Anonymity with Identity Escrow

Aybek Mukhamedov and Mark Ryan
The University of Birmingham

March 30, 2006

Outline

Big brother is watching you!

- Google
  - can track search terms via its cookie (expires 2038) and IP addresses
  - can build a profile of you, based on your gmail and your searches

  We are moving to a Google that knows more about you.
  Google CEO Eris Schmidt, Feb. 2005
- ISPs can log all transactions, monitor email, web accesses, etc.
- Mobile phone companies can log whereabouts, associations between people
- Credit card companies and other financial organisations can also log location, taste, habits

A future scenario

Your job/mortgage application is rejected because your profile matches that of people who move after one year

Applications of anonymity protocols

As well as general paranoia, there are some specific applications:

- Electronic voting: nobody (including the voting administrators) can link you and your vote.
- Digital cash: the bank doesn't know what you are buying or who is selling it; the seller doesn't know who you are.

Unrestricted anonymity may be thought undesirable

- Society has clearly demonstrated that it doesn't want digital cash. In the UK, here are even limitations on using ordinary cash.
- Currently in the UK, voting is not anonymous. An audit trail can link you to your ballot paper.

Anonymity with identity escrow

Escrow

Escrow is a legal arrangement whereby an asset (often money, but sometimes other property such as art, a deed of title, website, or software source code) is delivered to a third party (called an escrow agent) to be held in trust pending a contingency or the fulfillment of a condition or conditions in a contract. (from Wikipedia)

In order to use the *anonymity with identity escrow* service, Alice must:

- Apply for a service token from an escrow agent. In doing so, she places her identity in escrow with the agent.
- Use the service anonymously. The token guarantees to the service provider that she has placed her identity in escrow.

In the case of service mis-use, the service provider can appeal to the escrow agent to reveal Alice's identity.

Some existing frameworks

Group signatures

Group signatures allow Alice to join a group managed by an *issuer I*. He must agree to her joining. Once a member, she can sign on behalf of the group.

- Given a signed message, *I* can determine who is the signer.
- But without *I*'s secret key,
  - the identity of an individual signer cannot be revealed;
  - given two messages and their signatures, one cannot tell if they were signed by the same signer.

Anonymous credential systems

Anonymous credential systems allow Alice to anonymously prove possession of a credential issued by an issuer *I*.

- Proofs are unlinkable
- *I* can revoke anonymity for particular transactions

Problems with group signatures and credential systems

Group signatures and credential systems have some disadvantages:

- Alice is forced to *trust* the issuer. The issuer can reveal Alice's identity even if the agreed conditions for doing so are not satisfied.
- They use non-standard cryptography, such as zero-knowledge proofs, which are not widely implemented in APIs.

Distributing trust

L. Marshall and C. Molina-Jiminez present a protocol which distributes the escrowed identity among a set of issuers called token providers. It aims to provide the following properties.

- Alice may choose how many and which token providers are used.
- Alice's identity can be revealed only if all of them agree. Thus, the protocol preserves Alice's anonymity provided at least one token provider is honest.
- The protocol uses only standard cryptography (namely, encryption and digital signing).

The protocol comprises three parts:

- Sign-up
- Service usage
- Complaint resolution

MMJ: sign-up

A chooses a sequence $T_{a_1}, T_{a_2}, \ldots, T_{a_p}$ of elements of T.

$$1) \quad A \longrightarrow T_{a_1} : \{ [\, \texttt{ITKReq} \,]_{K_A^-} \}_{K_{T_{a_1}}}$$

$$2) \quad T_{a_1} \longrightarrow A : \{ \Phi_1 \}_{K_A}, \text{ where } \Phi_1 = [\, \{K_A\}_{K_{T_{a_1}}} \,]_{K_{T_{a_1}}^-}$$

`ITKReq` means "identity token request".

A anonymises the token by getting $T_{a_2}, \ldots, T_{a_p}$ to encrypt and sign it:

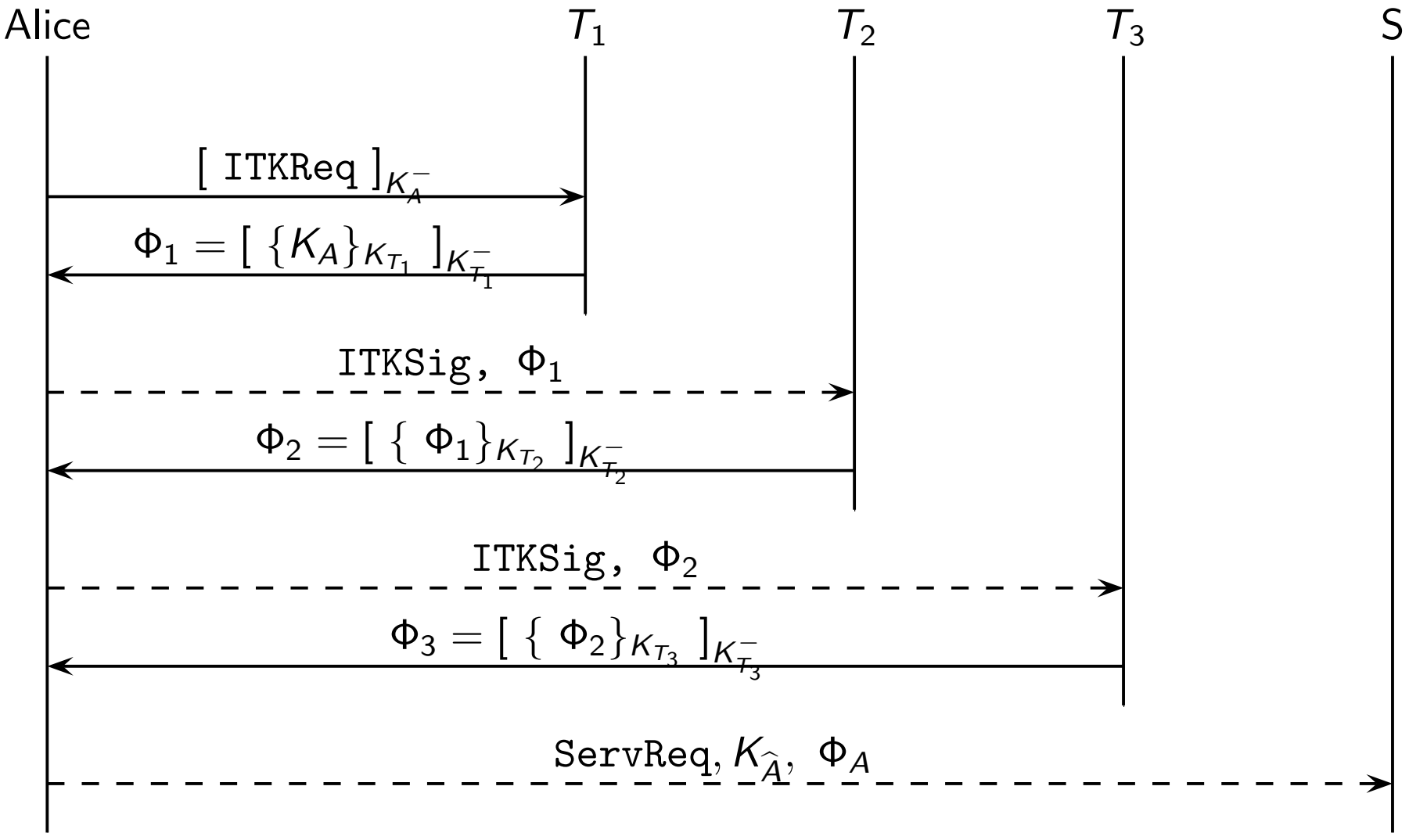
$$* \begin{cases} 1a) \quad A \dashrightarrow T_{a_{i+1}} : \{ \texttt{ITKSig}, \Phi_i \}_{K_{T_{a_{i+1}}}} \\ 2a) \quad T_{a_{i+1}} \longrightarrow \widehat{A} : \{ [\, \{ \Phi_i \}_{K_{T_{a_{i+1}}}} \,]_{K_{T_{a_{i+1}}}^-} \}_{K_{\widehat{A}}} \\ \qquad\qquad \text{where} \quad \Phi_{i+1} = [\{ \Phi_i \}_{K_{T_{a_{i+1}}}} \,]_{K_{T_{a_{i+1}}}^-} \end{cases}$$

`ITKSig` indicates a signature request. $*$ indicates repeated application. All signatures are checked. The dashed arrow indicates that a message is sent anonymously.

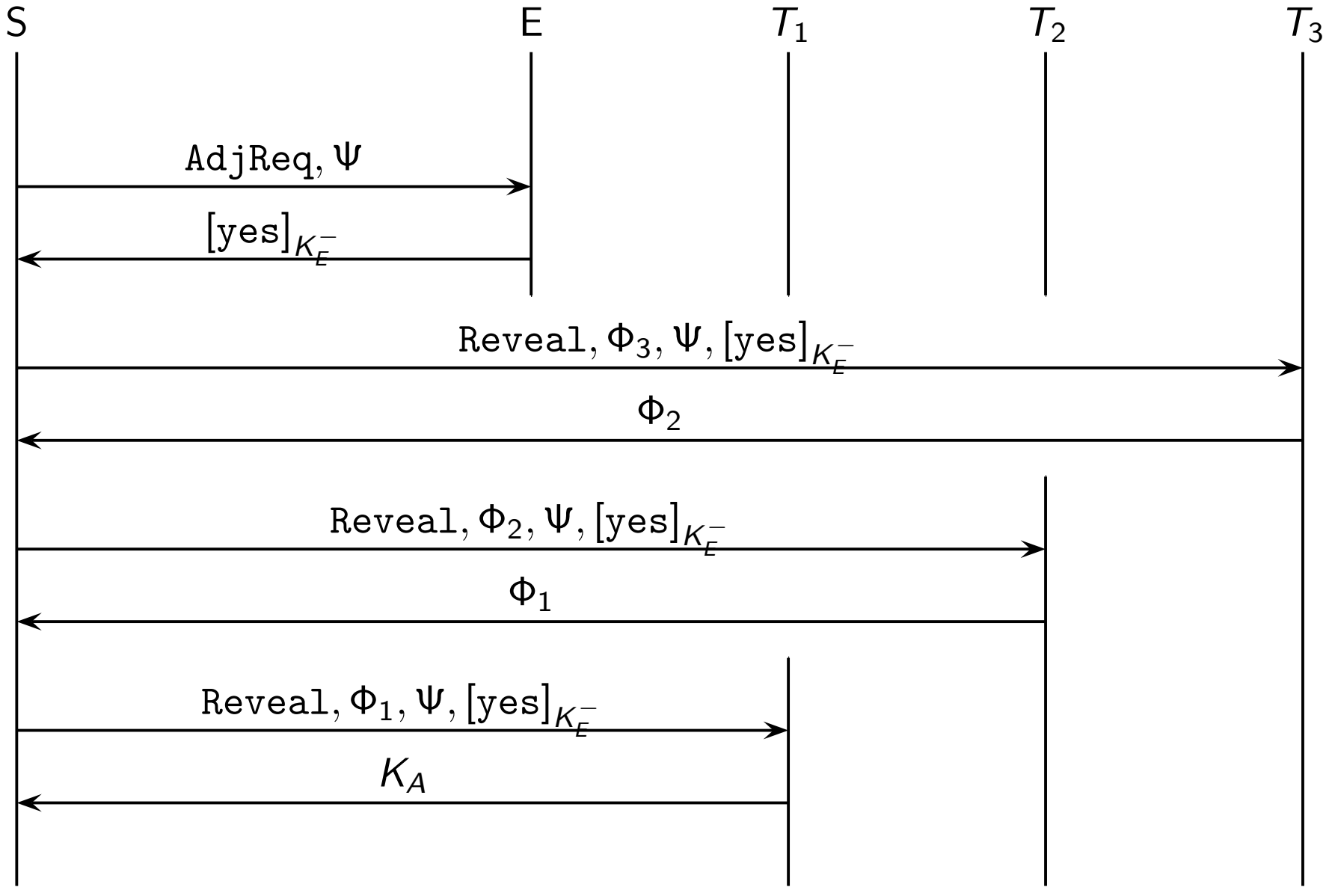
$$3) \quad A \dashrightarrow S : \{ \texttt{ServReq}, K_{\widehat{A}}, \Phi_A \}_{K_S}$$

MMJ: sign-up

Alice's keys: K_A long term, certified; $K_{\widehat{A}}$ temporary for comms/service.
All messages are encrypted with receiver's comms PK (not shown).



MMJ Complaint resolution



Flaws in MMJ

MMJ has serious flaws

- Framing: any token provider, or the service provider, can implicate any agent in any misuse of the service.
  - Token can be generated without A's participation
  - $K_{\widehat{A}}$ not tied to token
- Compromise anonymity: S in coalition with T_{a_1} can identify A
- Compromise anonymity: S can reveal A's identity via a false complaint resolution.

Our protocol

Based on MMJ, it also distributes the identity among a collection of token providers chosen by the user.

But it avoids the problems of MMJ.

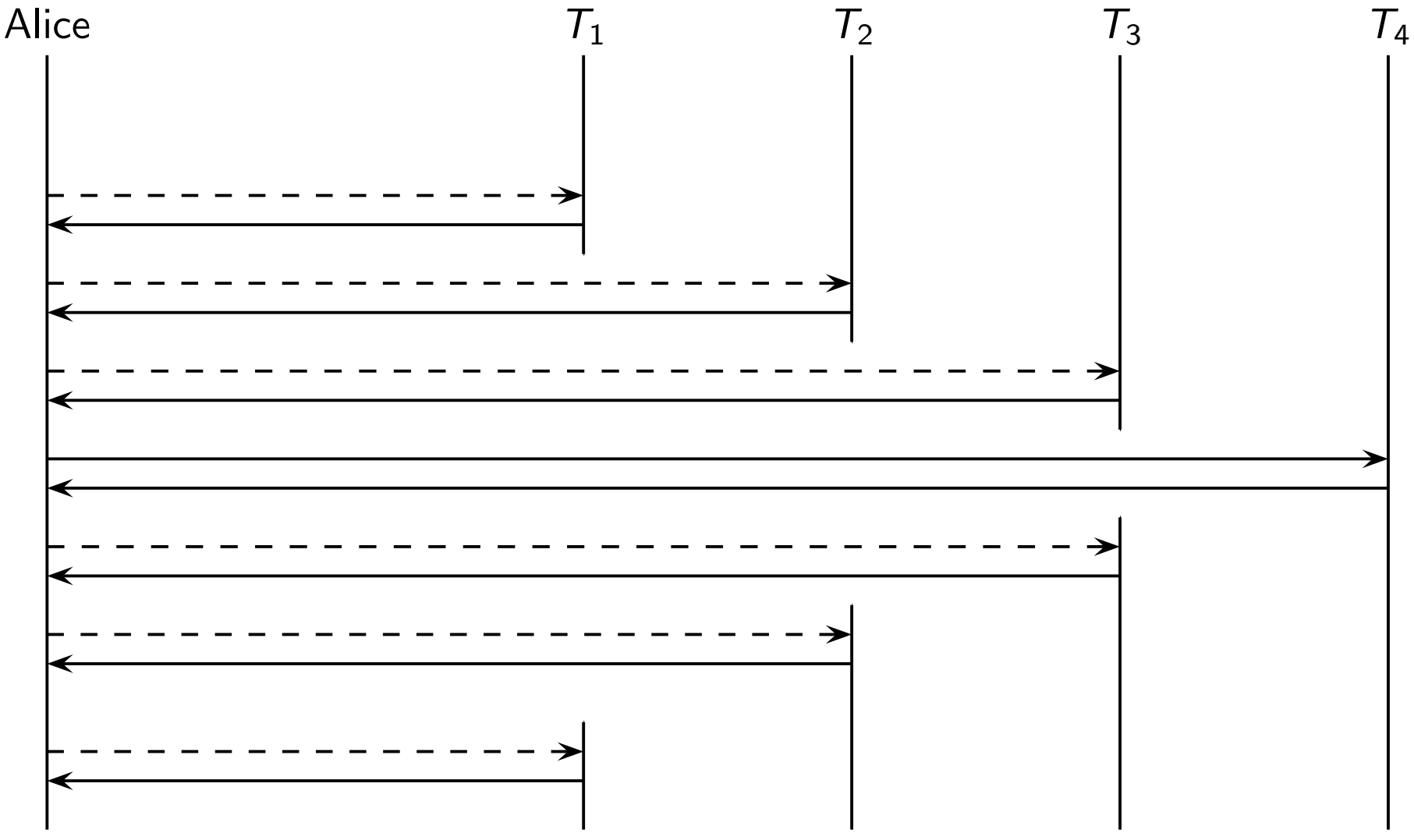
Properties of our protocol

- Φ_A cannot be generated without A's participation
- $K_{\widehat{A}}$ is tied to Φ_A and only A knows its secret counterpart
- If at least one of the T_a's does not reveal, then A's identity cannot be determined.

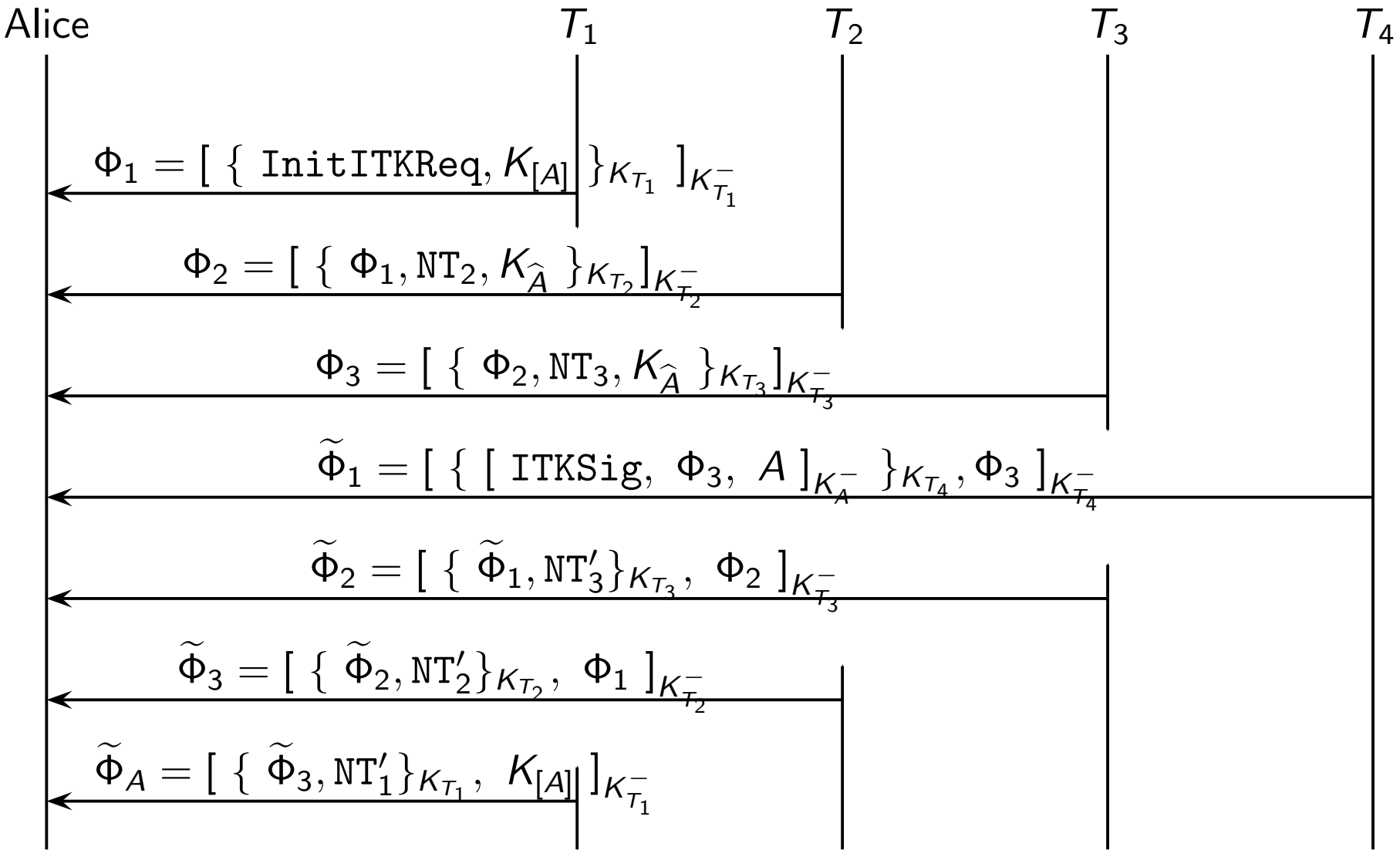
Our protocol: Sign-up

- A chooses a sequence $T_{a_1}, T_{a_2}, \ldots, T_{a_p}$ of elements of T.
- She chooses two new public keys:
  - $K_{[A]}$, for using the service;
  - $K_{\widehat{A}}$, for communicating anonymously.
- Through interactions with $T_{a_1}, T_{a_2}, \ldots, T_{a_p}$, she builds up an onion Φ with $K_{[A]}$ in its centre.
- Then, she reveals her identity to T_{a_p}, and through interaction with $T_{a_p}, T_{a_{p-1}}, \ldots, T_{a_1}$ she builds an onion with Φ, A in its centre.
  - During the construction of this onion, Φ is simultaneously decomposed and checked.

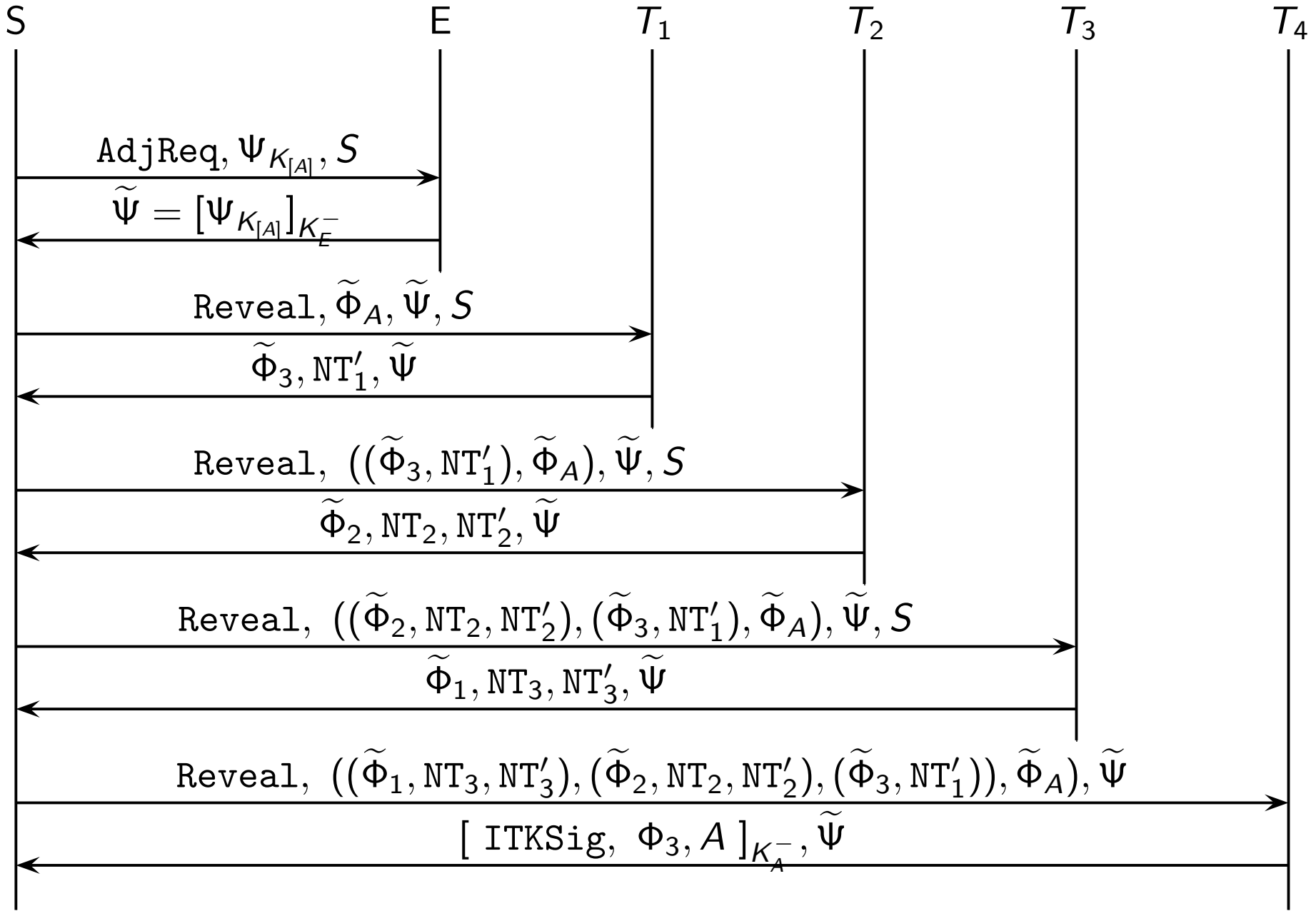
Our protocol: Sign-up schema



Our protocol: Sign-up messages received



Our protocol: Complaint resolution



Complaint resolution: checking the messages

The tuples in the messages to T_i, and the nonces, are to ensure that messages from one session cannot be used in others. The T_is check the consistency of the messages.

For example, in case $n = 4$, T_3 does the following checks

- From $\widetilde{\Phi}_2$, extract $\widetilde{\Phi}_1$ and $\mathtt{NT}'_3$.
- From $\widetilde{\Phi}_1$, extract Φ_3 and thence $\mathtt{NT}_3$.
  Now T_3 has enough to make his reply.
- Produce $\{\widetilde{\Phi}_2, \mathtt{NT}'_2\}_{K_{T_2}}$ and check equal to first component of $\widetilde{\Phi}_3$.
- Produce $\{\widetilde{\Phi}_3, \mathtt{NT}'_1\}_{K_{T_1}}$ and check equal to first component of $\widetilde{\Phi}_A$.

Verification in ProVerif

ProVerif is a tool for analysing protocols modelled in the applied pi calculus. We used it to verify whether our protocol guarantees the following properties:

- Service key secrecy. The private part of user's anonymous service key is secret.
- Fair adjudication. No honest user can be implicated in a misuse of services it did not commit.
- User anonymity. The identity token obtained by a user can not be linked to its identity, provided that at least one of the token providers is honest.

Our analysis is not fully exhaustive, but provides strong evidence that these properties are satisfied.

Conclusions and other work

Anonymity with identity escrow allows users of a service to remain anonymous, while providing the possibility that the service owner can break the anonymity in exceptional circumstances.

- Balance between security and privacy likely to be a major theme for the future.
- Anonymity with identity escrow may be a good solution in some applications.
- Future work: extend with
  - Guaranteed notification of identity revelation
  - Enforceable privacy policies