Sharp:

Short Relaxed Range Proofs

- Geoffroy Couteau — IRIF — CNRS
- Dahmun Goudarzi
- Michael Klooß — KIT
- Michael Reichle — INRIA — ENS — CNRS — PSL University

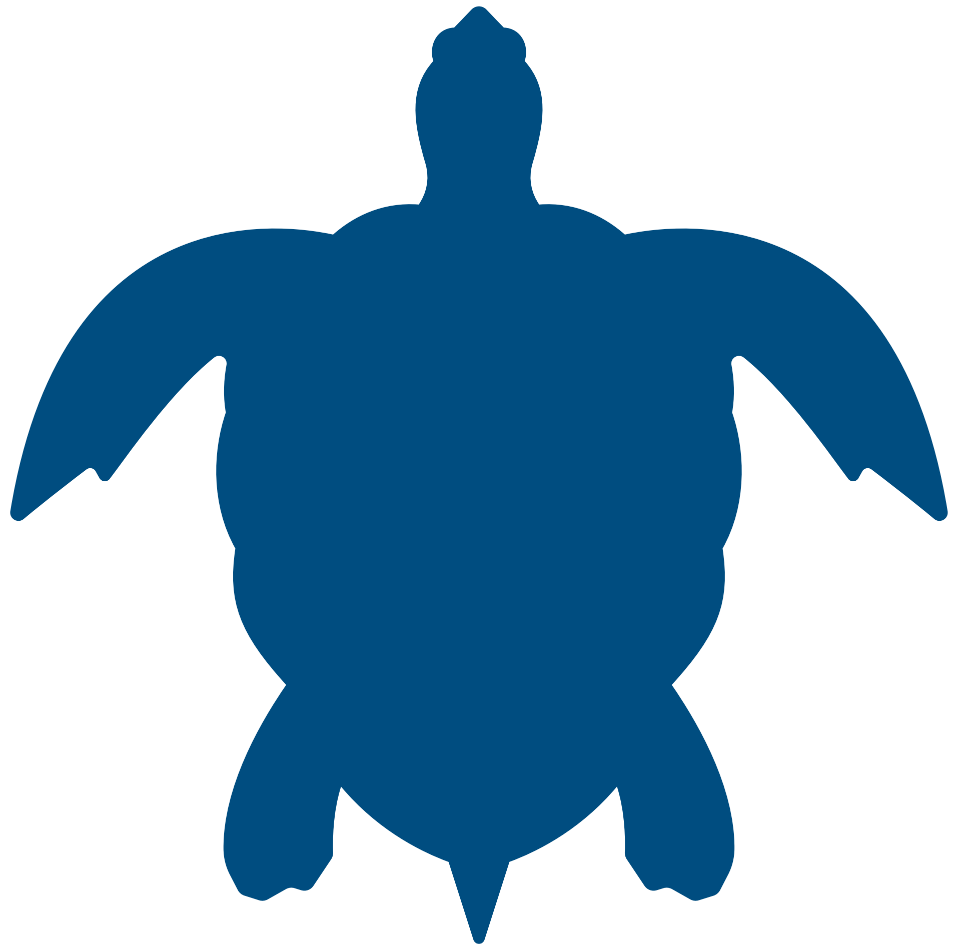
Range Proofs

x

prover

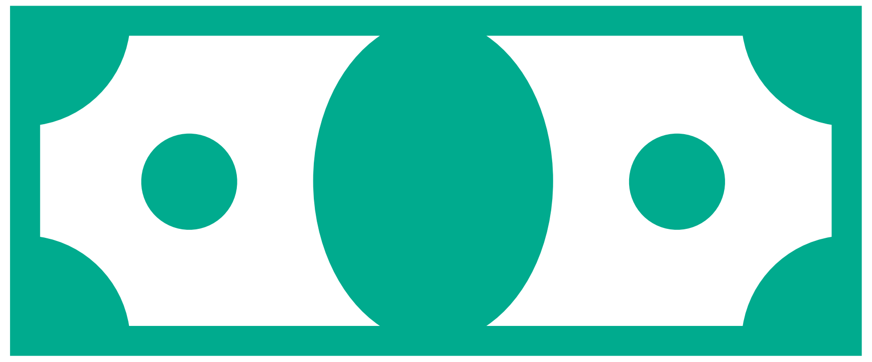
"My hidden but fixed value x
is in the range [a,b]"

[a,b]



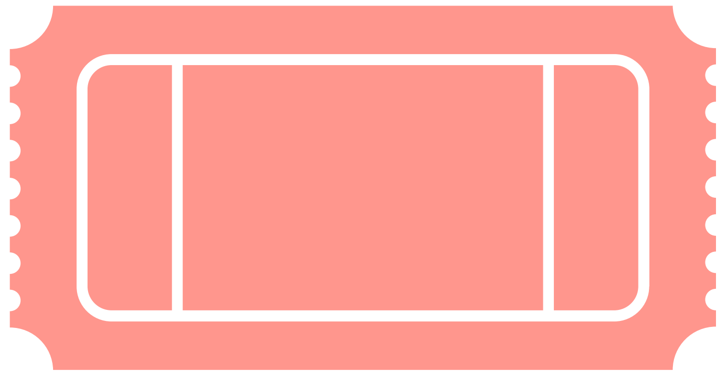
verifier

Applications



Anonymous Transactions
UAC/BBA-schemes

"I have enough money"



Anonymous Credentials

"My ticket in still valid"

Goal: efficient range proofs

CKLR

Great

- Efficient
  - Small communication + computation
- Transparent setup

Bad

- Restricted homomorphic properties
- Non-standard groups:
  - Large modulus

CKLR

- Relaxed Commitment:
  - $\frac{z}{c} \in \mathbb{Z}_p$ commits to $x = \left\lfloor \frac{z}{c} \right\rceil \in \mathbb{Z}$ (short z,c)
- Range Proof:
  - Proof of Short Opening ⋊{short z,c | $\frac{z}{c} \in \mathbb{Z}_p$ }
  - Square Decomposition $(x-a)(b-x) = \sum_{i=1}^{4} x_i^2 \iff x \in [a,b]$

$$\implies x = \left\lfloor \frac{z}{c} \right\rceil \in [a,b]$$

Sharp

Proof of Square Decomposition:

- Improved ∑-protocol
  - Allows for vector commitments
  - Less communication
- Group switching

→ Better efficiency

→ Smaller groups

Sharp

Proof of Short Opening

- Batching:
  - Vector Commitments
  - Shortness via Random Linear Combinations
- Adapted rejection sampling

→ Better efficiency

→ Smaller groups

Sharp

Augmentation via Hidden Order Groups:

- Addition of single RSA or Class Group element
  - Small impact on efficiency
  - Improves homomorphism

→ **Class Groups:** better homomorphism, transparent setup

→ **RSA:** additive homomorphism, trusted setup

Sharp

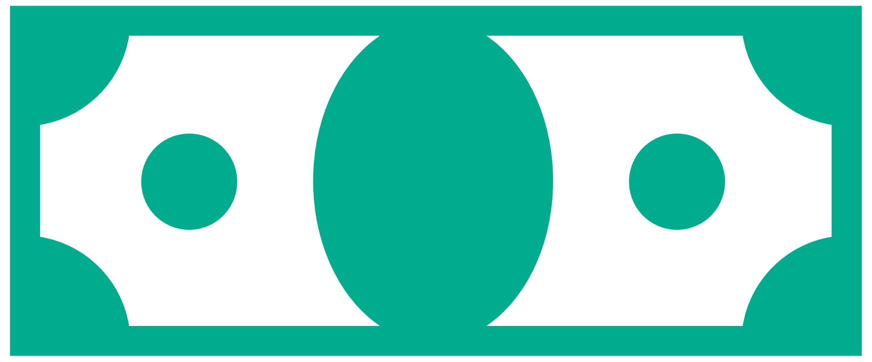
Great

- Very efficient
- Standard Groups
- Easy to implement

Care

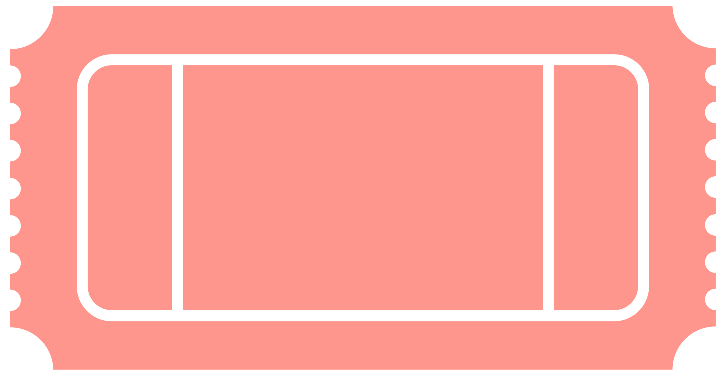
- Tradeoffs between
  - Homomorphism
  - Efficiency + Transparent setup

Applications



Anonymous Transactions
UAC/BBA-schemes

“I have enough money”



Anonymous Credentials

“My ticket in still valid”

“Applicable if initial values short”