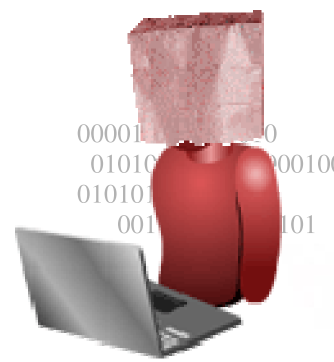
Anonymous Authentication

Andrew Lindell

Aladdin Knowledge Systems

&

Bar-Ilan University, Israel



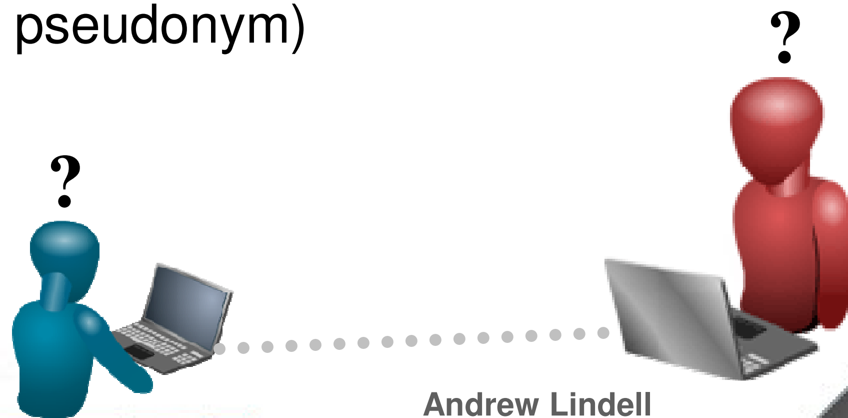
Chat Rooms

- **A huge success for youth and a huge concern for parents**
- **2006 survey (of 1500 US youth) by the Crimes against Children research centre**
  - 13% of youth received unwanted sexual solicitations (down from 19% in 2001)
  - 4% of youth received aggressive solicitations in which solicitors attempted to make offline contact (up from 3% in 2001)

Andrew Lindell
Aladdin Knowledge Systems

Chat Anonymity

- **Why are online sexual solicitations a concern? Aren't chats anonymous?**
  - **Problem 1:** 34% of children interviewed posted personal information online where anyone could see it
  - **Problem 2:** even when personal information is not explicitly posted, it can be found through multiple sources (e.g., linked by the user's pseudonym)



Andrew Lindell
Aladdin Knowledge Systems

Solutions

- **Education**
- **Parental control**
- **Law enforcement**
- **Technology**
  - Set up "safe chat rooms" which deploy strong authentication methods
  - Allow children to access safe chat rooms only
  - This has its own problems…

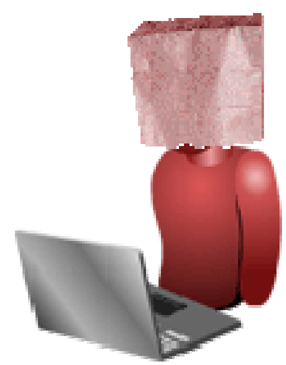
Authenticated Chat Rooms

- **One of the most attractive aspects of chat rooms is their anonymity**
  - Children can be freed from the bonds of peer pressure and can speak freely
  - Children can ask advice about embarrassing situations, (seemingly) without fear of being traced
- **The use of authentication destroys this aspect of chat rooms**

Andrew Lindell
Aladdin Knowledge Systems

Anonymous Authentication

- **Anonymous authentication – a contradiction in terms**
  - The user authenticates to the server and proves that she is an authorized user
  - The server has no idea which authorized user is authenticating
- **Is this really possible?**
  - **Yes**!



Other Applications

- **Professional forums**
  - Technical papers, technical help, discussion forums
  - These are “great” sources of information for (legal) industrial espionage
  - If authentication is required (to allow only registered or paying users), the problem becomes far more acute
- **Whistle blowing**
  - We want to be sure that the report is really from an employee, but we want to protect them…
- **Social networks**

Another Issue – Revocable Anonymity

- **Assume anonymous authentication is used**
- **Consider the case that one of the users is harassing others (or a pedophile stole someone's authentication device and is using it)**
  - The harasser's account cannot be closed because we don't know who the harasser is
- **Revocable anonymity: when needed, and upon court order, can reveal identity**
  - Without court order cannot reveal ID (provably)

Talk Outline

- **Privacy**
  - It is important – we all know that
  - But, ***why*** is it important?
- **Anonymous web surfing**
  - A very brief mention
- **Anonymous authentication**
  - Definitions
  - Protocols
  - Extensions

Privacy

A Concrete Perspective

Privacy

- **Everyone here agrees that privacy is important, but why?**
  - **Typically**
    - The loss of privacy is an invasion into our personal space
    - Warren and Brandeis: privacy is “the right to be let alone”
- **But what concrete damage is incurred?**

Andrew Lindell
Aladdin Knowledge Systems

Privacy – A Concrete Perspective

- **We will consider concrete damage that may be incurred due to privacy loss**
  - Understand these concrete damages are crucial for providing secure protocols that actually solve the problem at hand

Andrew Lindell
Aladdin Knowledge Systems

Privacy and Self Censorship

- **Storing user online information (emails, web and chat history and more), will likely result in self-censorship and inhibition**
  – Highly likely if linked to real identity (and otherwise possible due to fear of later linkage)
- **Think of the following uses of the Internet**
  – Teenagers on chat sites
  – University forums where students comment on lecturers and courses
  – Web sites that provide information on sensitive medical issues, sexual health and practice, and psychological first aid

Privacy – A Naïve Perspective

- **The above is usually only considered a problem if the user's online identity is linked to her real-world identity**
- **Business Week/Harris Poll in 2000**
  - 35% "not at all comfortable" with profiling online actions without linking to real identity
  - 81% "not at all comfortable" when this profiling **is** linked to real identity
  - (My guess: 35% also concerned that link may happen)
- **No identifier means no invasion of space**

Andrew Lindell
Aladdin Knowledge Systems

Information Without Identification

- **If it is 100% guaranteed that a user's profile can never be connected to their identity, then self censorship is unlikely to occur**
- **Example – online newspaper**
  - Newspaper records history of all articles read and all comments posted
  - Information used to construct a newspaper tailored to your interests
  - If identity never provided, this seems fine

Andrew Lindell
Aladdin Knowledge Systems

Basic Pseudonyms

- **Based on this, a basic pseudonym that cannot be linked to the user's real-world identity solves the problem!**
- **This is false!**
  - And not only because it is **impossible** to guarantee that a link will never be made

Privacy Loss Without Identification

- **Consider the newspaper example**
  – A user's profile reveals much about their political beliefs, financial status and so on
  – A newspaper with strong interests can tailor the content to influence the user
  – Since the newspaper has a lot of information about the user, and the user is not aware of this (or that it is getting tailored content), the user can be unfairly manipulated
- **This infringes on the user's personal autonomy**

Pseudonyms?

- **A pseudonym that cannot be linked to a user's true identity does not solve the problem at all**
  - In order to manipulate the user, the newspaper only needs to be able to link their history to their current actions

Industrial Espionage

- If a user's real identity is not known, then the information gathered from a professional forum cannot be used to identify what company the user works for
- However, it can be enough to just know that some competitor is researching and developing some product

Price Discrimination

- **Consider an online mall that tracks a buyer's prior purchases and shopping habits**
- **If a seller knows that a buyer does not "shop around", then they may charge higher prices**
  - The seller has more information about what the buyer is willing to pay than what the buyer has about the price for which the seller is willing to sell
  - The buyer is not aware of this asymmetry

Conclusions

- **Privacy is much more than being "let alone"**
- **Naïve solutions that rely on pseudonyms do not suffice**
- **We need *unlinkability* between transactions**
  - This is not easy even when no registration or payment, and so no authentication, is required
  - This is very difficult if **authentication is required** (registering from scratch or paying again each time is unrealistic)

Andrew Lindell
Aladdin Knowledge Systems

Anonymous Web Surfing

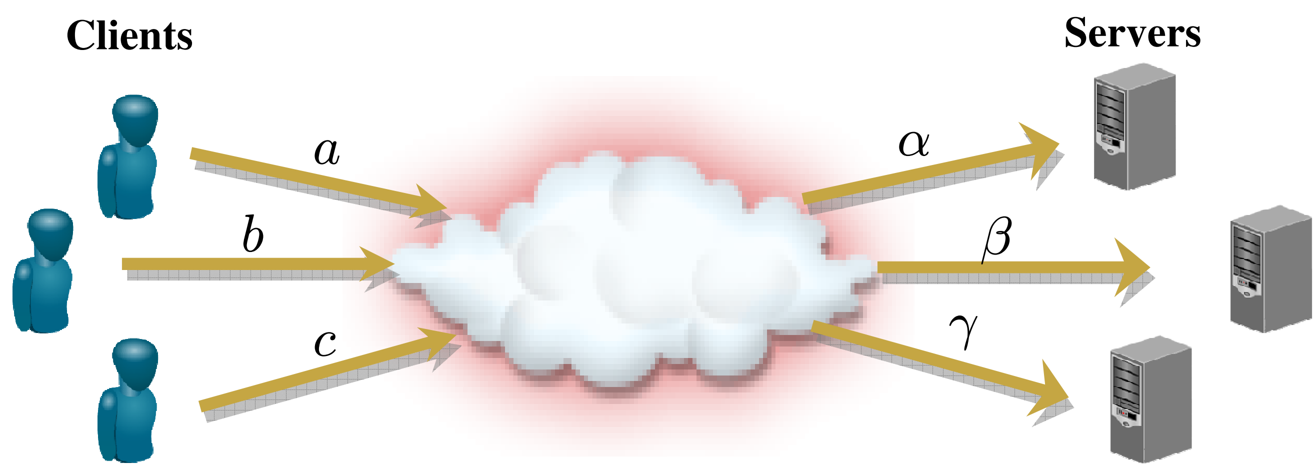
A Brief Survey

Anonymous Routing

- **Necessary infrastructure for anonymous authentication**
- **Two security goals**
  - **User anonymity:** modify packets so that user requests contain no identifying information
  - **Unlinkability:** ensure that an attacker who views Internet traffic (and possibly controls some routers) cannot know which client is interacting with which server
- **Achieving the goals**
  - **User anonymity:** not too difficult
  - **Unlinkability:** very difficult, depends on traffic

An Abstraction

- We assume that we have a magical mechanism that receives messages from all clients and sends them to their designated servers (without revealing the contents to an eavesdropper)



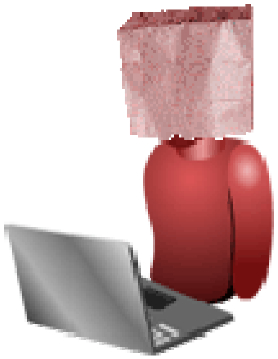
How is Anonymous Routing Achieved

- **There are numerous methods**
  - Mix-Nets
  - Onion routing
  - Dining cryptographers
  - Crowds
- **See the paper for references**

Andrew Lindell
Aladdin Knowledge Systems

Anonymous Authentication

What it is, and how it can be achieved



The High-Level Idea

- **It is impossible to authenticate a user without knowing something**
- **Anonymous authentication protocols have the following properties**
  - The authenticating server **knows** that the user belongs to a given set of (authorized) users
  - The authenticating server has **no idea** which member of the set has just authenticated
- **Of course, such a protocol must run on top of an anonymous routing mechanism**

Defining Security

- **Secure authentication**
  - No unauthorized user should be able to fool the server into granting it access (except with very small probability)
  - We mainly consider a public-key infrastructure model
- **Full (perfect) anonymity**
  - Let ℓ be the size of the set of users being considered
  - The protocol provides *perfect anonymity* if after authentication, the server can guess which user authenticated with probability at most $\frac{1}{\ell}$

Another Definition

- **It is sometimes useful to consider a more relaxed definition (that suffices for most applications)**
- **Verifiable (perfect) anonymity**
  - The user may receive a special **`cheat`** message as output
  - The guarantee is that **if** the user does not receive **`cheat`**, **then** the server can guess which user authenticated with probability at most $\frac{1}{\ell}$
- **This suffices in many cases, because the user has not yet done anything**

Solving the Mystery

- **How is it possible to achieve anonymity?**
- **A naïve idea**
  – Issue all users with the same password/secret key
  – This achieves perfect anonymity
- **The problem**
  – Cannot revoke a user's account without changing everyone's key!

Another Approach – Background

- **Let $U_1, \ldots, U_n$ be the users and let user U_i have a key-pair (sk_i, pk_i) for some public-key encryption scheme (say, RSA)**
  - The server has the record (U_i, pk_i) for every user (realistically, this can use a PKI and certificates)
  - A user's account can be cancelled by removing its record
  - We assume that each user knows all of the other users' public keys

The Protocol – First Attempt

- **User U_i sends first message**
  - Anonymous request to connect
- **Server first message**
  - The server chooses a long random string w
  - The server computes $c_i = E_{pk_i}(w)$ for every i
  - The server sends $c_1, \ldots, c_\ell$ to the user
- **User second message**
  - Upon receiving $c_1, \ldots, c_\ell$ the user U_i computes $w = D_{sk_i}(c_i)$ and sends w to the server
- **Server provides access if the user reply is w**

The Protocol – First Attempt

Server | User U_i

Request authentication $\longleftarrow$

Choose random w

$\forall j,\ c_j = E_{pk_j}(w)$

$\xrightarrow{c_1, \ldots, c_\ell}$

$w = D_{sk_i}(c_i)$

$\xleftarrow{w}$

Accept w

- **Security…**

Andrew Lindell
Aladdin Knowledge Systems

Problem – Cheating Server

- **A cheating server may encrypt a different w_i for every user U_i**
  - The user cannot tell the difference (it can only decrypt c_i)
  - The server can know exactly which user is authenticating by the value w_i that it returns
- **Solution**
  - Have the server “prove” that it encrypted the same value under all public keys

Andrew Lindell
Aladdin Knowledge Systems

Proof of Encryption Equality

- **One possibility**
  - The server sends all ciphertexts and proves that they encrypt the same value using a **zero-knowledge proof**
  - Very expensive!
- **Note**
  - The server cannot decrypt the ciphertexts for the user in order to check, because neither the user nor the server know the **private keys**

Andrew Lindell
Aladdin Knowledge Systems

Proof of Encryption Equality

- **Background:**
  - All secure encryption is probabilistic
- **RSA PKCS1#1 v1.5 encryption:**
  - First pad as below, then compute x^e **mod** N

RSA PKCS#1 v1.5 padding:

0002	random	00	the message **m**

Andrew Lindell
Aladdin Knowledge Systems

A Proof of Encryption Equality

- **The server needs to prove that all ciphertexts encrypt the same w**
- **The server cannot decrypt the ciphertexts, but can show how it encrypted them!**
  - The server sends the random padding that it used to encrypt each ciphertext
  - The user can then **re-encrypt** under each key and check that all ciphertexts encrypt the same value

Andrew Lindell
Aladdin Knowledge Systems

A Proof of Encryption Equality

- **In more detail**
  - Denote an encryption of w with public-key pk and random padding r (as in PKCS#1) by $c = E_{pk}(w;r)$
  - Given a public-key pk, a ciphertext c, a plaintext w, and random padding r, check:
    - If $E_{pk}(w;r) = c$ then c is an encryption of w
  - By **unambiguity** of decryption, c is not an encryption of any value $\tilde{w} \neq w$

Proof of Encryption Equality

- **Using the proof of equality**
  - The server cannot send this proof **before** the user replies, because then the user knows w and can get unauthorized access
  - If the server sends the proof **after** the user replies, then by sending a different w_i to every U_i, it already knows the user's identity
- **Verifiable anonymity**
  - The server sends it after, but if it learns the user's identity, the user will know for sure that it **cheated**

The Full Protocol

Server		User U_i
	$\xleftarrow{\text{Request authentication}}$	
Choose random w $\forall j,\ c_j = E_{pk_j}(w; r_j)$	$\xrightarrow{c_1, \ldots, c_\ell}$	
		$w = D_{sk_i}(c_i)$
	$\xleftarrow{w}$	
Accept w	$\xrightarrow{r_1, \ldots, r_\ell}$	
		Verify: $\forall j,\ c_j = E_{pk_j}(w; r_j)$

Andrew Lindell
Aladdin Knowledge Systems

Security Analysis

- **Theorem**
  - If the encryption scheme is secure against chosen-plaintext attacks, then the above is a secure authentication protocol that achieves verifiable anonymity
- **Proof**
  - **Secure authentication:** only an owner of one of the secret keys can find w
  - **Anonymity:** if server doesn't cheat, all users return the same value w
- **Formal proof (and definitions) in paper**

Andrew Lindell
Aladdin Knowledge Systems

Efficiency

- **Server overhead**
  - Compute one encryption per user (with RSA and small public exponent, not too expensive)
- **Client overhead**
  - Compute one encryption per user
  - Compute one decryption (on smartcard)
- **Important!**
  - Only one decryption on the smartcard
  - Any encryption scheme can be used and so standard smartcards and PKI can be utilized

Scalability

- **What about very large sets of users?**
  - Infeasible to carry out thousands of public-key operations to authenticate a single user
- ***k*-anonymity: user is guaranteed to be hidden amongst *k* other users**
  - We guarantee this, relative to **random** users
  - User chooses a random subset including itself and this is the set that is used

Andrew Lindell
Aladdin Knowledge Systems

Implementation Issue

- **The protocol assumes that all users know all of the public keys**
- **How is this accomplished?**
  - If the server posts a set of public-keys (certificates), then how does the user know that they are real?
  - If 90% are fake, then a user choosing a subset of 100 random users, will actually only be hiding amongst about 10 real users
  - Conclusion: if the server is not trusted (even at this level), users must share public keys amongst each other

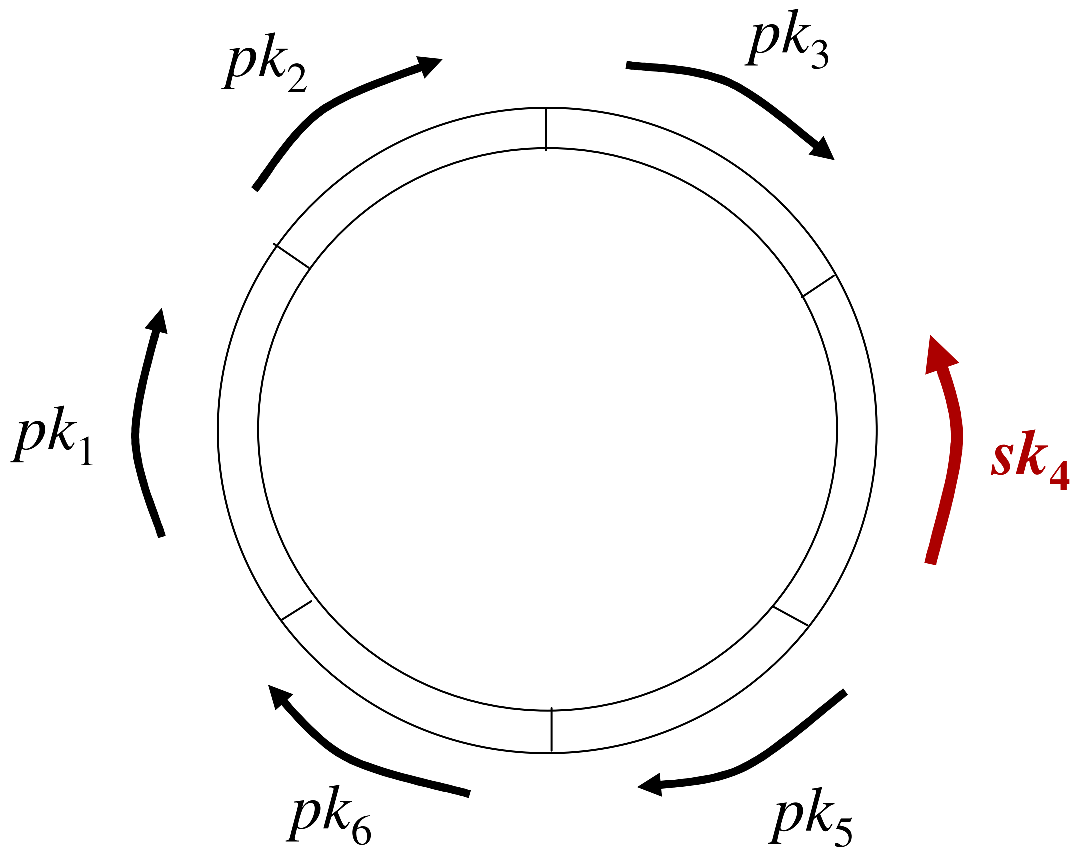
Achieving Full Anonymity

- **What if full anonymity is desired?**
- **Background – ring signatures** [RST]
  – A way of signing a message so that only someone from the "ring" could have signed, but it's impossible to know who actually did
    - *Unforgeability and anonymity*

  – Rings can be formed by anyone, on their own
  – Initial application: "how to leak a secret"
  – Construction of [RST]: uses regular RSA, requires one decryption and an additional encryption for every user in the ring

Andrew Lindell
Aladdin Knowledge Systems

Ring Signatures



Andrew Lindell
Aladdin Knowledge Systems

Anonymous Authentication with Ring Signatures

- **Incorporate ring signatures into SSL**
  - Use SSL with server and **client** authentication
  - In SSL, the client authentication is achieved by the client **signing** on the handshake messages
  - Use a **ring signature** instead of a normal one
- **Security**
  - **Secure authentication:** from unforgeability of ring signatures
  - **Anonymity:** from anonymity of ring signatures

Protocol Comparisons

- **Protocol based on encryption**
  - Seemingly higher bandwidth (but user needs to identify subset anyway)
  - Can use any secure encryption scheme (low requirements)
- **Protocol based on ring signatures**
  - Lower bandwidth (apart from identifying subset, requires same bandwidth as SSL with regular client authentication)
  - Assumes strong assumptions: **ideal cipher**

Revocable Anonymity

- **In some cases, anonymity needs to be revoked**
  - Ban access to users who misbehave
    - Hostile users in anonymous chat
    - Criminal activity
- **When anonymous authentication is used, this cannot be done**
- **Revocable anonymity**
  - There exists a **court authority** who can revoke anonymity when required (and only it can revoke)

Achieving Revocable Anonymity

- **There exist solutions, but they are all expensive and require dedicated hardware**
  - They don't use "standard" encryption techniques
- **As of yet, we also don't have a solution that doesn't require a special-purpose smartcard**
  - We do have solutions that are simple extensions of our protocols

Andrew Lindell
Aladdin Knowledge Systems

Achieving Revocable Anonymity

- **A first attempt**
  - The court authority has a public encryption-key pk_C
  - The user U_i includes an encryption $E_{pk_C}(ID_i)$ in its authenticating message to the server
- **Revocability**
  - If needed – and under court order – the court authority decrypts the additional ciphertext and finds the user's identity ID_i
- **Problem**
  - A cheating user can encrypt garbage or someone else's ID

Solving the Problem

- **We need to bind the encryption of the user's identity with its authentication message**
- **We assume that the user is given a smartcard by the organization, and cannot modify it**
  - The organization initializes the keys and so the user cannot replace it with a different smartcard
- **The requirement:**
  - If the user succeeds in authenticating, then its encrypted identity must be received by the server
  - We view the user as a man-in-the-middle adversary

Revocable Anonymity with Ring Signatures

- **Additional SSL modification**
  - The court authority has a public encryption-key pk_C
  - The user U_i includes an encryption $E_{pk_C}(ID_i)$ in the handshake messages
  - The handshake messages are all signed by the smartcard
  - Technically:
    - The smartcard receives a hash z of the handshake messages
    - The smartcard signs upon z and the ciphertext c

Revocable Anonymity with Ring Signatures

- **Security**
  - The smartcard operations are atomic
  - If the user modifies the ciphertext (that encrypts its identity), the ring signature generated by the smartcard will fail
  - In this case, the user will **fail** to gain access

Andrew Lindell
Aladdin Knowledge Systems

Revocable Anonymity Using Encryption

- **It is also possible to achieve a similar effect using our original protocol**
  - The full description appears in the paper

Password-Based Anonymous Authentication

- **What if we don't have a PKI setup?**
  – We wish to use symmetric keys, or passwords (regular, one-time or whatever)
- **We present a partial solution that can be based on any authentication mechanism (even biometrics)**

Andrew Lindell
Aladdin Knowledge Systems

High-Level Protocol

- **Step 1 – standard authentication**
  - The user authenticates using regular, non-anonymous authentication
- **Step 2 – register temporary public key**
  - After authenticating, the user generates a temporary key pair (pk, sk) and sends pk to the server
  - The server registers pk as an authorized public-key
- **Step 3 – disconnect and re-authenticate**
  - The user disconnects and connects again, running an anonymous authentication protocol using pk

Andrew Lindell
Aladdin Knowledge Systems

Properties of the Protocol

- **Security**
  - **Authentication:** no problems here
  - **Anonymity:** this is preserved as long as the server cannot link the anonymous authentication request to the user who just disconnected
- **Achieving anonymity**
  - User must either register key well before authenticating, or wait until a number of users join
  - Can use time slots

Properties of the Protocol

- **User keys**
  - This protocol intensifies the problem of how users know other users' public keys
  - Need to use some trusted bulletin board (not run by the same organization and assuming no collusion)

Conclusions

- **Privacy is far more than just the "right to be let alone"**
  - Online entities can learn large amounts of information and use that information against us, giving them an asymmetric advantage
  - We need unlinkability to preserve our privacy
- **Anonymous routing is the basic infrastructure needed for preserving privacy (unlinkability)**
- **The above is fine, as long as authentication is not needed**

Andrew Lindell
Aladdin Knowledge Systems

Conclusions

- **If authentication is needed, anonymity can still be preserved**
  - We saw two protocols
  - Implementation has a real cost, but a classic security/efficiency tradeoff makes it realistic (hide inside a not-too-large set of users)
  - Revocable anonymity is possible (but requires dedicated smartcards; not too bad with the invent of JavaCards, but still a disadvantage)
  - Partial solutions based on passwords are also possible

Future Work

- **Revocation**
  – Devise protocols that use only standard smartcard operations
- **Passwords**
  – Provide more satisfactory solutions that have stronger guarantees
- **System**
  – Come up with other methods of sharing public keys of users, so that server cannot introduce fake ones

Legal Notice

Restricted information and subject to change.

Before you access/view this presentation we draw your attention to the following terms and conditions and advise that by accessing, viewing, using or otherwise exploiting this document or its contents you are deemed to agree to these terms and to be bound thereby.

The information contained herein is confidential and proprietary to Aladdin.

The content herein is disclosed and may be viewed only by intended recipients this presentation solely for the purpose for which it is provided and shall not to be used or relied upon for any other purpose. You shall hold the information in strict confidence and will not use, disclose, copy, transfer or otherwise exploit the information without Aladdin's express prior written approval. The information, and any derivatives thereof is and shall remain the property of Aladdin and no license or other rights to such is granted or implied hereby to have been granted to you, now or in the future.

Notwithstanding, that certain information herein has been or may be made public, you are required to regard it as sensitive and confidential and not disclose information, unless Aladdin expressly permitted you to do so in writing.

Aladdin may make changes in the product(s) described in this presentation and/or to any specifications, at any time, without notice. Aladdin assumes no responsibility or liability arising from the use of the products described herein, except as expressly agreed to in writing by Aladdin and pursuant to an applicable license. Nothing herein conveys a license or any intellectual property rights whatsoever in the product(s).

If you are not willing to be bound by these terms, please do not access or view this document or its contents and return it immediately to Aladdin or otherwise delete it and any copies.

Andrew Lindell
Aladdin Knowledge Systems

Thank You!