# RSA accumulators

# Can we reduce the proof size?

- So far all the methods we have seen have proof size at least logarithmic
- Can we reduce the proof size?
- Yes!
- By changing the cryptographic primitive
- Are we loosing anything?

# RSA Accumulator

- Exponential accumulation of elements:

$$A = a^{x_1 x_2 \cdots x_n} \bmod N$$

  - $N = pq$ is an RSA modulus
  - $a$ and $N$ are relatively prime
  - Only the client knows $p$ and $q$, and thus $\phi(N) = (p-1)(q-1)$
  - Each $x_i$ is prime
- The basis is the accumulation $A$
- Proof of membership of $x_i$ (witness):

$$A_i = a^{x_1 \cdots x_{i-1} x_{i+1} \cdots x_n} \bmod N$$

- Verification:
  - Test $A = A_i^{x_i} \bmod N$
- [Benaloh de Mare]

# Accumulator as a Hash Function

- Quasi-commutative hash function

$$h(h(a, x_1), x_2) = h(h(a, x_2), x_1)$$

- Exponential accumulation yields quasi-commutative hash function

$$h(a, x) = a^x \bmod N$$

- Witness verification as hash computation

$$A = A_i^{x_i} \bmod N = h(A_i, x_i)$$

- Collision resistance
  - Given $a, x, y$ difficult to find $a'$ such that

$$h(a, x) = h(a', y)$$

# Security

- Why should elements be prime?
  - Witness can be computed for factors of elements
- Why should the factorization of N be kept secret?

# Security based on strong RSA assumption:

- Given a modulus *N* of unknown factorization and a base g, it is infeasible to find some e-th root of g mod N.
- How do we prove security based on the above assumption?