UADK 加速大数据在 openEuler 操作系统上的实践

徐国栋 I Linaro I 2024-07-05

OpenAtom openEuler（简称"openEuler"） Meetup Online——大数据Meetup

- Big Data 的挑战与需求
- UADK 技术概述
- UADK 软件生态建设
- UADK 与 Big Data 的结合实践
- 成果展示与分析
- 快速上手指南

Big Data 的挑战与需求

大数据时代的加密需求

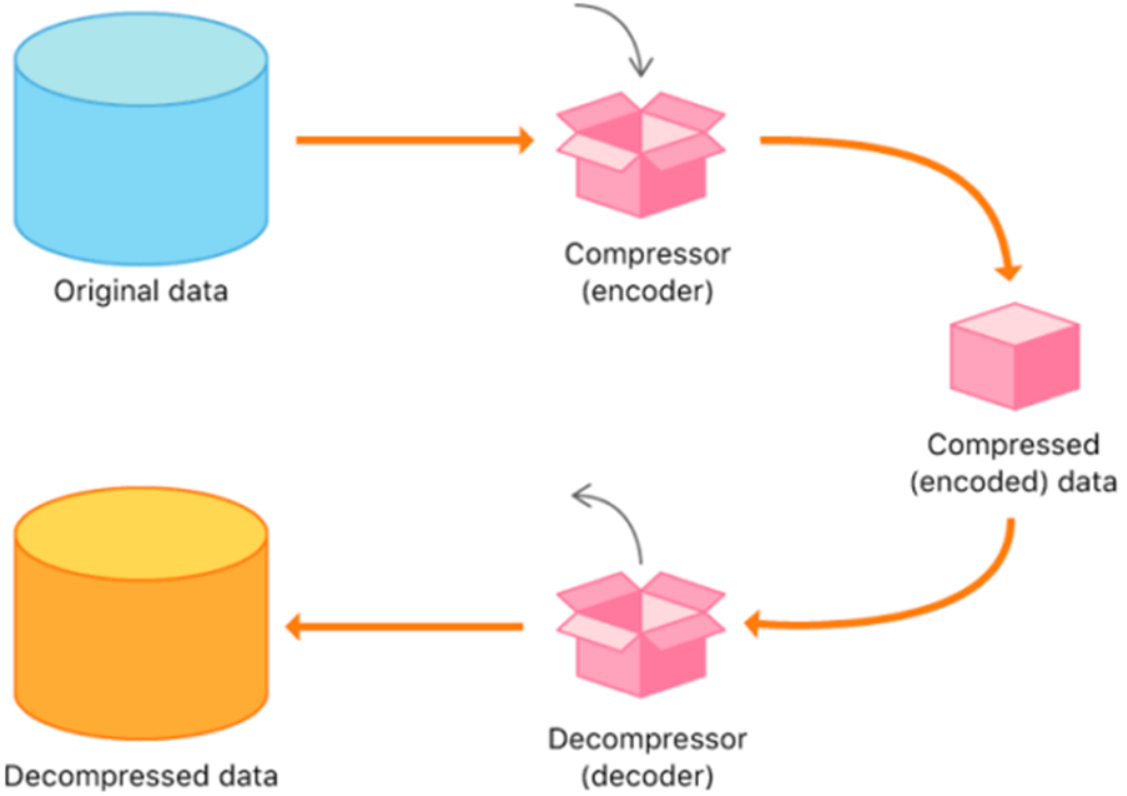
1. 数据爆炸与安全挑战

数据增长：数字化转型导致数据爆炸，需求对高效存储和计算。

安全法规：中国的商用密码应用推广，美国的HIPAA和FISMA规定。

2. AI与大数据加密

AI需求：AI依赖大数据分析，强调数据的安全与可用性。



Encryption & Decryption

Both the Architecture of processor designers, like Arm Aarch64

and,

The chipset vendors, by implementing specialized Hardware accelerators,

- worked hard and did serious jobs to conquer that need.

硬件加速器

Hardware Accelerators

- Dedicate Purposed
  - AWS: Nitro Cards
  - Nvidia: DPU
  - Smart NIC, etc.
- General Purposed
  - Huawei （Aarch64）: Kunpeng 920+ Embedded Engines
    - ZIP Engine （ZIP，Compression）
    - SEC Engine（SEC， Security）
    - HPRE Engine （HPRE，High Performance RSA Engine）
    - RDE Engine （RDE，RAID DIF Engine）

https://en.wikipedia.org/wiki/HiSilicon#Kunpeng_920_(formerly_Hi1620)

UADK 技术概述

UADK 的起源和能力

UADK，全称为用户态硬件加速器开发工具包（User Space Accelerator Development Kit），支持共享虚拟地址（SVA）技术，为用户提供高效利用硬件加速器能力的统一编程接口。它为用户提供了基础的库和驱动支持。UADK 提供了一组不断扩展的高性能算法实现，涵盖了加密、压缩等功能。在最新的openEuler 24.03 LTS版本中，UADK已经能够同时支持硬件加速引擎和Arm64 SVE / Crypto Extension CPU指令加速。

在最新社区稳定版 **openEuler 24.03-LTS** 中，UADK支持的加速算法有：

- **压缩算法**: GZIP，ZLIB，DEFLATE，LZ77_ZSTD
- **非对称加解密**: RSA，DH，ECC（SM2，ECDSA，ECDH，X25519/X448）
- **对称加解密**: AES，SM4，DES/3DES
- **摘要算法**: SHA-1，SHA-2，SM3，MD5

Introducing UADK - a user-space framework

UADK

- a general User-space Application Development Kit

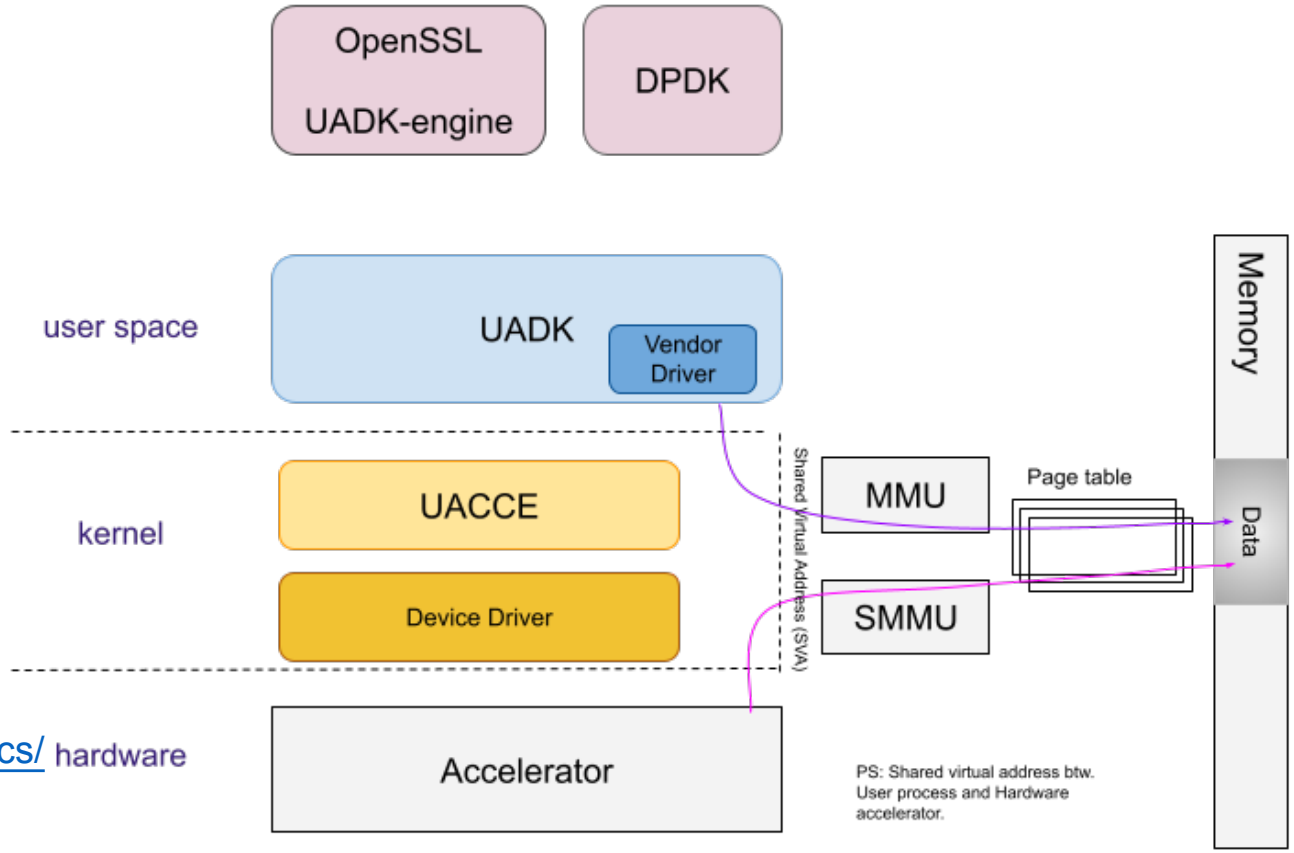
⇒ Utilize the hardware accelerator capabilities

⇒ Using SVA (shared virtual addressing) technology,

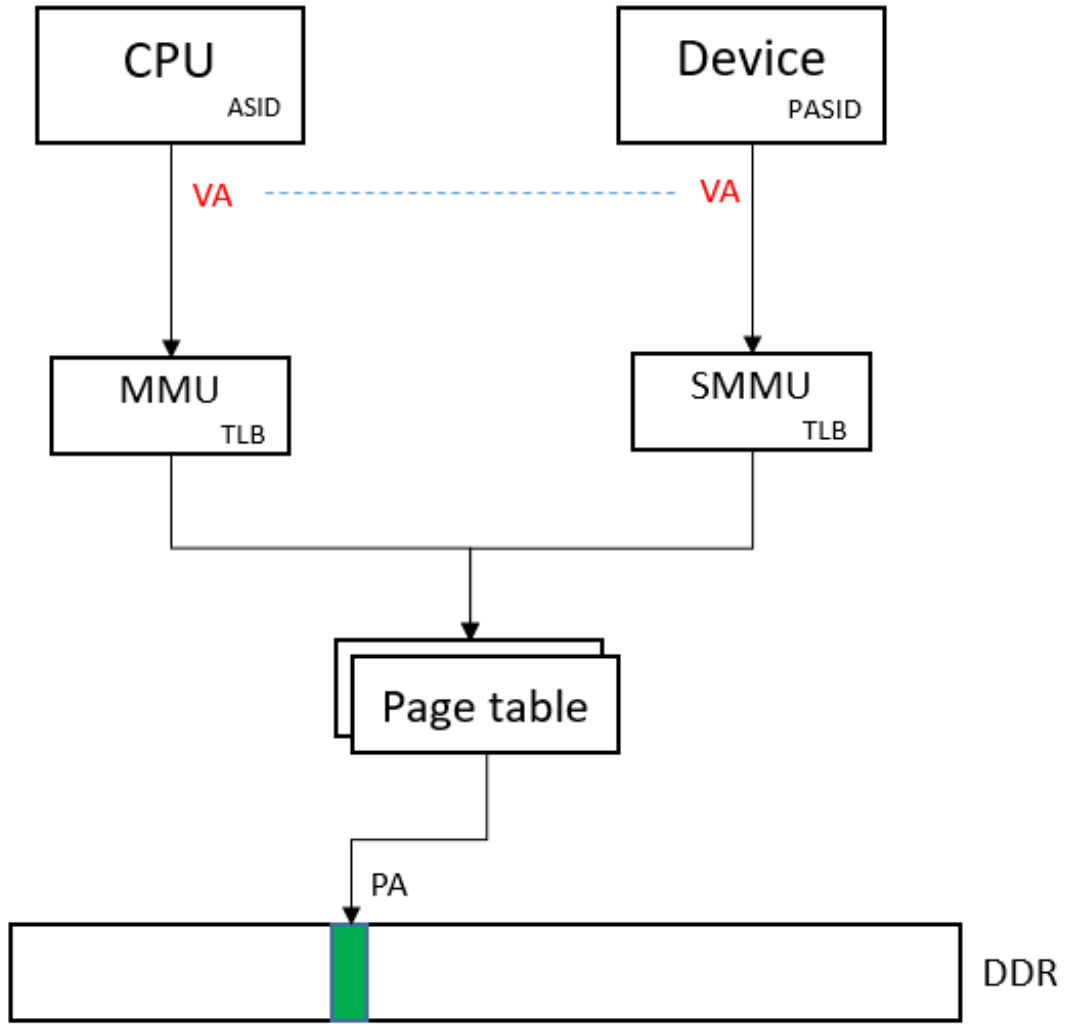
⇒ Achieving zero-copy.

⇒ An openEuler AccLib SIG project

- A Quick Start Guide: https://docs.openeuler.org/en/docs/22.03_LTS/docs/UADK/UADK-quick-start.html
- Source code: https://github.com/Linaro/uadk



Introducing UADK - SVA (shared virtual address)

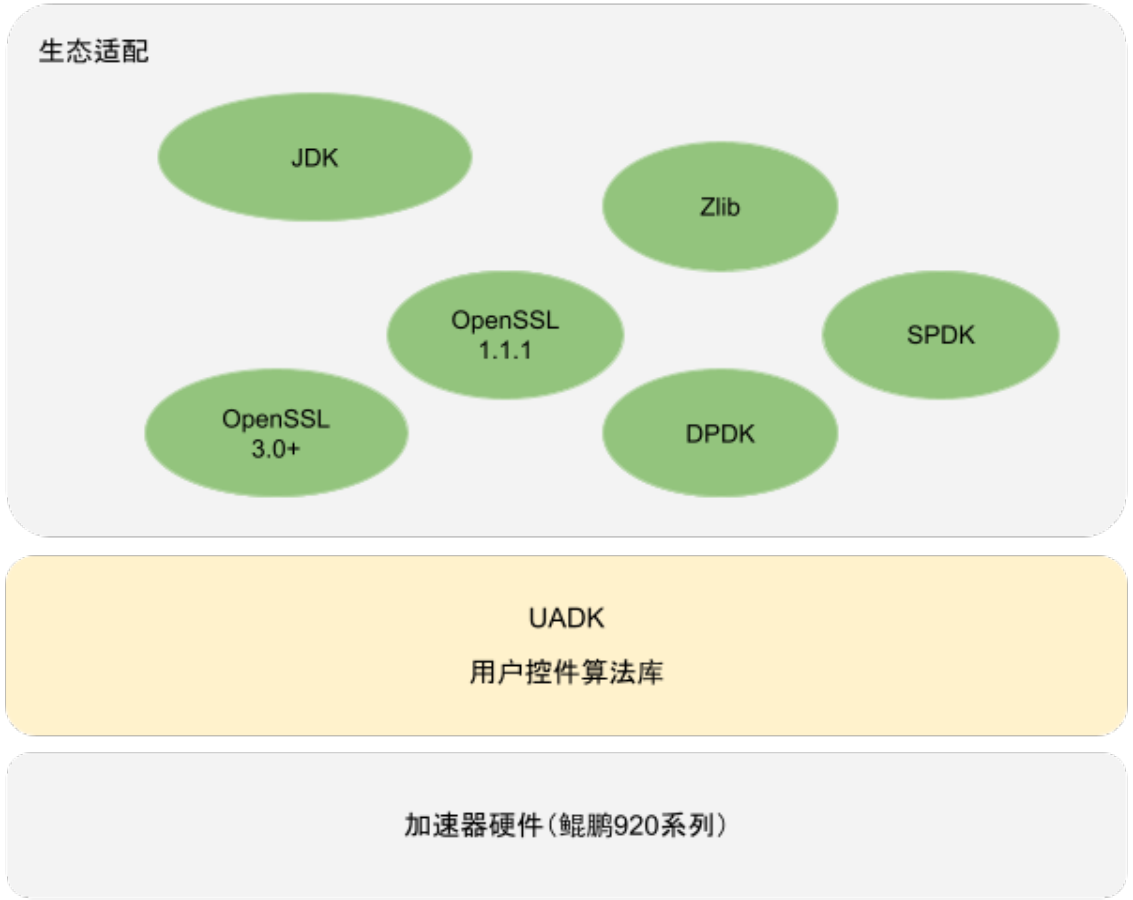


UADK 的软件生态建设

UADK 的软件生态建设

目前已经对接的生态链加速组件包括：

- OpenSSL 1.1.1f+
- OpenSSL 3.0+
- DPDK，支持UADK crypto PMD 和UADK compress PMD
- SPDK，支持UADK crypto PMD 和UADK compress PMD
- OpenJDK / BishengJDK
- Zlib 压缩库
- GmSSL 3.0，服务于国密算法 SM2/3/4 应用场景
- Nginx 1.20.0，对https短连接场景有很好的加速效果



通过对JDK的支持，让UADK能够进一步惠及大数据和AI数据处理场景。

UADK 与 Big Data 的结合实践

大数据领域的应用场景识别

1. 加密

HDFS Transparent Encryption

HDFS（Hadoop Distributed File System）透明加密是一个保护存储在HDFS中数据的安全功能。透明加密的主要目的是在不改变现有应用程序代码的情况下，对存储在HDFS上的数据进行加密和解密。这种方式为数据的存储和访问提供了一层透明的安全保护，用户无需关心底层的加密细节。

1. 压缩

HBase

HDFS 透明加密支持多种加密算法，包括 AES 和 SM4。

大数据领域的应用场景识别

1. 加密

HDFS Transparent Encryption

1. 压缩

HBase

在HDFS透明加密中，首先需要定义加密区（Encryption Zone），每个加密区都会使用一个密钥来加密其中的文件。这些密钥由一个集中的密钥管理服务（如Apache Ranger或Cloudera Navigator Key Trustee）进行管理，确保密钥的安全性和生命周期管理。

当用户访问加密区中的文件时，HDFS透明地对数据进行解密，用户感受不到加密解密的过程。这样，即使HDFS的物理存储被非法访问，数据也因为被加密而保持安全。

在实践中，我们使用 SM4 作为加密算法。

UADK-BigData 创新项目 - openEuler

BigData + UADK: 加速大数据处理的全栈解决方案

https://gitee.com/openeuler/uadk-bigdata

UADK-BigData 创新项目

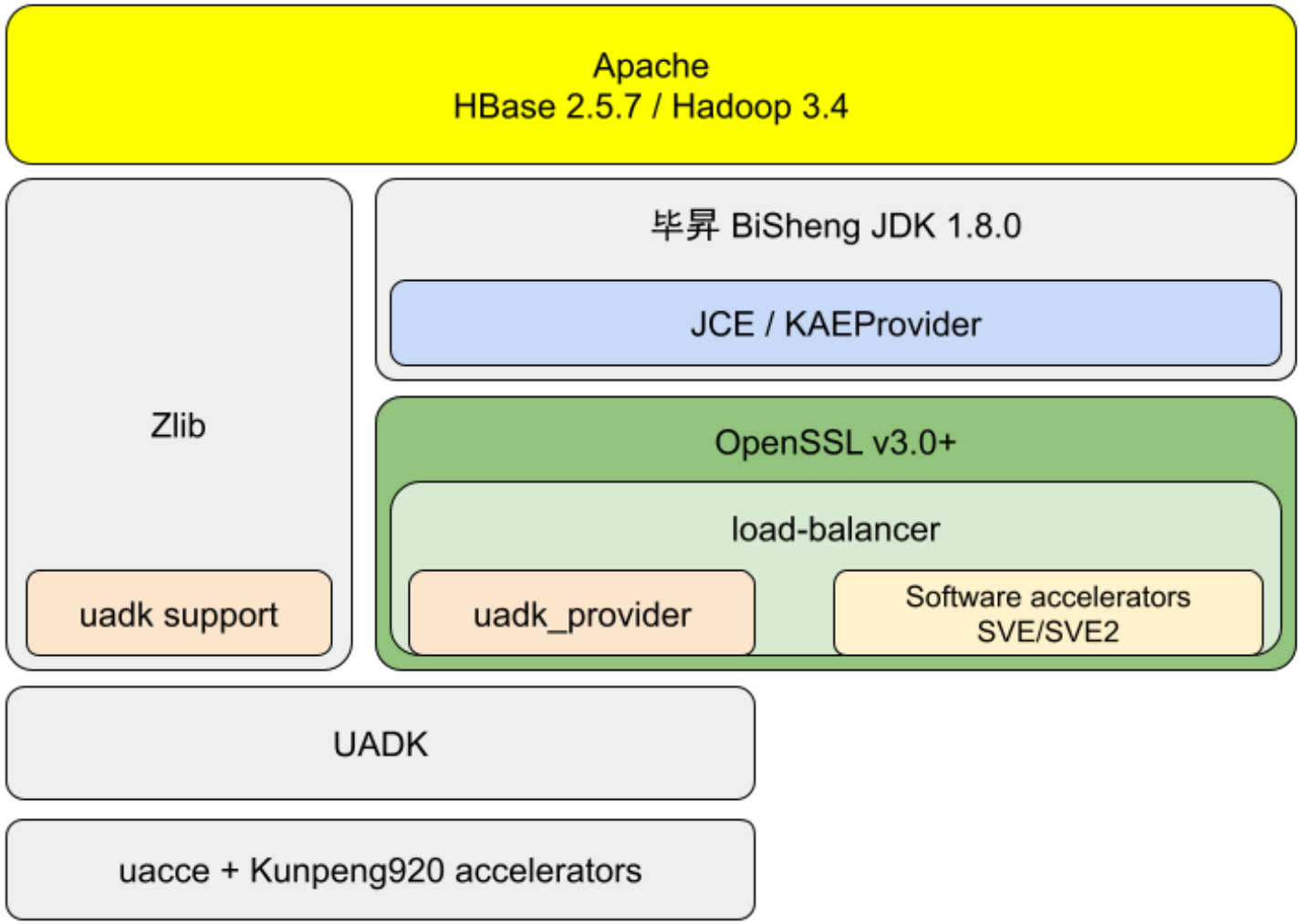
UADK 与 JDK 的对接

Bring the Abilities to the Java World

⇒ KAEProvider is an encryption interface based on **JCA (Java Cryptography Architecture)** that uses the EVP interface to call the computing power provided by OpenSSL.

⇒ 在前人工作的基础上，增加了对 OpenSSL 3.0+ 的支持

⇒ With addition of UADK, it is possible to use hardware accelerations into Java world, powering even more applications.



具体代码修改，和搭建步骤，请参考稍后展示的 “快速上手指南”

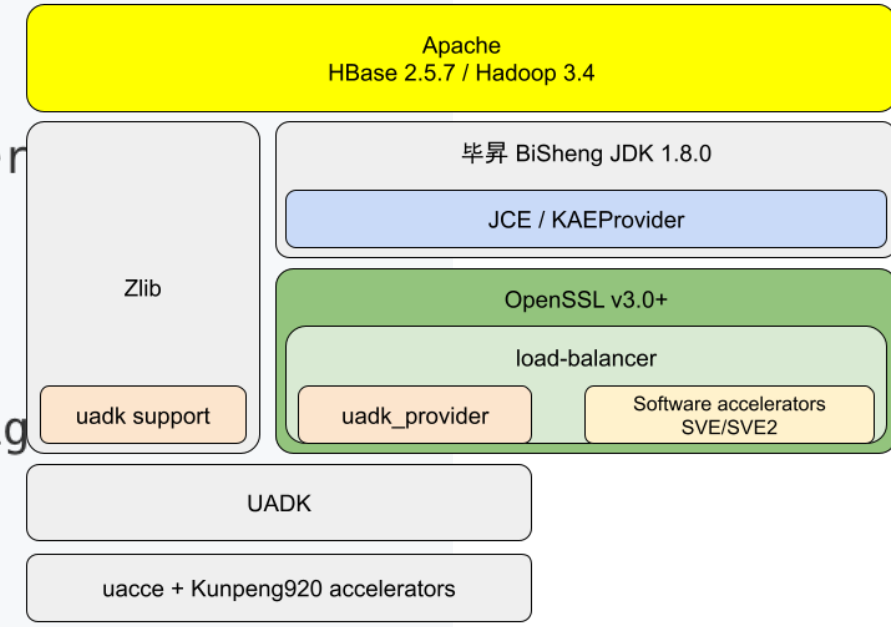
UADK 与 JDK 的对接

Bring the Abilities to the Java World

java.security :

⇒ KAEProvider is an encryption interface based

```
security.provider.1=org.openeuler.security.openssl.KAEProvider
security.provider.2=sun.security.provider.Sun
security.provider.3=sun.security.rsa.SunRsaSign
security.provider.4=sun.security.ec.SunEC
security.provider.5=com.sun.net.ssl.internal.ssl.Provider
security.provider.6=com.sun.crypto.provider.SunJCE
security.provider.7=sun.security.jgss.SunProvider
security.provider.8=com.sun.security.sasl.Provider
security.provider.9=org.jcp.xml.dsig.internal.dom.XMLDSig
security.provider.10=sun.security.smartcardio.SunPCSC
security.provider.11=sun.security.mscapi.SunMSCAPI
```



成果展示与分析

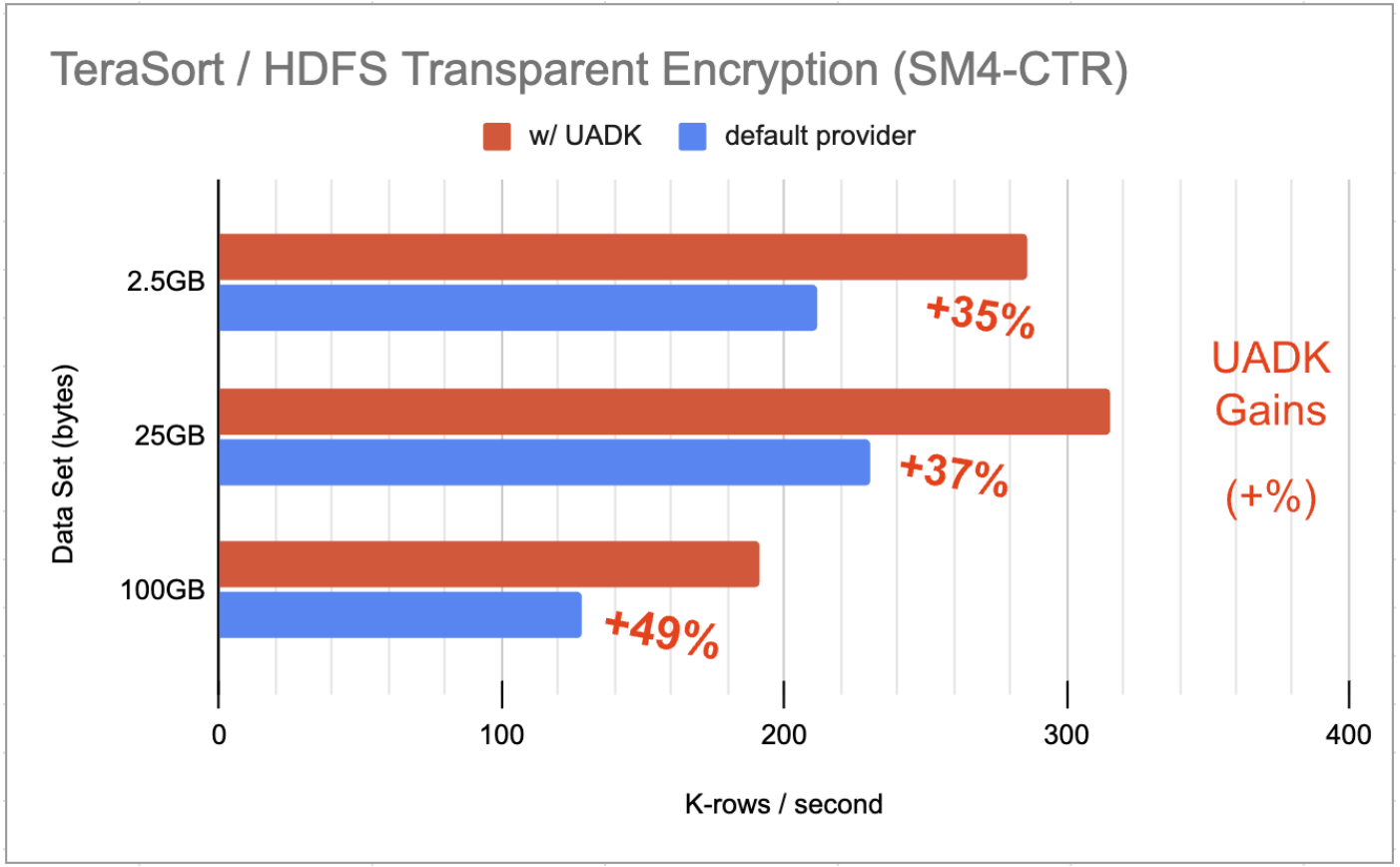
Benchmark - TeraSort

Measured with 100GB data in TeraSort, on the HDFS Transparent Encryption.

```
# hdfs crypto -getFileEncryptionInfo -path /
 zone2/terasort-input/part-m-00000

    {cipherSuite: {name: SM4/CTR/NoPadding,
    algorithmBlockSize: 16}, ...}

# hadoop jar $HADOOP_HOME/share/hadoop/mapreduce/
 hadoop-*examples*.jar terasort /zone2/terasort-
 input /zone2/terasort-output
```



快速上手指南：

https://gitee.com/openeuler/uadk-bigdata/blob/master/Quick.Start.Guide.md

UADK-BigData 创新项目

BigData + UADK: 加速大数据处理的全栈解决方案

https://gitee.com/openeuler/uadk-bigdata

UADK-BigData 创新项目

openEuler Big Data SIG

双周例会会议纪要：https://etherpad.openeuler.org/p/bigdata-meetings

openEuler Big Data SIG 主页

THANKS