Why Does MPC Operate in Rings/Fields?

安全多方计算（MPC）一般是在有限环或者域中进行（Ring/Field）进行。比如，Additive Secret Sharing是计算在环 $(\mathrm{mod}\ 2^\ell)$中，而Shamir's Secret Sharing则是定义在 $(\mathrm{mod}\ P)$域中。对于初学者而言，一个常见的疑问是为什么不直接在实数内定义秘密分享等安全多方计算原语？本次，我们简单整理以下背后的原理，并给出一些推荐材料。

0. 从入门

在利用秘密分享等技术实现MPC协议时，核心的指导思想在于利用关联随机数实现mask-and-compute。为了安全性的保障，mask之后的数据要满足均匀分布，即 $x + r$ 之后的数据要能够和一个全新的随机数 r' 不可区分。
以Additive Secret Sharing为例，如果所有的数据都编码在环$\mathbb{Z}_{2^\ell}$中，r可以均匀选取，则$x + r$在一次一密的情况下时满足安全性要求的；但是，如果是在实数$\mathbb{R}$中，不存在一个均匀分布，因而r不是均匀随机的，故$x + r$也无法满足安全性要求。

1. 到放弃

接下来，我们简单证明为什么在$\mathbb{R}$不存在一个均匀分布。

证明：

假设存在一个均匀分布，那么对于任意的整数n，对于一个实数x满足 $n \leq x < n + 1$的概率应该是相等的。记这个概率是 p。

记事件 $E_n = \{x | n \leq x < n + 1\}$，则对于无限互斥事件，应该有

$$P(\cup_n E_n) = \sum_n P(E_n)。$$

因为对于每一个实数x存在n 满足 $n \leq x < n + 1$，那么$P(\cup_n E_n) = 1$。
另一方面，对于$\sum_n P(E_n) = p + p + p + \ldots$，有如下两种情况：

- 如果 $p > 0$，$\sum_n P(E_n)$ 是没有上限的；
- 如果 $p = 0$, $\sum_n P(E_n) = 0$。

任意一种情况，都得不到 $\sum_n P(E_n) = 1$。因此，假设不成立。证毕。

Reference

[1] https://math.stackexchange.com/questions/14777/why-isnt-there-a-uniform-probability-distribution-over-the-positive-real-number
[2] https://crypto.stackexchange.com/questions/10701/shamirs-secret-share-over-the-reals