The Group Theory

Ryan J. Kung
ryankung@ieee.org
Member, IEEE Blockchain Community

February 1, 2019

1 Group

1.1 Definition

Definition: Group [1]:

A set $\mathbb{G} = a, b, c, ...$ is called a group, if tehere exists a group multipliaction connecting the elements in $\mathbb{G}$ in the following way:

(1) $a, b \in \mathbb{G} : \ c = ab \in \mathbb{G}$ (closure)

(2) $a, b, c \in \mathbb{G} : (ab)c = a(bc)$ (associativity)

(3) $\exists e \in \mathbb{G} : ae = e, \forall a \in \mathbb{G}$ (identity / neutral element)

(4) $\forall a \in \mathbb{G}, \exists b \in \mathbb{G} : ab = e, i.e., b \equiv a^{-1}$

1.2 Pubic-key cryptography

"The mathematics of public-key cryptography uses a lot of group theory. Different cryptosystems use different groups, such as the group of units in modular arithmetic and the group of rational points on elliptic curves over a finite field. This use of group theory derives not from the "symmetry" perspective, but from the efficiency or difficulty of carrying out certain computations in the groups. Other public-key cryptosystems use other algebraic structures, such as lattices."' [1]

References

[1] Luca Cardelli. Type systems. *ACM Comput. Surv.*, 28(1):263–264, March 1996.