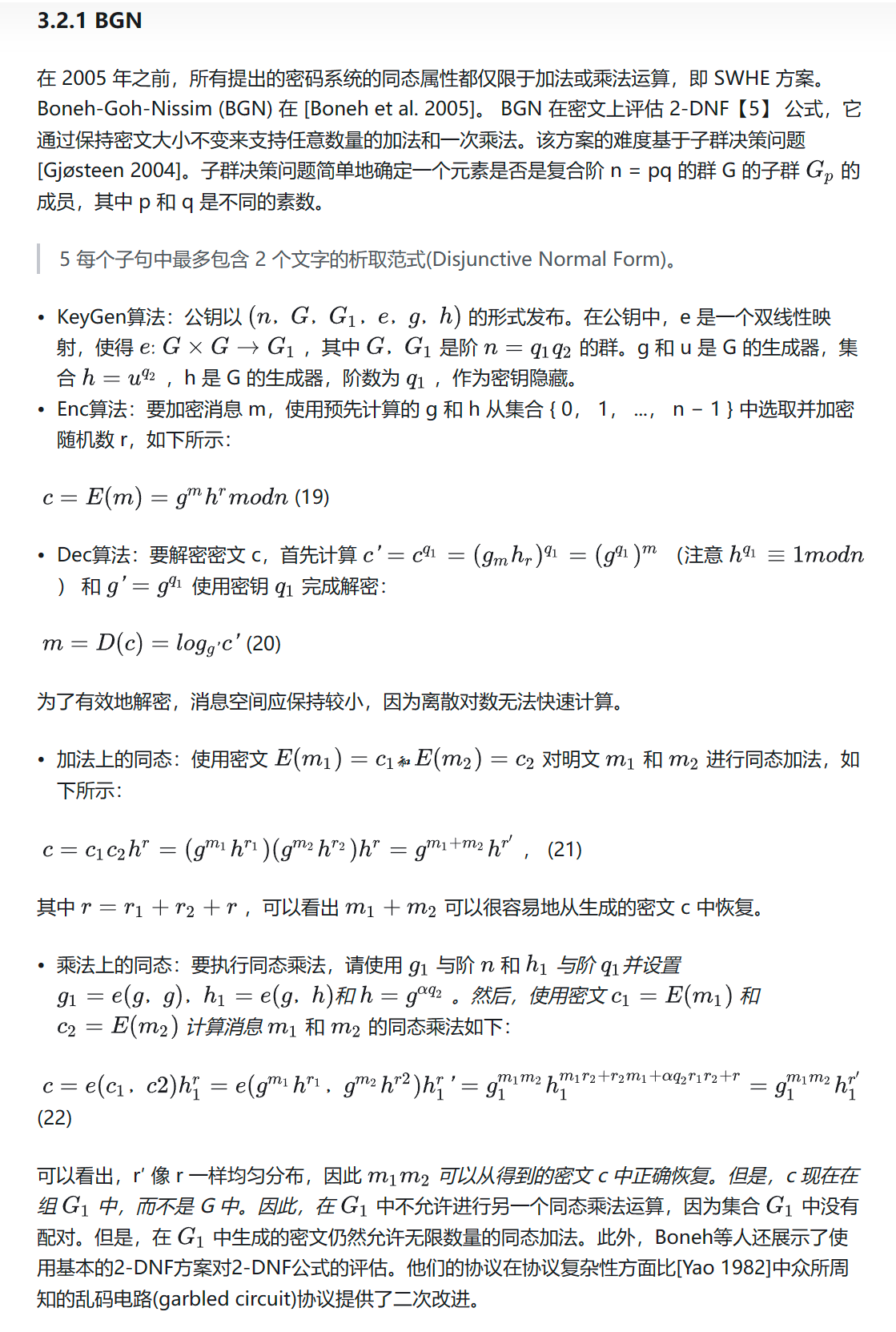
boneh-goh-nissim方案

·BGN介绍：利用双线性映射实现的支持任意数量加法和一次乘法的有限次全同态加密算法，

具体实现方式：



BGN通常基于椭圆曲线密码学，使用椭圆曲线上的点作为公钥，而私钥则是与之相关的离散对数

·BGN在联邦学习中的潜在优势：

·与Paillier方案相比：BGN方案支持一次乘法运算，可以对更复杂的数据模型进行加密上传

·与全同态加密方案相比：全同态加密通常涉及更复杂的数学结构和计算，因此其性能可能较低。BGN提供了一种在某种程度上折中了性能和同态性的选择——BGN相较于全同态加密方案进行的运算较少，计算方法和数据结构更简单，易于实现；且生成的密文体积可能较小，通信所需的开销也随之减少，降低通信负担。

·特定应用场景：椭圆曲线同态加密方案相关情况下BGN方案效率最高。

·BGN在联邦学习中可能存在的缺点：

·不安全性[On Insecure Uses of BGN for Privacy Preserving Data Aggregation Protocols - IOS Press](https://content.iospress.com/articles/fundamenta-informaticae/fi222143)

·缺乏普遍性：适合较复杂模型的加密，但过于复杂（乘法超过一次）则会失去准确性，在加密模型近似椭圆曲线同态加密时其实用性才能最大化