A new approach for Arithmetization-Oriented symmetric primitives

Clémence Bouvier[1,2]

[1]Sorbonne Université, France
[2]Inria, France

Abstract. In recent years, new symmetric primitives have been designed to be executed in abstract contexts such as Zero-Knowledge (ZK) proof systems, widely used in crypto-currency applications such as Bitcoin or Ethereum. In particular, these protocols have highlighted the need to minimise the number of multiplications performed by the primitive in large finite fields. As the number of the so-called Arithmetization-Oriented (AO) designs increases, e.g. MiMC-Hash, Rescue–Prime, Poseidon, `Reinforced Concrete` and Griffin to name a few, it is important to better understand the properties of their underlying operations.
After introducing the background and explaining the need to design new primitives, we will present a new approach to ZK-friendliness. More precisely, we will propose a family of hash functions: `Anemoi`, exploiting a link, previously unknown, between AO primitives and CCZ-equivalence. One of the main features that set `Anemoi` apart from other such families is that it has been designed to be efficient within multiple proof systems (R1CS, Plonk, AIR, etc.) but it has particularly competitive performance for implementation in Plonk constraints.
Besides pushing further the frontier in understanding the design principles behind AO hash functions, we also offer two standalone components that can be easily reused in new designs. Our new S-box: the `Flystel`, is highly inspired by the well-studied Butterfly structure. We will see how the CCZ-equivalence between its two variants (the Open `Flystel` and the Closed `Flystel`) leads to good ZK performances and high security level. We will also describe a new mode of operation for Merkle trees: Jive, inspired by the "Latin dance" symmetric algorithms (Salsa, ChaCha and derivatives).

Keywords: Anemoi · Flystel · Jive · Arithmetization-oriented · Hash functions · CCZ-equivalence · Plonk · R1CS · Merkle tree · Zero-knowledge · Arithmetic circuits