Space-Efficient IBE without Pairings

Dan Boneh, Craig Gentry, Mike Hamburg

Stanford University

Appearing in FOCS 2007

IBE without Pairings

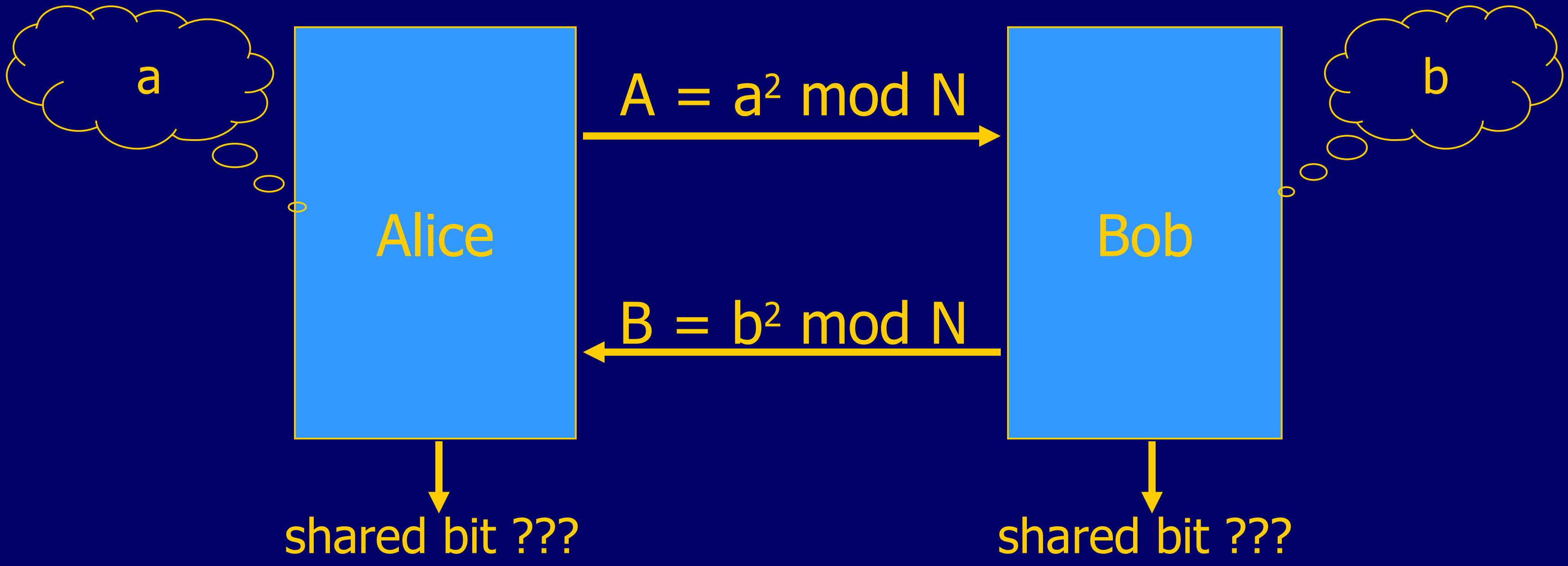
- Most work on IBE uses pairings (a.k.a. bilinear maps):
  - Boneh-Franklin (2001),
    BB04a, BB04b, Wat05, Gen06, etc.

- An IBE Scheme by Clifford Cocks (2001)
  - No pairings!
  - Based on quadratic residuosity mod N (w/ R.O.)
  - … but CT is 2×1024 times longer than PT

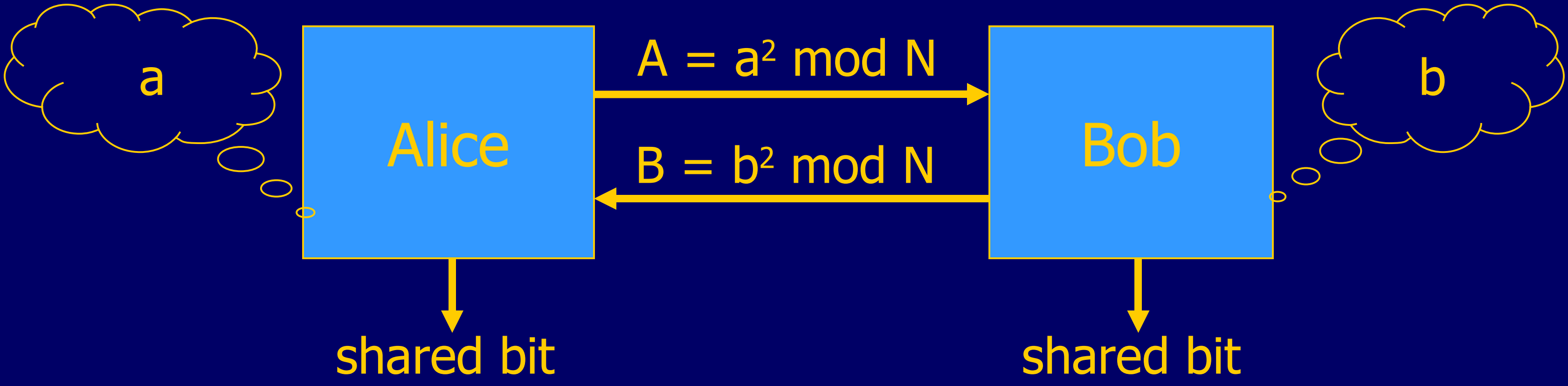
- **New system**:

$$\boxed{|CT| = |PT| + \log_2 N + 1}$$

Prelude to our scheme: 1-bit Key Agr.



Prelude to our scheme: 1-bit Key Agr.



$$\boxed{A \cdot x^2 + B \cdot y^2 = 1 \bmod N}$$

Shared bit = $\mathrm{Jac}(ax+1, N) = \mathrm{Jac}(2by+2, N)$

$A\cdot x^2 + B\cdot y^2 = 1 \bmod N$ (*)

- Ong-Schnorr-Shamir (1984) signature scheme:

  For PK=(N,A),

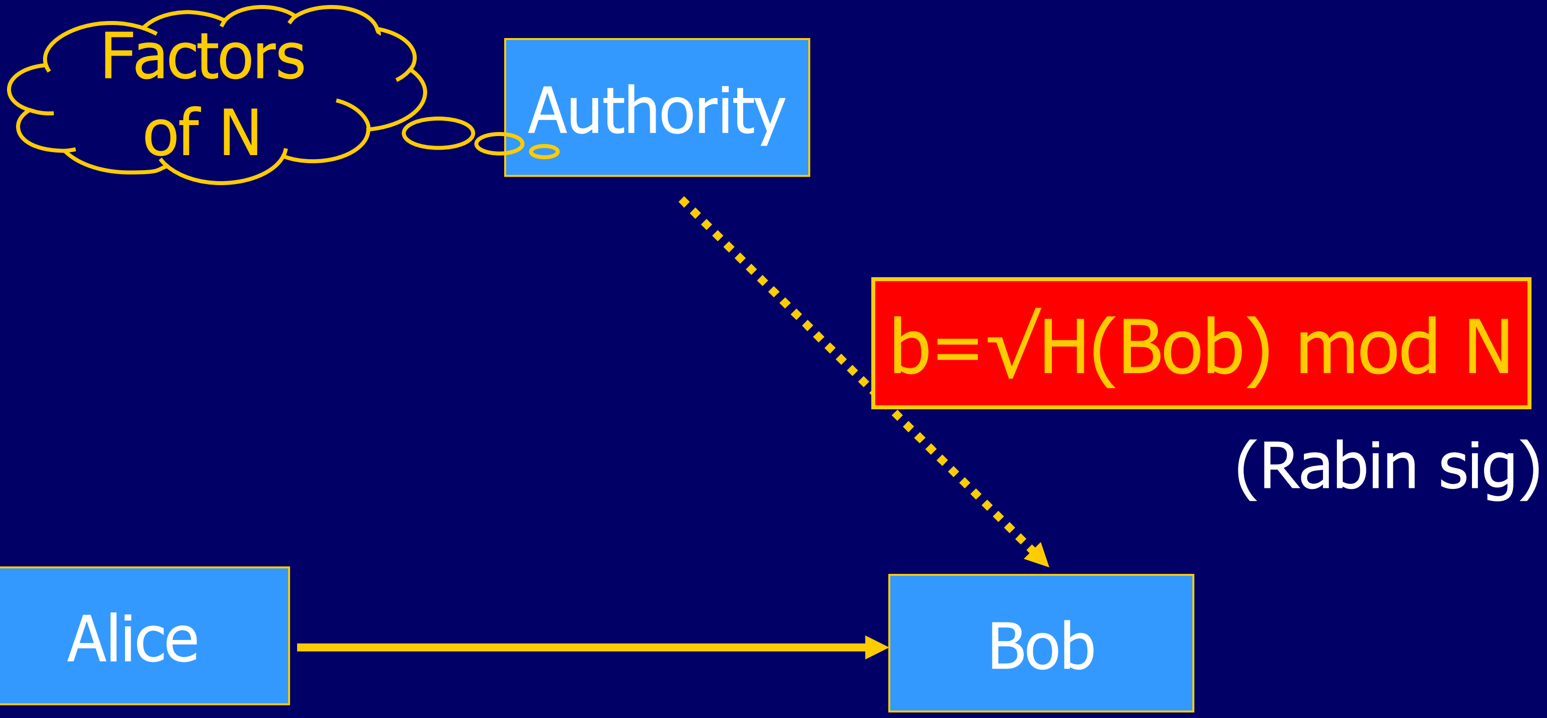
  sig(m) = (x,y) s.t.

  $A\cdot x^2+m\cdot y^2 = 1 \bmod N$

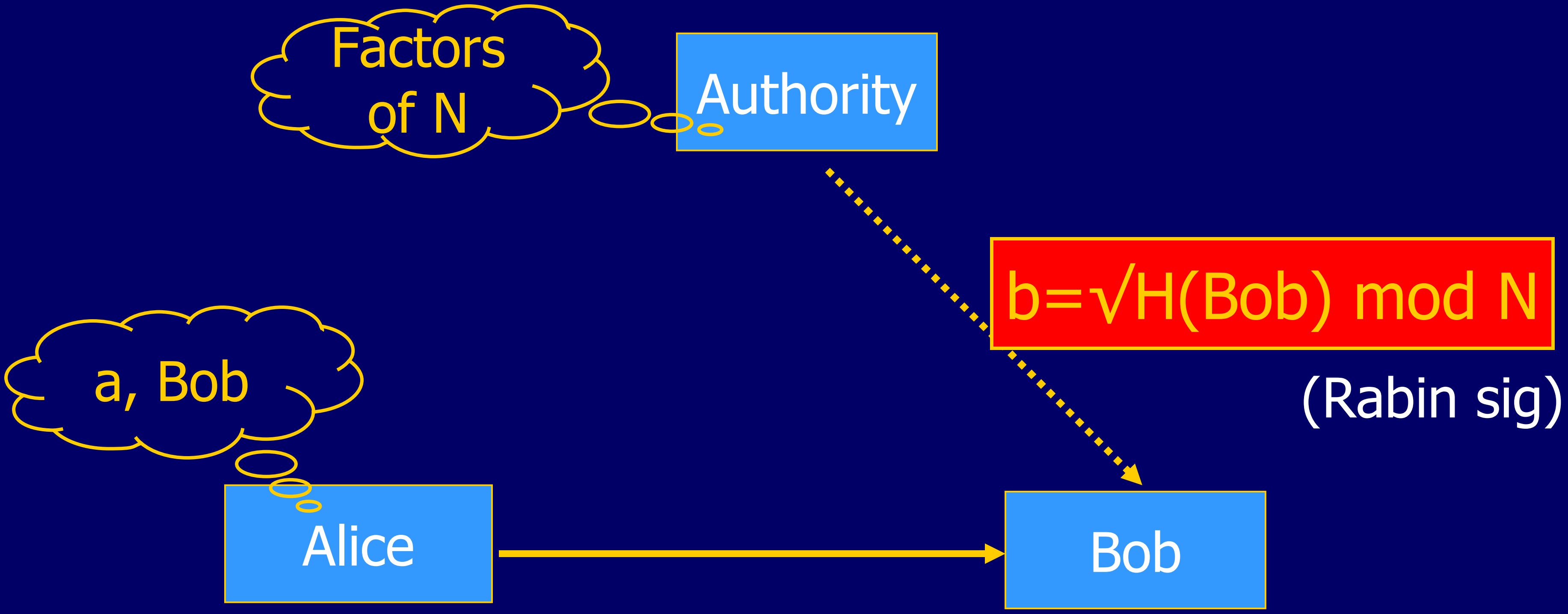
  - … but efficient algorithm to solve (*)
    Pollard-Schnorr algorithm

- So, our 1-bit key agreement scheme works

The 1-bit IBE system



The 1-bit IBE system



Factors of N

Authority

a, Bob

Alice

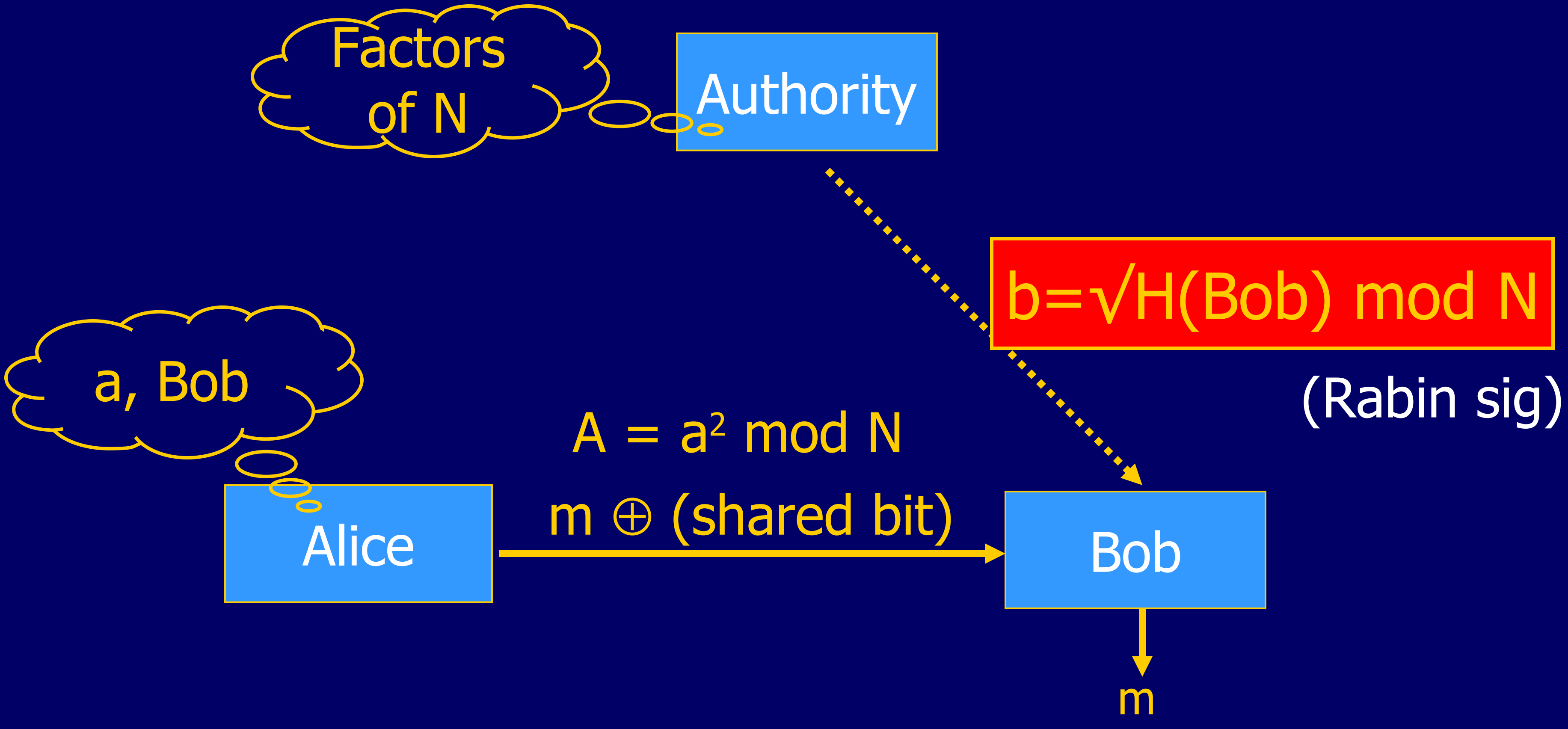
Bob

$b=\sqrt{H(\mathrm{Bob})} \bmod N$

(Rabin sig)

The 1-bit IBE system

(x,y) s.t. $\boxed{A \cdot x^2 + H(Bob) \cdot y^2 = 1 \bmod N}$



Factors of N

Authority

$b = \sqrt{H(Bob)} \bmod N$

(Rabin sig)

a, Bob

Alice

$A = a^2 \bmod N$

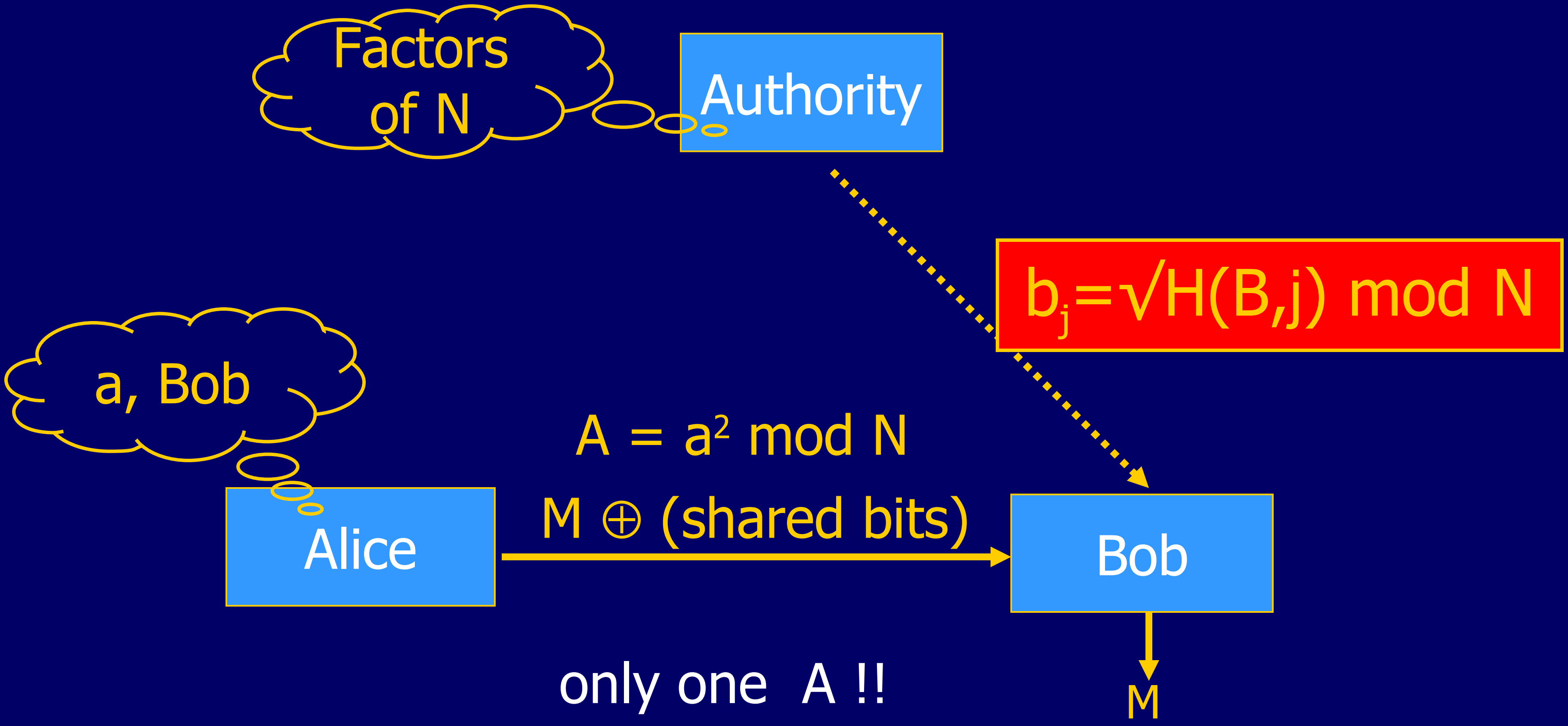
$m \oplus$ (shared bit)

Bob

m

Multi-bit IBE system

(x,y) s.t. $\boxed{A \cdot x^2 + H(B,j) \cdot y^2 = 1 \bmod N}$



Factors of N

Authority

$b_j = \sqrt{H(B,j)} \bmod N$

a, Bob

Alice

$A = a^2 \bmod N$

$M \oplus$ (shared bits)

Bob

M

only one A !!

Security, Extensions, Open Problems

- Security:
  - ANON-IND-ID-CCA based on QR (w/ R.O.)
  - R.O. needed for Rabin sigs security
- Extensions:
  - New hash proof system based on QR
    → New standard model PKE system based on QR
- Open Problems:
  - Solve $Ax^2 + By^2 = 1 \bmod N$ faster!
  - Remove random oracles