在看完IIoT安全性研究综述这篇论文之后，区块链的应用主要是在解决IoT/IIoT的设备管理上，我觉得这就涉及到了数据的安全性问题，所以我就看了几篇算法。

一种低耗能的数据融合隐私保护算法

<https://kns.cnki.net/KCMS/detail/detail.aspx?dbcode=CJFQ&dbname=CJFD2011&filename=JSJX201105004&v=MjAyOTdJUjhlWDFMdXhZUzdEaDFUM3FUcldNMUZyQ1VSTE9lWnVSc0Z5cmhVYjNQTHo3QmRyRzRIOURNcW85Rlk=>

本文提到了一种新的低能耗无线传感器数据融合隐私保护算法ESPART。

ESPART--本质上是对SMART算法的相应改进。

1、优点：计算复杂度和数据传输量小、对QS（查询服务器）具备隐私保护性。

2、如何降低数据融合时间？

给每个节点分配随机时间片，以避免节点间的碰撞，限制节点间串通的数据范围（降低数据丢失对精确度的影响）。

3、如何降低数据传输量？

采用了依靠数据融合树形结构本身特性的办法。

相比于SMART算法，ESPART可以在有效保护数据隐私的前提下，花费与TAG算法（是一种典型的应用在无线传感器网络中的数据融合技术）相同的时间和较少的数据通信量，得到精确的数据融合结果。

基于Elliptic-curve及Hilbert-curve的簇间数据压缩融合加密算法

<https://kns.cnki.net/KCMS/detail/detail.aspx?dbcode=CJFQ&dbname=CJFDLAST2019&filename=XXYK201902016&v=MTM3MzdydktQVFhTWmJHNEg5ak1yWTlFWW9SOGVYMUx1eFlTN0RoMVQzcVRyV00xRnJDVVJMT2VadVJzRnlyaFY=>

公钥加密，也叫非对称（密钥）加密（public key encryption），属于通信科技下的网络安全二级学科，指的是由对应的一对唯一性密钥（即[公开密钥](https://baike.baidu.com/item/%E5%85%AC%E5%BC%80%E5%AF%86%E9%92%A5/7453570)和私有密钥）组成的加密方法。它解决了密钥的发布和管理问题，是目前商业密码的核心。在[公钥加密体制](https://baike.baidu.com/item/%E5%85%AC%E9%92%A5%E5%8A%A0%E5%AF%86%E4%BD%93%E5%88%B6/7080546)中，没有公开的是私钥，公开的是[公钥](https://baike.baidu.com/item/%E5%85%AC%E9%92%A5/6447788)。

算法ECHCPA--基于Elliptic-curve及Hilbert-curve的数据融合加密算法

Elliptic-curve：进行公钥加密的椭圆曲线。

Hilbert-curve：实现数据维度转换的曲线（数据是离散的时候可以使用）。

1、之所以对数据进行多级压缩融合和加密，是因为在WSN中，要确保网络的连通性和可靠性不受单个偏差较大的数据影响，传输数据又是庞大的，且存在被盗取的可能，数据安全性就得不到保障。

2、如何降低开销（通讯开销）？

对融合加密过程的通讯开销，用椭圆曲线公钥加密、Hilbert-curve压缩融合，从而降低复杂度，降低开销。