“Hades” Design Strategy for MPC/SNARKs/STARKs/Picnic/...

Lorenzo Grassi, Daniel Kales, Dmitry Khovratovich, Reinhard Lüftenegger, Sebastian Ramacher, Christian Rechberger, Arnab Roy and Markus Schofnegger

March, 2019

Research of New Designs

Research of new designs is motivated by recent progress in practical applications of

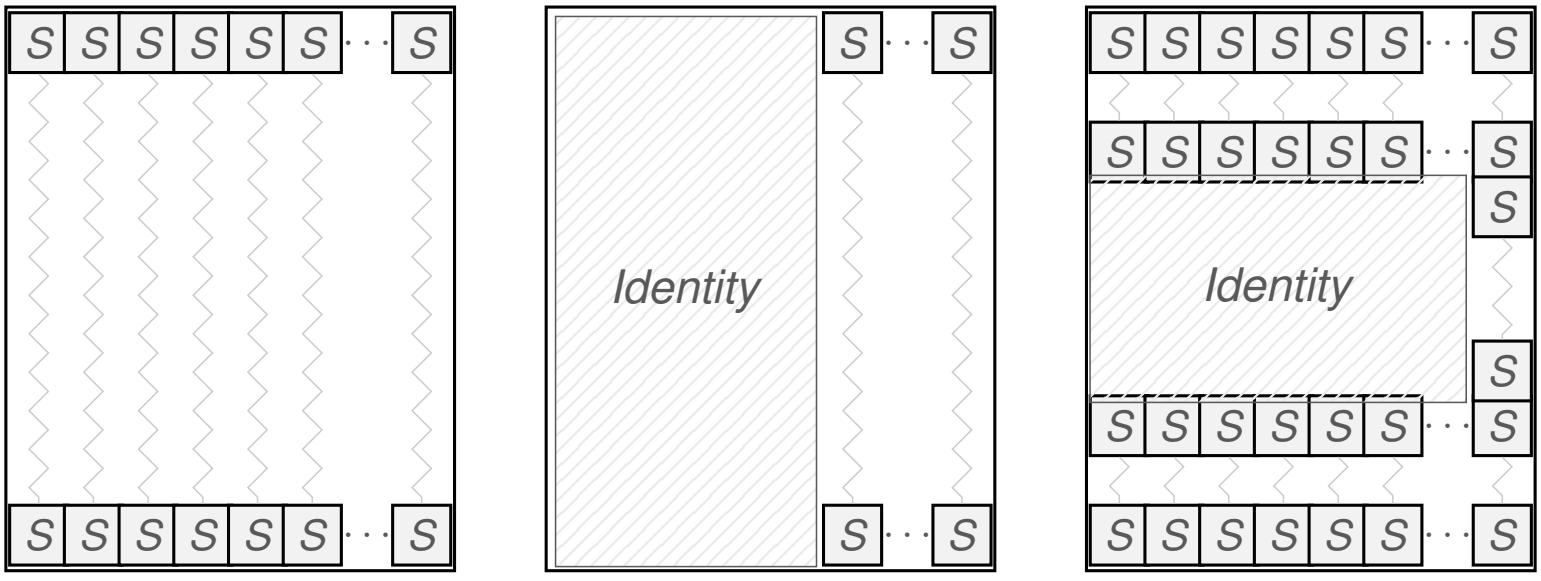
- secure multi-party computation (MPC)
- zero-knowledge proofs (ZK)
- (post-quantum) signature scheme
- SNARKs and STARKs

where *primitives from symmetric cryptography are needed* and where linear computations are essentially “free”:

Performance of symmetric-key algorithms influences the protocols efficiency.

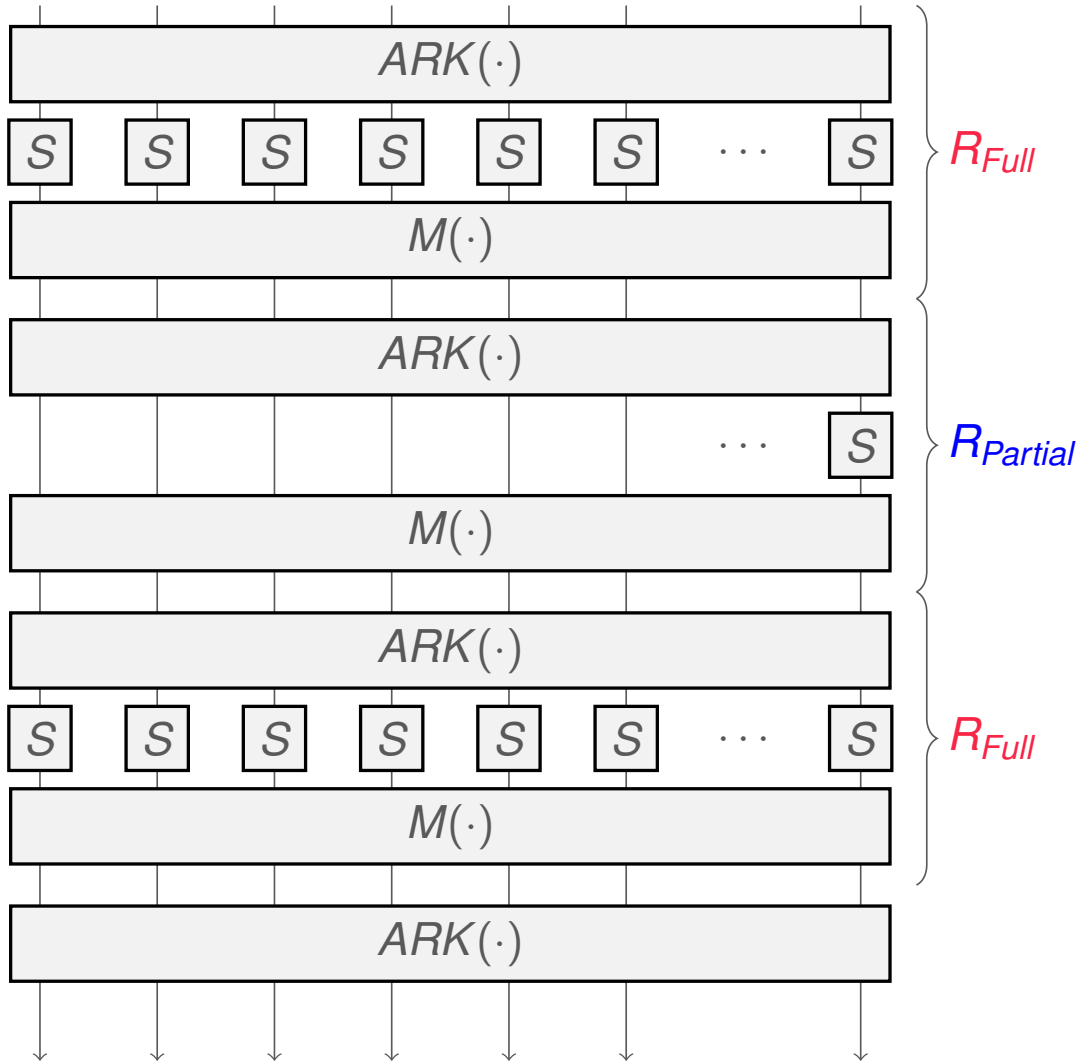
“Hades” Strategy

How to reduce number of non-linear operations?



(a) SPN (b) P-SPN (c) “Hades” strategy

HadesMiMC (in $\mathbb{F}_p$ and/or in $\mathbb{F}_{2^n}$)



Experimental Results

- PQ-Signature ($\mathbb{F}_{2^n}$ case):

  better than LowMC: smaller signature size (777 bits *vs* 1140 bits) and 10x faster;

- MPC ($\mathbb{F}_p$ case):

  better than MiMC and Legendre PRF (the current best schemes for this application);

- SNARKs/Bulletproof ($\mathbb{F}_p$ case) and STARKs ($\mathbb{F}_{2^n}$ case):

  on-going work: 5-10x less constraints per bit than e.g. the recently introduced Pederson hash.