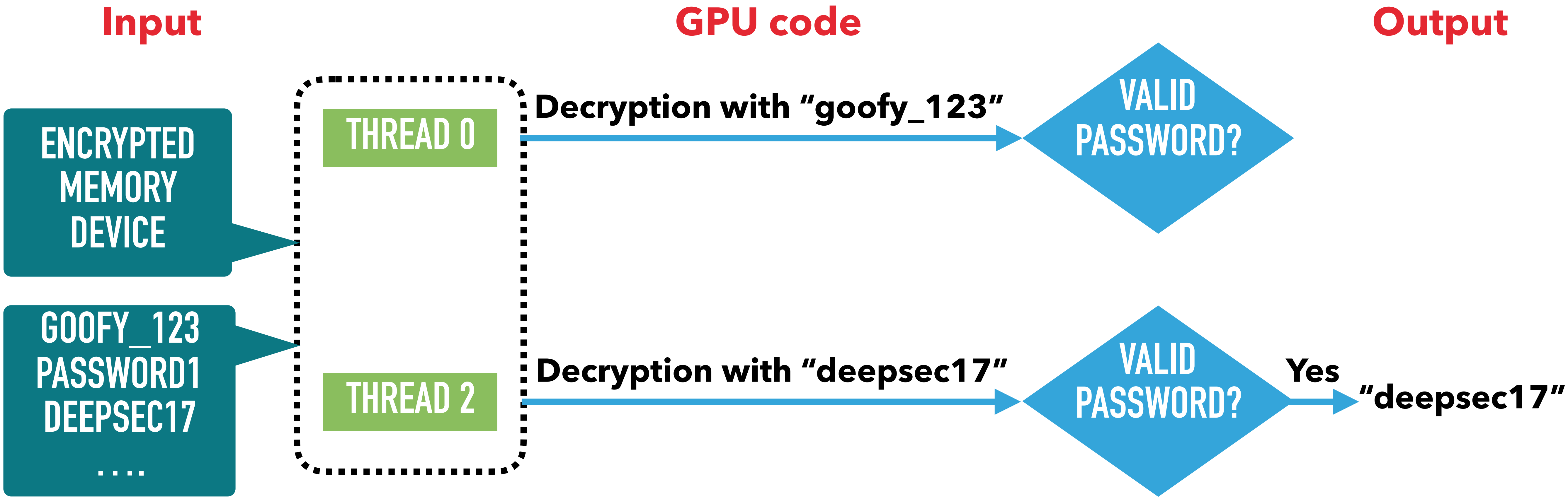
□ Automatically unlock on this computer from now on

I forgot my password

Why do I have to unlock the drive?

BITCRACKER

- First open source password cracking tool for memory devices encrypted with BitLocker
- User password authentication method
  - Find the right password to decrypt an encrypted memory unit
- **Dictionary attack** by means of **GPUs**
  - Every thread decrypts the device testing a different password

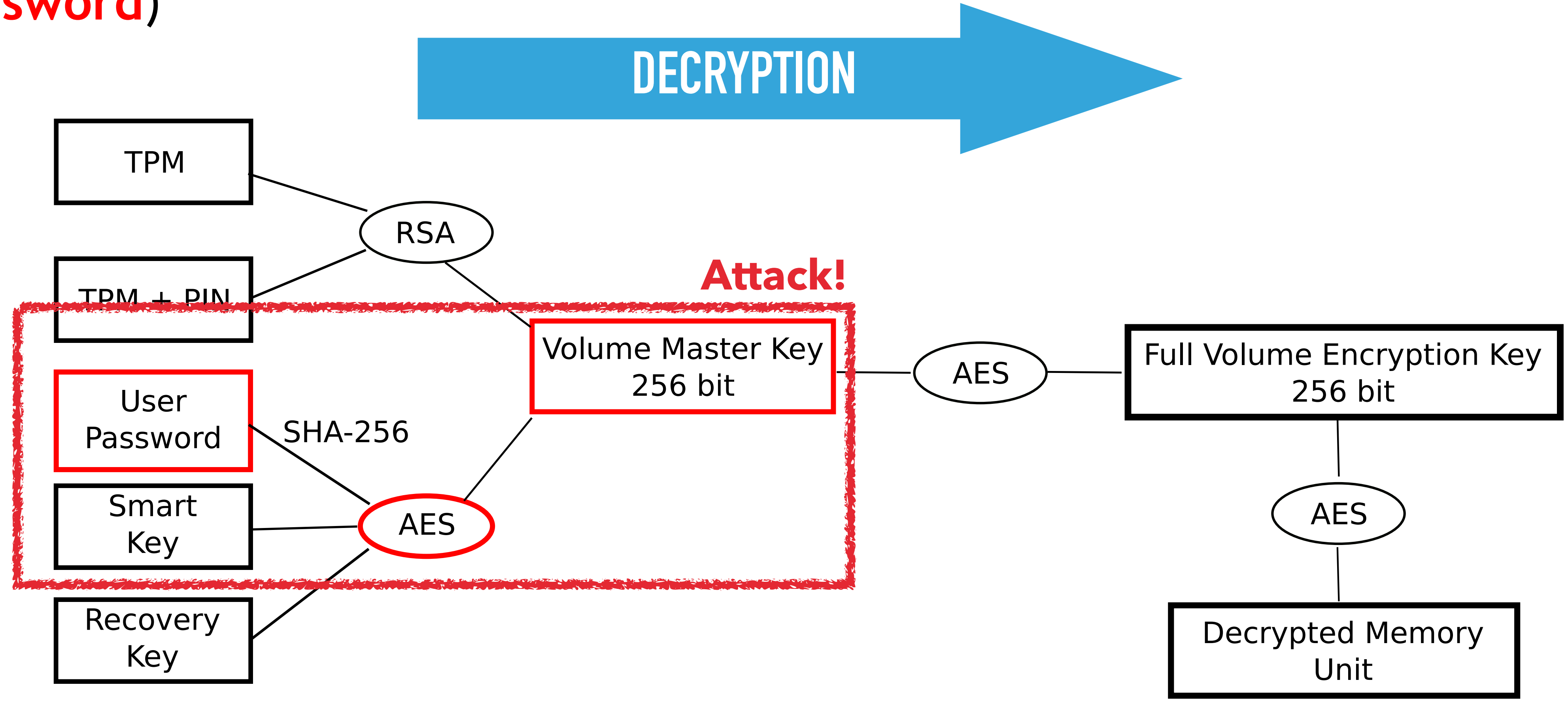


BITLOCKER FORMAT

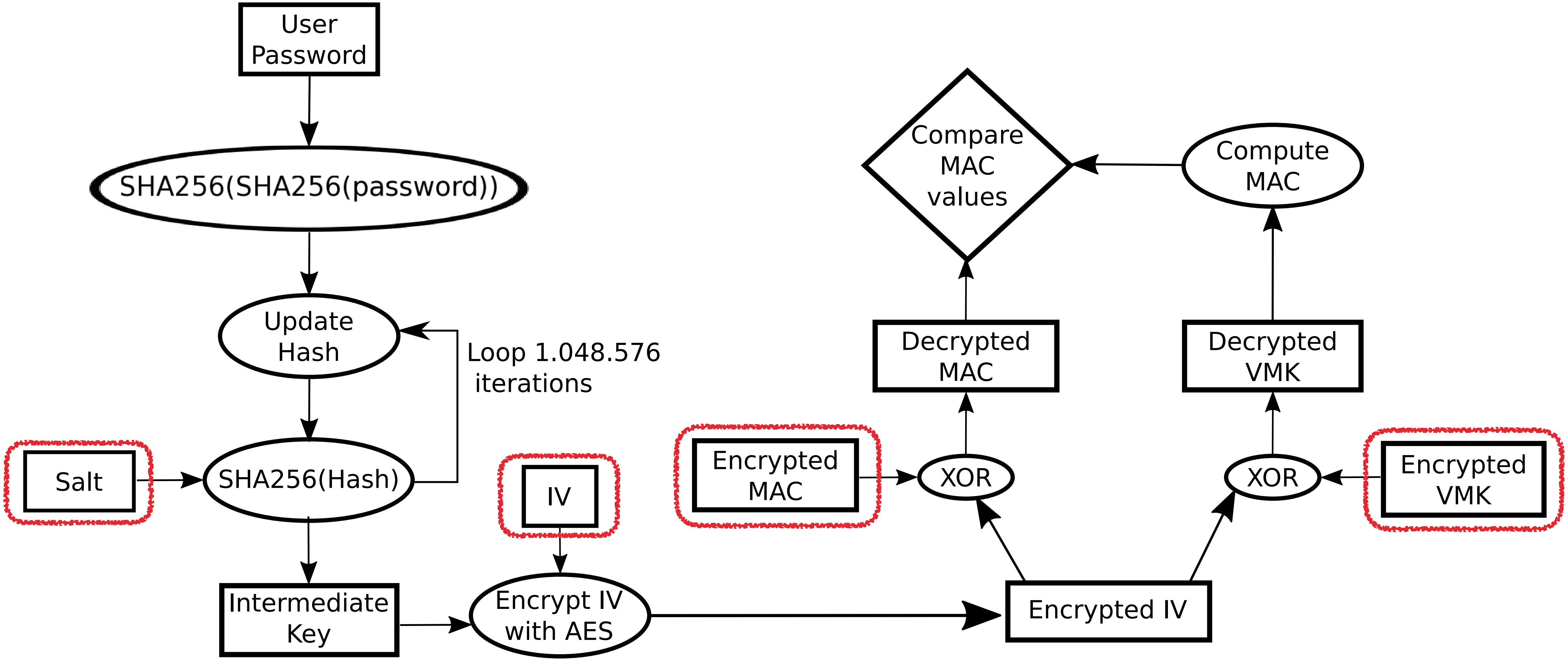
- Decryption algorithm
- Headers and metadata inside BitLocker encrypted devices
- Sources:
  - Microsoft (https://technet.microsoft.com)
  - **libbde**: Library and tools useful to access the BitLocker encrypted volumes (https://github.com/libyal/libbde)
  - **dislocker**: FUSE driver to read/write Windows' BitLocker-ed volumes under Linux/Mac OSX (https://github.com/Aorimn/dislocker)

BITLOCKER KEYS

- Complex architecture of keys to encrypt devices
- Encryption:
  - Sectors are encrypted by using a key called **FVEK** (Full-Volume Encryption Key)
  - The FVEK is, in turn, encrypted with a key called **VMK** (Volume Master Key)
  - The VMK is also encrypted with an authentication method (*e.g.*, **user** provided **password**)



BITLOCKER VMK DECRYPTION ALGORITHM



User Password

SHA256(SHA256(password))

Update Hash

Loop 1.048.576 iterations

Salt

SHA256(Hash)

Intermediate Key

IV

Encrypt IV with AES

Encrypted IV

Encrypted MAC

XOR

Decrypted MAC

Compare MAC values

Compute MAC

Decrypted VMK

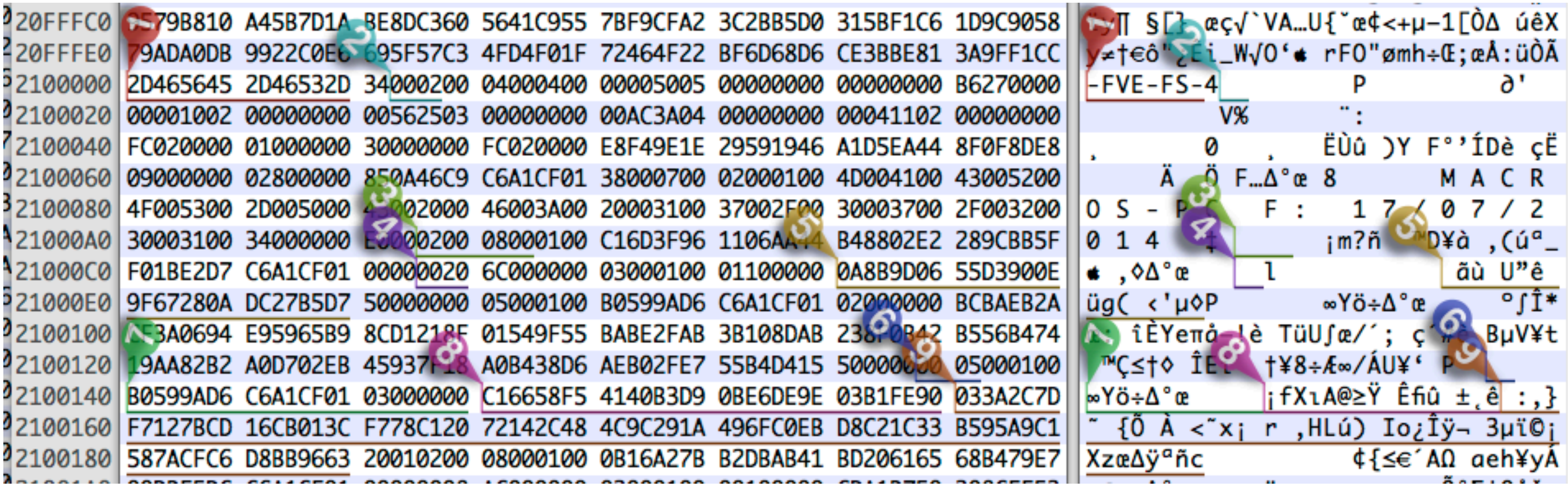
XOR

Encrypted VMK

?

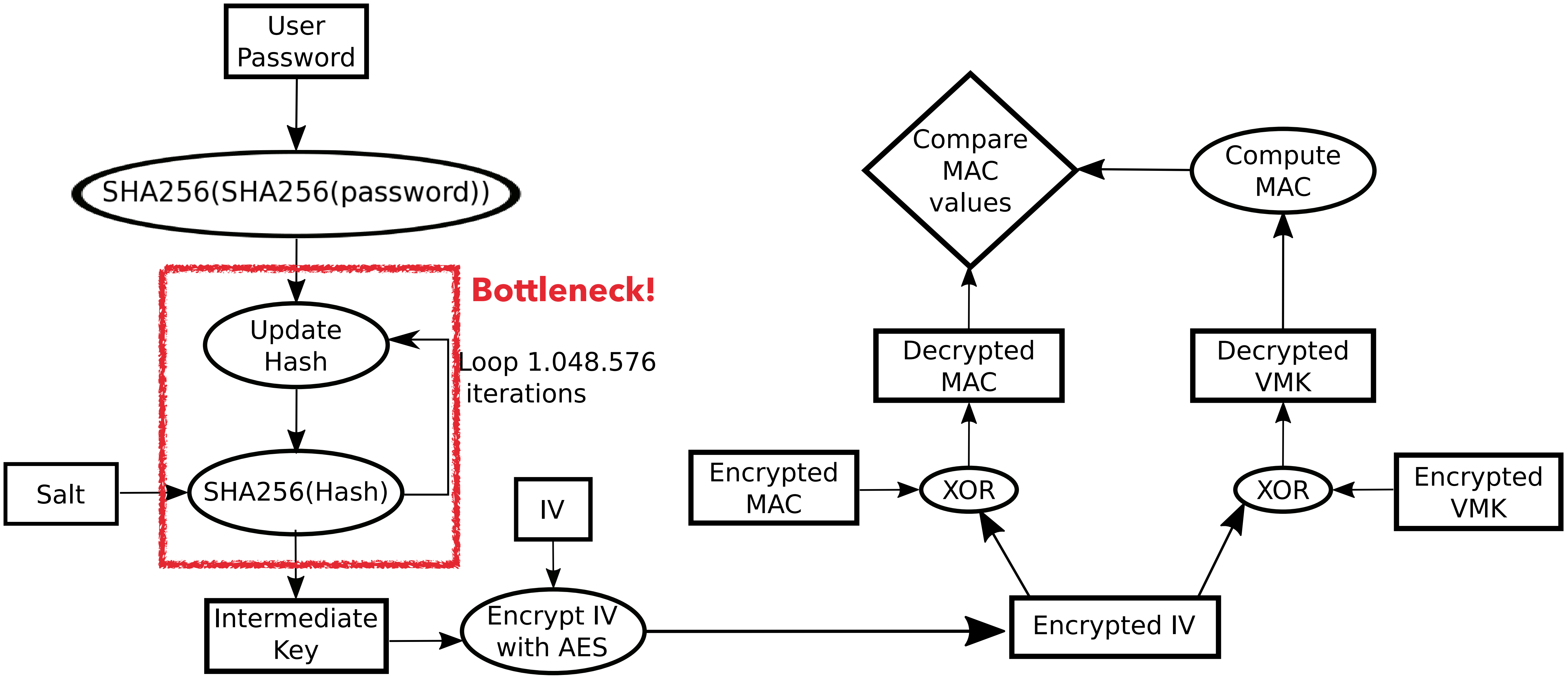
BITLOCKER METADATA

- 3 FVE (*Full Volume Encryption*) metadata blocks
- Initial signature "-FVE-FS-"
- Windows 8.1, FVE block: salt (5), VMK encrypted with AES-CCM (6), encrypted MAC (8), encrypted VMK (9), etc…



```
20FFFC0 9579B810 A45B7D1A BE8DC360 5641C955 7BF9CFA2 3C2BB5D0 315BF1C6 1D9C9058  ÿ∏ §[] æç√`VA…U{˘æ¢<+µ–1[ÒΔ úêX
20FFFE0 79ADA0DB 9922C0E6 695F57C3 4FD4F01F 72464F22 BF6D68D6 CE3BBE81 3A9FF1CC  y≠†€ô"¿Ei_W√O‘ rFO"ømh÷Œ;æÅ:üÒÃ
2100000 2D465645 2D46532D 34000200 04000400 00005005 00000000 00000000 B6270000  -FVE-FS-4        P          ∂'
2100020 00001002 00000000 00562503 00000000 00AC3A04 00000000 00041102 00000000            V%      ¨:
2100040 FC020000 01000000 30000000 FC020000 E8F49E1E 29591946 A1D5EA44 8F0F8DE8  ,        0   ,   ËÙû )Y F°’ÍDè çË
2100060 09000000 02800000 850A46C9 C6A1CF01 38000700 02000100 4D004100 43005200        Ä   Ö F…Δ°œ 8       M A C R
2100080 4F005300 2D005000 45002000 46003A00 20003100 37002F00 30003700 2F003200  O S - P E   F :   1 7 / 0 7 / 2
21000A0 30003100 34000000 E0000200 08000100 C16D3F96 1106AA74 B48802E2 289CBB5F  0 1 4   ‡         ¡m?ñ ™D¥à ,(úª_
21000C0 F01BE2D7 C6A1CF01 00000020 6C000000 03000100 01100000 0A8B9D06 55D3900E   ,◊Δ°œ       l              ãù U”ê
21000E0 9F67280A DC27B5D7 50000000 05000100 B0599AD6 C6A1CF01 02000000 BCBAEB2A  üg( <'µ◊P       ∞Yö÷Δ°œ      °∫Î*
2100100 0E3A0694 E95965B9 8CD1218F 01549F55 BABE2FAB 3B108DAB 238F0B42 B556B474  Ä: îÈYeπå!è TüU∫æ/´; çè B µV¥t
2100120 19AA82B2 A0D702EB 45937F18 A0B438D6 AEB02FE7 55B4D415 50000000 05000100  ™Ç≤†◊ ÎEì  †¥8÷Æ∞/ÁU¥‘ P
2100140 B0599AD6 C6A1CF01 03000000 C16658F5 4140B3D9 0BE6DE9E 03B1FE90 033A2C7D  ∞Yö÷Δ°œ     ¡fXıA@≥Ÿ Êfiû ±¸ê :,}
2100160 F7127BCD 16CB013C F778C120 72142C48 4C9C291A 496FC0EB D8C21C33 B595A9C1  ˜ {Õ À <˜x¡ r ,HLú) Io¿Îÿ¬ 3µï©¡
2100180 587ACFC6 D8BB9663 20010200 08000100 0B16A27B B2DBAB41 BD206165 68B479E7  XzœΔÿªñc         ¢{≤€´AΩ aeh¥yÁ
```

BITCRACKER VMK DECRYPTION ALGORITHM, INITIAL VERSION



- Poor performance: 100 password/sec, NVIDIA GPU Tesla K80
- Limited by instructions number!

IMPROVEMENT – W BLOCKS

Each iteration: SHA-256 to a 128 bytes structure

Block1: 64 byte	Block2: 64 byte			
64 byte	**16 byte**	**8 byte**	**32 byte**	**8 byte**
Results previous iteration	Salt	Counter	Padding	Size
Variable	Fixed	Variable	Fixed	Fixed
Not predictable	Memory unit salt	0 - 1048575	10 … 0	88

Precomputation is possible!

1.048.576 iterations x 64 W blocks = 67.108.800 blocks (256 Mb)

SHA-256 to 128 byte:

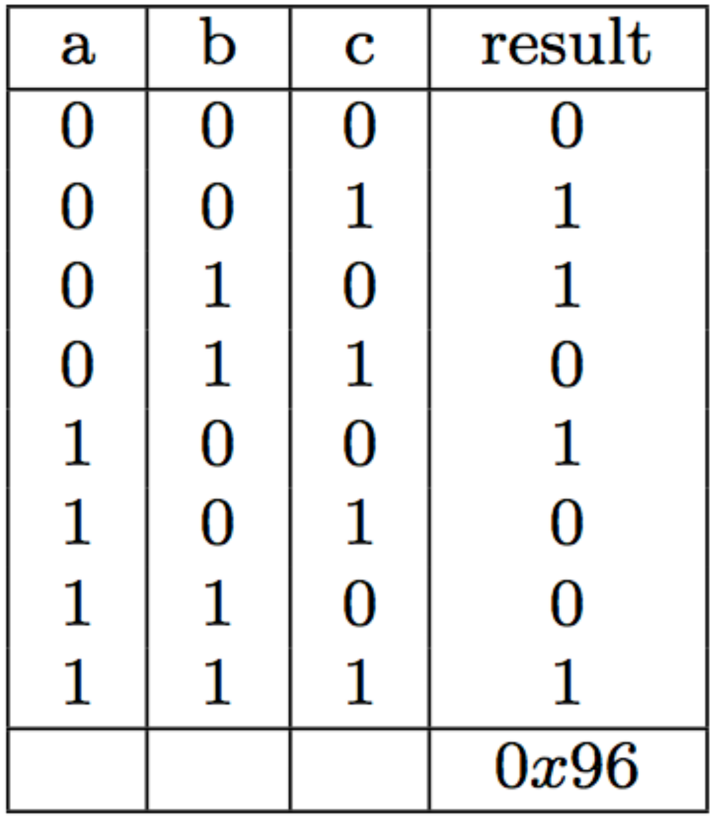
- 128 byte split into two 64 byte blocks
- PreviousHash = SHA-256 (Constants [32 byte], Message1 [Block1: 64 byte])
- FinalHash = SHA-256 (PreviousHash [32 byte], Message2 [Block2: 64 byte])

$$W_t = \begin{cases} M_t^i & \text{if } 0 \le t \le 15 \\ \sigma_1^{256}(W_{t-2}) + W_{t-7} + \sigma_0^{256}(W_{t-15}) + W_{t-16} & \text{if } 16 \le t \le 63 \end{cases}$$

64 byte Message –> 64 W blocks

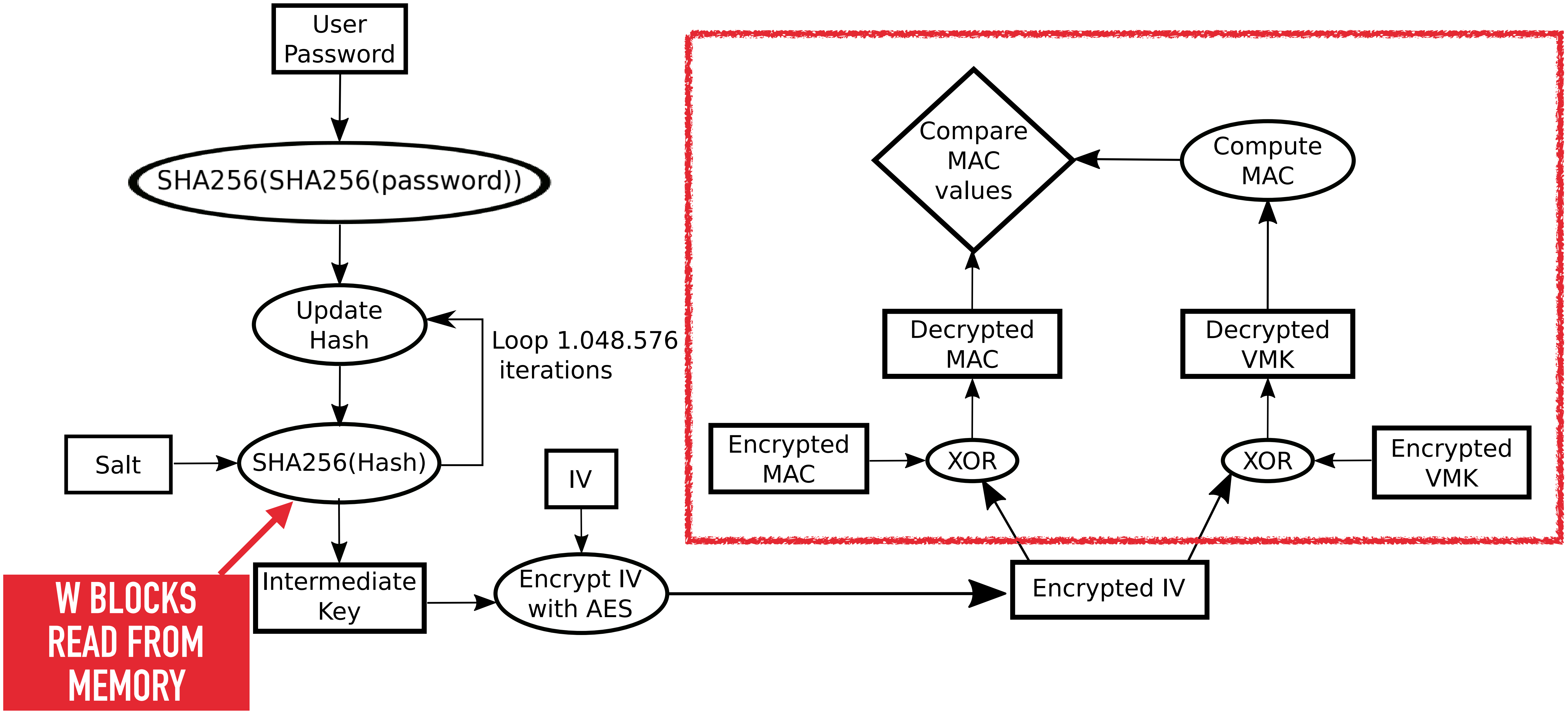
IMPROVEMENT - CUDA

- No W blocks computation –> less instructions!
- Less registers usage, no local memory, occupancy 100%, etc…
- Instructions like IADD3 and LOP3.LUT (logical operation on 3 inputs with lookup table) –> d = (a XOR b XOR c)))
    - CC 3.x (Kepler arch) :
        1. lop.xor a, b, tmp;
        2. lop.xor tmp, c, d;
    - CC 5.x (Maxwell arch) :
        1. lop3.lut (d, a, b, c, 0x96)



a	b	c	result
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1
			$0x96$

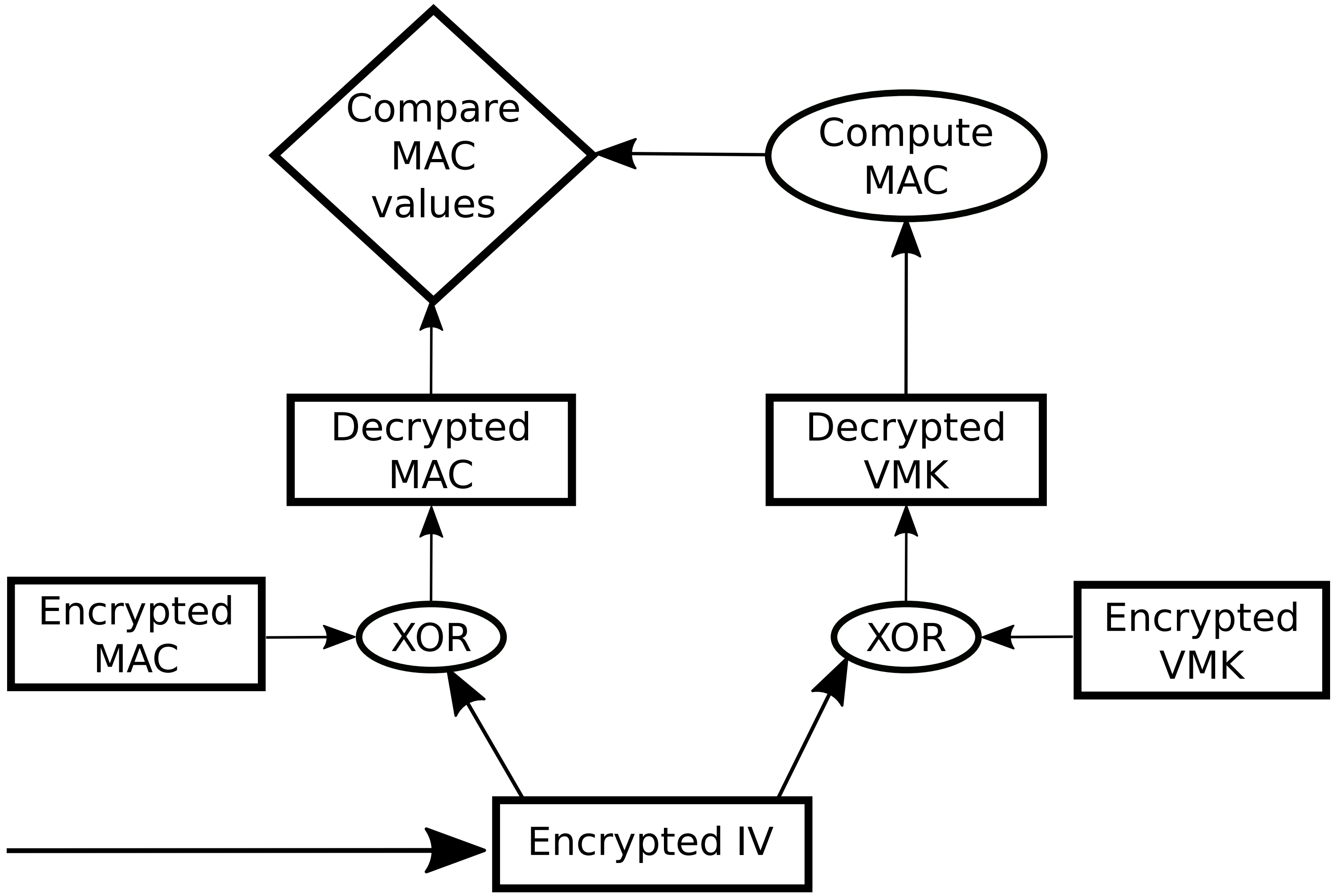
BITCRACKER VMK DECRYPTION ALGORITHM



Speed up x3: from 100 password/sec to 340 password/sec, NVIDIA GPU Tesla K80

IMPROVEMENT – MAC COMPARISON

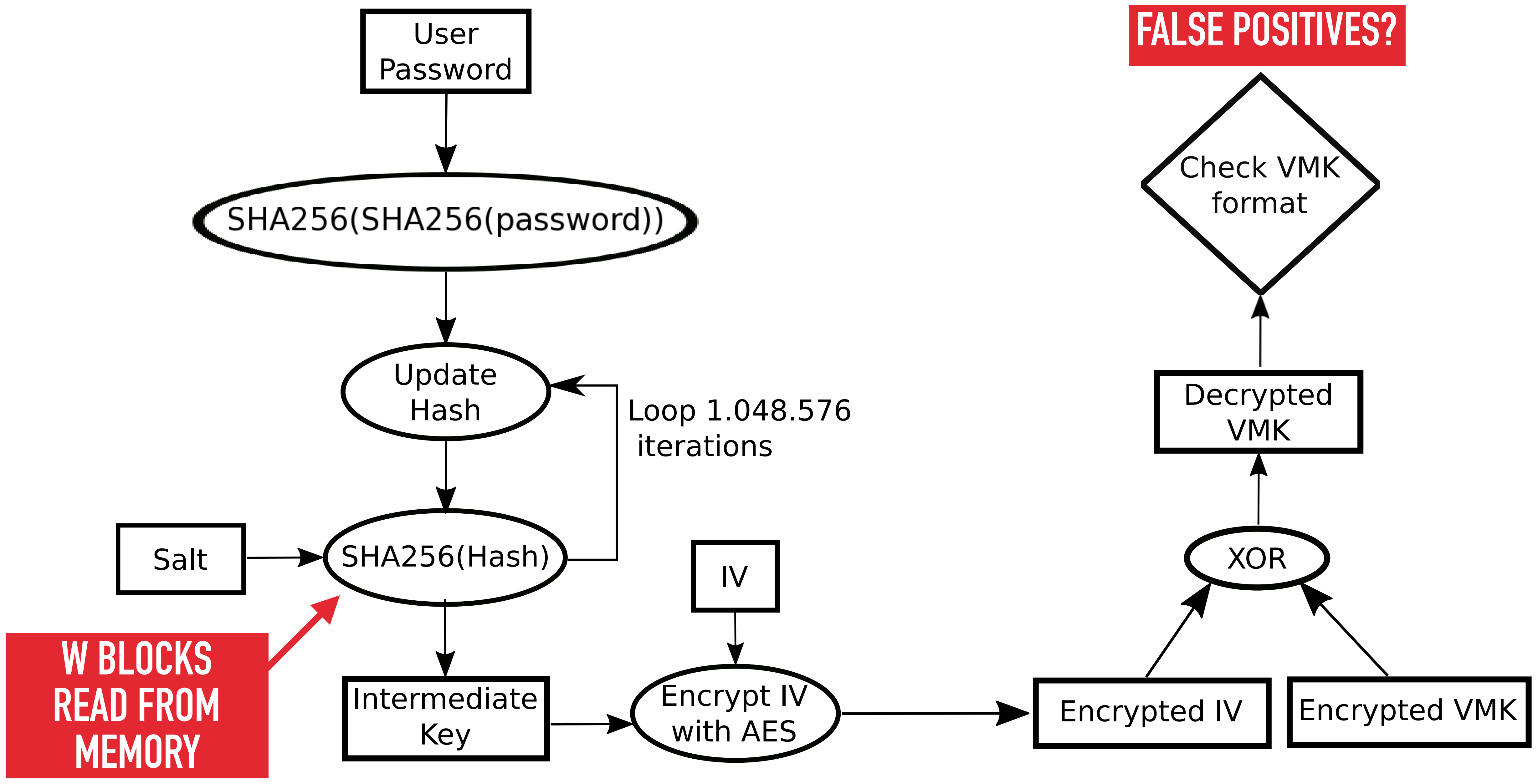
- Decrypt VMK: 3 AES, 44 XOR
- Decrypt MAC: 1 AES, 16 XOR
- Compute MAC: 4 AES, 44 XOR



IMPROVEMENT - MAC COMPARISON

- According to Microsoft standard, decrypted VMK structure:
  - First 12 bytes hold info about the key:
    1. Bytes 0 and 1: VMK length, always 44
    2. Bytes 4 and 5: version number, always 1
    3. Bytes 8 and 9: type of VMK encryption. In case of user password, the value is between 0x2000 and 0x2005
  - Last 32 bytes are the real VMK
- Improvement: avoid MAC comparison and check the decrypted VMK values

BITCRACKER FINAL ALGORITHM

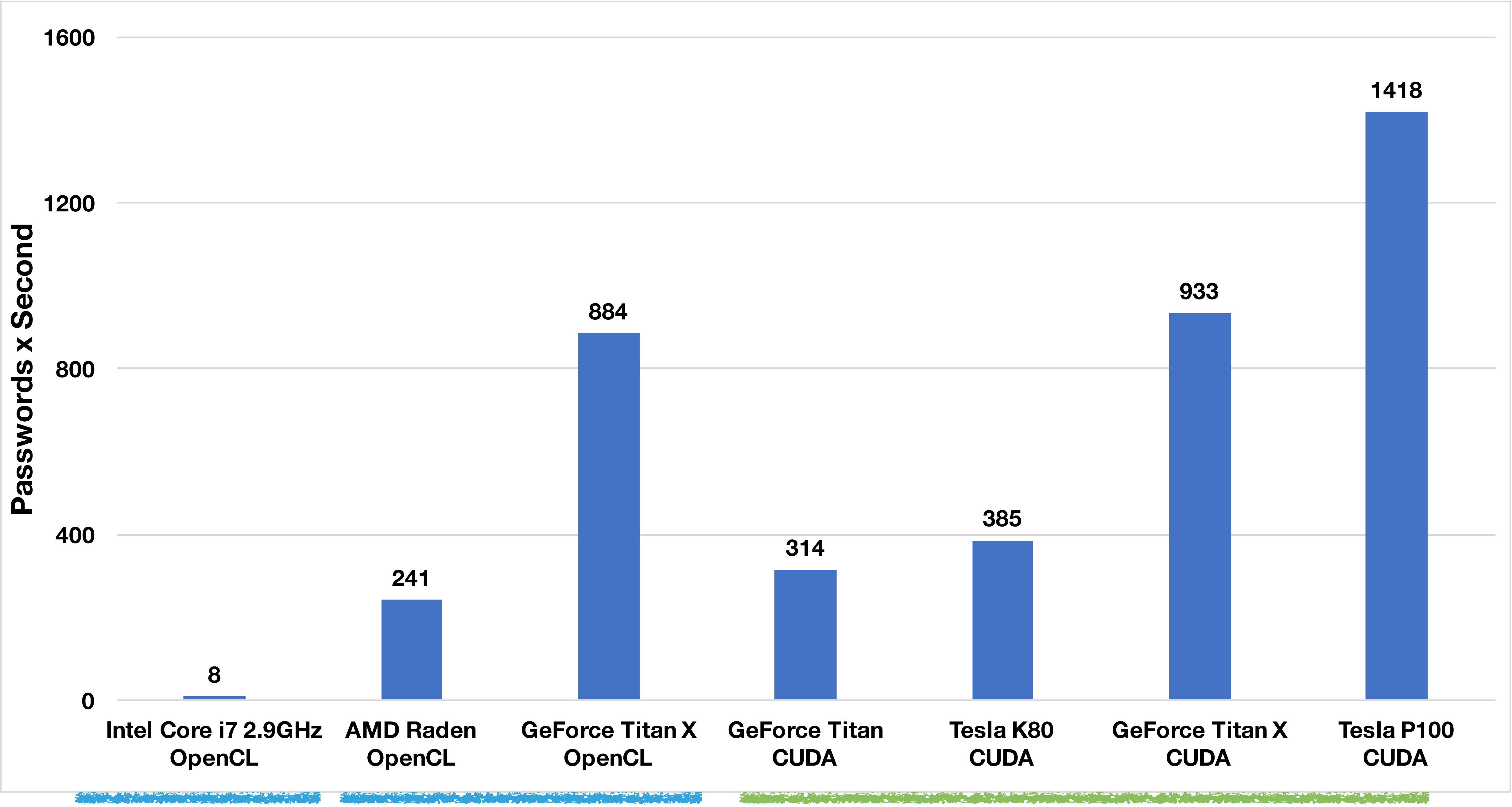


Speed up 11%: from 340 password/sec to 385 password/sec, NVIDIA GPU Tesla K80

BITCRACKER & WINDOWS VERSIONS

- Tested with BitLocker on Windows Vista, 7 , 8.1 and 10
- Windows 10 has 2 different modes:
  - **Compatible**: nothing different from previous Windows
  - **Not Compatible**: XTS-AES instead of AES-CCM, only for FVEK and device sectors

BITCRACKER PERFORMANCE: PASSWORDS/SECOND



OpenCL - CPU **OpenCL - GPU** **CUDA**

BITCRACKER PERFORMANCE: HASH/SECOND

- Each password requires 1.048.576 x 2 = 2.097.152 SHA-256
- 1418 psw/sec –> 2.973.761.536 SHA-256/sec
- Compared with Hashcat v 3.5.0 … **Not fair!**

	Hashcat	BitCracker
Implementation	OpenCL	CUDA
Format	Raw SHA-256	2.097.152 SHA-256 + AES + XOR
Improvements	None	W blocks
Hash/sec	**3070 MH/sec**	**2973 MH/sec**

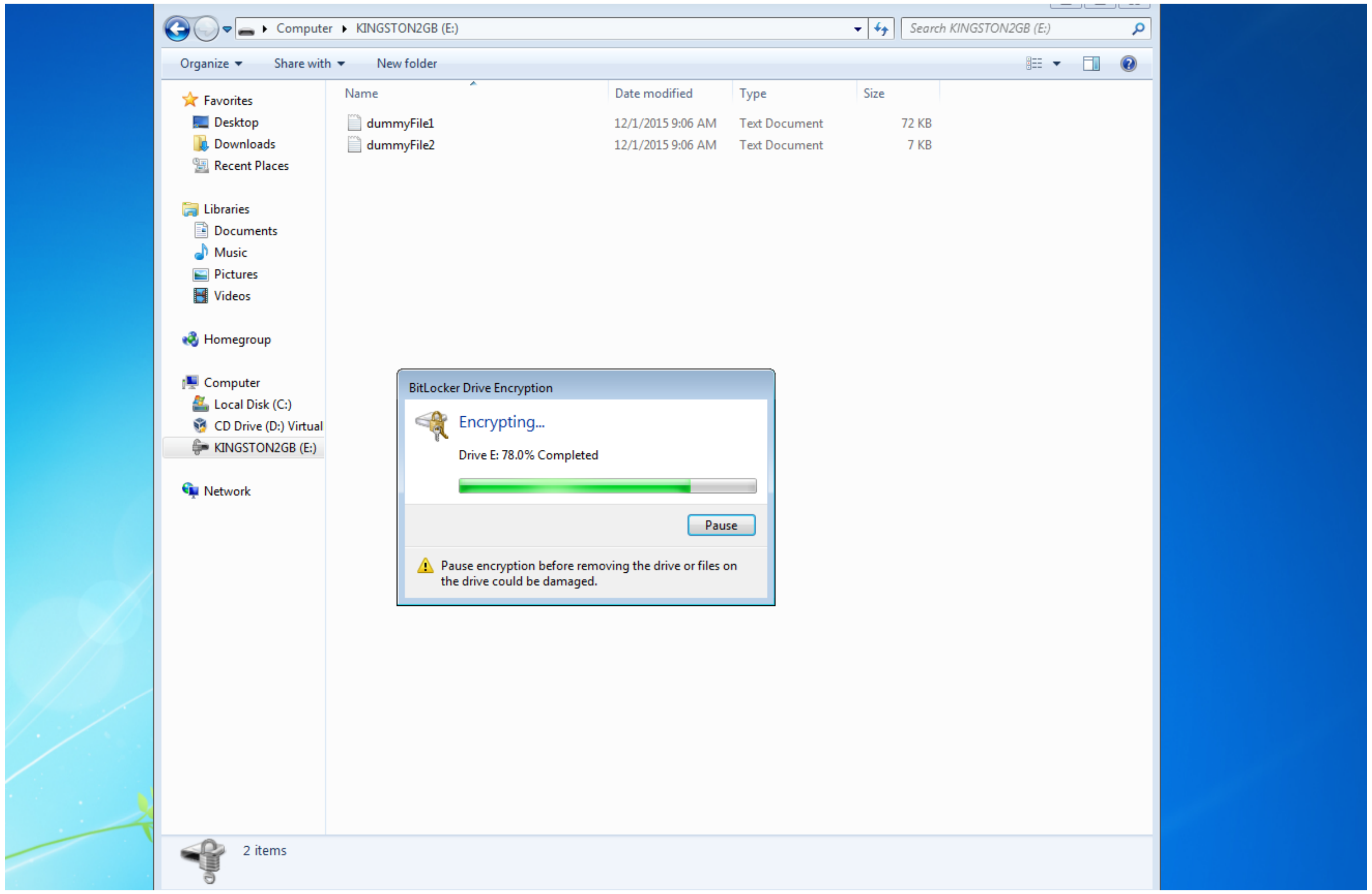
NVIDIA GPU Tesla P100 (Pascal architecture)

BITCRACKER IS AVAILABLE ONLINE!

- **GitHub repository:** **https://github.com/e-ago/bitcracker**
    - Standalone implementation, both CUDA-C and OpenCL
    - Most updated version with several command line options
    - No dictionary manipulation, mask attacks, etc..
- **John the Ripper - OpenCL BitLocker format:**
    - Bleeding jumbo: https://github.com/magnumripper/JohnTheRipper
    - Wiki page: http://openwall.info/wiki/john/OpenCL-BitLocker
    - Slightly slower due to JtR internal engine
- GPLv2.0 but we are open to collaborations!

BITCRACKER: HOW TO

- Step 1: get the image of your encrypted memory unit
- Example 1: *dd* command is a Linux command-line utility to create bit-by-bit images of entire drives



Name	Date modified	Type	Size
dummyFile1	12/1/2015 9:06 AM	Text Document	72 KB
dummyFile2	12/1/2015 9:06 AM	Text Document	7 KB

BitLocker Drive Encryption

Encrypting...

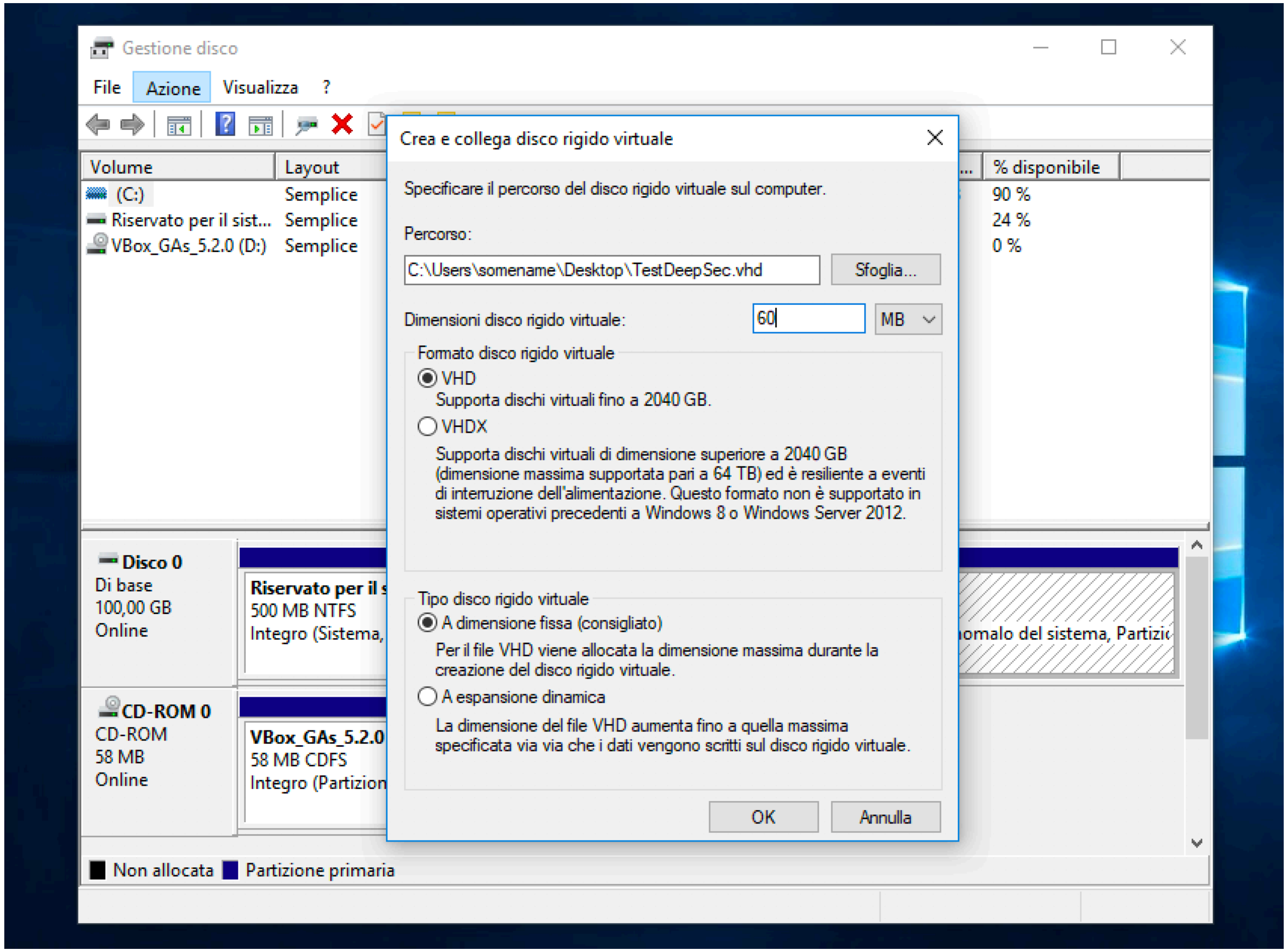
Drive E: 78.0% Completed

Pause encryption before removing the drive or files on the drive could be damaged.

```
sudo dd if=/dev/disk2 of=/somepath/imageEncrypted conv=noerror,sync
4030464+0 records in
4030464+0 records out
2063597568 bytes transferred in 292.749849 secs (7049013 bytes/sec)
```

BITCRACKER: HOW TO

- Step 1: get the image of your encrypted memory unit
- Example 2: test with an encrypted VHD



Volume	Layout	% disponibile
(C:)	Semplice	90 %
Riservato per il sist...	Semplice	24 %
VBox_GAs_5.2.0 (D:)	Semplice	0 %

Crea e collega disco rigido virtuale

Specificare il percorso del disco rigido virtuale sul computer.

Percorso: C:\Users\somename\Desktop\TestDeepSec.vhd

Dimensioni disco rigido virtuale: 60 MB

Formato disco rigido virtuale

● VHD
Supporta dischi virtuali fino a 2040 GB.

○ VHDX
Supporta dischi virtuali di dimensione superiore a 2040 GB (dimensione massima supportata pari a 64 TB) ed è resiliente a eventi di interruzione dell'alimentazione. Questo formato non è supportato in sistemi operativi precedenti a Windows 8 o Windows Server 2012.

Tipo disco rigido virtuale

● A dimensione fissa (consigliato)
Per il file VHD viene allocata la dimensione massima durante la creazione del disco rigido virtuale.

○ A espansione dinamica
La dimensione del file VHD aumenta fino a quella massima specificata via via che i dati vengono scritti sul disco rigido virtuale.

Disco 0
Di base
100,00 GB
Online

Riservato per il s
500 MB NTFS
Integro (Sistema,

omalo del sistema, Partizio

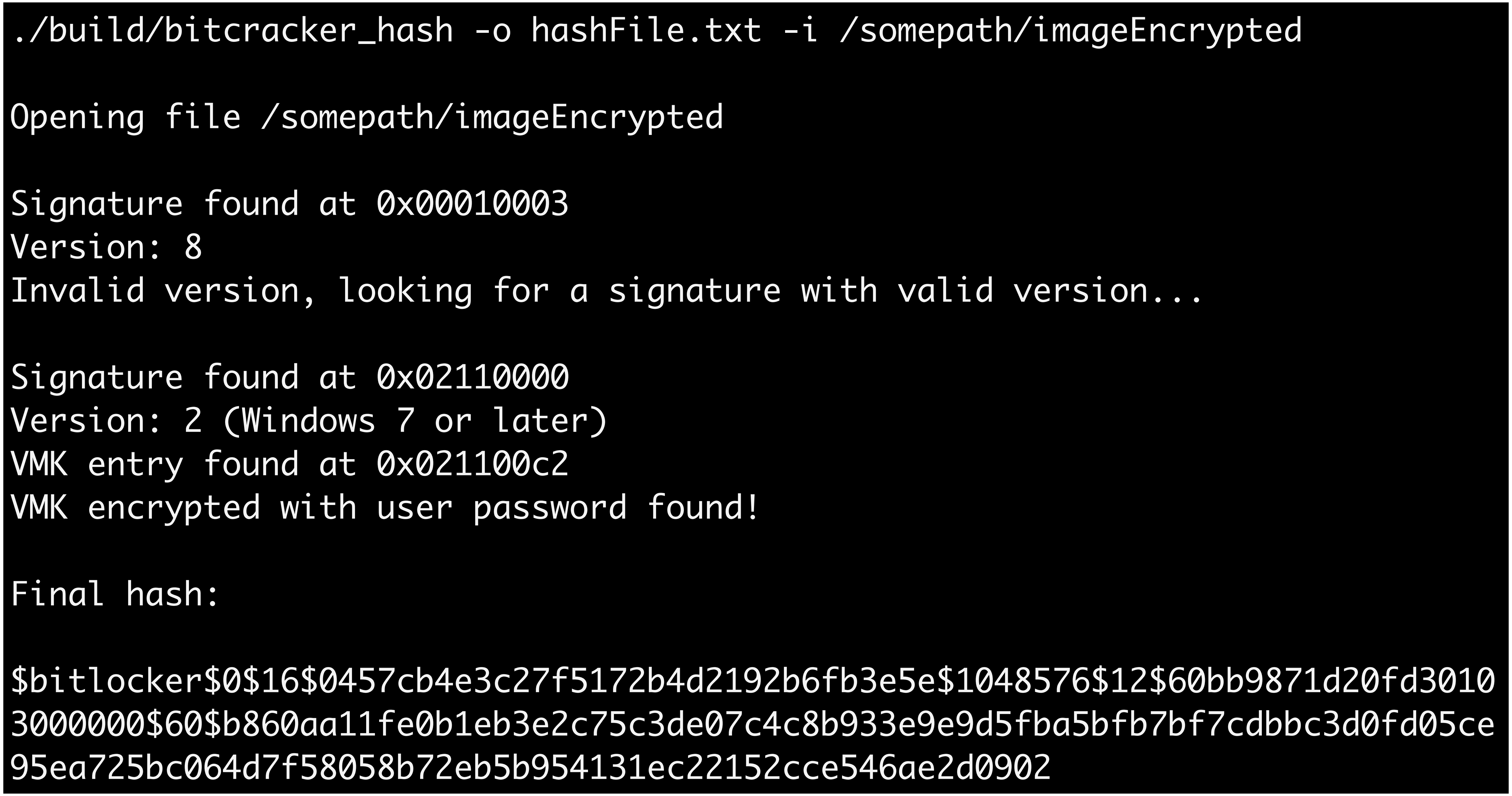
CD-ROM 0
CD-ROM
58 MB
Online

VBox_GAs_5.2.0
58 MB CDFS
Integro (Partizion

■ Non allocata ■ Partizione primaria

BITCRACKER: HOW TO

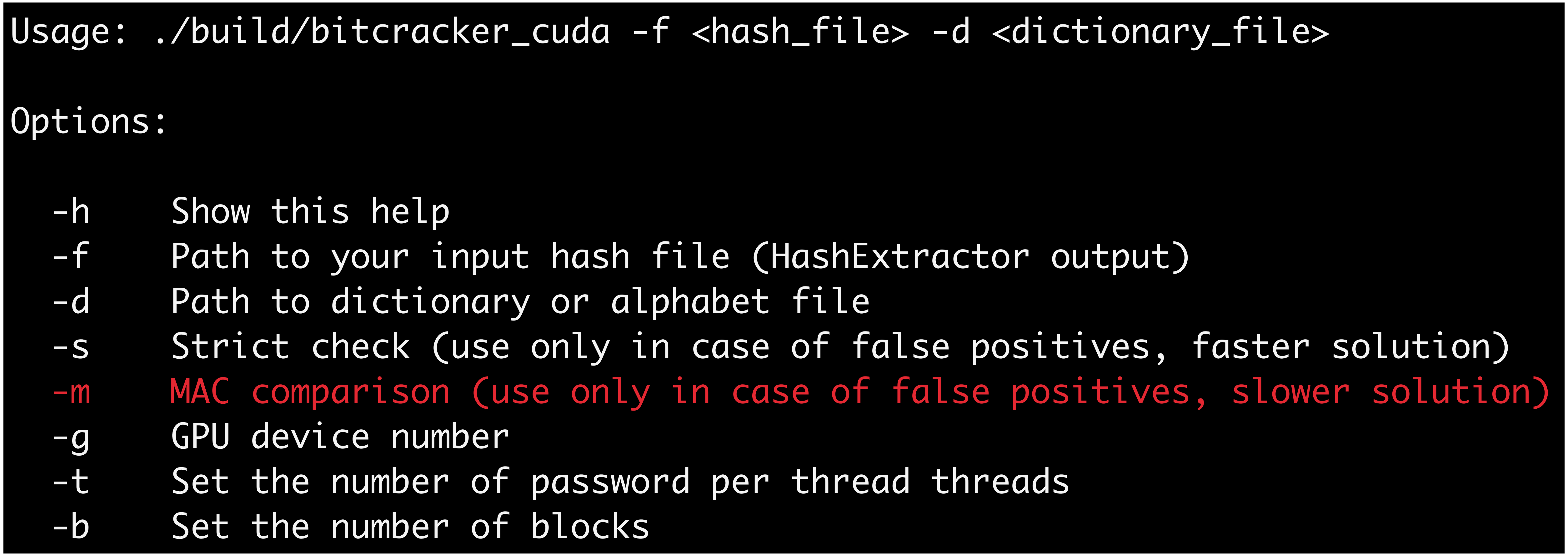
- Step 2: *bitcracker_hash* to extract the hash and check the format



```
./build/bitcracker_hash -o hashFile.txt -i /somepath/imageEncrypted

Opening file /somepath/imageEncrypted

Signature found at 0x00010003
Version: 8
Invalid version, looking for a signature with valid version...

Signature found at 0x02110000
Version: 2 (Windows 7 or later)
VMK entry found at 0x021100c2
VMK encrypted with user password found!

Final hash:

$bitlocker$0$16$0457cb4e3c27f5172b4d2192b6fb3e5e$1048576$12$60bb9871d20fd3010
3000000$60$b860aa11fe0b1eb3e2c75c3de07c4c8b933e9e9d5fba5bfb7bf7cdbbc3d0fd05ce
95ea725bc064d7f58058b72eb5b954131ec22152cce546ae2d0902
```

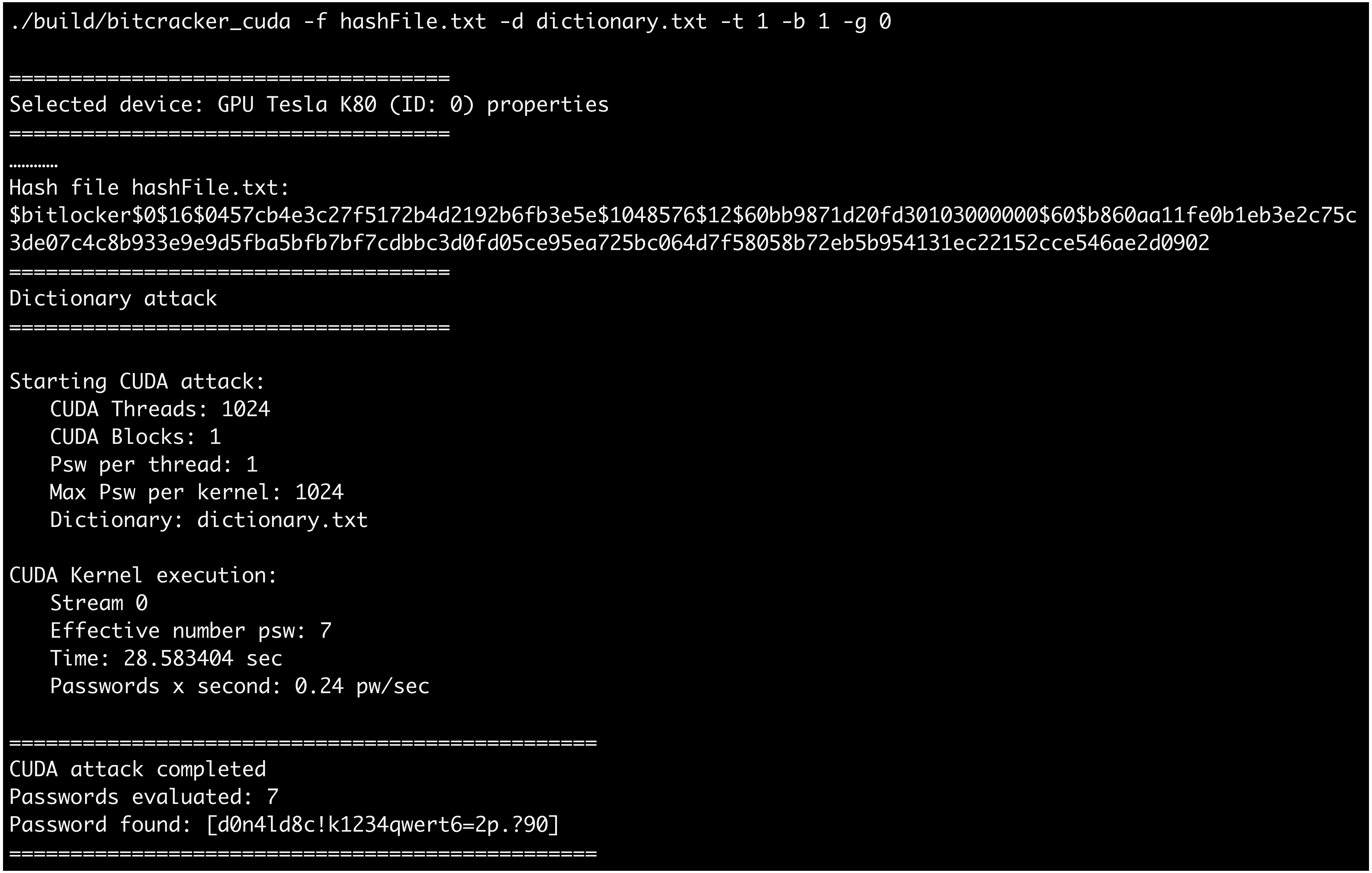
BITCRACKER: HOW TO

- Step 3: start the attack with *bitcracker_cuda*



```
Usage: ./build/bitcracker_cuda -f <hash_file> -d <dictionary_file>

Options:

  -h    Show this help
  -f    Path to your input hash file (HashExtractor output)
  -d    Path to dictionary or alphabet file
  -s    Strict check (use only in case of false positives, faster solution)
  -m    MAC comparison (use only in case of false positives, slower solution)
  -g    GPU device number
  -t    Set the number of password per thread threads
  -b    Set the number of blocks
```

BITCRACKER: HOW TO



```
./build/bitcracker_cuda -f hashFile.txt -d dictionary.txt -t 1 -b 1 -g 0

====================================
Selected device: GPU Tesla K80 (ID: 0) properties
====================================
…………
Hash file hashFile.txt:
$bitlocker$0$16$0457cb4e3c27f5172b4d2192b6fb3e5e$1048576$12$60bb9871d20fd30103000000$60$b860aa11fe0b1eb3e2c75c
3de07c4c8b933e9e9d5fba5bfb7bf7cdbbc3d0fd05ce95ea725bc064d7f58058b72eb5b954131ec22152cce546ae2d0902
====================================
Dictionary attack
====================================

Starting CUDA attack:
   CUDA Threads: 1024
   CUDA Blocks: 1
   Psw per thread: 1
   Max Psw per kernel: 1024
   Dictionary: dictionary.txt

CUDA Kernel execution:
   Stream 0
   Effective number psw: 7
   Time: 28.583404 sec
   Passwords x second: 0.24 pw/sec

================================================
CUDA attack completed
Passwords evaluated: 7
Password found: [d0n4ld8c!k1234qwert6=2p.?90]
================================================
```

RECOVERY KEY

- There are other authentication methods!
- Common element: Recovery Key
  - 48-digit key, 8 integers of 6 digits

```
693847-235455-692186-324313-509487-374682-487388-263670
```

  - For every authentication method “you can restore access to a BitLocker-protected drive in the event that you cannot unlock the drive normally”
- Ready next month!

NEXT STEPS

- BitLocker encrypted format in case of other authentication methods
- Multi-GPU distributed solution
- More tests: newest NVIDIA Volta GPUs and non-NVIDIA GPUs

National Research Council of Italy

DEEPSEC

PLEASE SHARE!

HTTPS://GITHUB.COM/E-AGO/BITCRACKER

THANK YOU!

ELENA.AGO@GMAIL.COM

BITCRACKER

Elena Agostini, Massimo Bernaschi