

Acceleration

```
graph LR; A[Acceleration] --> B[Accelerating arithmetic over Galois Field]; A --> C[Accelerating matrix multiplication]; A --> D[Reducing data transfer overhead]; B --> E["loop-based vs. table-based?"]; B --> F[removing MOD]; B --> G[removing branches]; style F fill:#ffff00,stroke:#ff0000,stroke-width:2px; style G fill:#ffff00,stroke:#ff0000,stroke-width:2px;
```

Accelerating arithmetic
over Galois Field

loop-based
vs.
table-based?

removing MOD

Accelerating matrix multiplication

removing branches

Reducing data transfer overhead