IBM Zurich Research Laboratory

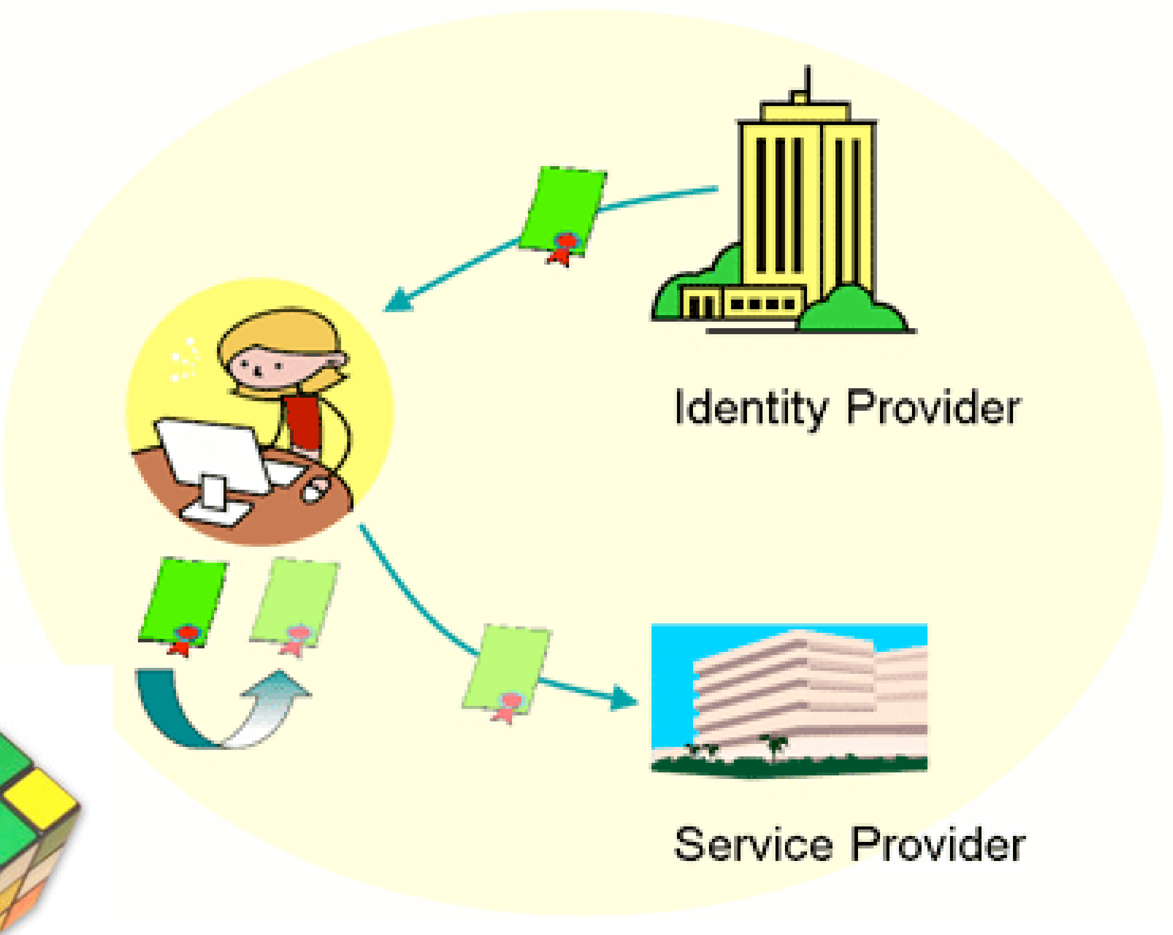
Privacy Enhancing Technologies

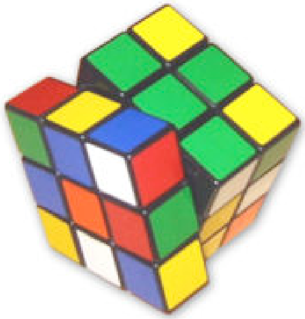
Dr. Susan Hohenberger (IBM)
Dr. Panos Papadimitratos(EPFL)

What are some Privacy Enhancing Technologies?

- **Anonymous Credentials**
  - Electronic Passports and Driver's Licenses
  - Can prove over 21 and *nothing* else
  - IDEMIX: http://www.zurich.ibm.com/security/idemix
- **Anonymous e-Cash**
  - Toll booths, Train tickets
  - Can get privacy of cash and speed of Metro Pass
- **k-Anonymous Authentication per Time Period**
  - Car-to-Car, Car-to-Infrastructure Communication
  - Can gather safety data without tracking users
- **and more ....**

Anonymous Credentials



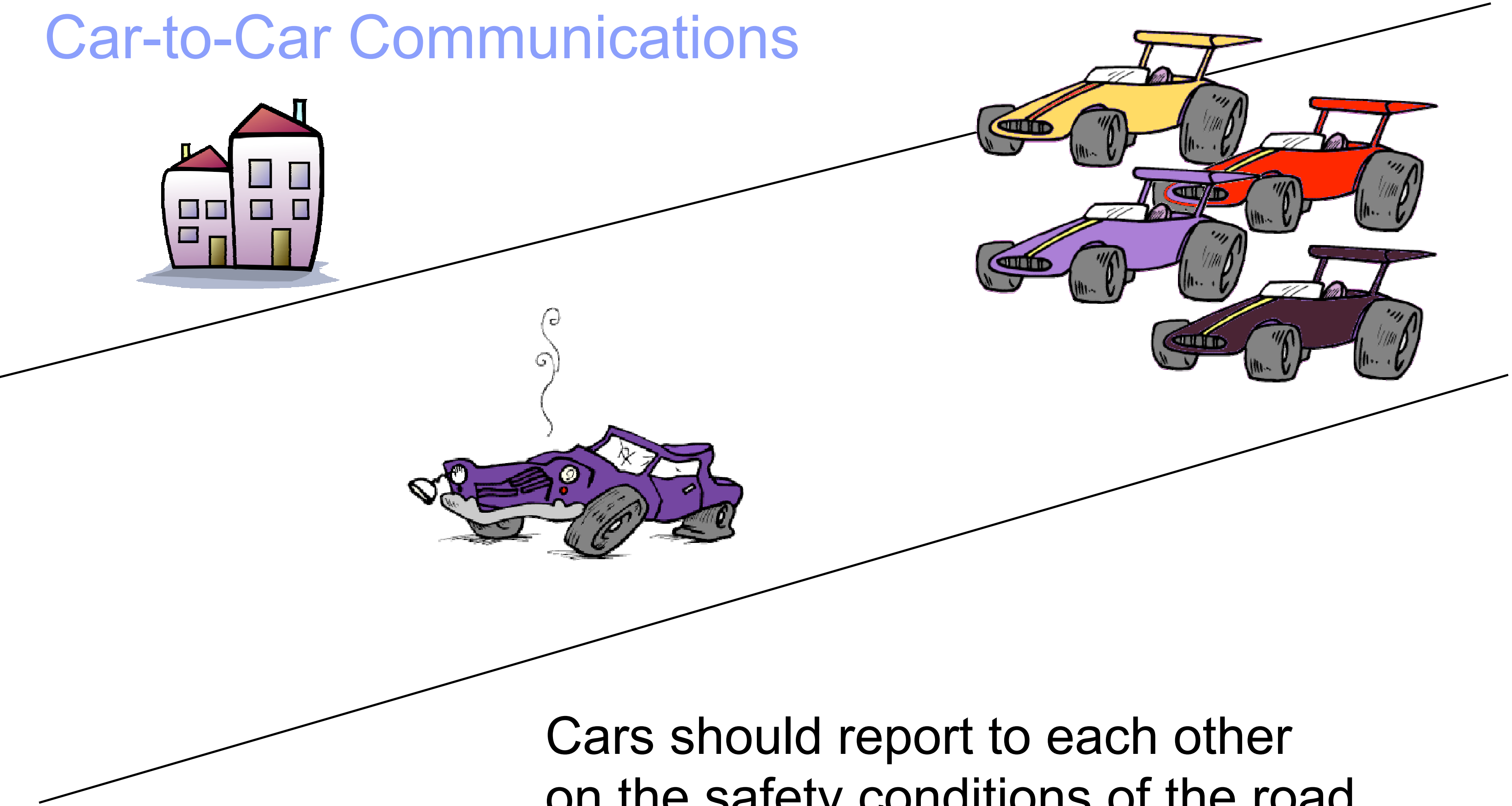


IDEMIX - Identity Mixer

User

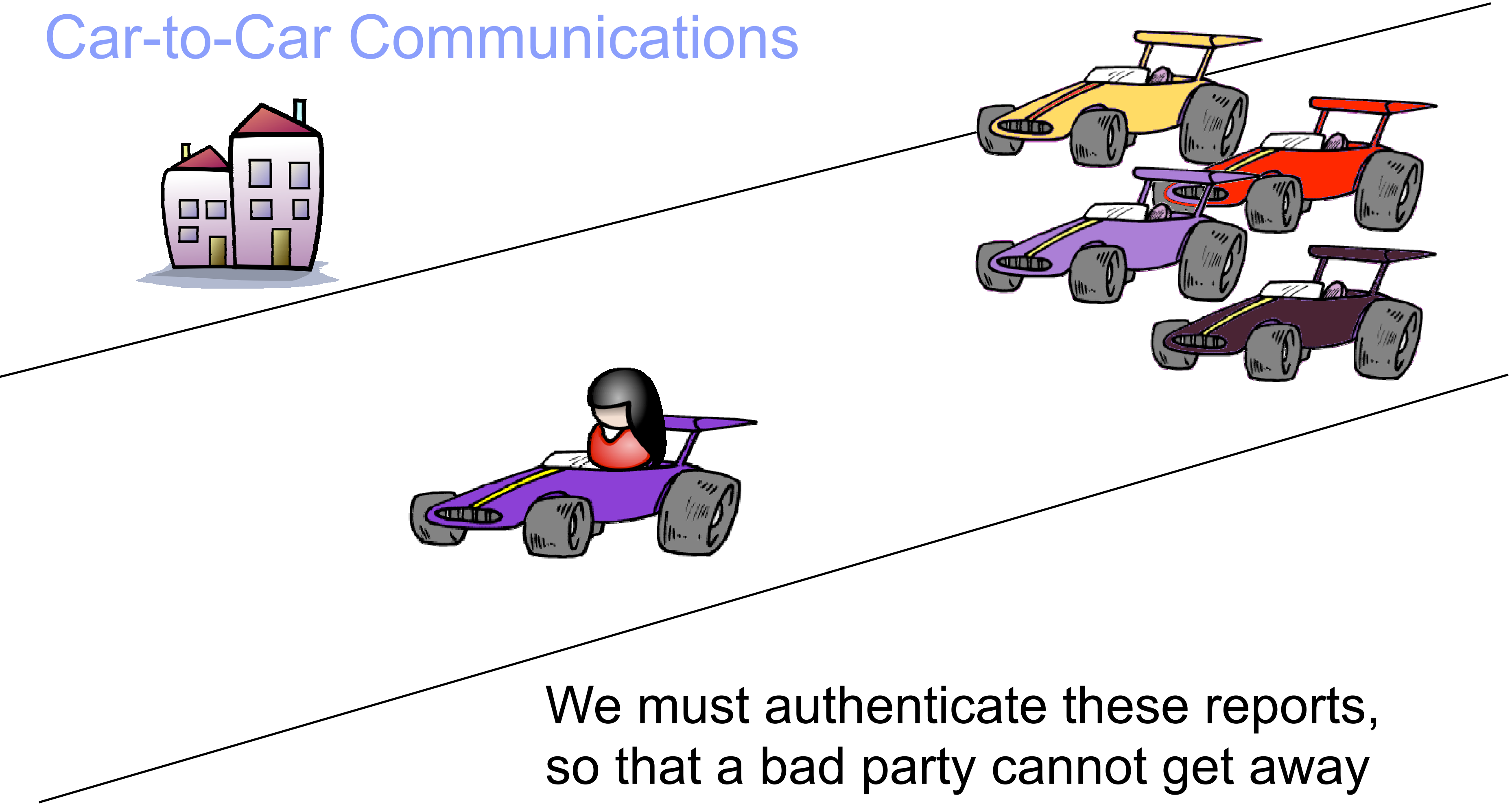
- IBM proof-of-concept implementation
- Computer-to-computer setting
- Anonymous authentication takes a few seconds
- Plans to open source the code, join with Higgins
- http://www.zurich.ibm.com/security/idemix

Car-to-Car Communications



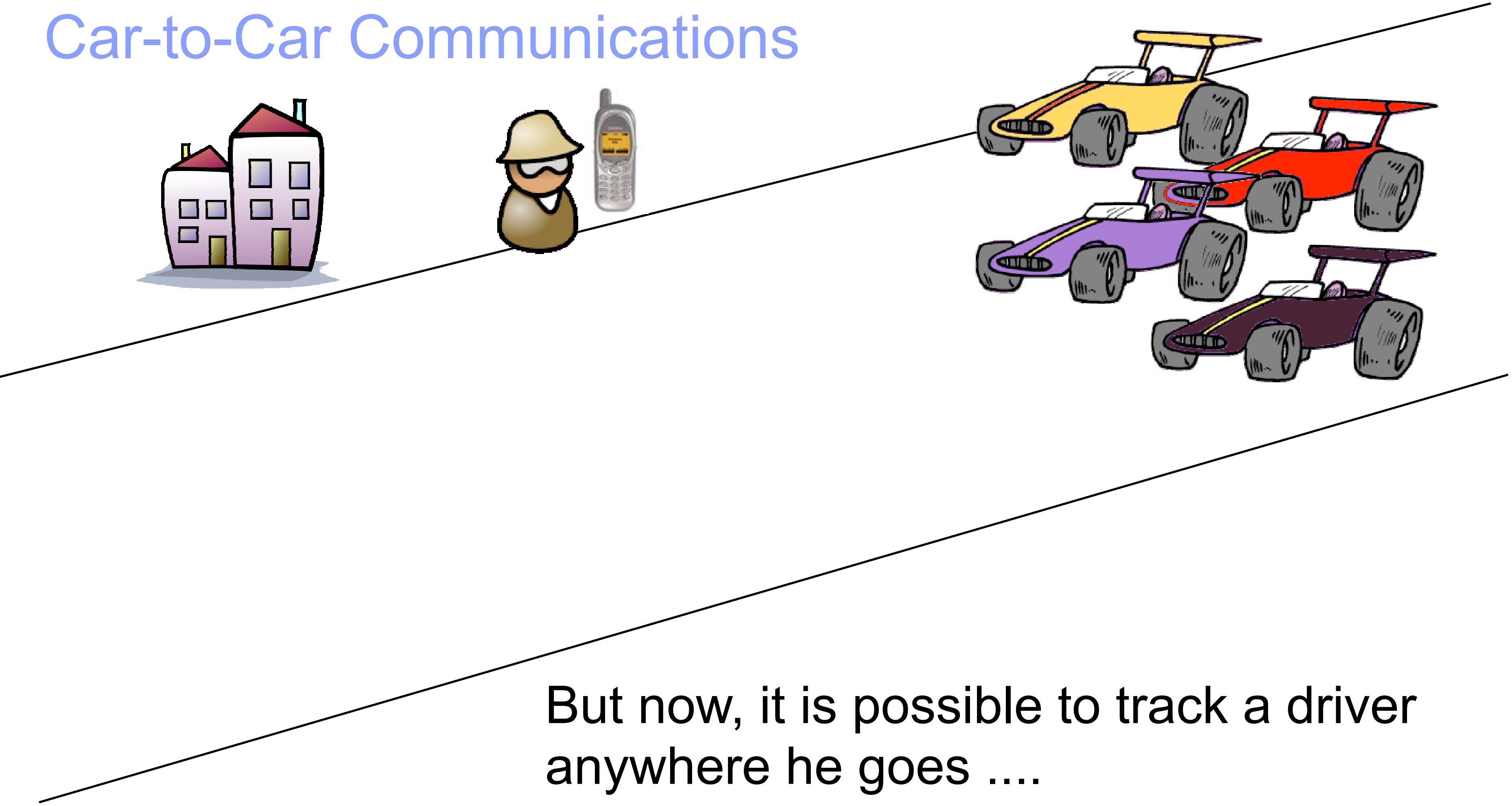
Cars should report to each other
on the safety conditions of the road.

Car-to-Car Communications



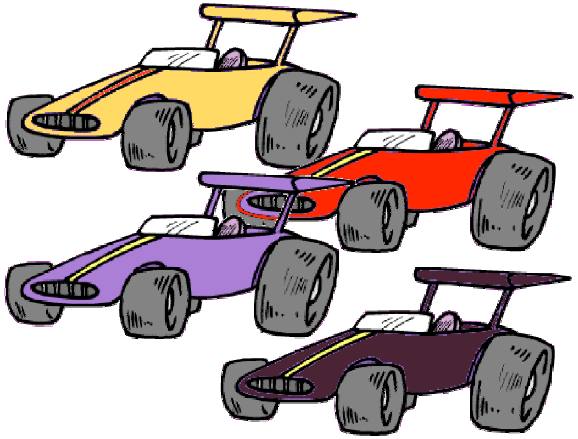
We must authenticate these reports, so that a bad party cannot get away with submitting false information.

Car-to-Car Communications



But now, it is possible to track a driver anywhere he goes ....
(celebrities, smart bombs)

Car-to-Car Communications



IDEA: limit each car to k **anonymous** reports per time period.

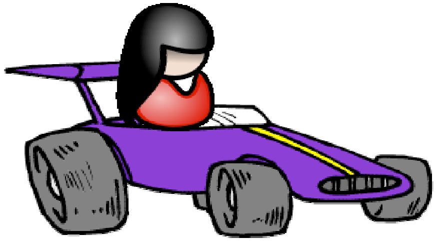
Now, a rogue sensor cannot submit “too much” false information.

Honest users remain anonymous.

Periodic k-times Anonymous Authentication

IDEA: If **k or less** reports per period,
then reports are **anonymous** and **unlinkable**.

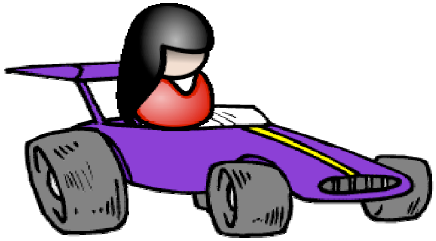
If **more than k** reports per period,
then reports are **identifiable** and **linkable**.



Periodic k-times Anonymous Authentication

IDEA: If **k or less** reports per period, then reports are **anonymous** and **unlinkable**.

If **more than k** reports per period, then reports are **identifiable** and **linkable**.



GLITCH PROTECTION:

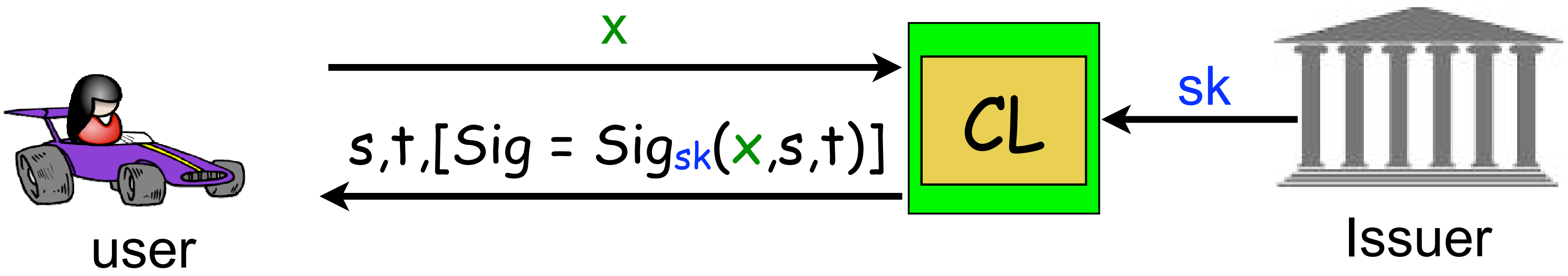
If **no more than m** extra reports per year, then reports are **anonymous**, but **linkable**.

Periodic k-times Anonymous Authentication

SETUP: (pk,sk)
Issuer signing key

(secret) x
for each user

OBTAIN DISPENSER:



x

$s,t,[Sig = Sig_{sk}(x,s,t)]$

CL

sk

user

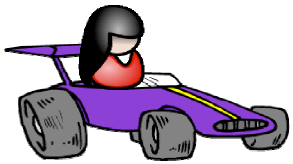
Issuer

Dispenser = (x, s, t, Sig).
(for all tokens from now to eternity)

Periodic k-times Anonymous Authentication

SHOW A TOKEN: Let $F_{(\ )}(\ )$ be a PRF Family.

random R



user

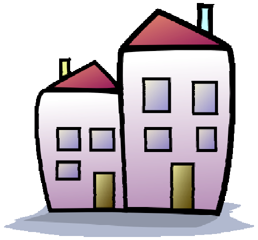
(x, s, t, Sig)

$S = F_s(\text{time}, i)$ (token serial number)

$T = x + F_t(\text{time}, i) * R$ (double-show equation)

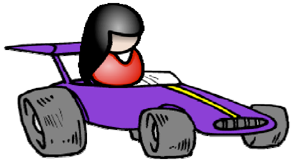
ZKPOK of (i,x,s,t,Sig) such that

1. $1 \le i \le k$
2. S, T formed correctly
3. VerifySig(pk,(x,s,t),Sig) = TRUE



verifier

Periodic k-times Anonymous Authentication



user

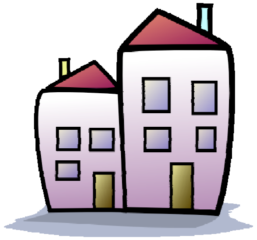
(x, s, t, Sig)

$S = F_s(\text{time}, i)$ (token serial number)

$T = x + F_t(\text{time}, i)*R$ (double-show equation)

ZKPOK of (i,x,s,t,Sig) such that

1. $1 <= i <= k$
2. S, T formed correctly
3. VerifySig(pk,(x,s,t),Sig) = TRUE



verifier

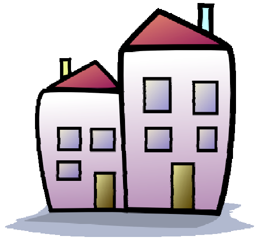
Why is this anonymous?

Periodic k-times Anonymous Authentication

$S = F_s(\text{time}, i)$ (token serial number)

$T = x + F_t(\text{time}, i) * R$ (double-show equation)

ZKPOK of (i, x, s, t, Sig) such that token is correctly formed.



verifier

Suppose a user shows k+1 tokens in a time period.

DETECT: then two tokens will have same serial number S.

IDENTIFY: given (S,T1,R1) and (S,T2,R2), compute

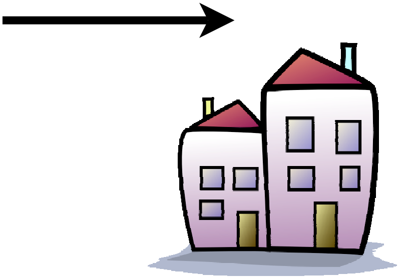
- $F_t(\text{time}, i) = (T1 - T2)/(R1 - R2)$
- $x = T1 - F_t(\text{time}, i) * R1$

Periodic k-times Anonymous Authentication

$S = F_s(\text{time}, i)$ (token serial number)

$T = x + F_t(\text{time}, i) * R$ (double-show equation)

ZKPOK of (i,x,s,t,Sig) such that token is correctly formed.



How efficient is it to Show and Verify a token?

Can optimize this construction so that:

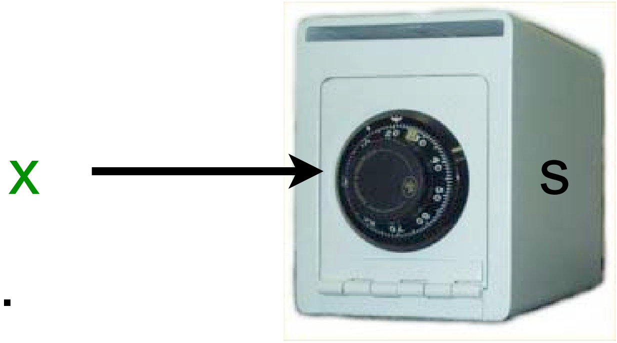
* User does 35 multi-base exps to Show
* Verifier does 20 multi-base exps to Verify

(If k=1, reduces to 13 and 8 respectively.)

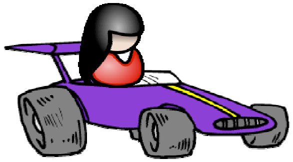
Periodic k-times Anonymous Authentication

$S = F_s(\text{time}, i)$ (token serial number)

Tracing of Misbehaving Users:



1. During Obtain, Issuer gets safe.
2. If user double-shows, x is revealed.
3. Use x to unlock safe and get s.
4. Use s to compute all serial numbers.



PRIME

- **IDEMIX Proof-of-Concept, Usage**
  - deployment and user feedback
  - open source of code, join with Higgins
  - http://www.zurich.ibm.com/security/idemix
- **Signatures: short and efficient**
  - RSA signatures: 2048 bits, but quick verification
  - Bilinear signatures: 400 bits, but slower verification
- **What else??**
  - lots of issues larger than cryptography

Susan Hohenberger

sus@zurich.ibm.com