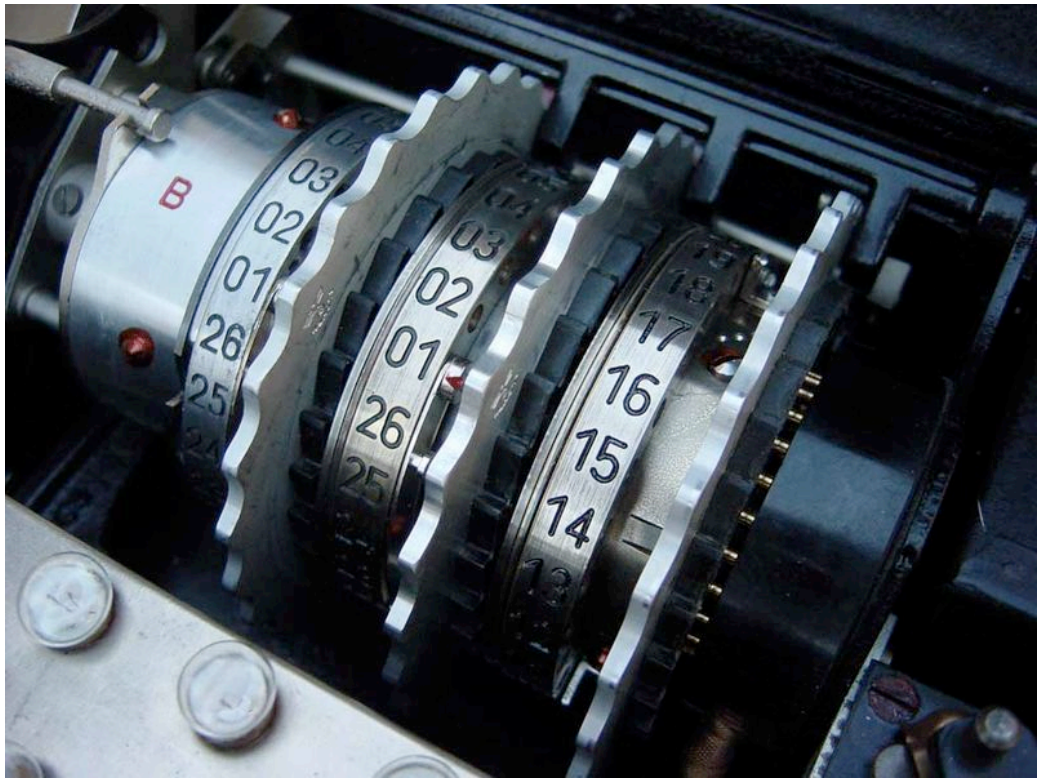


Cryptography II

Ben Adida
CIS, CSAIL, MIT

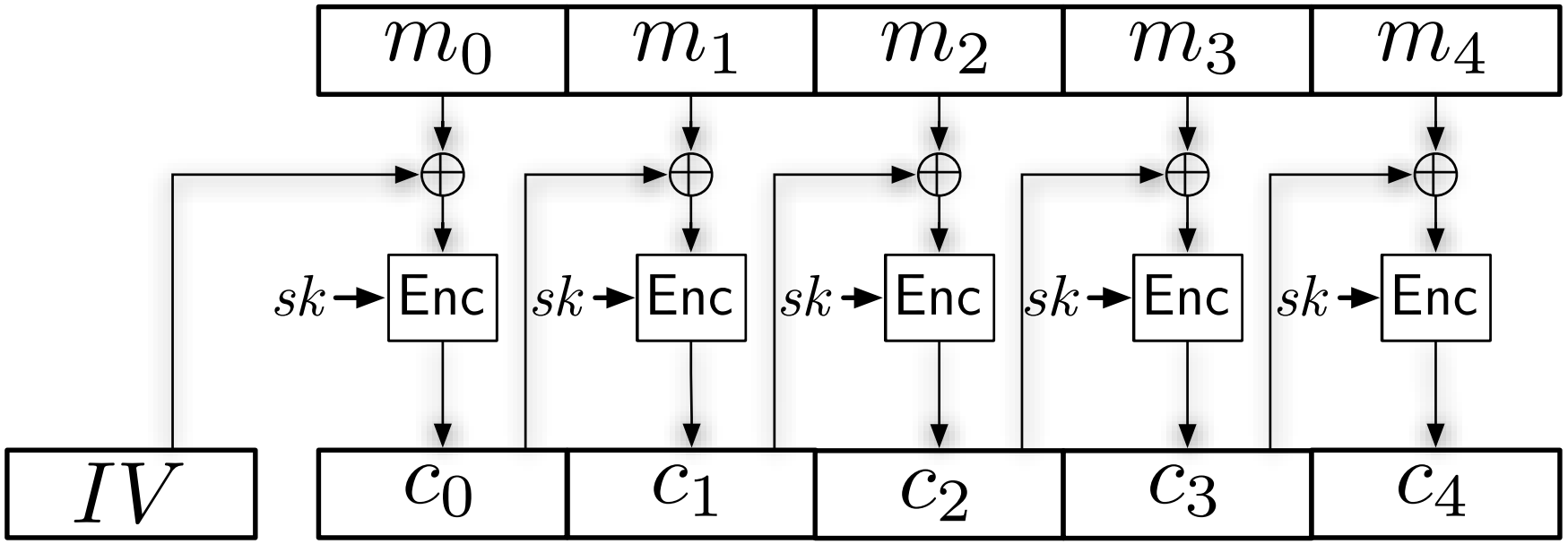
3 May 2006

SOME RIGHTS RESERVED

http://ben.adida.net/presentations/

Last Time....

Secret-Key Encryption

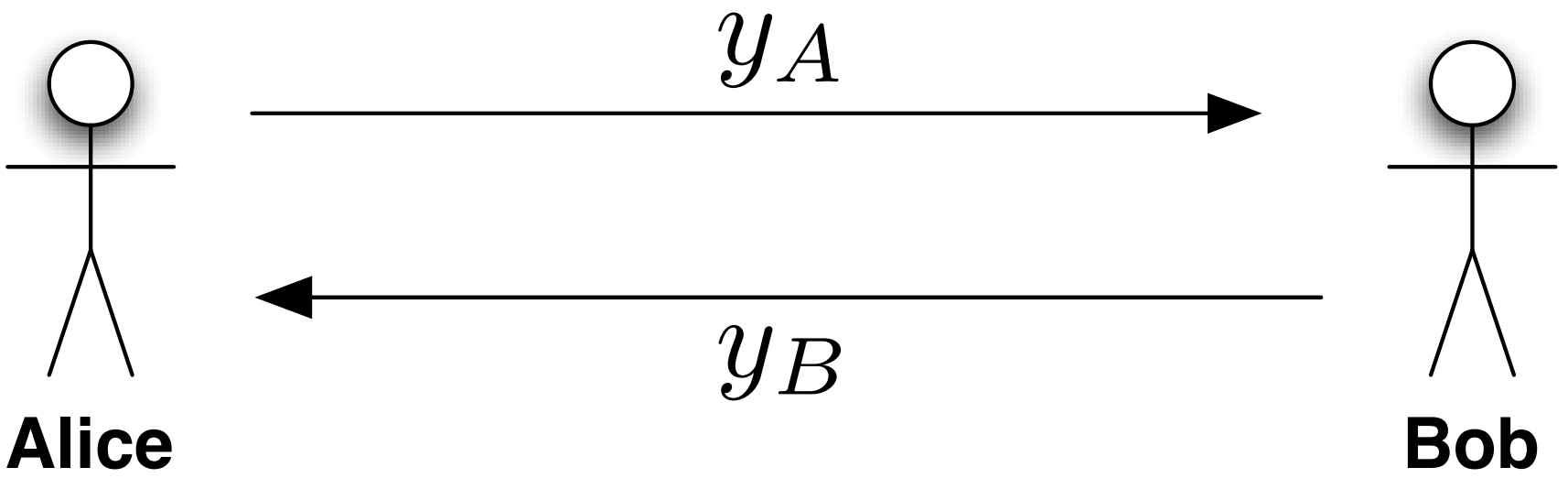


Number Theory

$$\text{computing } g^x \ mod \ p \text{ is easy}$$

$$\text{computing } \log_g y \ mod \ p \text{ is hard}$$

Diffie-Hellman Key Exchange



x_A

$y_A = g^{x_A}$

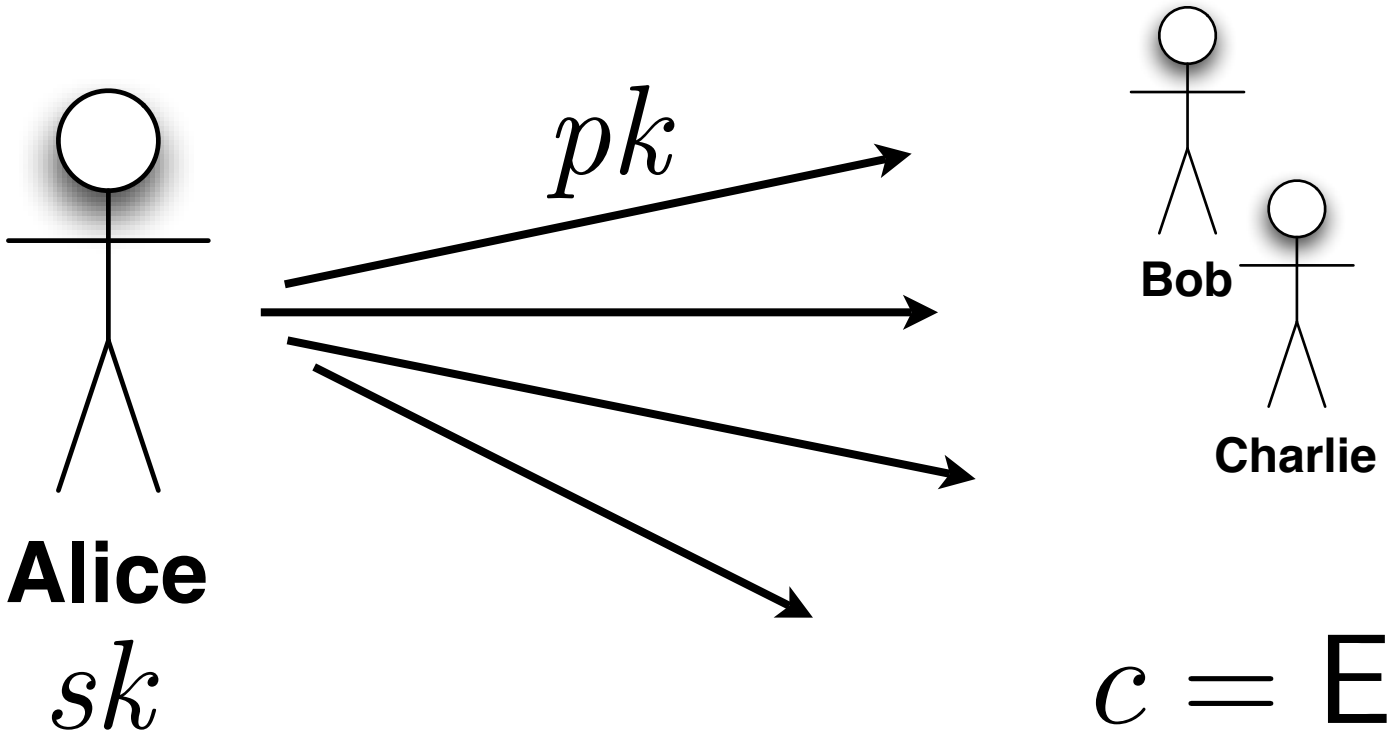
x_B

$y_B = g^{x_B}$

$y_B^{x_A} = g^{x_A x_B}$

$y_A^{x_B} = g^{x_A x_B}$

Public-Key Encryption



$$c = \mathsf{Enc}_{pk}(m)$$

$$m = \mathsf{Dec}_{sk}(c)$$

Hybrid Encryption

generate a session key $session_key$

$$c = \mathsf{Enc}_{session_key}(m), \mathsf{Enc}_{pk}(session_key)$$

Signatures

$$\mathsf{Sign}_{sk}(m) = \sigma$$

$$\mathsf{Verify}_{pk}(m, \sigma) = \mathsf{True/False}$$

Reverse the
Public-Key Encryption operation!

$$\mathsf{Sign}_{sk}(m) = \mathsf{Dec}_{sk}(m)$$

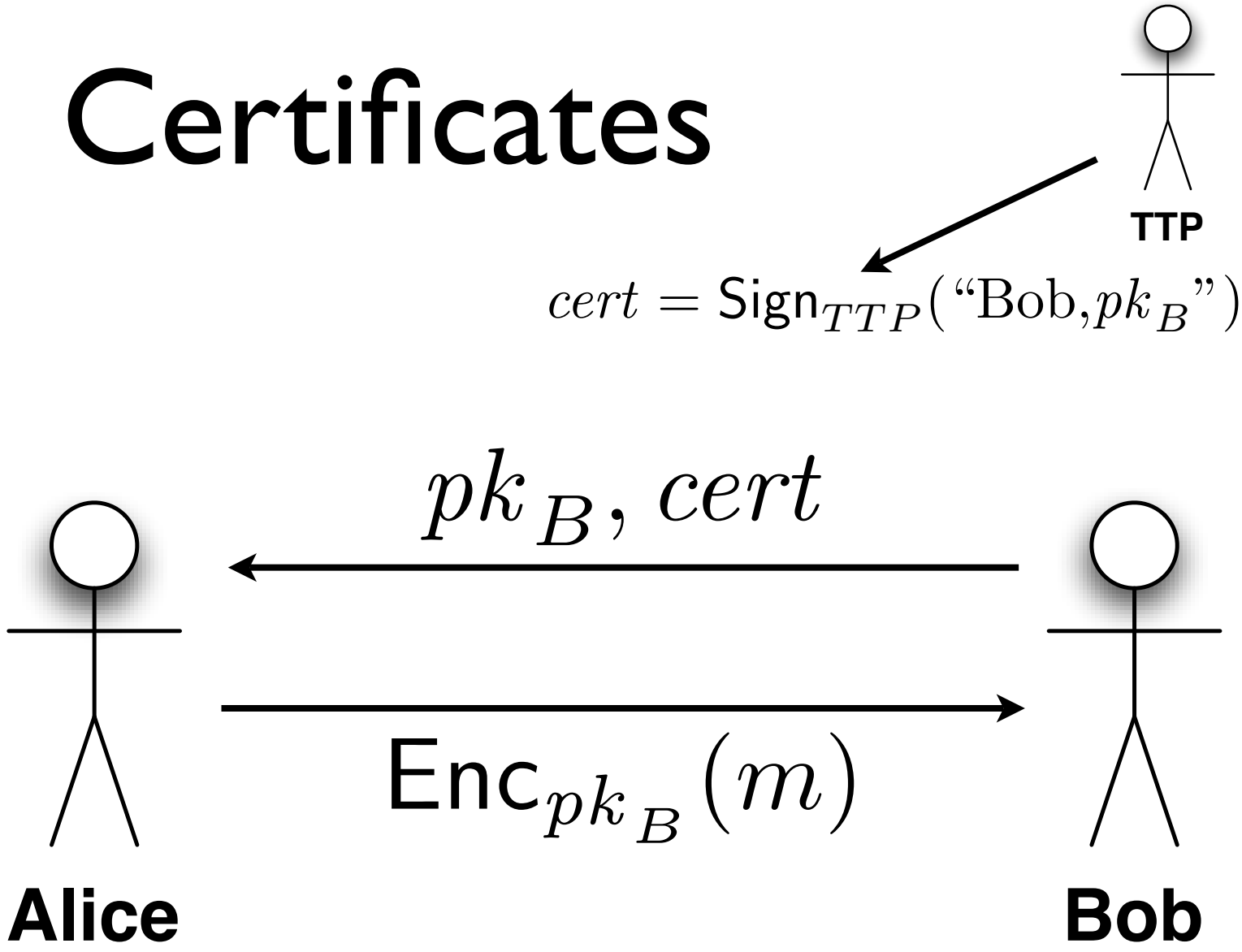
$$\mathsf{Verify}_{pk}(m, \sigma) \rightarrow \mathsf{Enc}_{pk}(\sigma) \stackrel{?}{=} m$$

Hash Functions

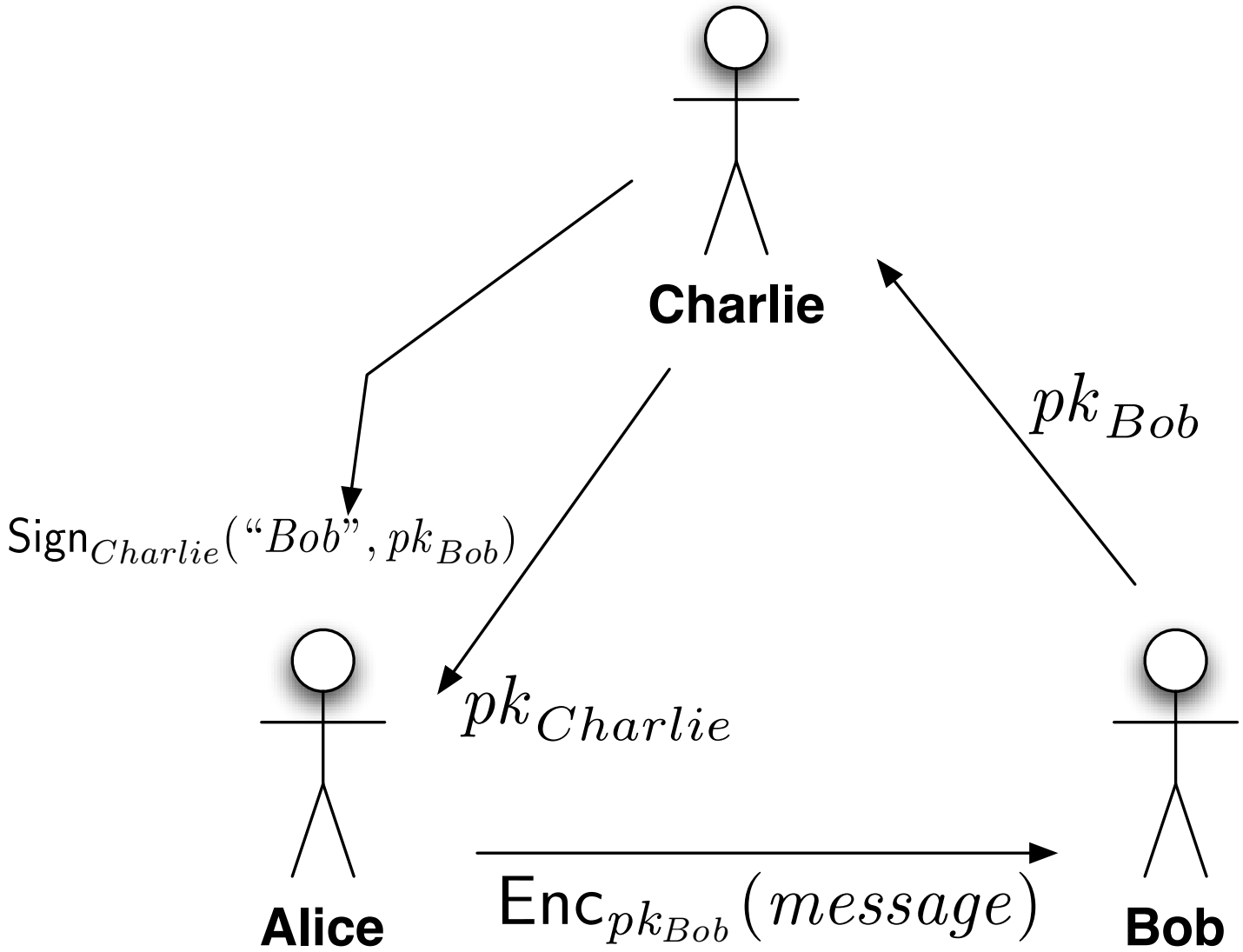
$$H(m) = hash, \text{Sign}_{sk}(H(m))$$

- "fingerprint" of a long document
- MD5 hashes to 128 bits, SHA1 hashes to 160 bits
- Properties
  - ⋆ Collision Attack
  - ⋆ Pre-Image Attack
  - ⋆ Second Pre-Image Attack

Certificates

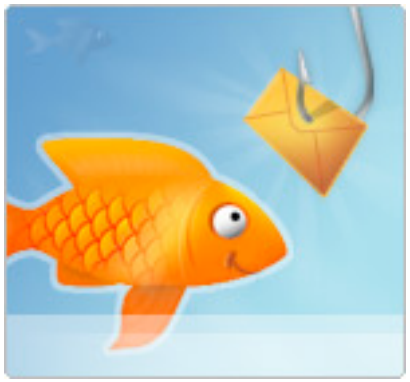


PGP

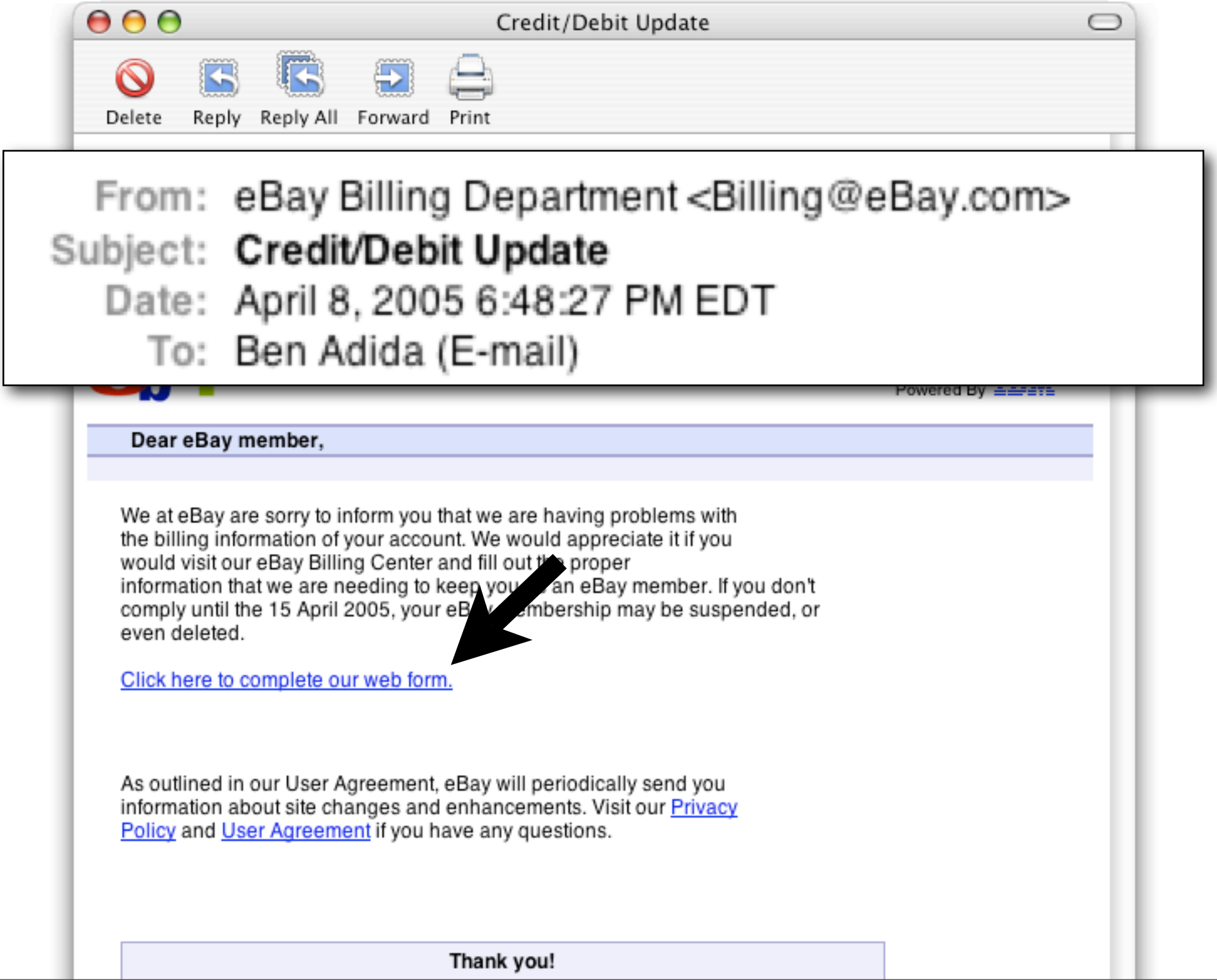

Charlie
pk_{Bob}
$\text{Sign}_{Charlie}(\text{“}Bob\text{”}, pk_{Bob})$
$pk_{Charlie}$
Alice
$\text{Enc}_{pk_{Bob}}(message)$
Bob

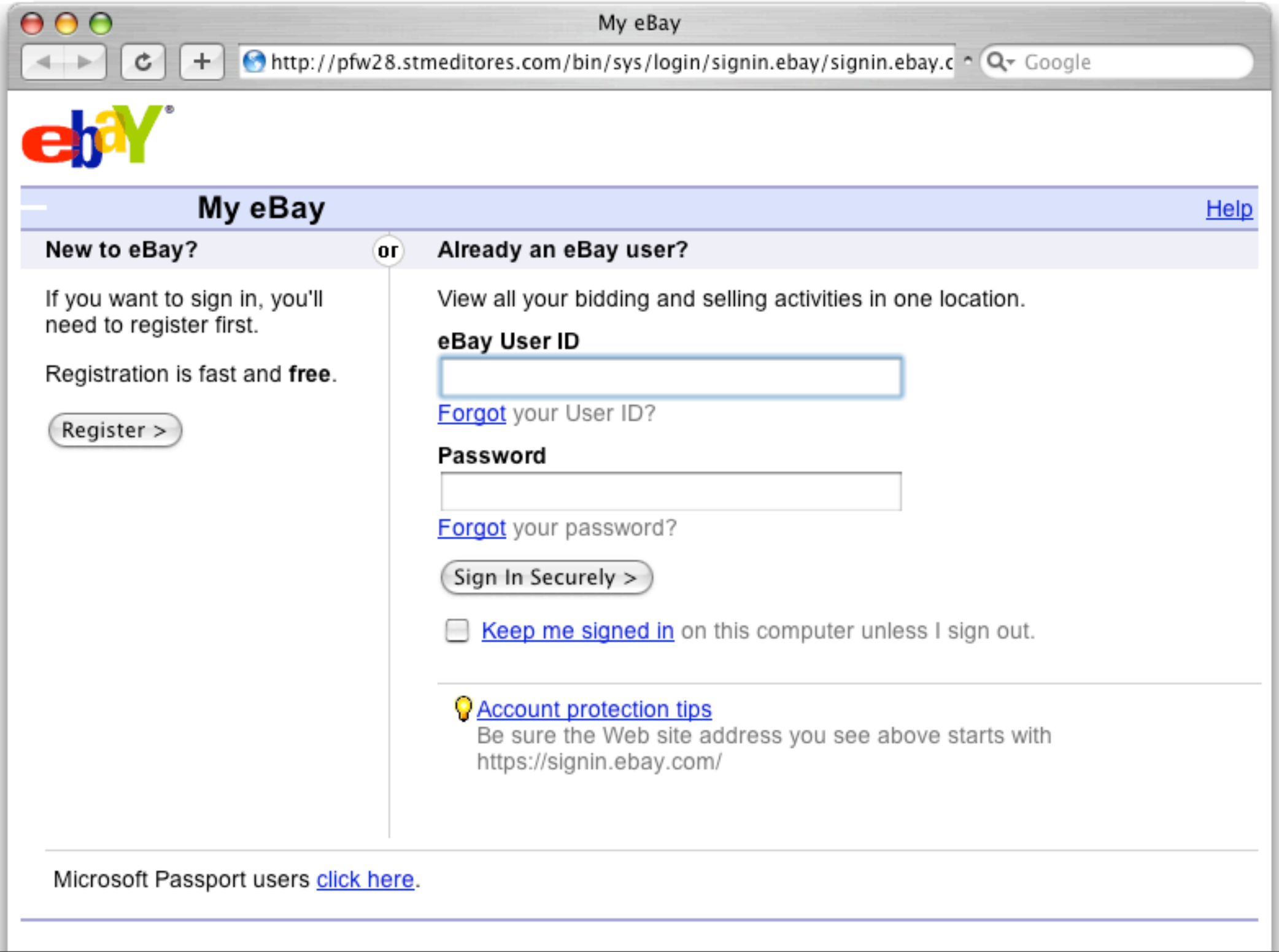
Advanced Applications

Anti-Phishing



© Scott Adams, Inc./Dist. by UFS, Inc.


Credit/Debit Update
Delete
Reply
Reply All
Forward
Print
From: eBay Billing Department <Billing@eBay.com>
Subject: Credit/Debit Update
Date: April 8, 2005 6:48:27 PM EDT
To: Ben Adida (E-mail)
Powered By
Dear eBay member,
We at eBay are sorry to inform you that we are having problems with the billing information of your account. We would appreciate it if you would visit our eBay Billing Center and fill out the proper information that we are needing to keep you an eBay member. If you don't comply until the 15 April 2005, your eBay membership may be suspended, or even deleted.
Click here to complete our web form.
As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.
Thank you!


My eBay
http://pfw28.stmeditores.com/bin/sys/login/signin.ebay/signin.ebay.c
Google
My eBay
Help
New to eBay?
or
Already an eBay user?
If you want to sign in, you'll need to register first.
Registration is fast and free.
Register >
View all your bidding and selling activities in one location.
eBay User ID
Forgot your User ID?
Password
Forgot your password?
Sign In Securely >
Keep me signed in on this computer unless I sign out.
Account protection tips
Be sure the Web site address you see above starts with https://signin.ebay.com/
Microsoft Passport users click here.

BBC NEWS WORLD EDITION

Last Updated: Tuesday, 3 May, 2005, 10:44 GMT 11:44 UK

E-mail this to a friend Printable version

One in 20 'fall for online fraud'

One in 20 UK internet users say they have lost money through online scams, research into spam emails suggests.

Almost half say they have received so-called phishing emails aimed at tricking them into revealing details like online banking passwords.

Online frauds are becoming more sophisticated

From: Susan Hockfield <med-survey@MIT.EDU>
Subject: **Survey on Medical Care**
Date: April 15, 2005 12:38:00 PM EDT
To: Benjamin Adida <ben@MIT.EDU>

this review is gathering information from community members on their usage of and satisfaction with medical care at MIT, and the Task Force has constructed a survey for students to provide their feedback.

Your time is valuable, especially at this busy time of year, but I hope that you might be willing to take about fifteen minutes to complete a web-based questionnaire. Your participation is entirely voluntary, and you may answer as few or as many questions as you wish. Your response will be treated as confidential, and data gathered will be reported in summary format. I urge you to be as candid as possible in your answers, as this is a very important issue for you and for the students who will follow you at MIT.

You may enter the survey from <http://web.mit.edu/surveys/medical/>. This survey authentication requires a current MIT certificate.

If you have any questions, please send them to med-survey@mit.edu.

Sincerely,
Susan Hockfield

Beware: E-Mailed Surveys May Involve 'Phishing'

Scammers Seek Bank Account Numbers

By Audrey Laganas

From: Burgess-Gregg, Mary
Sent: Thursday, December 02,
Subject: Presidential Recogniti

r Presidential recognition.

I am pleased to inform you tl
more specific at this point be
candidates.

I am contacting you now because we need to request a name check from the FBI, as we do with all persons being considered for Presidential recognition. In light of procedures put in place by the White House Counsel's Office, we must receive your written consent prior to requesting the name check. The

request a name check from the FBI,

http://ostp.gov/FBInamecheck.pdf

it no
o
se do

NOT send a hard copy by mail. If you have questions about this process, please contact Mary Burgess-Gregg at (202) 456-6130 or MBurgess-Gregg@ostp.eop.gov

form should be **faxed immediately**,

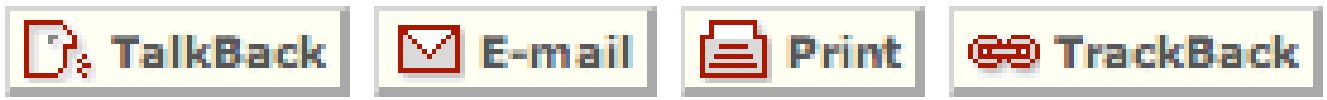
NEOB
(202) 456-6130
(202) 456-6027 (fax)
MBurgess-Gregg@ostp.eop.gov

Fax Attack

New scam asks people to fax away data

Published: August 11, 2005, 7:48 AM PDT

By Dawn Kawamoto
Staff Writer, CNET News.com



Phishers have added a new lure to their tackle boxes: e-mails that ask people to fax sensitive information to bogus security investigators.

Phone Attack

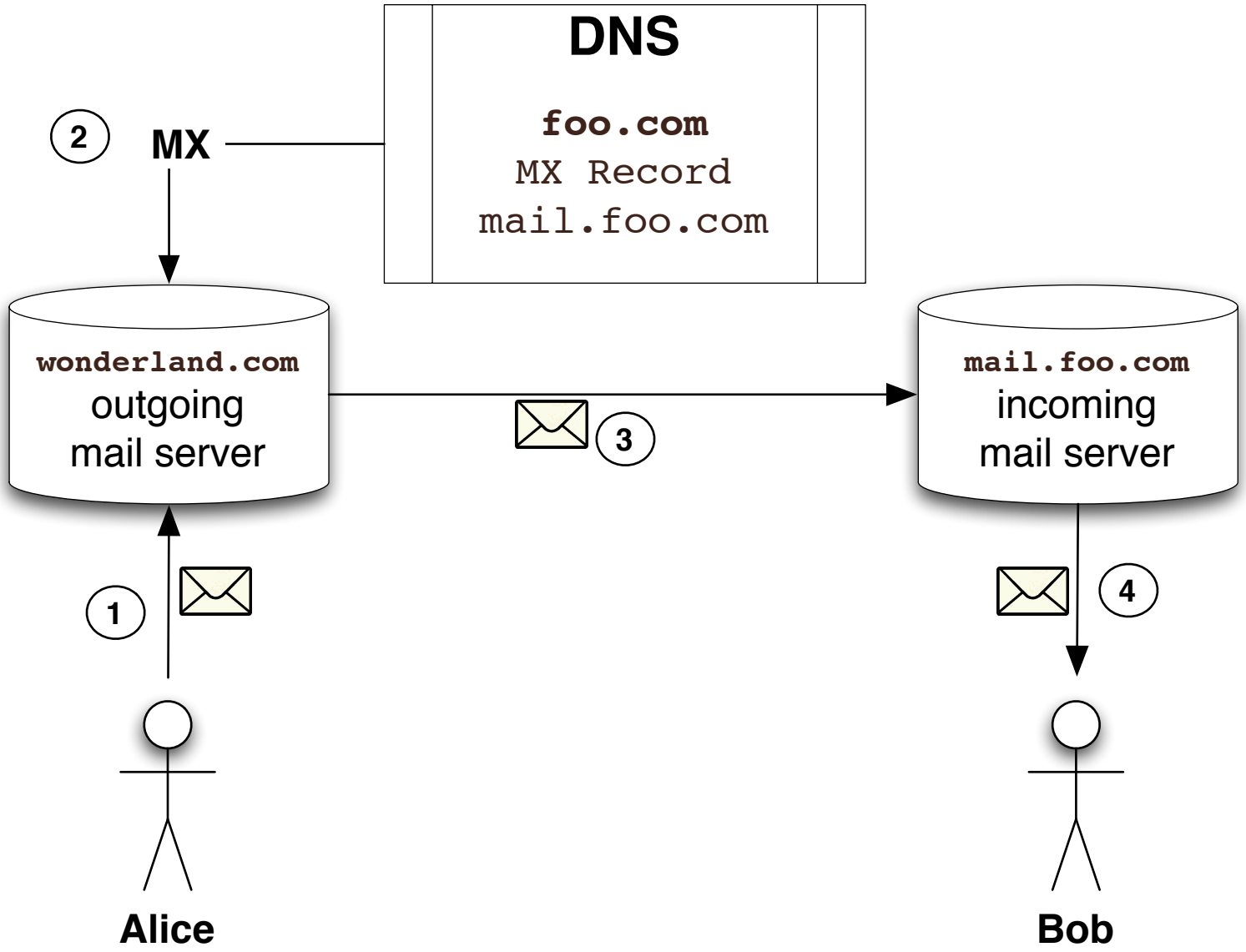
Phishers try a phone hook

By Joris Evers
Staff Writer, CNET News.com
Published: April 27, 2006, 5:51 PM PDT

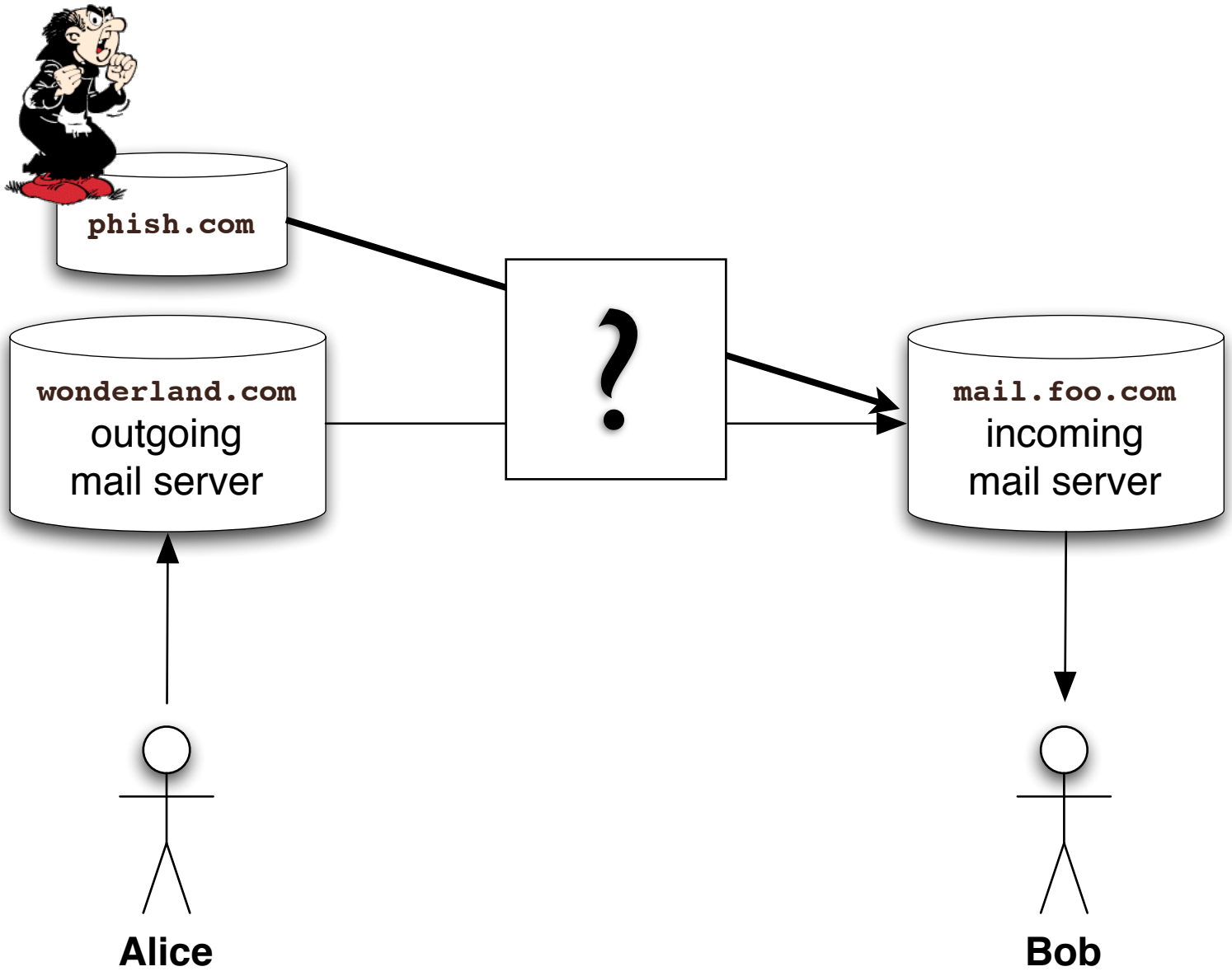
TalkBack E-mail Print

In a new twist on phishing, fraudsters are sending out e-mails that attempt to trick people into sharing personal information over the phone.

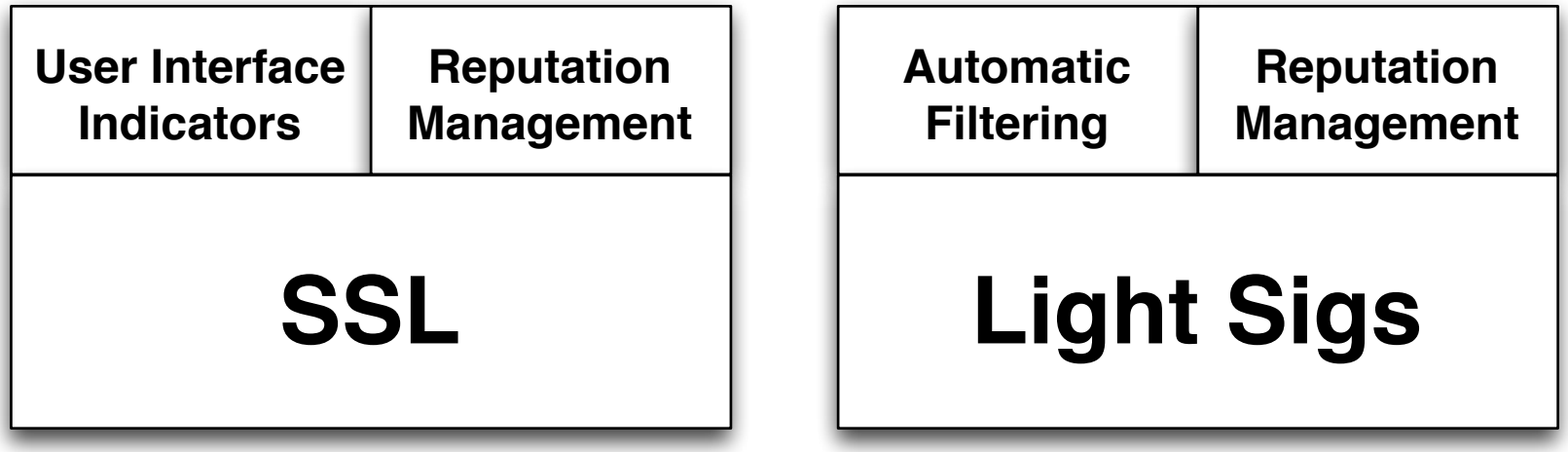
SMTP Today


DNS
foo.com
MX Record
mail.foo.com
2
MX
wonderland.com
outgoing
mail server
3
mail.foo.com
incoming
mail server
1
4
Alice
Bob

No Proof of Origin

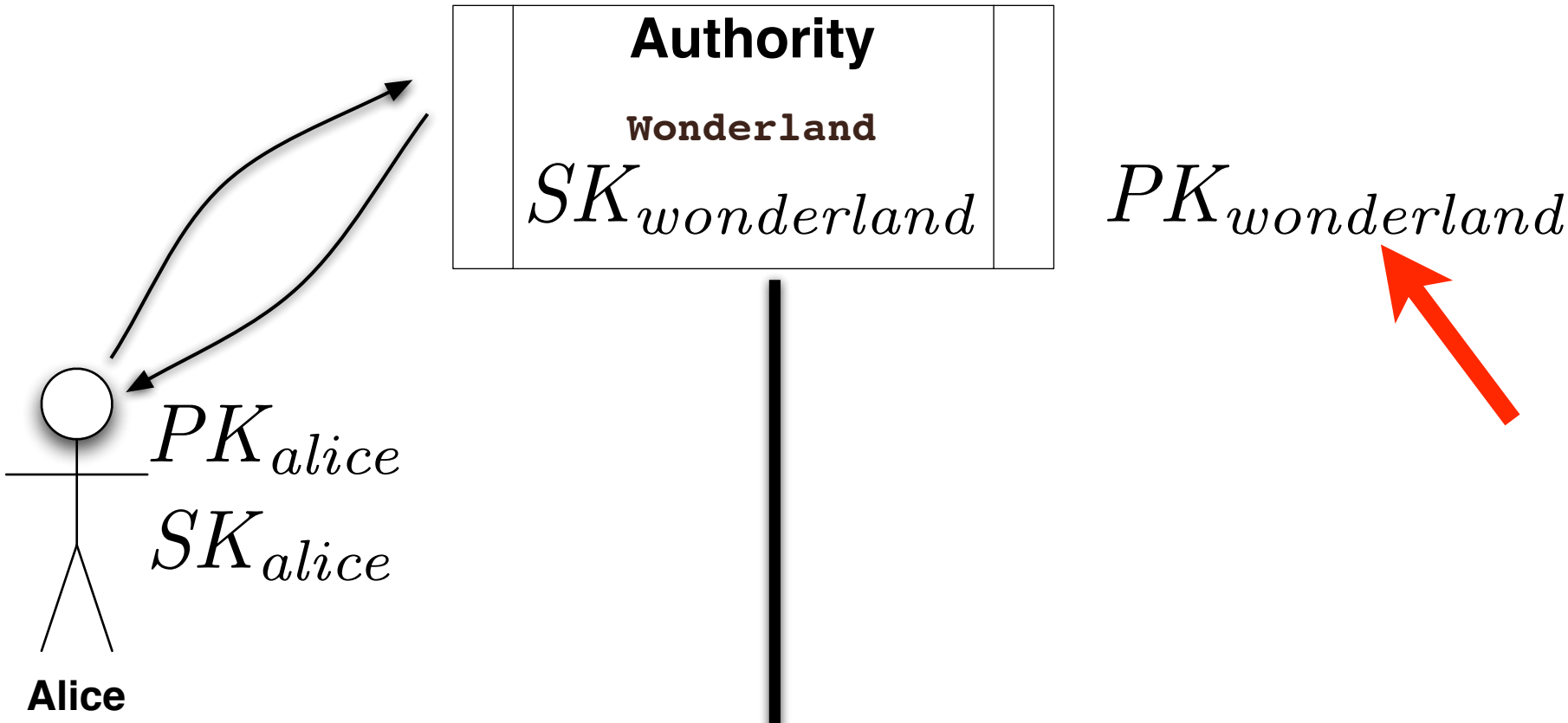


A Platform of Trust



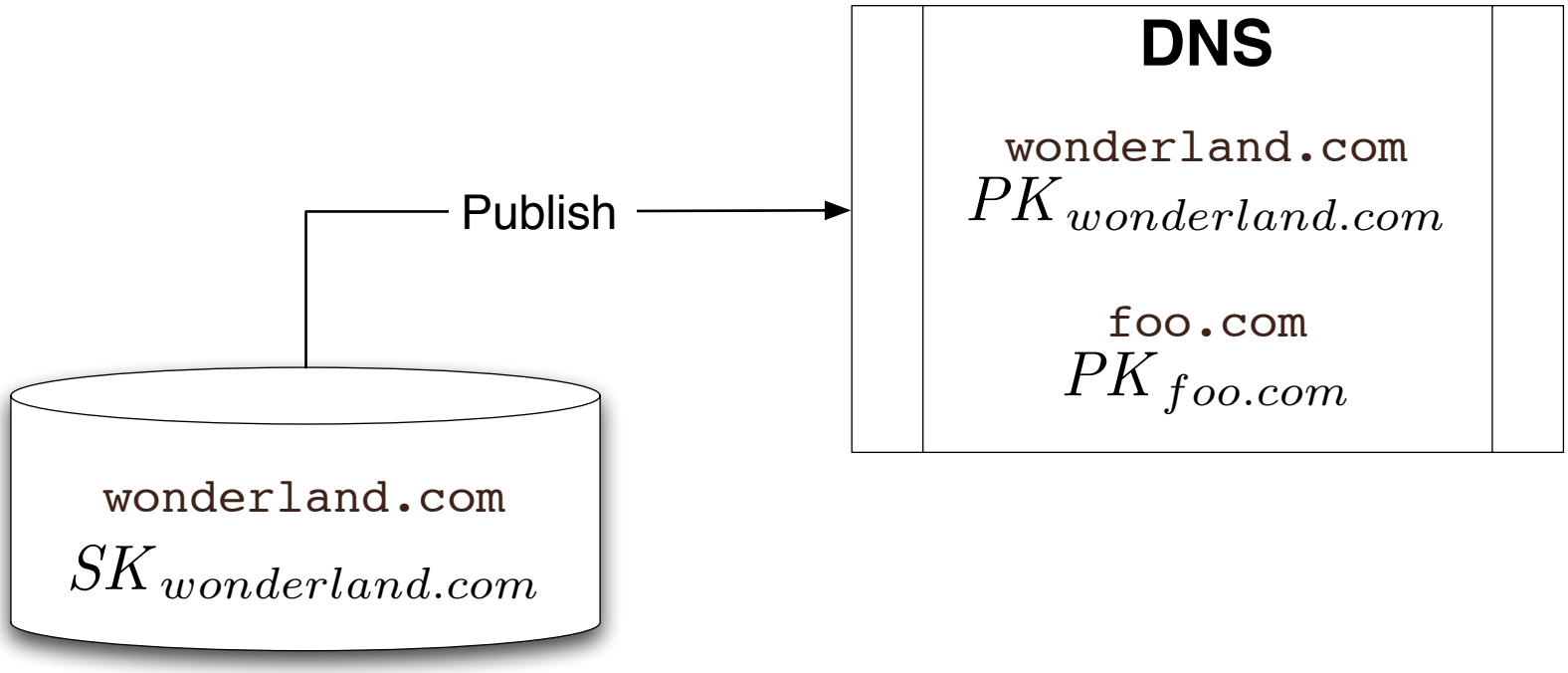
We want to provide Just Enough Trust

Basic Signatures



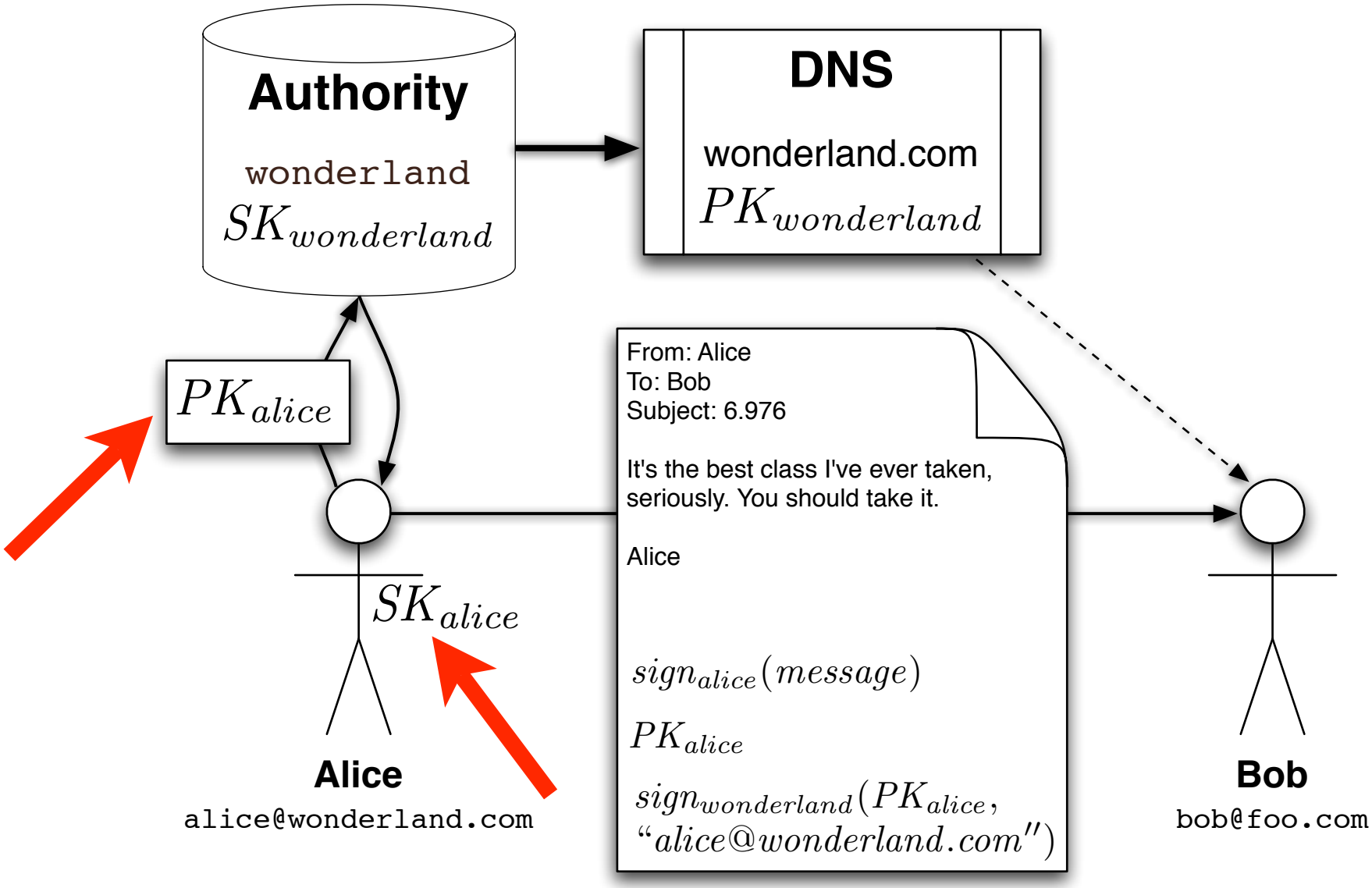
$$sign_{wonderland}(PK_{alice}, \text{“}alice@wonderland.com\text{”})$$

DNS to distribute Domain-Level Keys

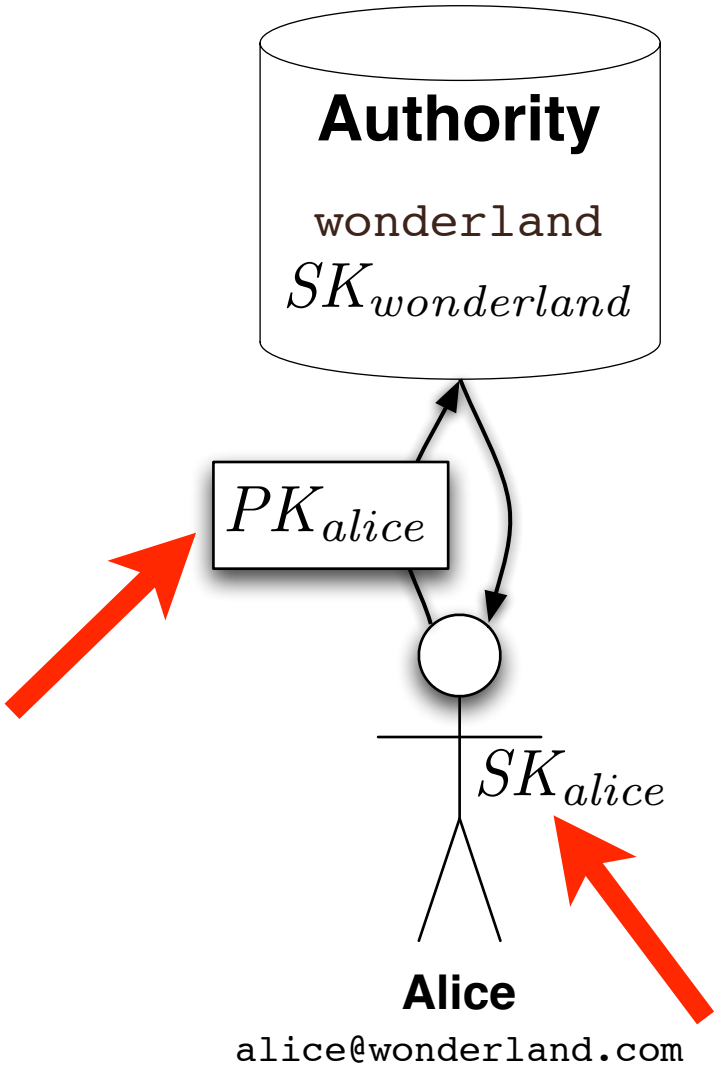


[DomainKeys]

Email Authentication



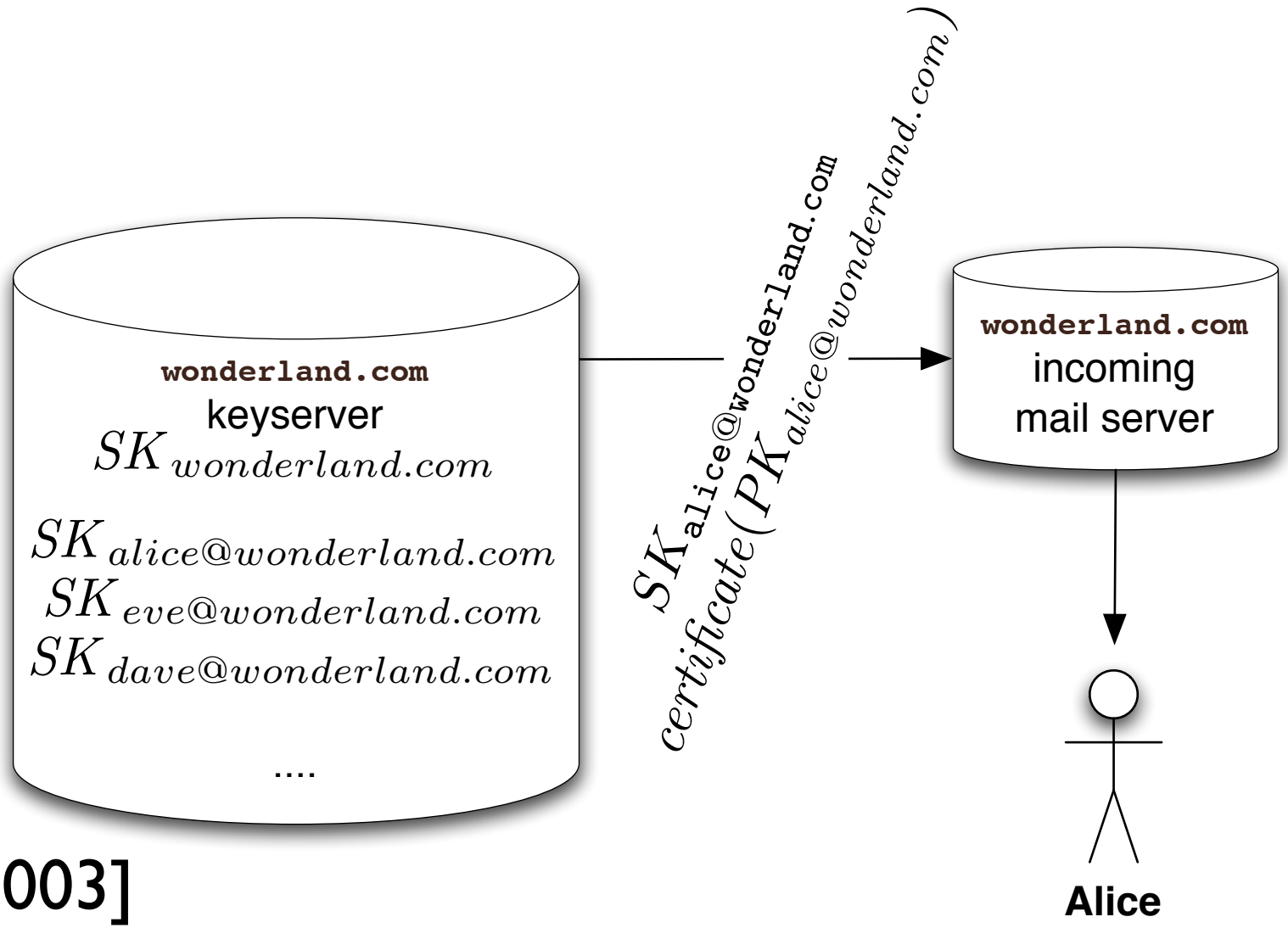
Email Authentication



- certifying a user's public key can add significant overhead.
- distributing the secret key to all user access points is tricky.

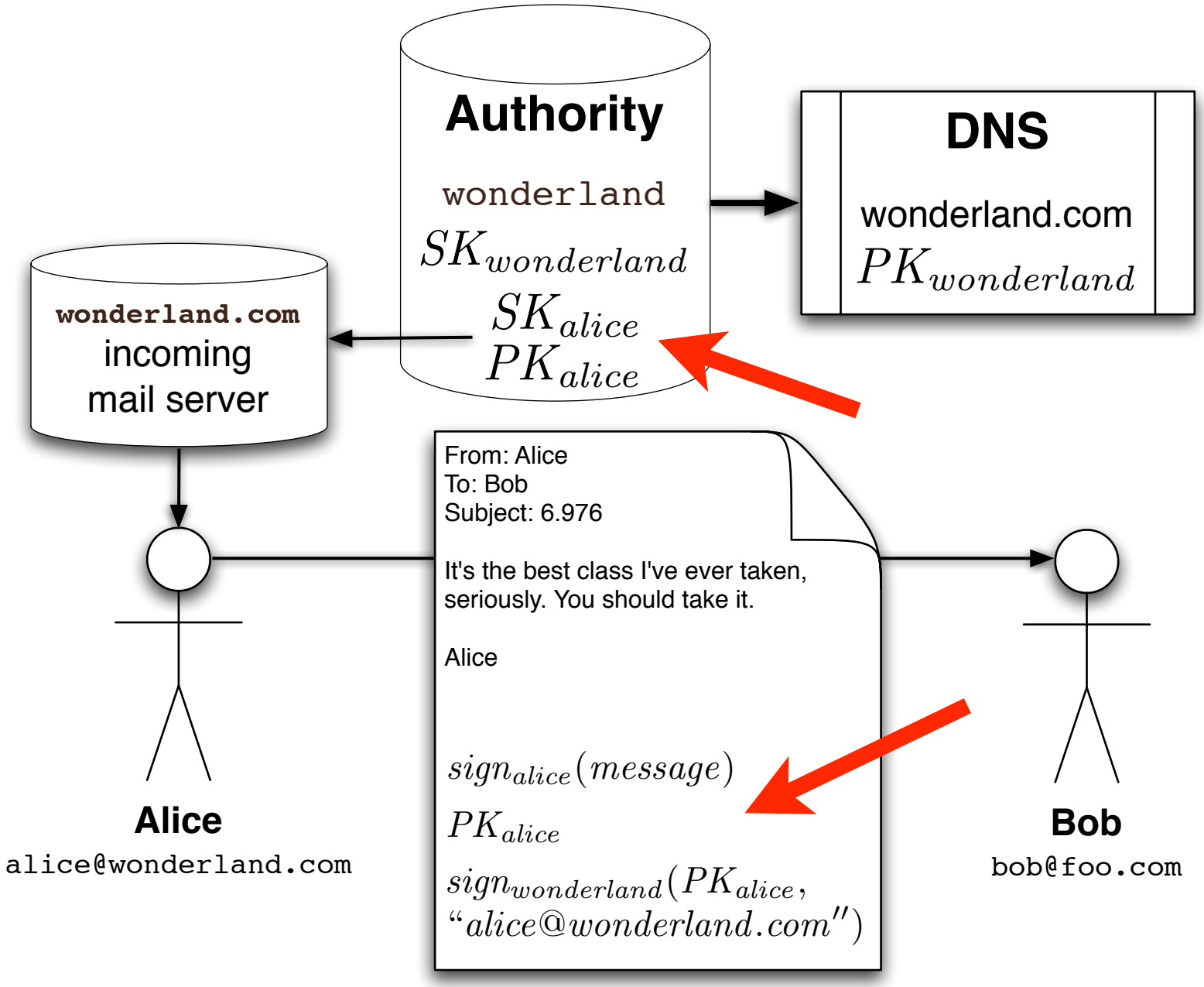
... unless we rethink the security requirements a bit.

Email-Based Authentication

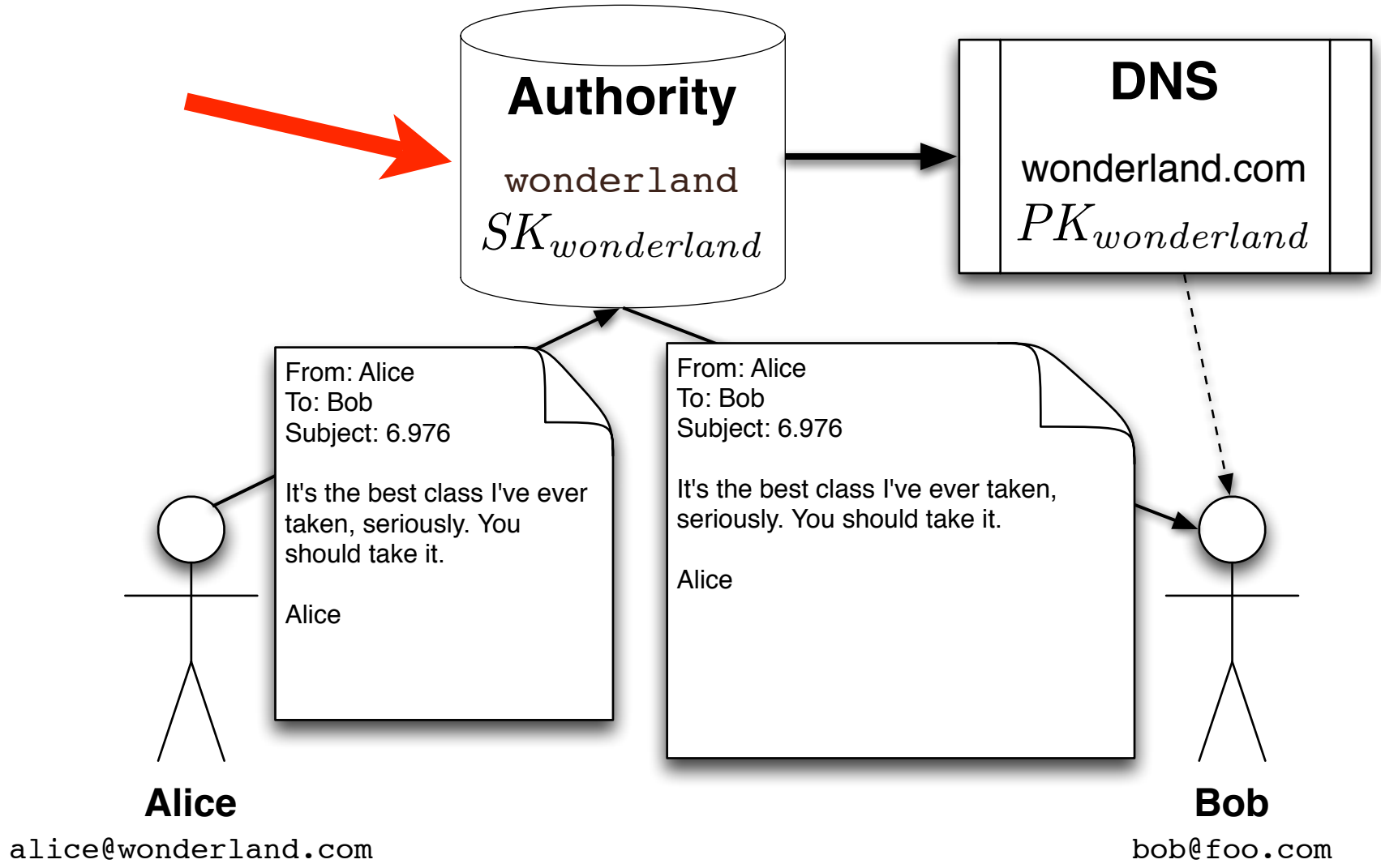


[Gar2003]

Server-Managed User Keys

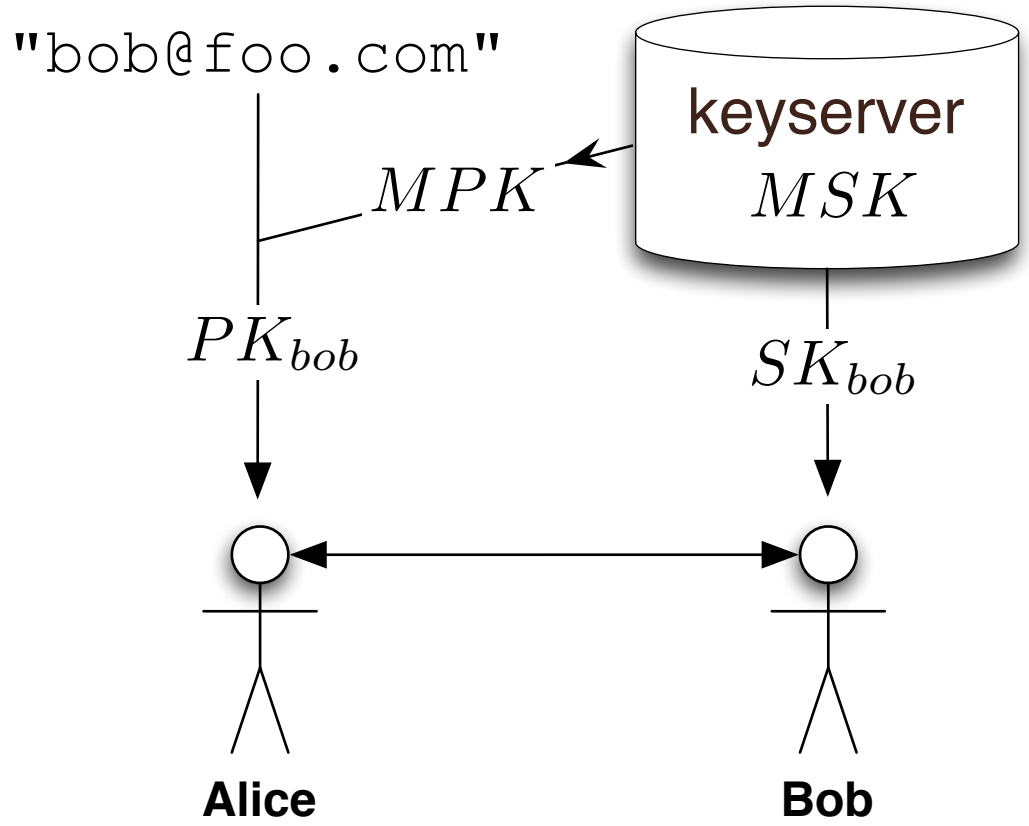


DomainKeys

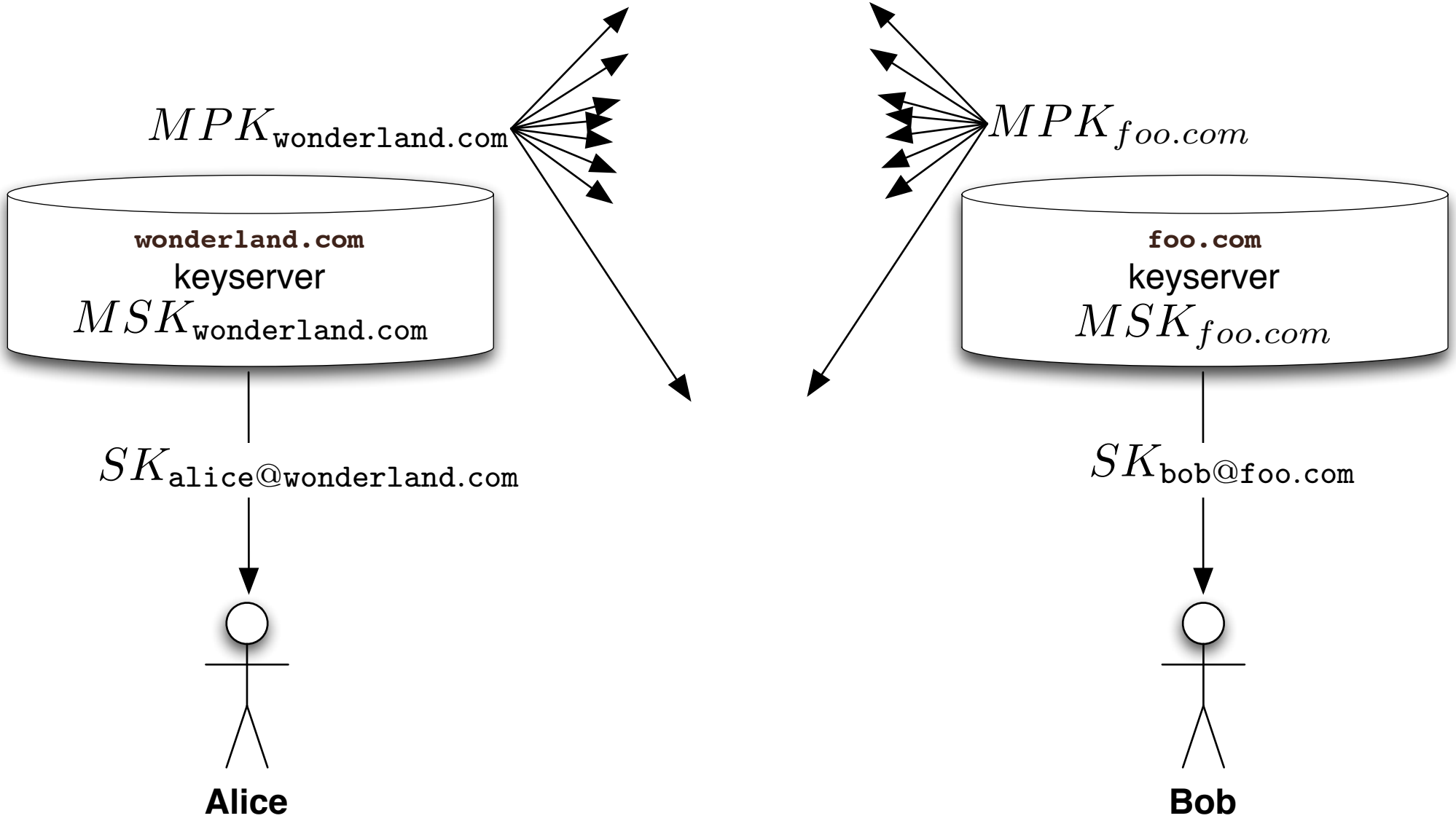

Authority
wonderland
$SK_{wonderland}$
DNS
wonderland.com
$PK_{wonderland}$
From: Alice
To: Bob
Subject: 6.976
It's the best class I've ever taken, seriously. You should take it.
Alice
From: Alice
To: Bob
Subject: 6.976
It's the best class I've ever taken, seriously. You should take it.
Alice
Alice
alice@wonderland.com
Bob
bob@foo.com

Can we get the benefits of both user keys and domain keys?

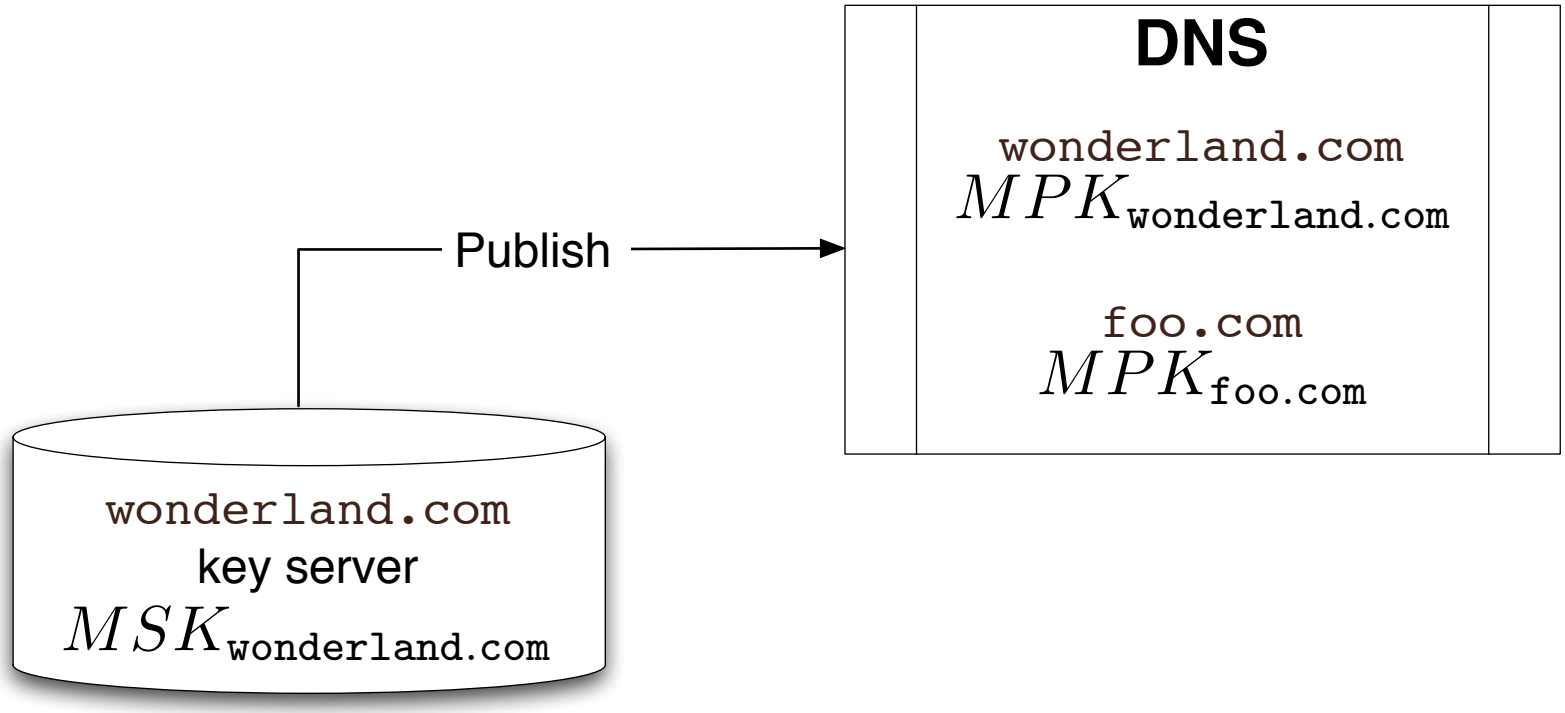
ID-Based Crypto



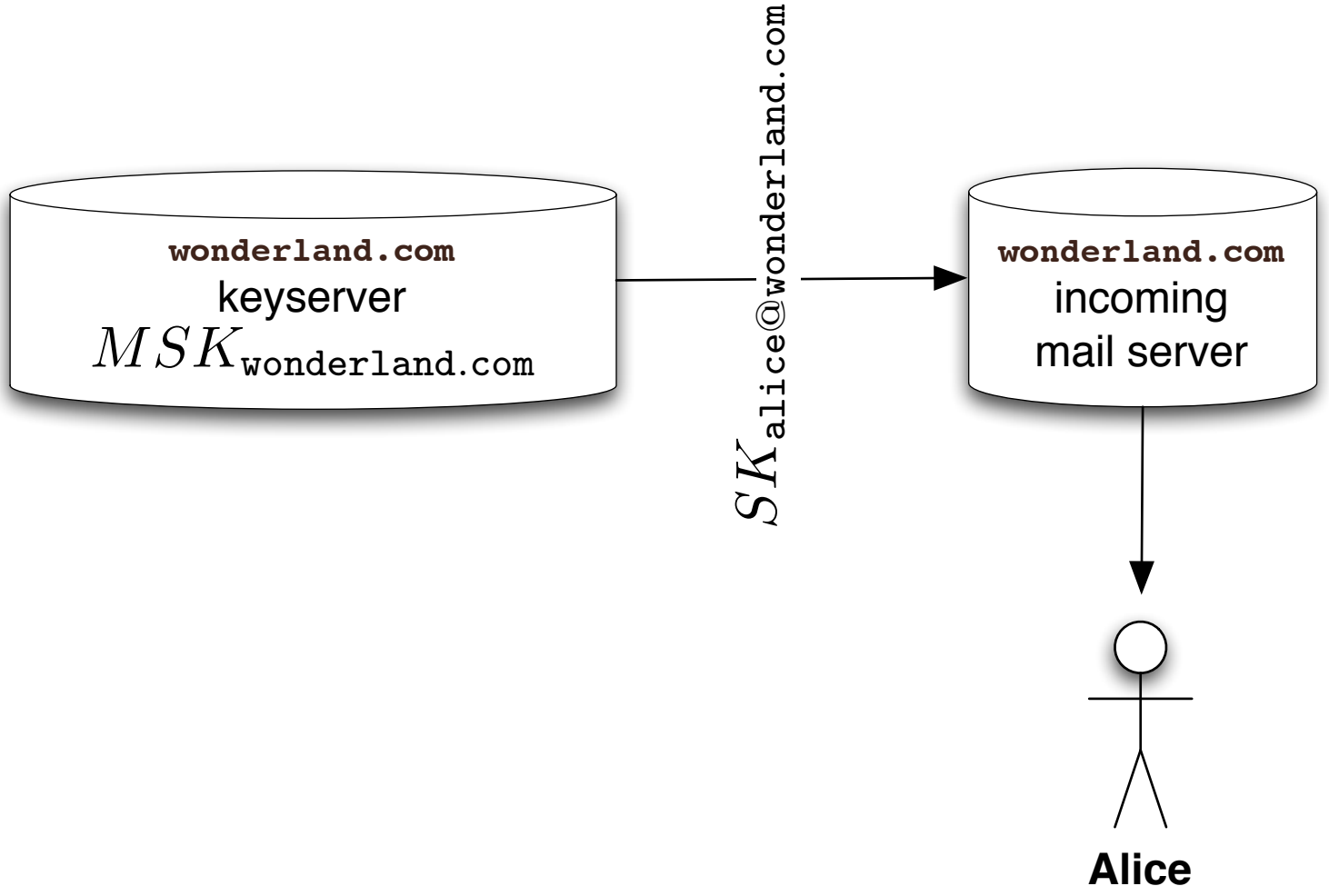
ID-based Domains



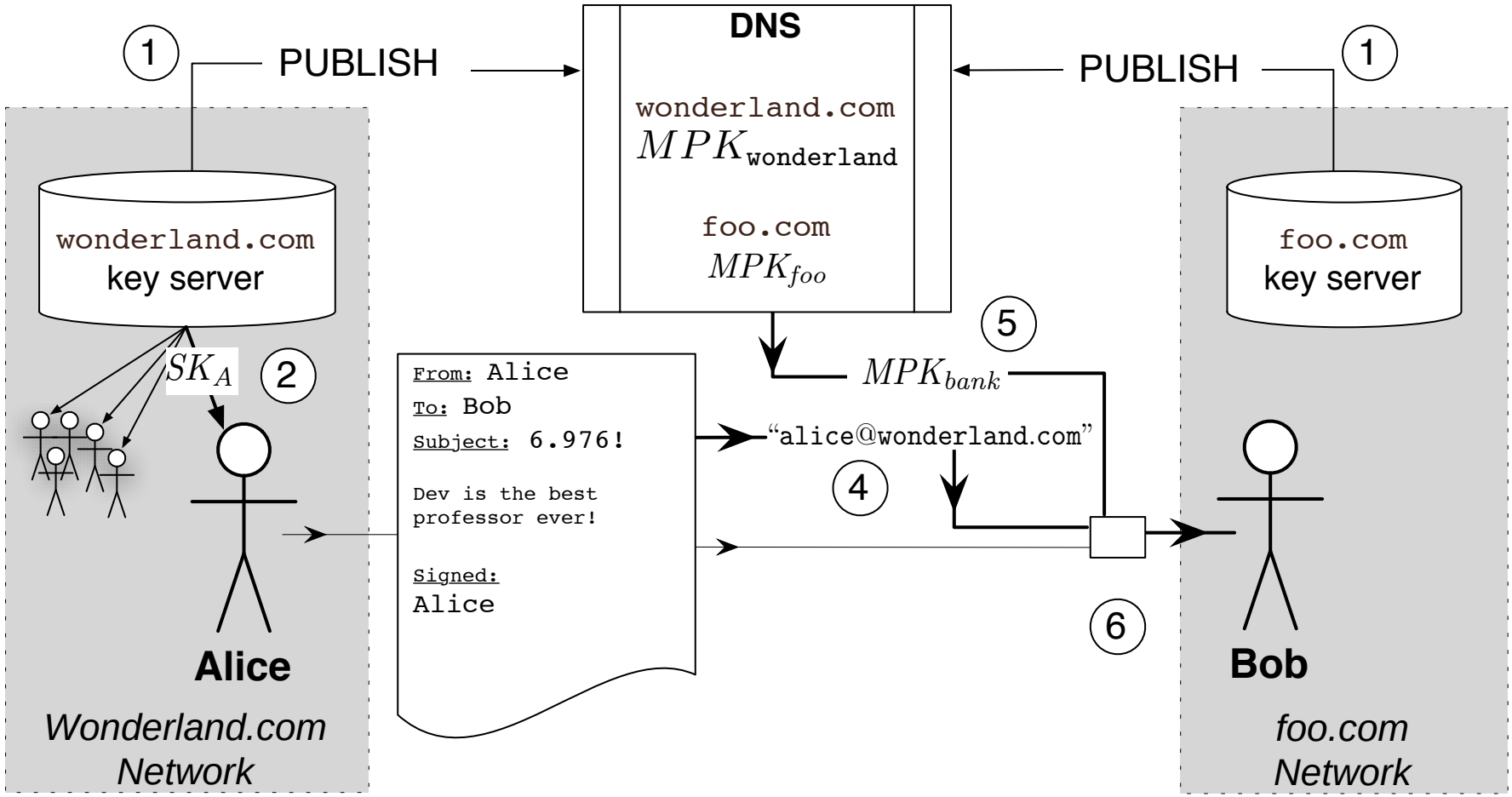
DNS to distribute Master Public Keys



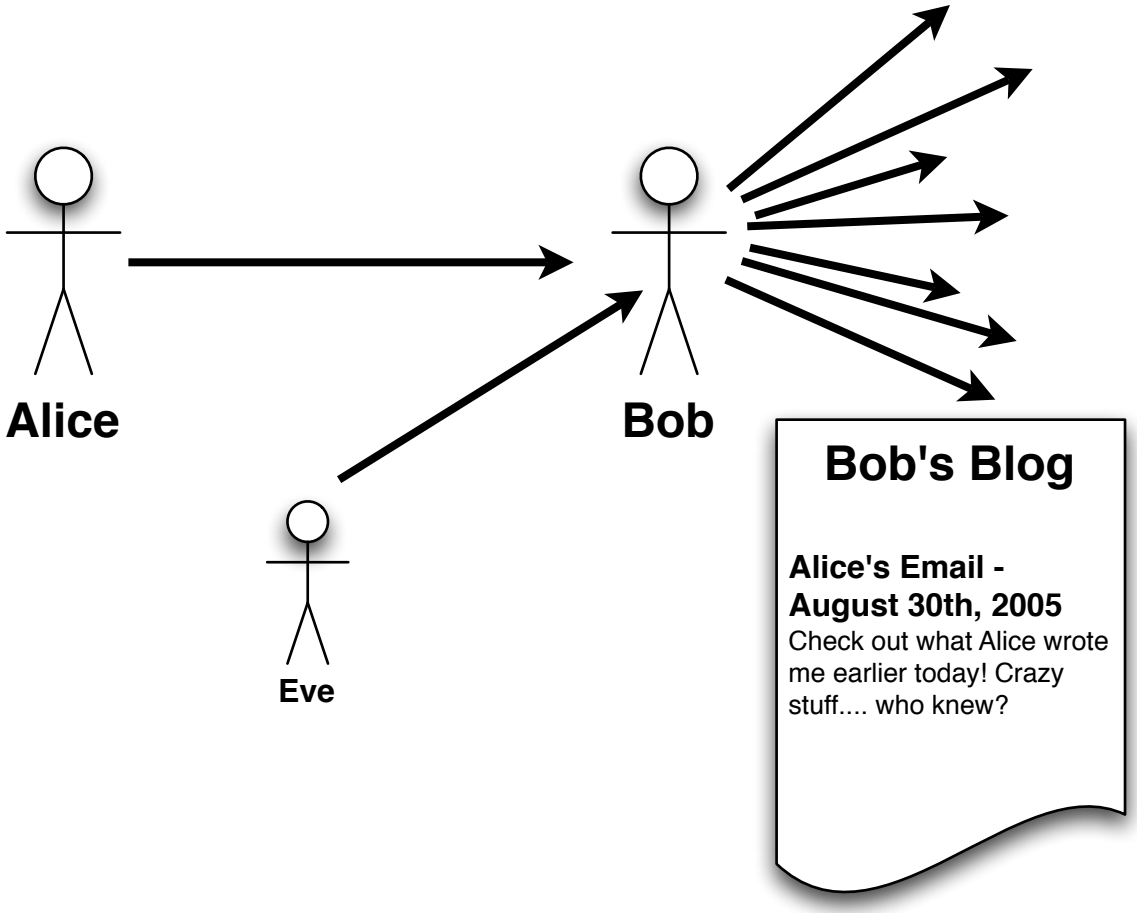
Email-Based Authentication for User Secret Keys



Lightweight Signatures



So What?



- Alice likes Bob
- Eve likes Bob
- Bob likes to gloat.

What if Bob publishes Alice's Email on his blog?

This changes the nature of email.

Ad-Hoc Group Sigs

From: Alice

To: Bob

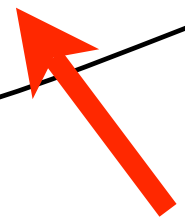
Subject: Coffee?

Hey Bob,

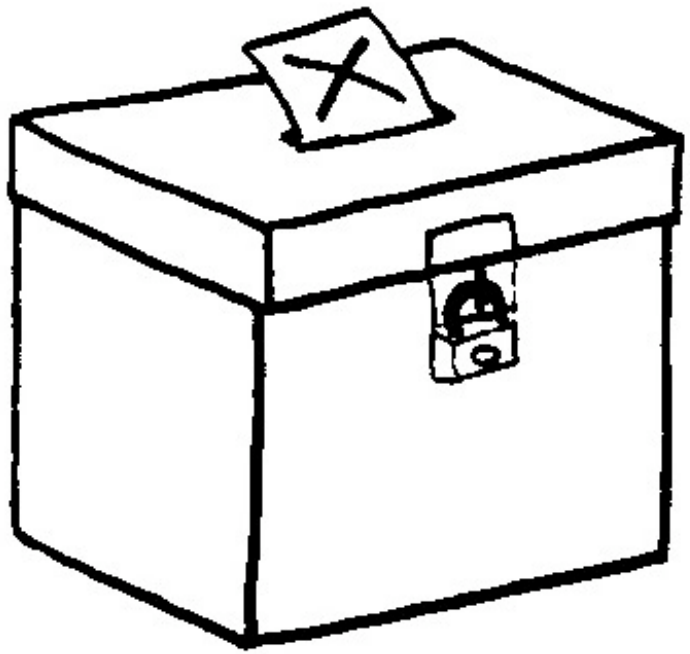
Wanna meet for coffee? I'd love to get to know you better.

Signed:

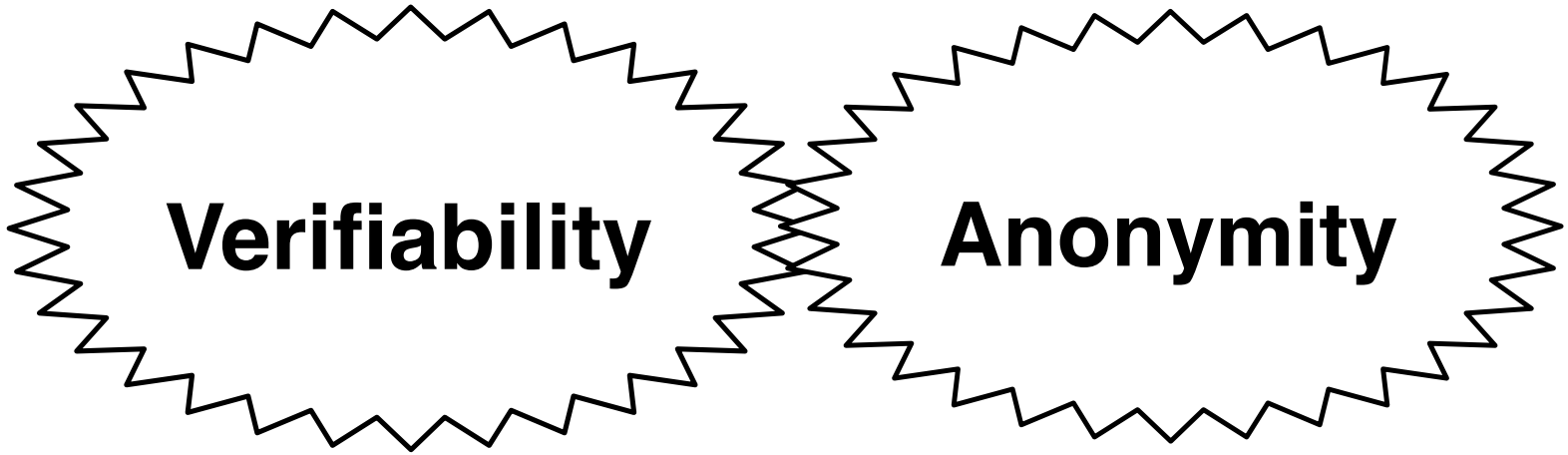
Alice or Bob



A Taste of Voting



Voting is Hard



The Point of An Election

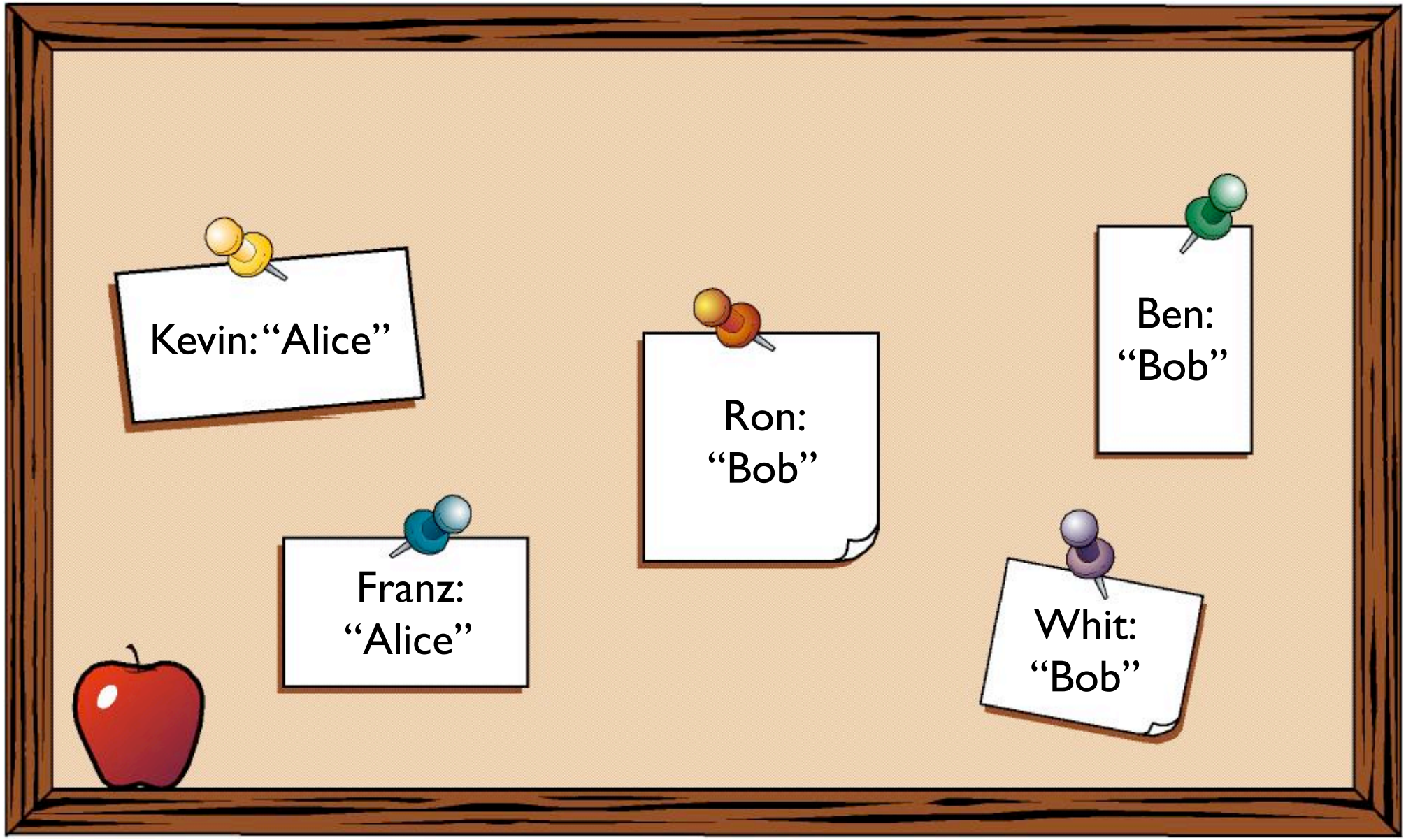
"The People have spoken.... the bastards!"

Dick Tuck
1966 Concession Speech

concession speeches given before acceptance speeches.

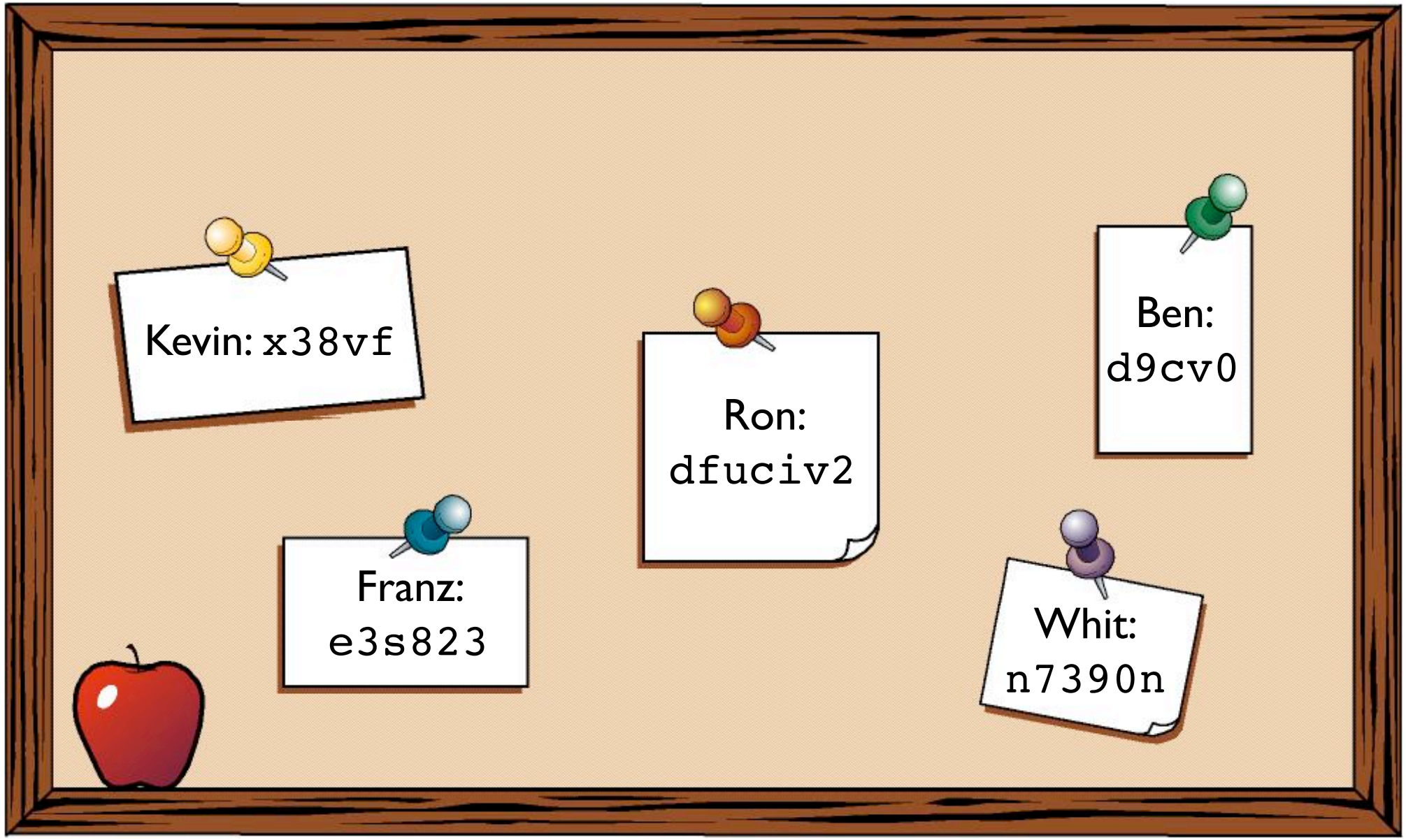
Provide enough evidence to convince the loser.

Bulletin Board

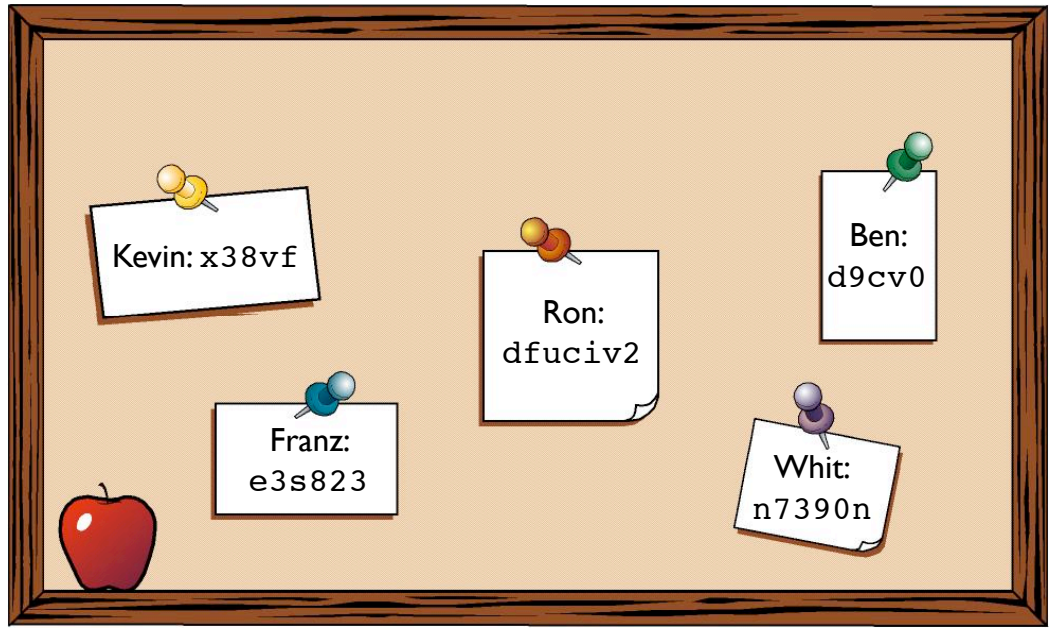


Can we get
ballot secrecy ***and***
election audit-ability?

Encrypted Bulletin Board

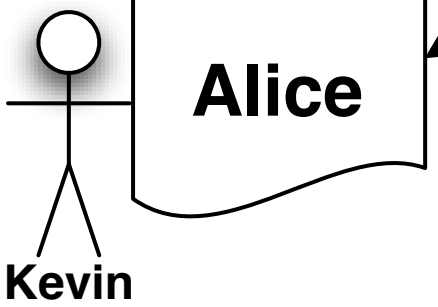


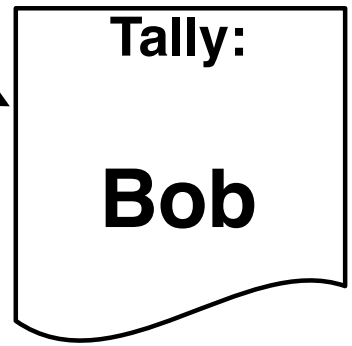
Verification?



Ballot Casting Assurance

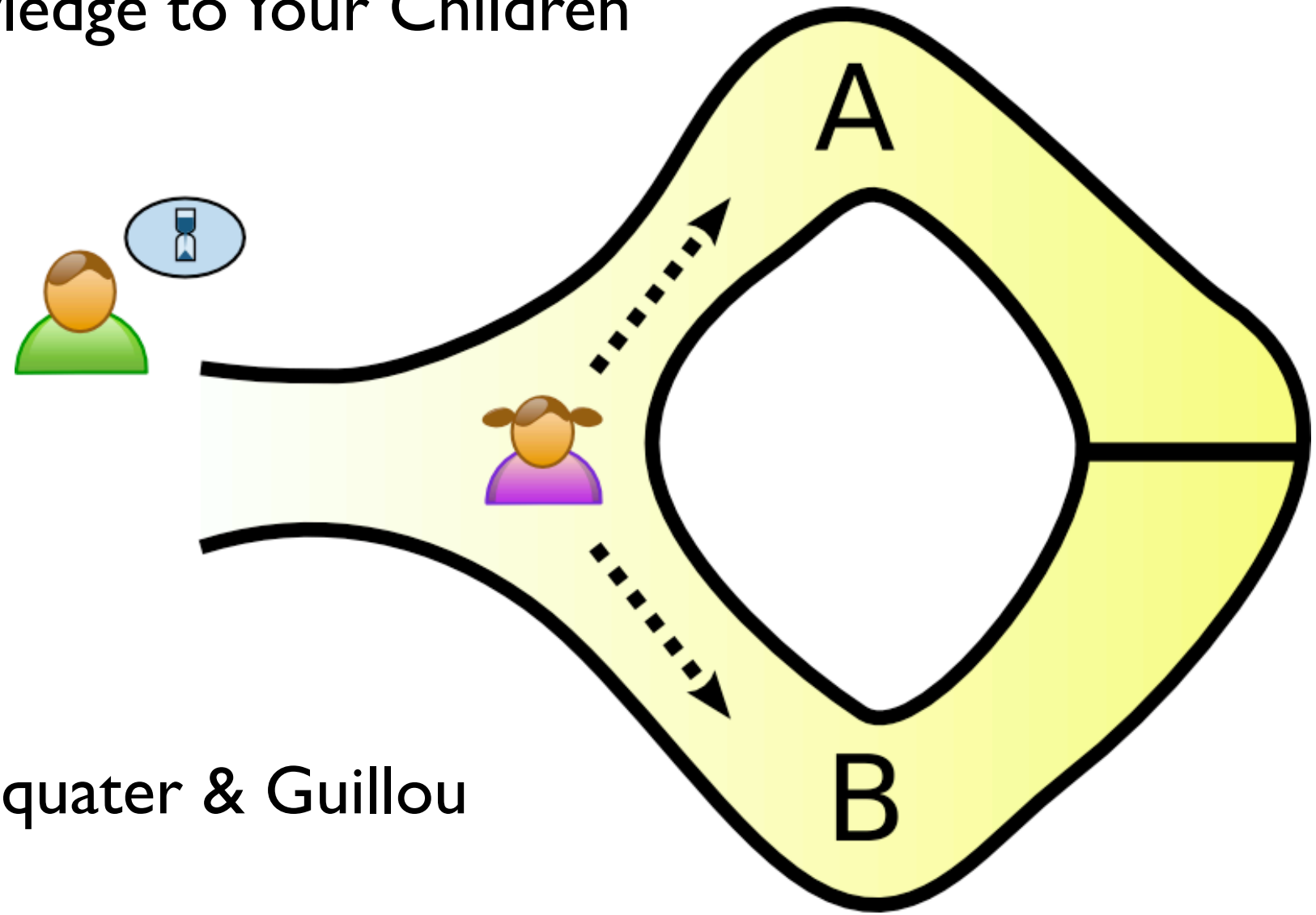
Universal Verifiability





Zero-Knowledge Proofs

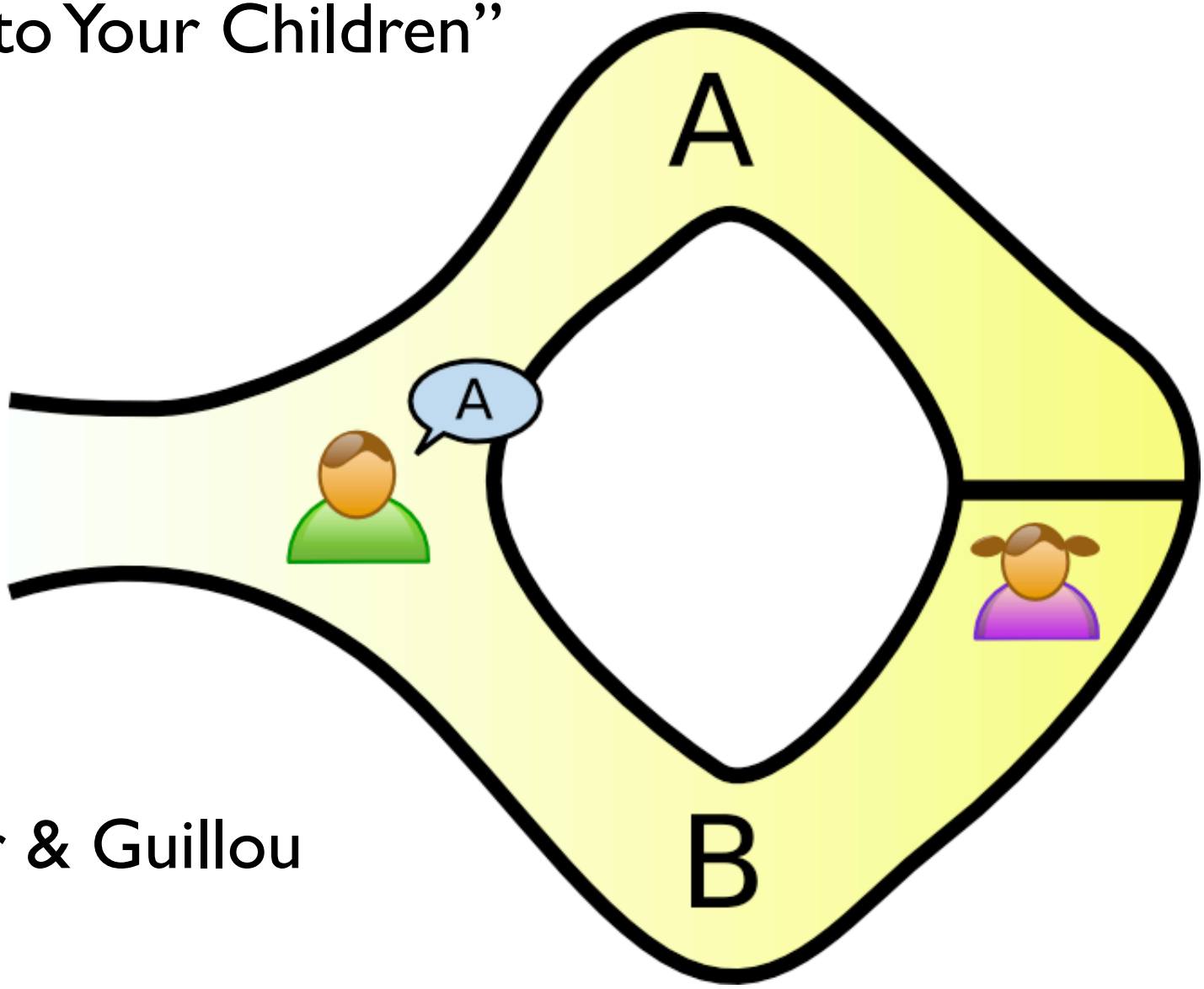
“How to Explain Zero-Knowledge to Your Children”



Quisquater & Guillou

graphics from Wikipedia

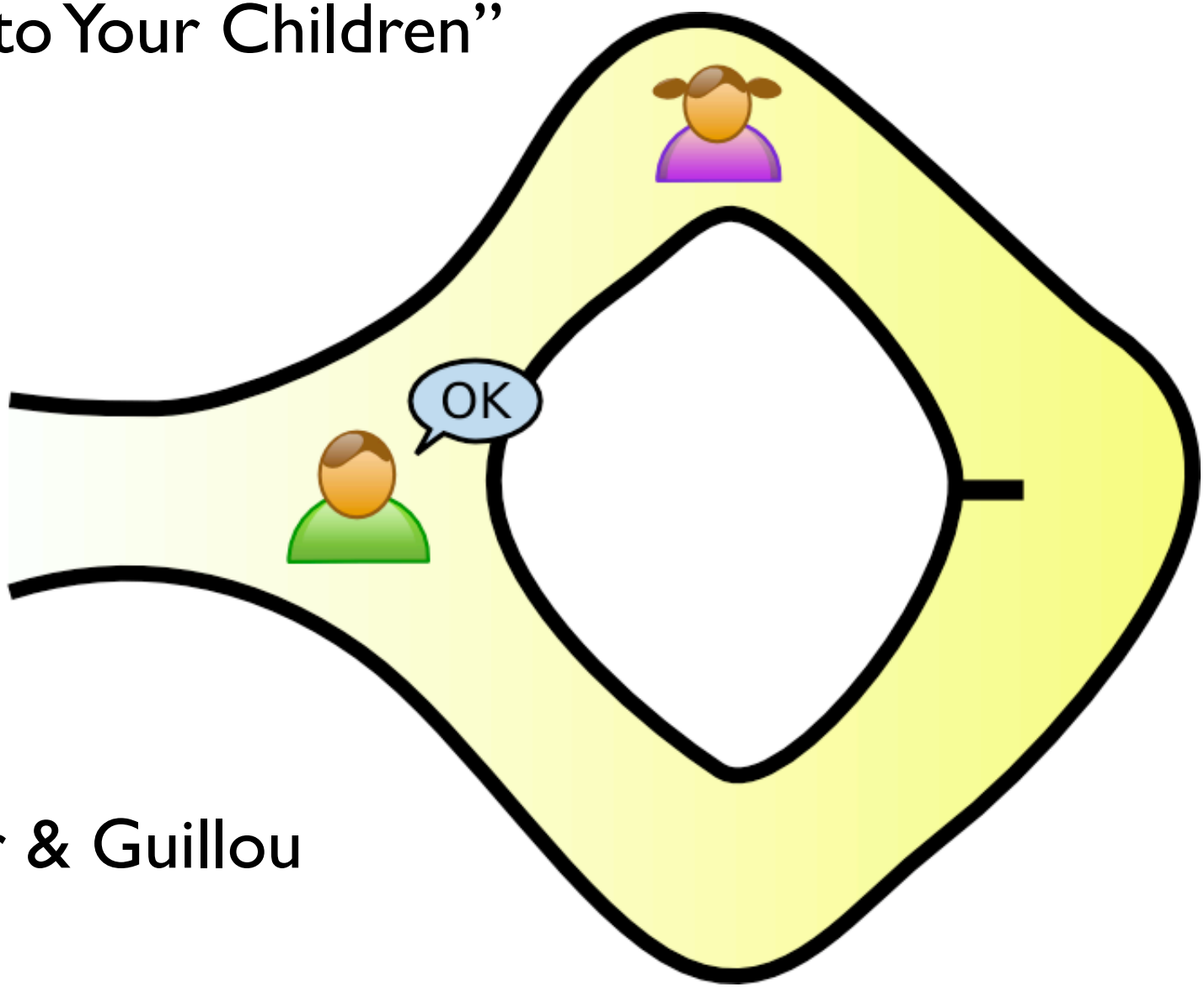
“How to Explain Zero-Knowledge to Your Children”



Quisquater & Guillou

graphics from Wikipedia

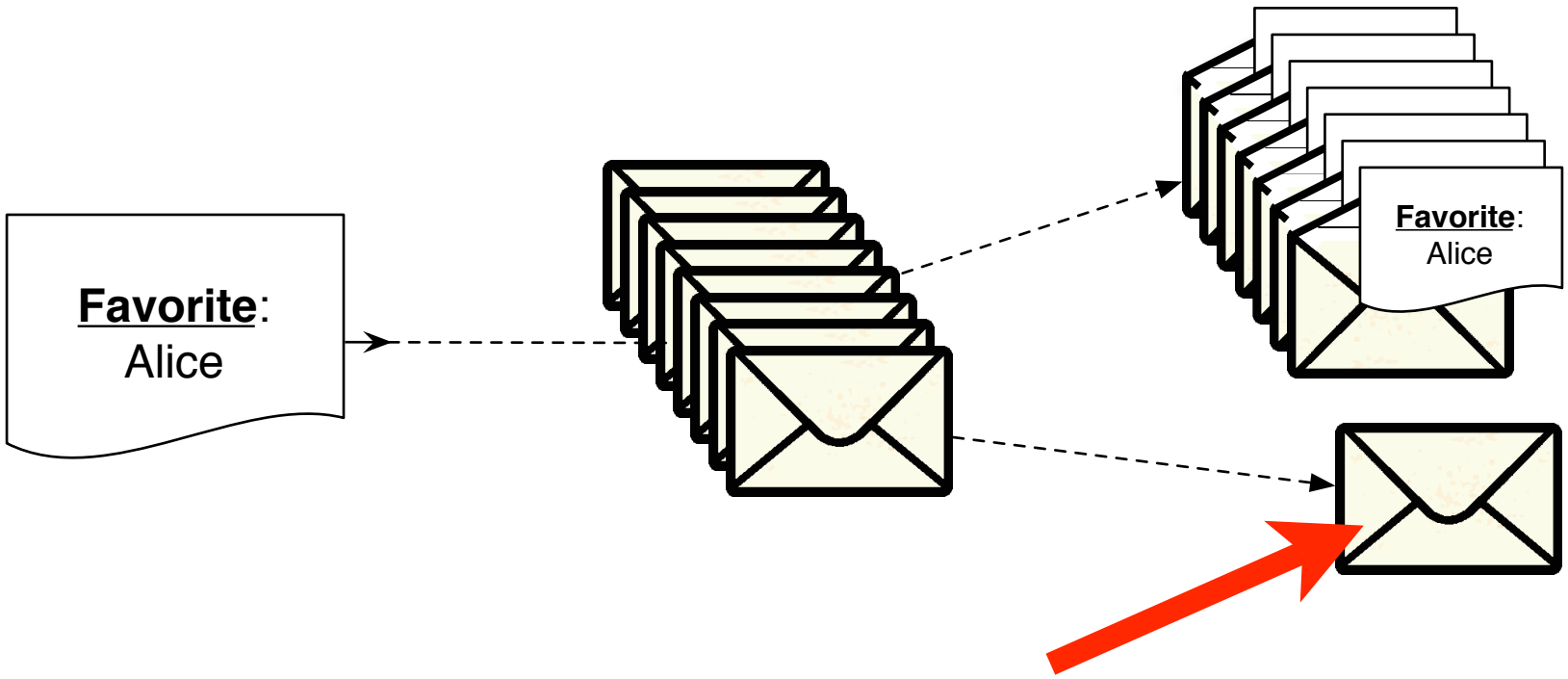
“How to Explain Zero-Knowledge to Your Children”



Quisquater & Guillou

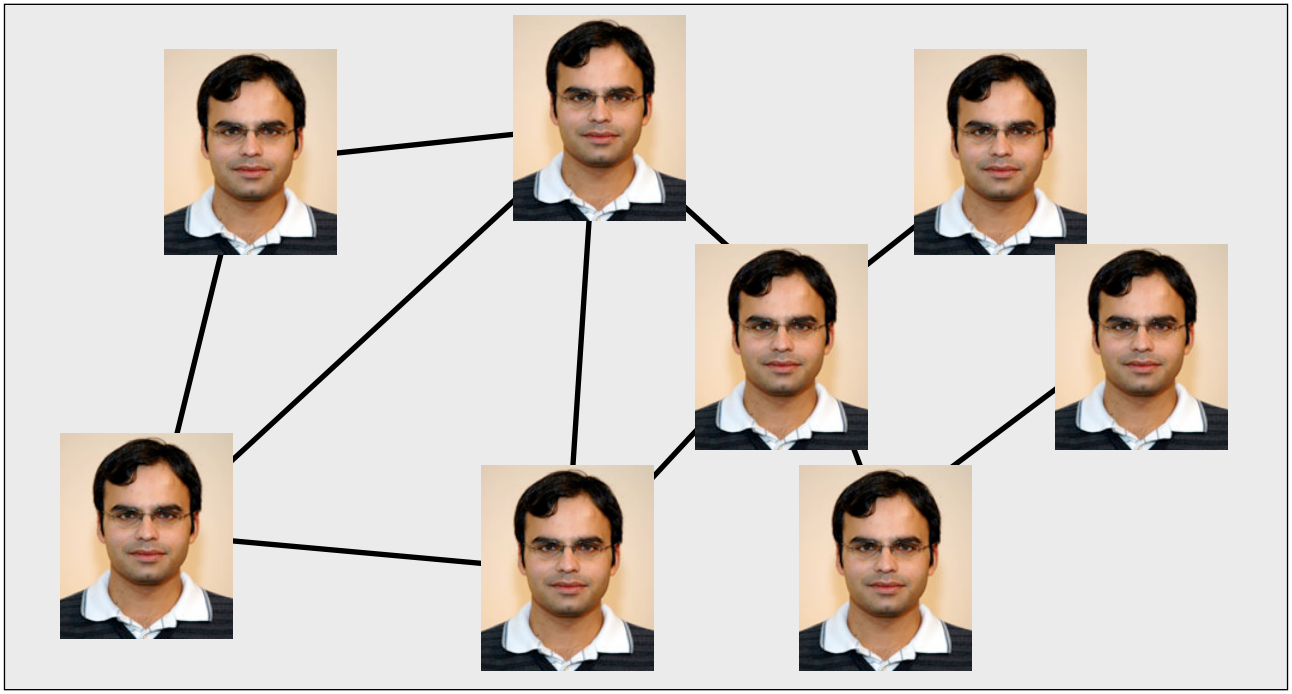
graphics from Wikipedia

Envelopes

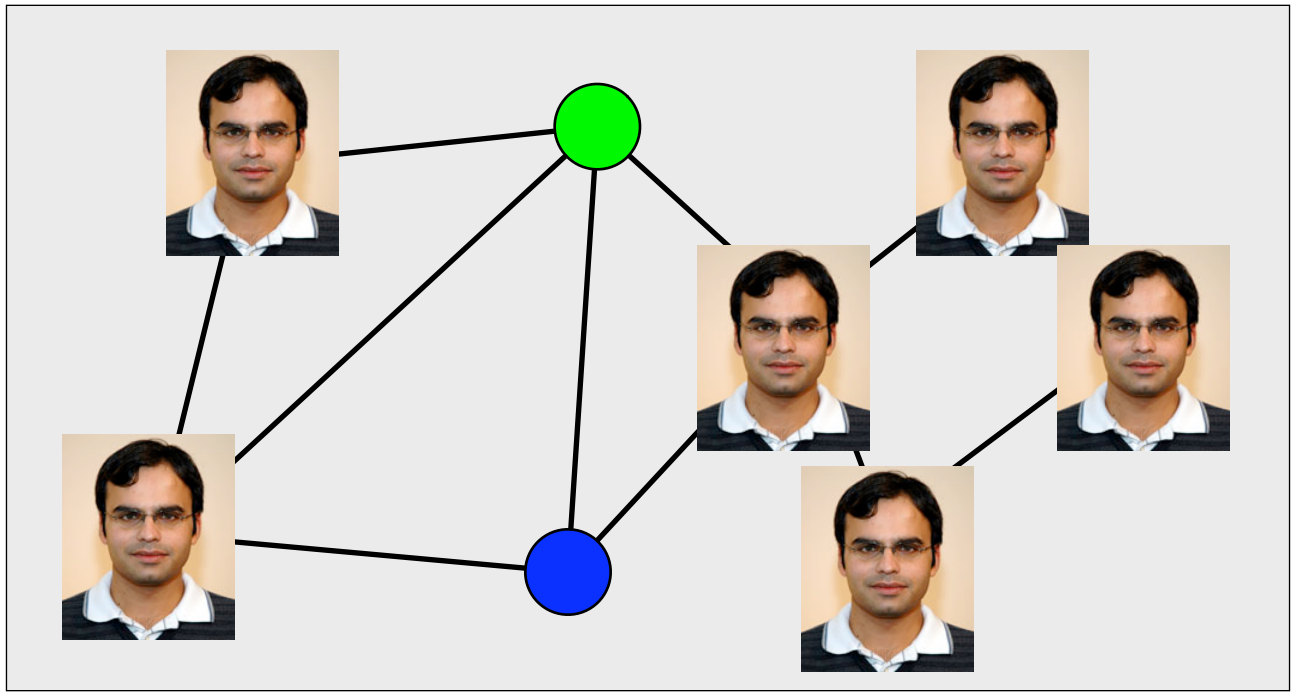


This last envelope
probably contains “Alice”

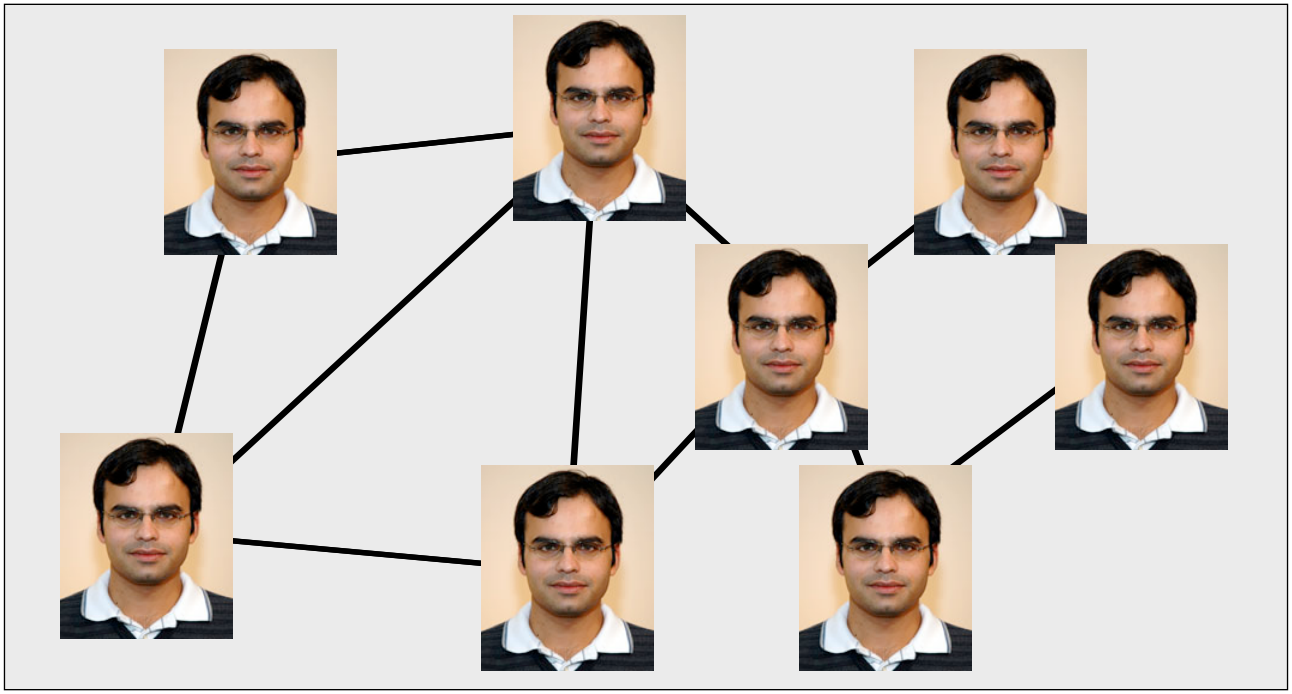
Graph 3-Coloring



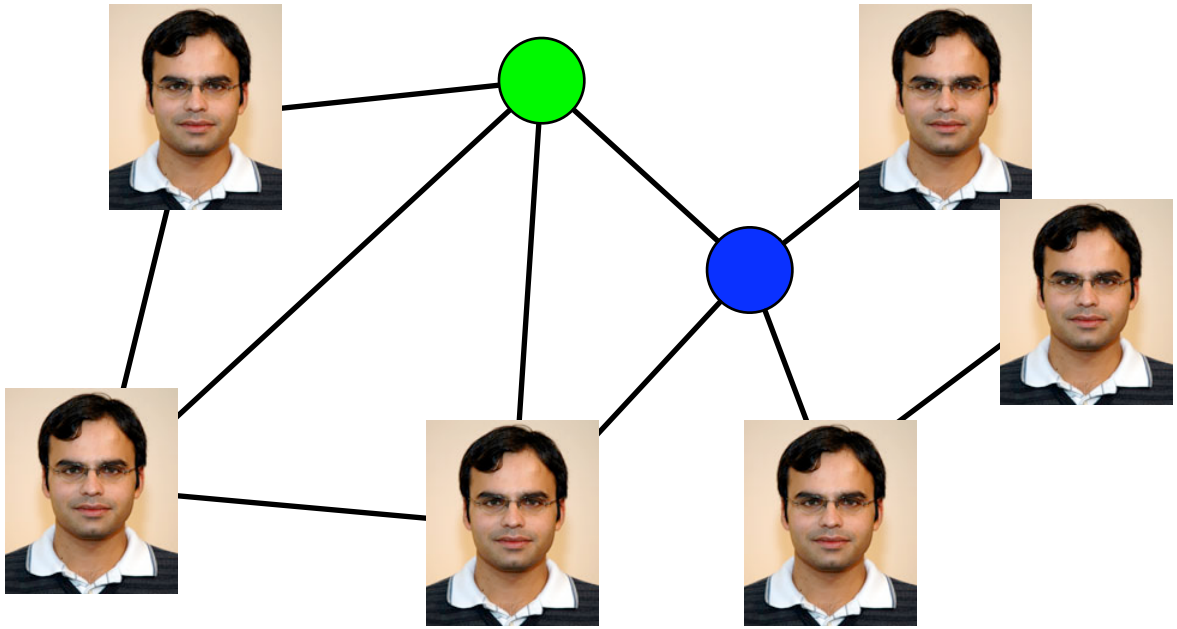
Graph 3-Coloring



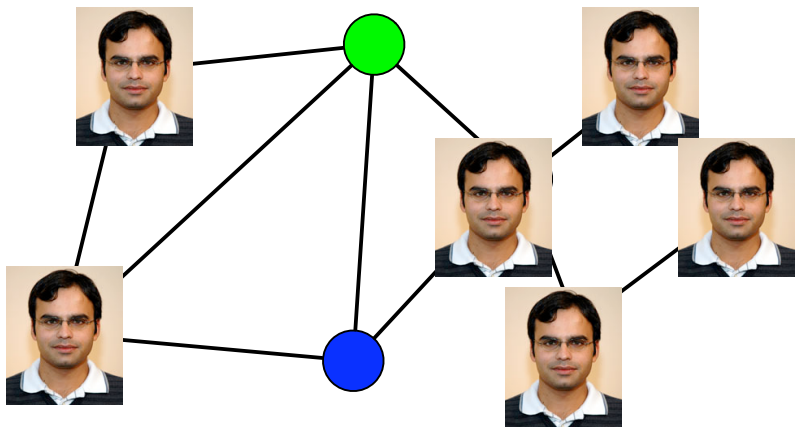
Graph 3-Coloring

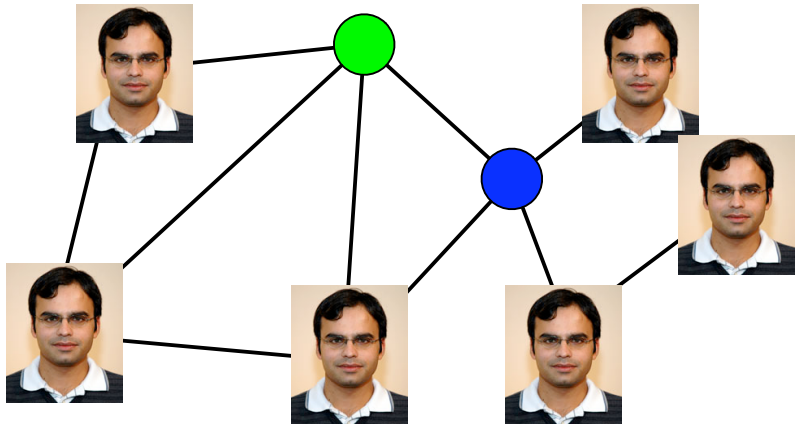


Graph 3-Coloring



What did you learn?



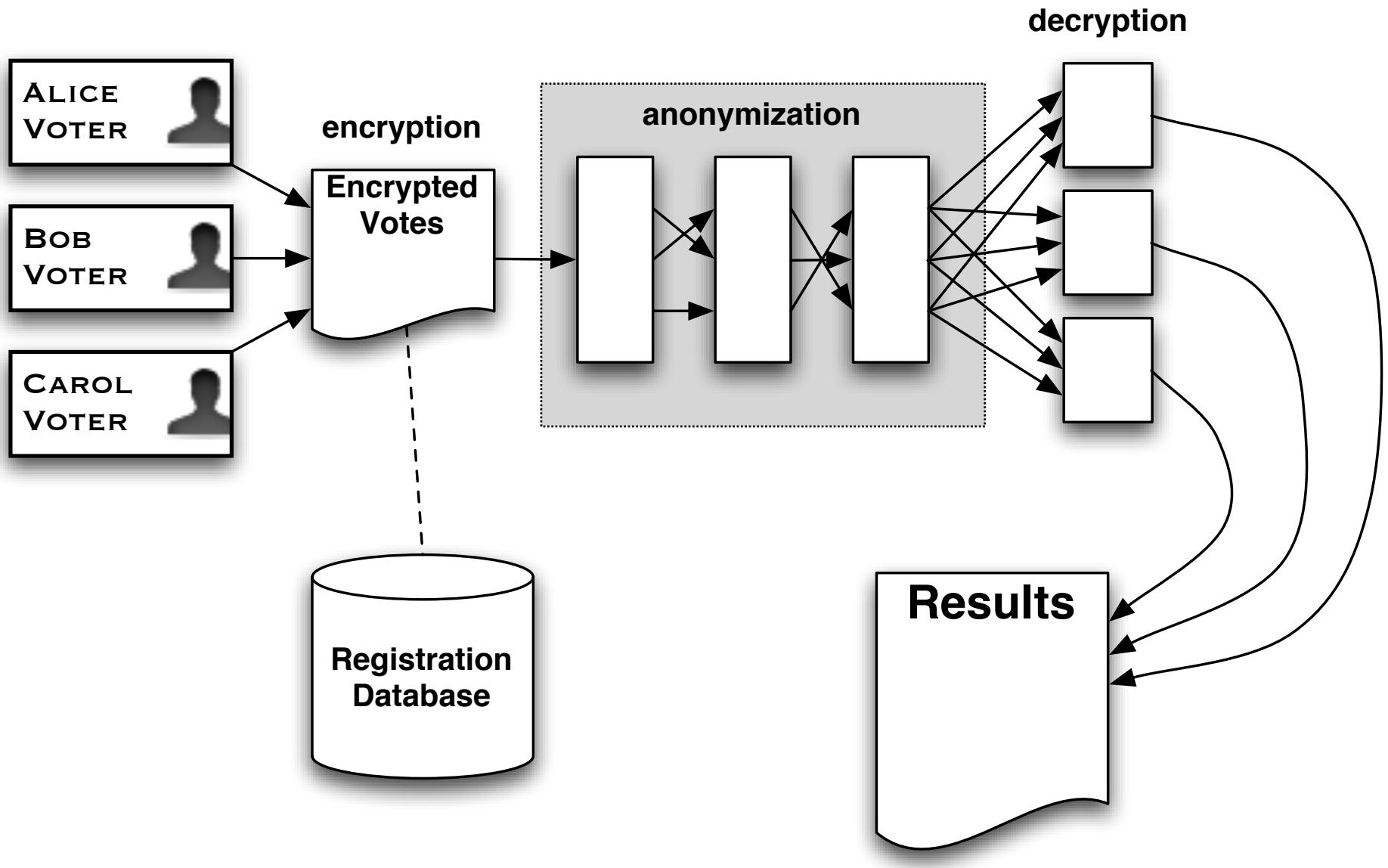


Nothing more than the fact that
I probably know a true 3-coloring.

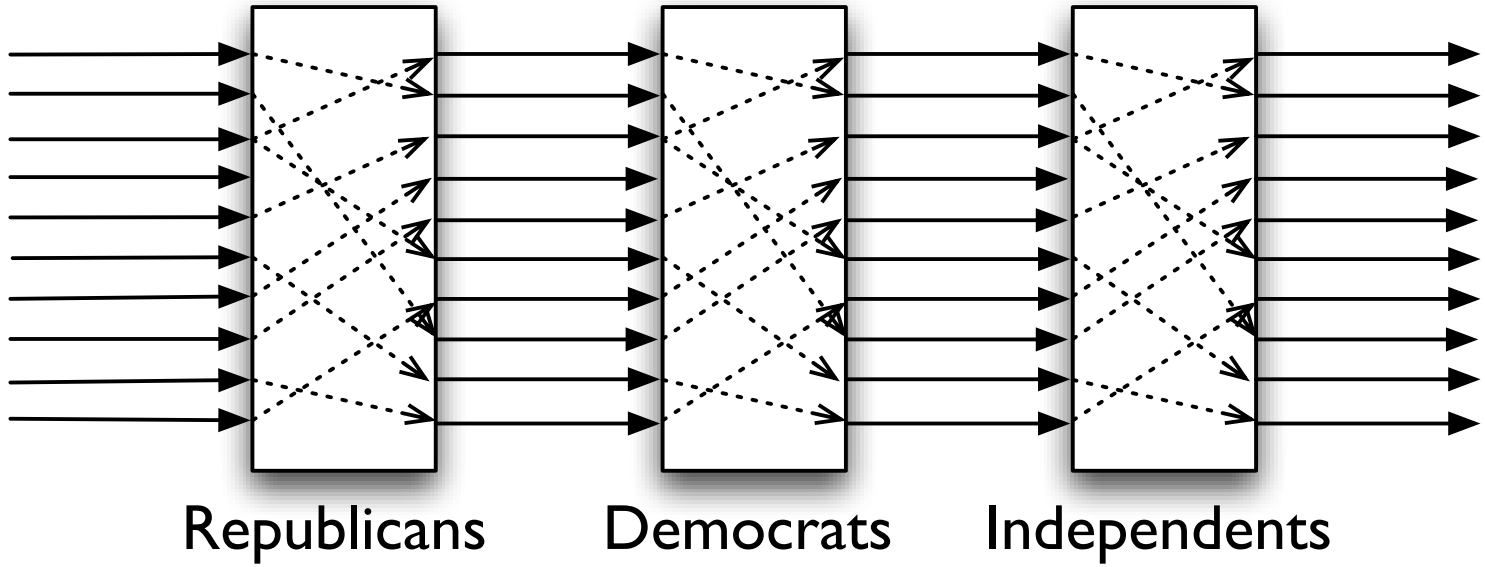
In particular

You did not learn enough to prove this same property to someone else.

Smells like....
Proving the content of a vote while preventing vote selling!

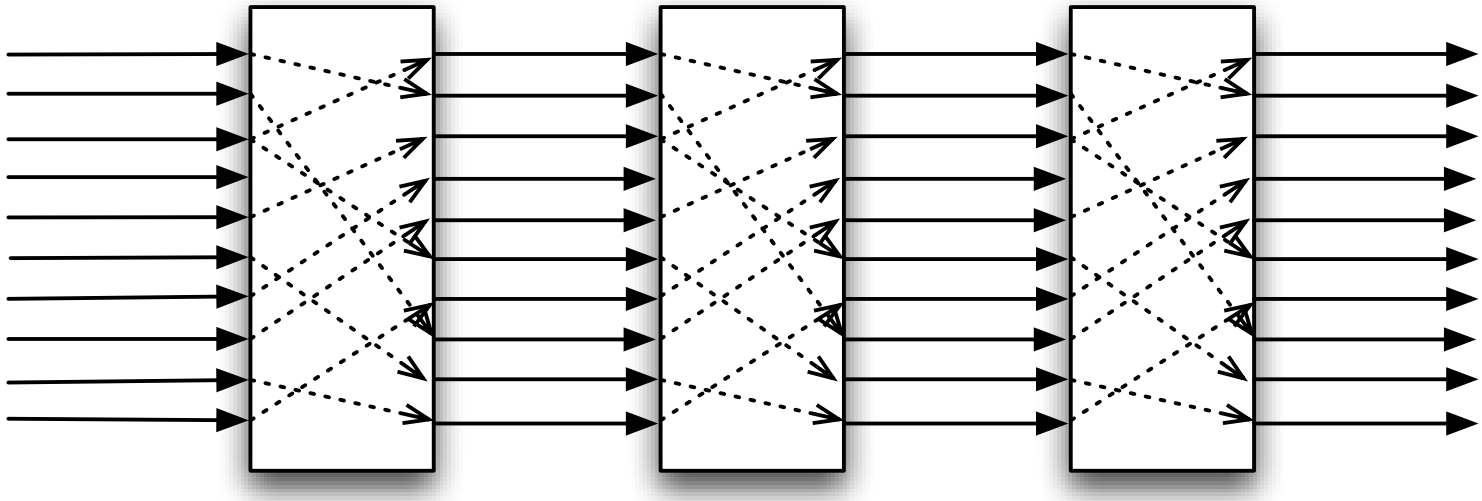

decryption
Alice
Voter
Bob
Voter
Carol
Voter
encryption
Encrypted
Votes
anonymization
Registration
Database
Results

Mixnet



Each mix server shuffles and rerandomizes the ciphertexts in private.

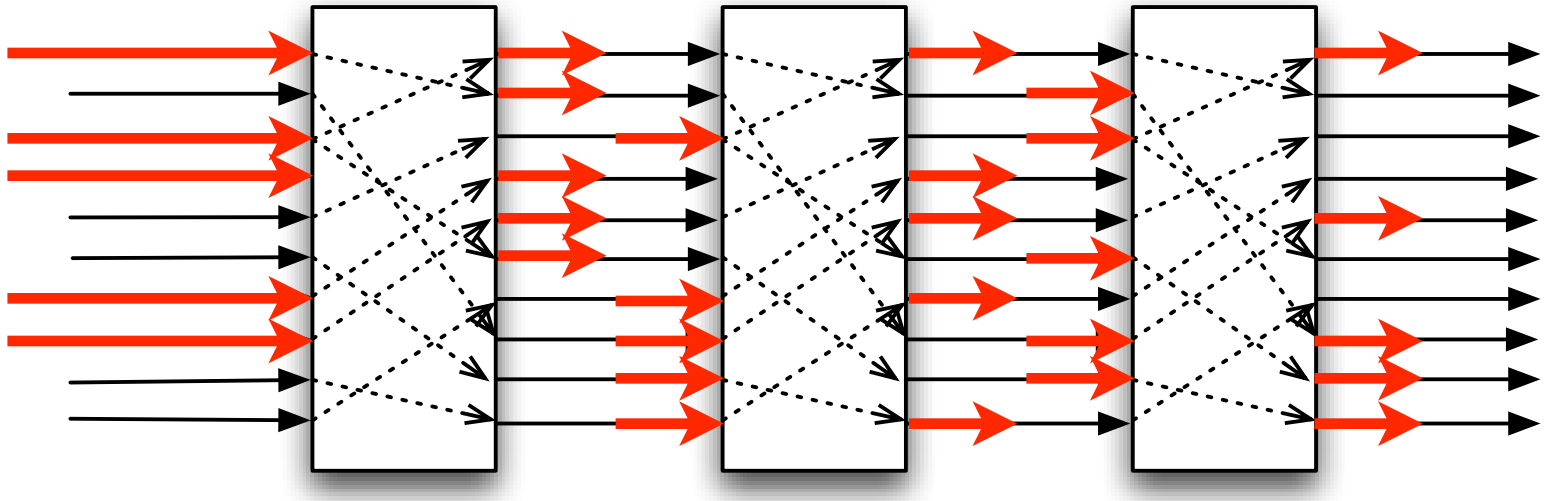
Decryption Mixnet



$$c = \mathsf{Enc}_{pk_0}(\mathsf{Enc}_{pk_1}(\mathsf{Enc}_{pk_2}(m)))$$

Each mix server "unwraps"
a layer of this encryption onion.

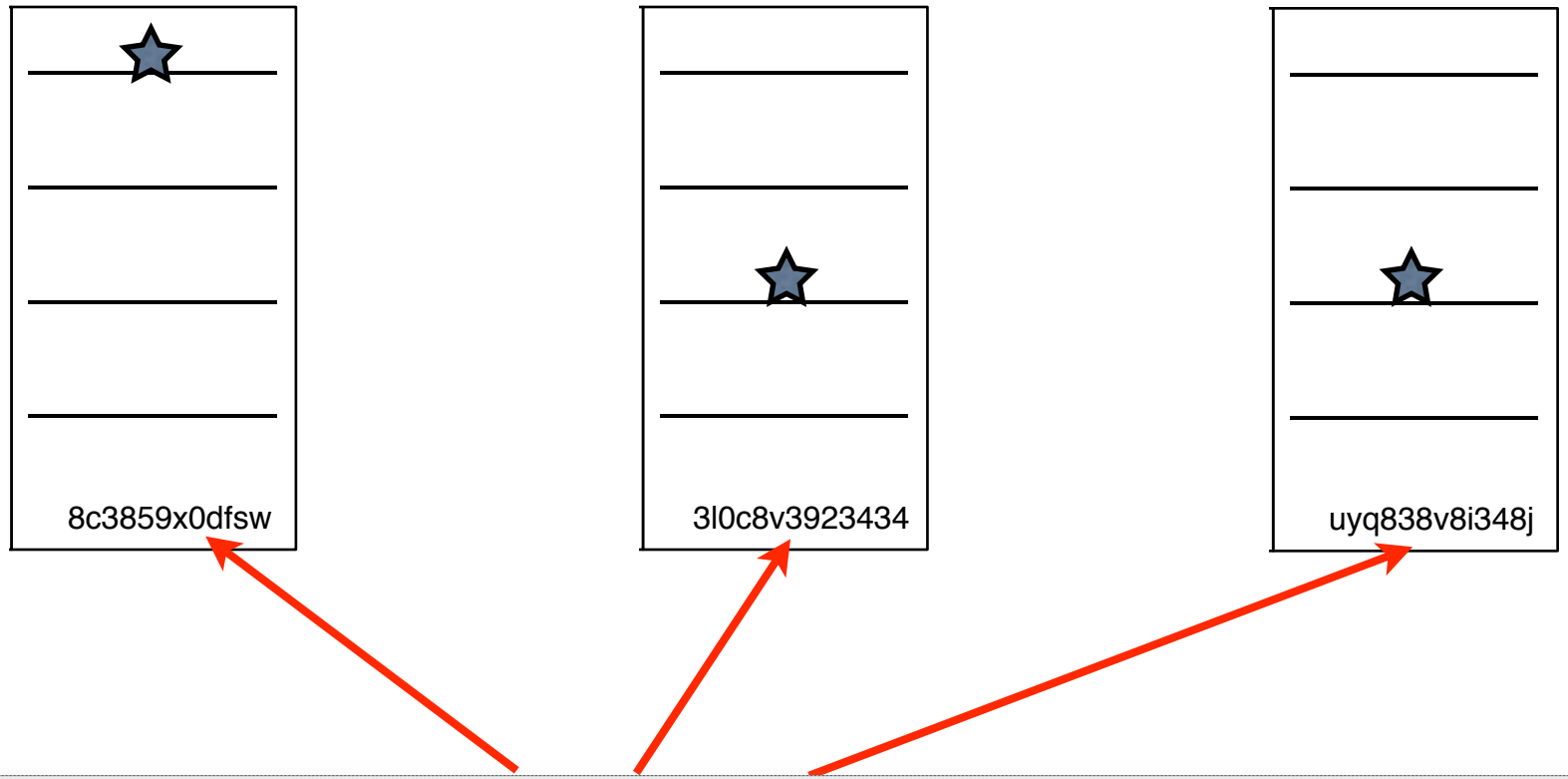
Verifying a Dec. Mixnet

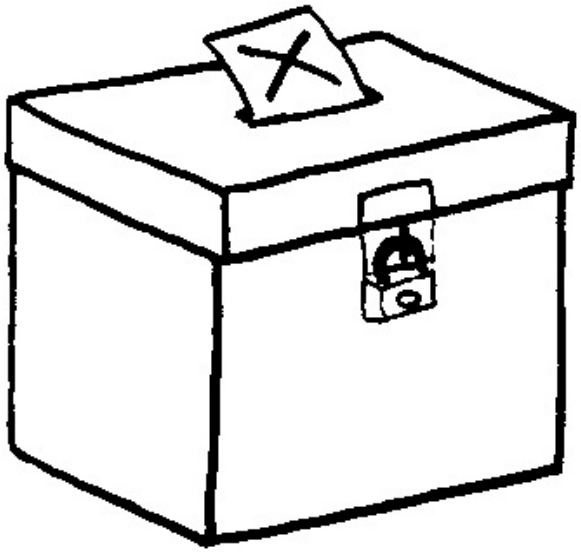
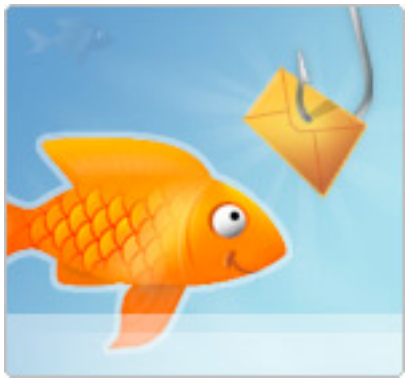


1/2 of mix servers honest =
no complete path is revealed

Randomized Partial Checking - Juels, Jakobsson, Rivest 2002

Prêt-à-Voter



H(Onion) that routes the ballot through
a Chaumian mixnet to recover the candidate order

Questions?