Research at Aztec

12. januar 2026

Type of research/theory work at Aztec

1. General snark research
2. Snark research questions relevant to current Aztec system (EC-based).
3. specing and proving security of Aztec protocol

Obviously categories overlap

General snark research

- Proximity gaps conjecture - Improve/simplify writeup of CA/MCA proof.
- Research on Fiat-Shamir security
- cryptographic trilinear maps

Snark research questions derived from current Aztec system

- small value, low randomness zero-evading sets: Primes p,s of 256/128 bits respectively. Parameter $\mathbf{n \sim 50}$. Let $\mathbb{F} = \mathbb{F}_{\mathbf{p}}$. We choose random $\mathbf{r} \in \mathbf{F}_{s}$, define $\boldsymbol{v} = (\mathbf{r}, \mathbf{r^2 \bmod s}, \mathbf{r^n \bmod s}) \in \mathbb{F}^{\mathbf{n}}$ Prove for non-zero $\mathbf{a} \in \mathbb{F}^{\mathbf{n}}$ that w.h.p. $< \mathbf{a}, \boldsymbol{v} > \neq \mathbf{0}$.

Snark research questions derived from current Aztec system

- small value, low randomness zero-evading sets: Primes p,s of 256/128 bits respectively. Parameter $\mathbf{n \sim 50}$. Let $\mathbb{F} = \mathbb{F}_{\mathbf{p}}$. We choose random $\mathbf{r} \in \mathbf{F}_{s}$, define $\boldsymbol{v} = (\mathbf{r}, \mathbf{r^2 \bmod s}, \mathbf{r^n \bmod s}) \in \mathbb{F}^{\mathbf{n}}$ Prove for non-zero $\mathbf{a} \in \mathbb{F}^{\mathbf{n}}$ that w.h.p. $< \mathbf{a}, \boldsymbol{v} > \neq \mathbf{0}$.
- Assessing NFS attack progress on pairing-friendly EC's

specing and proving security of Aztec protocol

- stackproofs
- Ongoing formalization of chonk.

Formats of work with reserachers

- *less intense:* Meet once in 2-3 weeks, discuss what research problems are relevant for us.
- *more intense:* 1-2 days per week. Expect in this case more contribution to the "boring" third category.