数牍科技软硬协同产品介绍

数牍科技隐私计算软硬协同产品，可将隐私计算平台 Tusita 与国产化隐私计算硬件产品完美融合，面向政务、金融、电信等行业领域，在多方数据要素流通协作中，提供国产化底层关键基础设施，输出隐私计算软硬件全栈技术解决方案及服务能力。

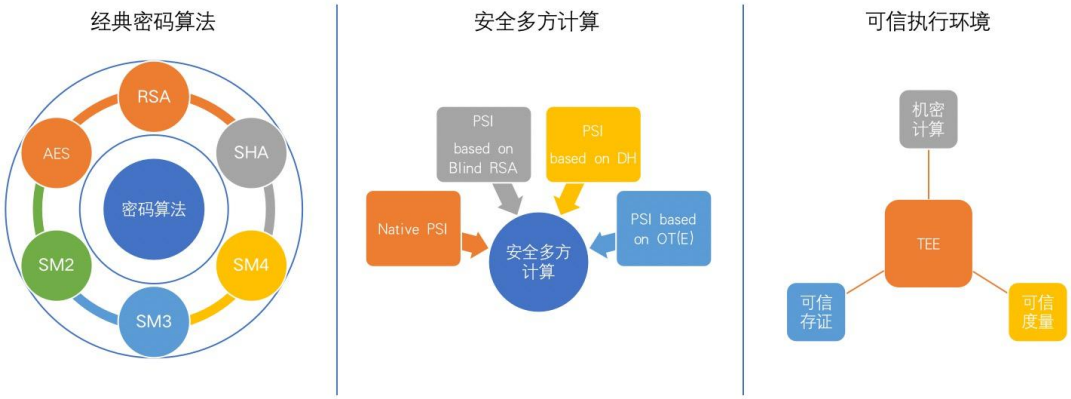
产品从底层芯片选择、硬件电路的设计、国产密码算法的研发，到上层的隐私计算平台，均实现完全的国产自主可控。具体而言，在计算层面，本产品可将平台隐私计算核心算法、算子等进行功能抽取，将其能力下沉并部分托管至硬件环境中，通过调用芯片的加速能力提升平台算力；在存储方面，数牍单独引入了物理隔离的存储区域，实现算法及算子的单独运行、敏感数据的隔离存储等，从逻辑上封装了算法、算子的安全加速单元。

一、产品定位：

- 计算加速
  关键运算使用专用硬件实现，提升MPC、FL等计算的性能；
- 安全隔离
  硬件物理隔离方式，专有数据空间，增强对于敏感数据的安全保护；
- 贴源处理
  将计算数据和计算处理更贴近数据源，减少不必要的数据传输；
- 自主可控
  全国产化技术，更好面向政务、金融、电信等关键技术设施行业；
- 资源复用
  标准的接口形式，灵活插拔，实现对过剩的资源的改造复用；
- 算力扩展
  取决主板上的插槽数量，进行多卡配置，增强算力；

以上述“安全隔离”特点为例：**使用数牍专用硬件产品，可针对中间参数、模型梯度等信息，尤其是对于隐私计算中使用的部分算法密钥以及用于系统安全启动、安全通道建立、身份认证的数字证书等进行隔离保护**，并进行更加独立的使用和运算，从而实现对于业务处理、用户环境交互等动作进一步的物理隔离。

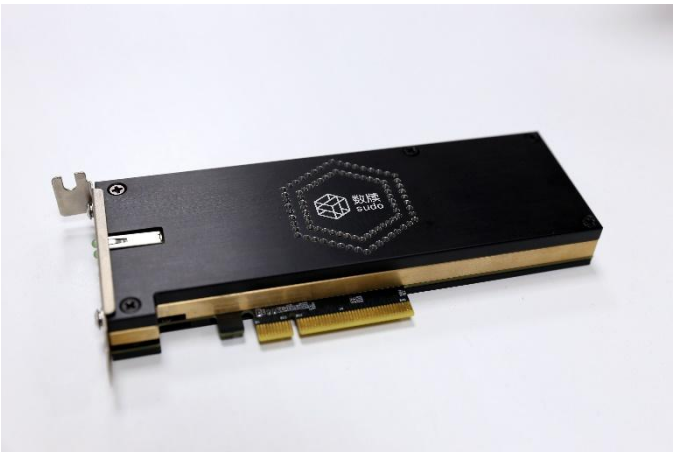
二、产品功能



数牍隐私计算软硬结合产品可在技术多样性融合、单一软件实现增强、信创一体化战略等方面进行提升。目前功能层面支持经典的密码算法，如 AES、RSA、SHA 等，国密 SM2、SM3、SM4 等；支持安全多方计算 PSI 的功能，以及对于可信执行环境的功能支持，部分功能参数列表如下。

算法名称	操作类型	性能参数
AES	加解密	50Gbps
RSA	公钥运算	2048：10 万次/秒 1024：20 万次/秒
	私钥运算	2048：3500 次/秒 1024：13000 次/秒
HASH	SHA-256	10Gbps
SM2	签名	15 万次/秒
	验签	5 万次/秒
SM3	--	20Gbps
SM4	加解密	25Gbps
Beaver 三元组	--	64 位：120W 组/秒

三、产品形态



产品以 PCIE 板卡形式，具体形态为：

- 尺寸：167.25mm*69mm（半高半长）
- 接口：USB2.0，一路；UART，二路三线制接口；WAN，二路千兆 GMII；PCIE 2.0，支持 X4/8/16 高速；SPI，二路 SPI master，一路 SPI slave；GPIO，16 个 GPIO；
- 供电：PCIE 供电；外部 12V 供电

与其他隐私计算加速卡的区别：

- 采用了专用集成电路（ASIC）的形式，虽然降低了可编程的灵活性，但是提高了对于数据保护的安全性；
- 全国产化的设计，全面实现数据安全应用场景下技术的安全可信；
- 密码算法的高性能和可扩展性。

四、部分认证

数牍硬件模块可灵活插拔，支持将任意的通用服务器进行功能展成隐私计算服务器。数牍专用硬件已完成与银河麒麟高级服务器操作系统（飞腾版）V10、浪潮英信服务器产品 NF2180M3、飞腾信息技术有限公司 FT-2000+/64 处理器平台及 S2500 处理器平台的兼容适配认证，专用硬件的性能及可靠性能够满足用户的关键性应用需求。

五、其他说明

在性能的表现上，以常用的 RSA-2048 算法为例，数牍的硬件方案在 8 核的服务器上即可实现 RSA 公钥加密性能约 12 万次每秒，私钥解密性能约 4000 次每秒；在同等配置的通用服务器上，基于纯软实现的 openssl 的 RSA 公钥加密性能约为 2.5 万次每秒，私钥解密性能约为 700 次每秒。

在秘密分享方案中，部分场景通过使用数牍的专有硬件能够避免同态加密计算造成的性能严重损耗，以 DH 方案的 PSI 实现为例，整体计算性能可带来约 2~3 个数量级的提升。

数牍科技仍在基于自有的硬件产品进行安全多方计算的相关算法的实现，新的功能特性敬请期待!