Introduction of virtio crypto device

arei.gonglei@huawei.com

CLK 2016

www.huawei.com

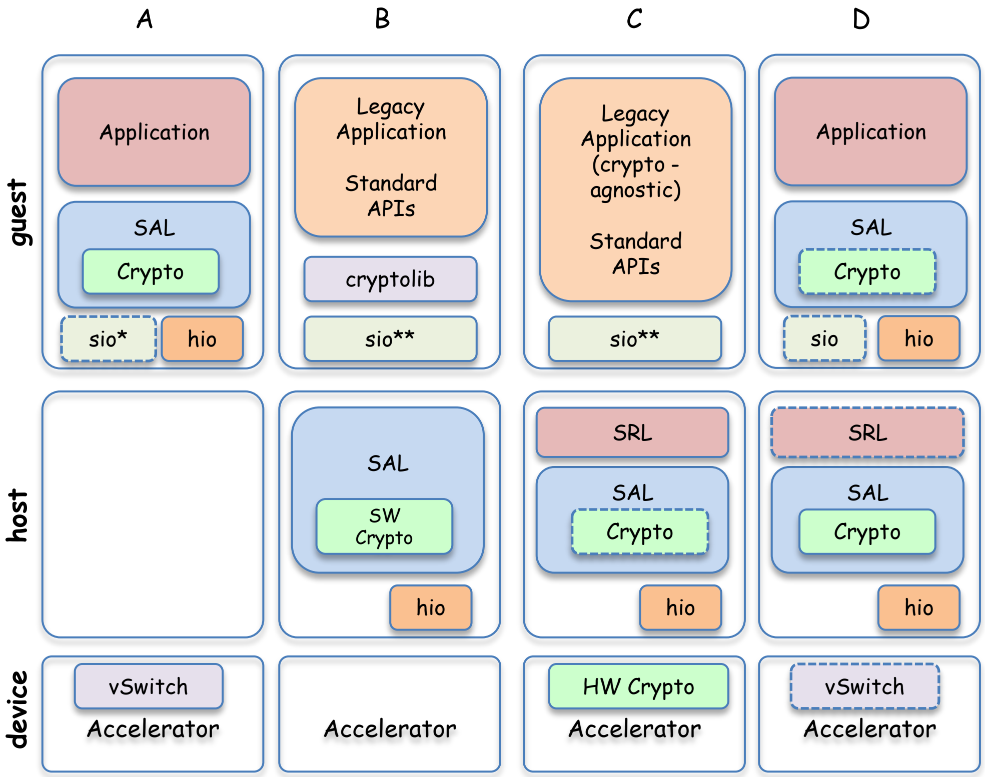
HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Agenda

- Crypto use cases
- Crypto in Linux
- Overview of virtio-crypto
- Performance
- Status of virtio-crypto

Crypto use cases (VNF Acceleration)



* Standard VirtIO and Kernel based vHost, Kernel layer not shown

** Standard or enhanced VirtIO to vHost-user in the SAL

Showing a number of possible options:

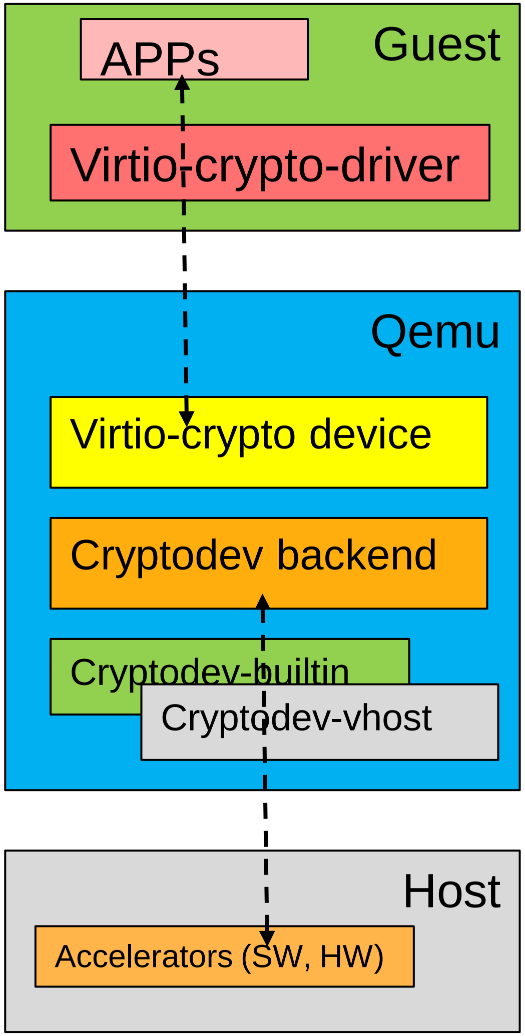
- Example A (non-hio packets have poor performance)
  - VM with a SAL for direct access to external device
  - The sio is optional for host access for management
  - VM to VM support only supplied by vSwitch or external device
- **Example B**
  - **Legacy application using crypto lib via VirtIO to accelerate crypto operations in the host**
  - VM to VM still missing, but can be supported by SAL to external vSwitch accelerator
- **Example C**
  - **Legacy application being agnostic to the encrypted traffic being handled in the host/accelerator**
  - Adding a SRL (vSwitch/vRouter) for VM to VM communication
- **Example D**
  - **Accelerated application using SAL in guest to access crypto accelerator directly**
  - Flexible vSwitch or vRouter support in SW or HW
  - SAL allows for some/all crypto operations to be done in the guest on passed to the host for processing

Note: The slide is picked up from “DPACC : Platform Performance Acceleration Session” Keith Wiles (Intel) & Bob Monkman (ARM)

Crypto in Linux

- A cryptography framework in the Linux kernel
- Can do Cipher, Hash, Compress, RNG,. . .
- Can register supported algorithms for hardware crypto accelerators
- Used by:
  - ✓ Network stack: IPsec, . . .
  - ✓ Device Mapper: dm-crypt, RAID, . . .
  - ✓ Userland Accessing:
    - ✓AF_ALG (in-kernel, socket-based API)
    - ✓Cryptodev (Out-of-kernel tree code for years)
- Maillist: linux-crypto@vger.kernel.org

Overview of virtio-crypto



- **Host emulate virtio-crypto device for the Guest**
- **Host add cryptodev backend object for Virtio-crypto device**
- Cryptodev backend object can be realized to different child objects, like:
  - cryptodev-backend-builtin
  - cryptodev-vhost (vhost-user and/or vhost-kernel)
- **Guest install virtio-crypto driver**
  - user space: virtio-crypto pmd driver for DPDK/ODP
  - kernel space: adapt to Linux Crypto Framework

Cryptodev backend

- An user creatable object in QEMU

  cmds: -object/object-add/object_add

  Example:

  ```
  #./qemu-system-x86_64 -object cryptodev-backend,id=cy0
  ```

- Can be realized with different child objects
- Key code:

```
static const TypeInfo cryptodev_backend_info = {
    .name = TYPE_CRYPTODEV_BACKEND,
    .parent = TYPE_OBJECT,
    .instance_size = sizeof(CryptoDevBackend),
    .instance_init = cryptodev_backend_instance_init,
    .instance_finalize = cryptodev_backend_finalize,
    .class_size = sizeof(CryptoDevBackendClass),
    .class_init = cryptodev_backend_class_init,
    .interfaces = (InterfaceInfo[]) {
        { TYPE_USER_CREATABLE },
        { }
    }
```

Cryptodev backend builtin

- A cryptodev backend child
- Realized with QEMU cipher APIs
- Support nettle、gcrypt or cipher-buitlin in QEMU
- Limited algorithms, Only few Cipher algorithms currently
- Software acceleration
- Poor performance
- Should not be used in production environment
- Examples:

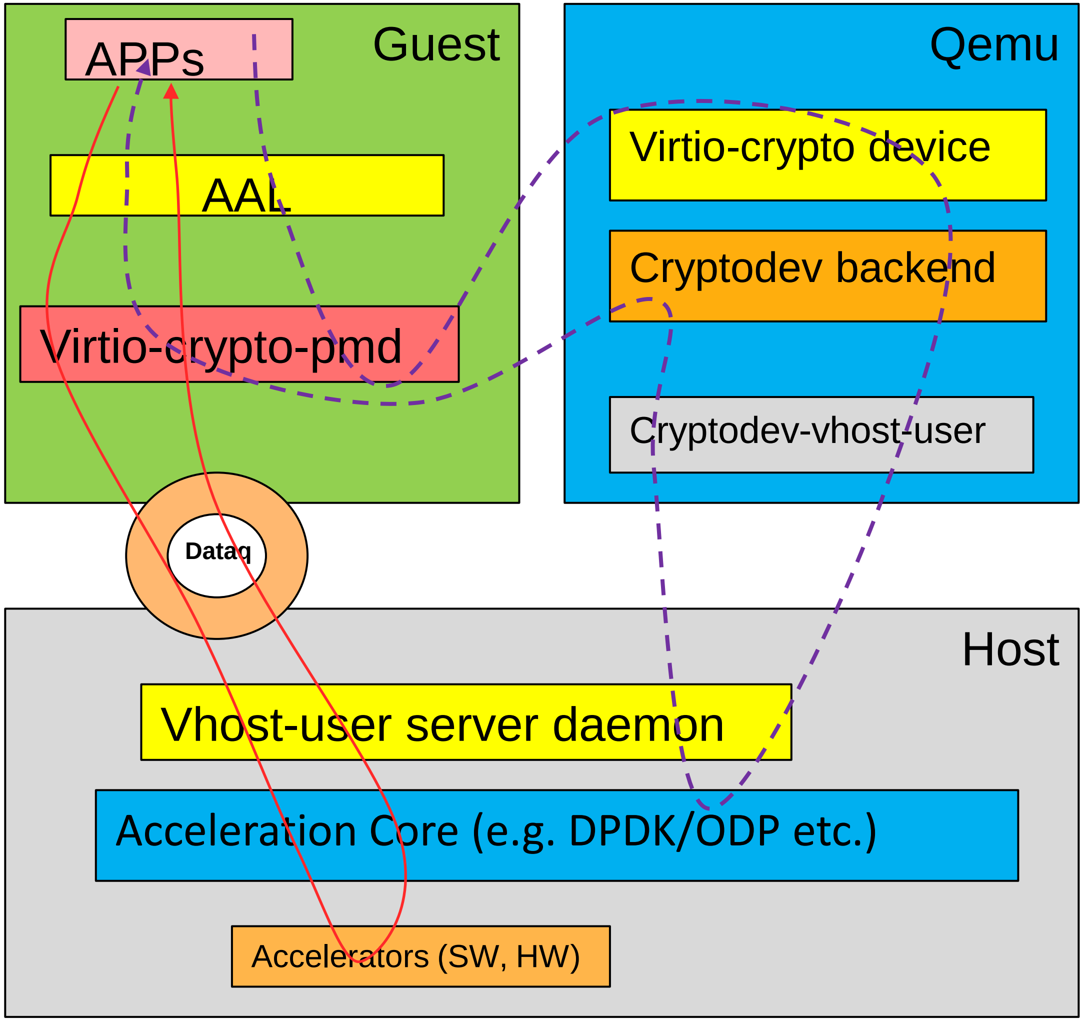
```
# qemu-system-x86_64 \
[...] \
    -object cryptodev-backend-builtin,id=cryptodev0 \
    -device virtio-crypto-pci,id=crypto0,cryptodev=cryptodev0 \
[...]
```

Cryptodev backend vhost-user

- Another cryptodev backend child
- More algorithms supported
- Software and/or Hardware acceleration
- Can use high performance software framework, such as DPDK.
- Support multiple queues
- Good performance, can be used in production environment
- Examples:

```
# qemu-system-x86_64 \
[...] \
    -chardev socket,id=charcrypto0,path=/your/path/socket0
    -object cryptodev-vhost-user,id=cryptodev0 ,chardev=charcrypto0\
    -device virtio-crypto-pci,id=crypto0,cryptodev=cryptodev0 \
[...]
```

Cryptodev-vhost-user architecture



- AAL:
  - Acceleration Abstract Layer
- Dashed Line:
  - flow of control virtqueue
  - Need to trap into QEMU and communicate with vhost-user server
- Full Line:
  - flow of data virtqueue
  - Do not need pass QEMU
- Acceleration Core
  - e.g. DPDK, ODP or other acceleration implementation
- Virtio-crypto-pmd
  - User space driver for virtio-crypto device, e.g. the poll mode driver in DPDK.
- Vhost-user server dameon
  - Create the socket communicated with QEMU
  - Invoke AC crypto APIs

Virtio crypto device design

- A virtual crypto device as well as a kind of virtual hardware accelerator for virtual machines
- Include data virtqueue and control virtqueue
  - **Control virtuqueue:** create or destroy sessions for sym algos, …
  - **Data virtuqueue:** crypto requests transmition in data plane
- Support the following crypto services currently: CIPHER, MAC, HASH, AEAD
- Support multiple virtual data queues
- Follow the virtio-1.0 specification
- Virito device ID: 20
- Virtio PCI device ID: 0x1054 (= 0x1040 + 20)

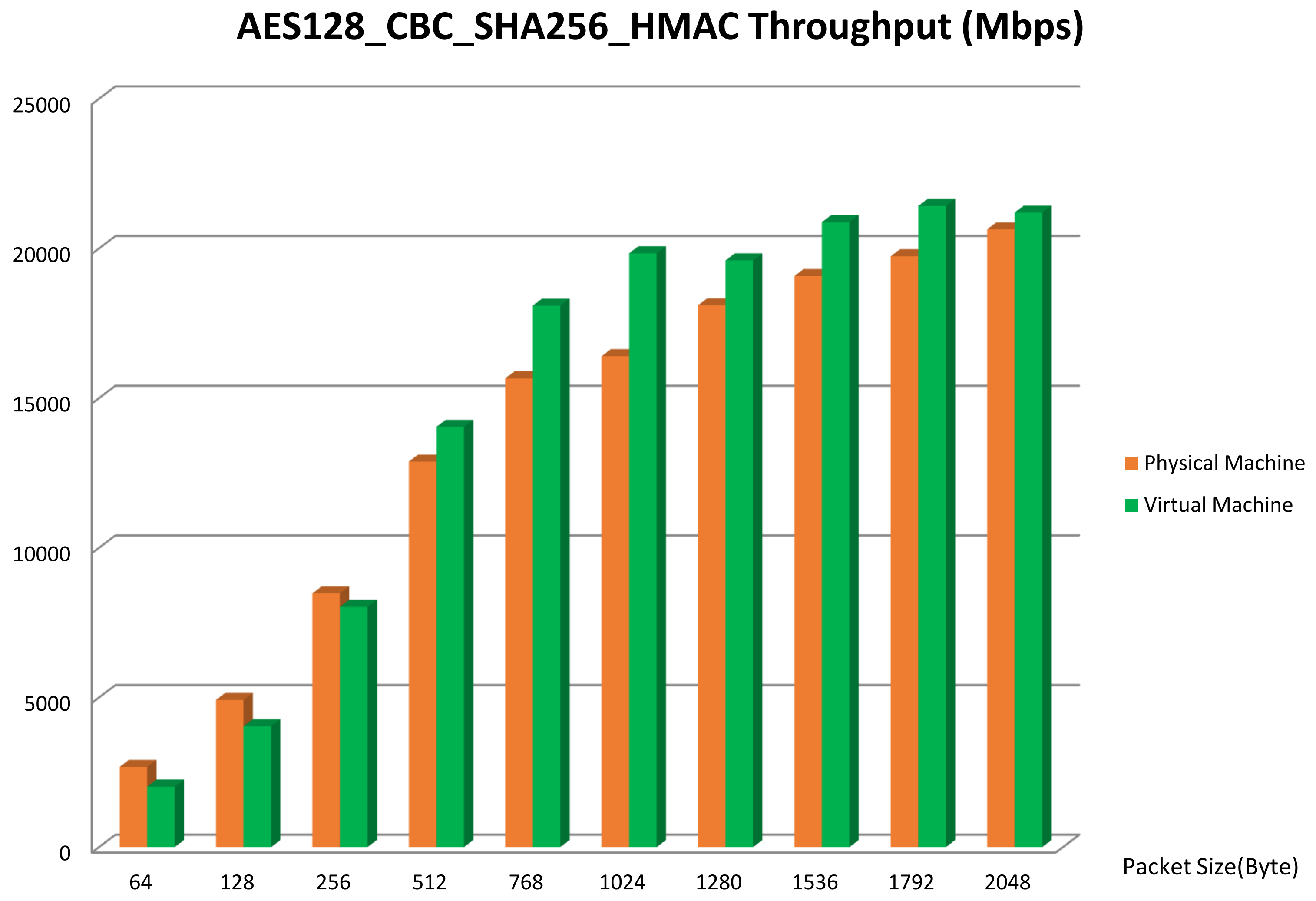
Performance - configuration

- **Hardware**
  1) Server: HUAWEI RH2288H V3
  2) CPU: Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz
  3) Intel QAT Coleto Creek PCIe DH895xCC SKU2
- **Software**
  1) Host: UVP-V200R002C00SPC300B062
  2) Guest: Suse11.3 with 8 GB memory, 4vcpu

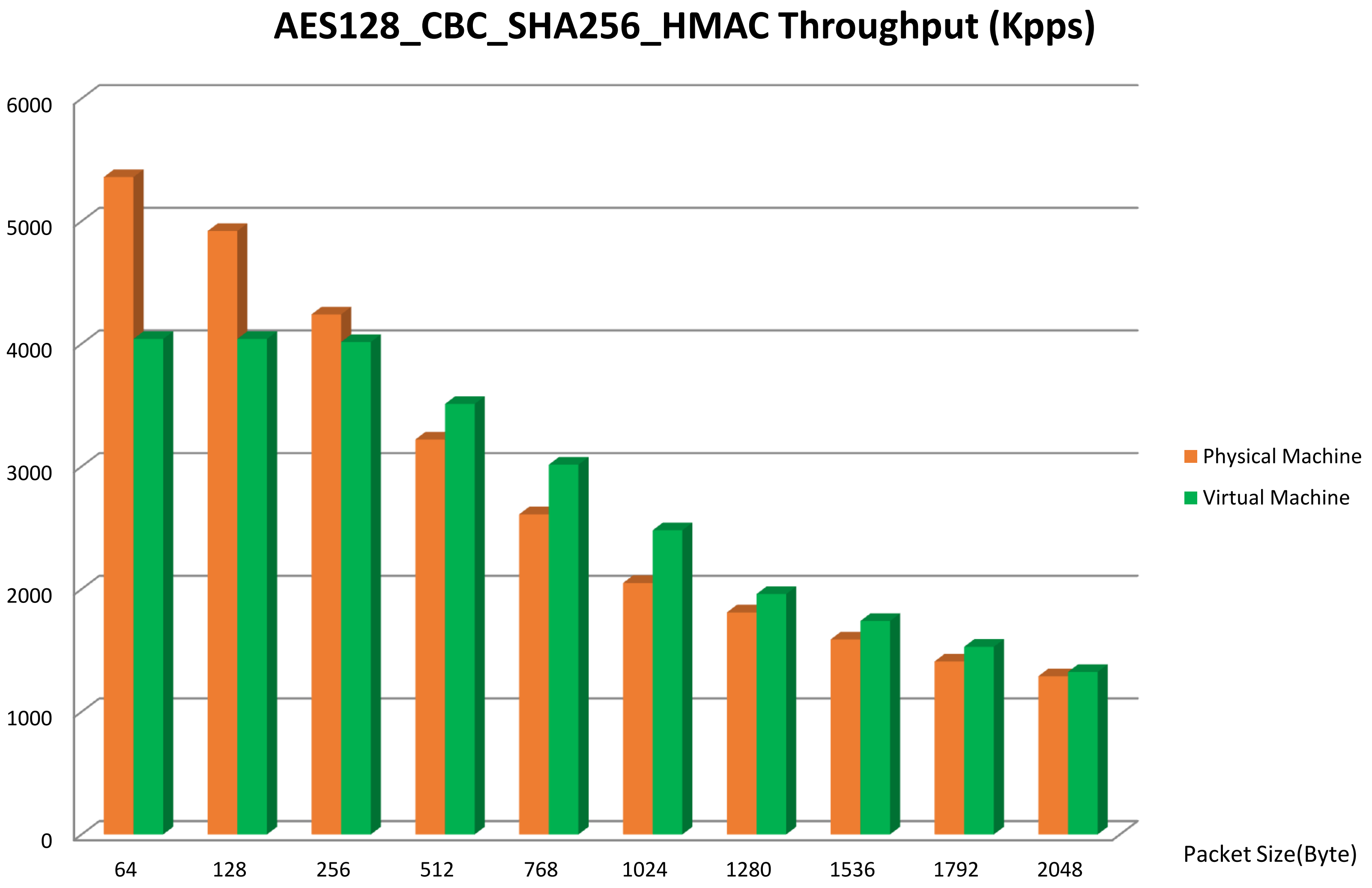
Numa Info	available: 2 nodes (0-1) node 0 cpus: 0 1 2 3 4 5 12 13 14 15 16 17 node 0 size: 65141 MB node 0 free: 61013 MB node 1 cpus: 6 7 8 9 10 11 18 19 20 21 22 23 node 1 size: 65536 MB node 1 free: 11251 MB node distances: node 0 1 0: 10 21 1: 21 10

```
<vcpu placement='static'>4</vcpu>
 <cputune>
   <vcpupin vcpu='0' cpuset='10'/>
   <vcpupin vcpu='1' cpuset='22'/>
   <vcpupin vcpu='2' cpuset='11'/>
   <vcpupin vcpu='3' cpuset='23'/>
   <emulatorpin cpuset='10-11,22-23'/>
 </cputune>
```

Performance



Performance



Status of virtio-crypto's patches

Virtio and DPDK	Host	Guest
🟩 Virtio crypto specification	🟩 QEMU -device virtio-crypto	🟨 virtio-crypto-pmd
🟨 Vhost-user-crypto based on DPDK	🟩 QEMU -object cryptodev-backend-builtin	🟩 Virtio-crypto Linux Kernel Driver
	🟨 QEMU -object cryptodev-vhost-user	⬜ Support more algorithms, live migration etc.

🟨 Patches not yet posted

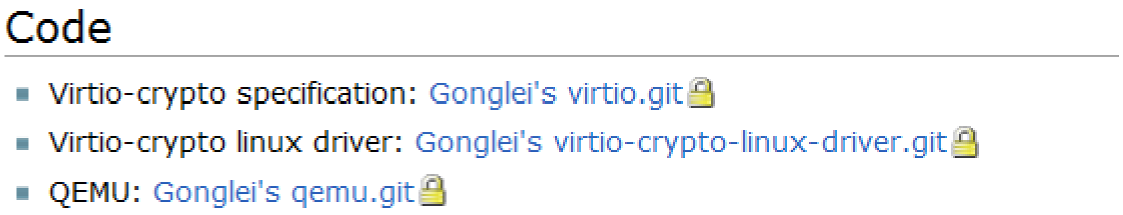
🟩 Patches not yet merged

⬜ Not yet implemented

Questions?

- Email:
  - arei.gonglei@huawei.com
  - arei.gonglei@hotmail.com
- For information about virtio-crypto:

  http://qemu-project.org/Features/VirtioCrypto



Code

- Virtio-crypto specification: Gonglei's virtio.git
- Virtio-crypto linux driver: Gonglei's virtio-crypto-linux-driver.git
- QEMU: Gonglei's qemu.git

Thank you

www.huawei.com

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.